kaspersky

Kaspersky Endpoint Security 14.2 for Windows

© 2026 AO Kaspersky Lab

Índice

Ajuda do Kaspersky Endpoint Security for Windows
- Novidades
- Problemas corrigidos
- Perguntas frequentes

Kaspersky Endpoint Security for Windows
- Modos do aplicativo: Standard, EDR Agent, Light Agent
- Kit de distribuição
- Requisitos de hardware e software
- Comparação de recursos de aplicativo disponíveis dependendo do tipo de sistema operacional
- Comparação de funções de aplicativo, dependendo das ferramentas de gerenciamento
- Compatibilidade com outros aplicativos

Instalar e remover o aplicativo
- Implementação por meio do Kaspersky Security Center
  - Instalação padrão do aplicativo
  - Criar um pacote de instalação
  - Atualização de bancos de dados no pacote de instalação
  - Criar uma tarefa de instalação remota
- Instalar o aplicativo localmente usando o assistente de instalação
- Instalar remotamente o aplicativo usando o System Center Configuration Manager
- Descrição das configurações de instalação do arquivo setup.ini
- Processos do Kaspersky Endpoint Security for Windows
- Alterar componentes do aplicativo
- Upgrade de uma versão anterior do aplicativo
  - Atualizar o aplicativo sem reiniciar
  - Atualização SMU do aplicativo
- Remoção do aplicativo

Licenciamento do aplicativo
- Sobre o Contrato de Licença do Usuário Final
- Sobre a licença
- Sobre o certificado da licença
- Sobre a assinatura
- Sobre chave de licença
- Sobre o código de ativação
- Sobre o arquivo de chave
- Comparação da funcionalidade do aplicativo dependendo do tipo de licença para estações de trabalho
- Comparação da funcionalidade do aplicativo dependendo do tipo de licença para servidores
- Ativar o aplicativo
- Remover uma chave de licença
- Exibir informações da licença
- Comprar uma licença
- Renovar a assinatura

Iniciar
Sobre o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows
Considerações especiais ao trabalhar com versões diferentes de plug-ins de gerenciamento
Considerações especiais ao usar protocolos criptografados para interagir com serviços externos
Interface do aplicativo
Ícone do aplicativo na área de notificação da barra de tarefas
Interface de aplicativo simplificada
Configurar a exibição da interface do aplicativo
Preparação do aplicativo para uso
Gerenciamento de políticas
Criar uma política
Exportação e importação de uma política
Indicador do nível de segurança
Gerenciamento de tarefas
Definir as configurações locais do aplicativo
Iniciar e interromper o Kaspersky Endpoint Security
Pausar e reiniciar a Proteção e Controle do computador
Criar e usar um arquivo de configuração
Restaurar as configurações padrão do aplicativo
Desempenho e compatibilidade do Kaspersky Endpoint Security com outros aplicativos
Ativar ou desativar o modo de economia de energia
Ativar ou desativar a concessão de recursos a outros aplicativos
Práticas recomendadas para otimizar o desempenho do Kaspersky Endpoint Security
Verificação de malware
Verificar o computador
Verificar unidades removíveis quando conectadas ao computador
Verificação em segundo plano
Verificar pelo menu de contexto
Verificação de integridade de aplicativos
Editar o escopo da verificação
Execução de uma verificação programada
Execução de uma verificação como um usuário diferente
Otimização da verificação
Atualizar bancos de dados e módulos do software aplicativo
Cenários de atualização do banco de dados e do módulo de aplicativo
Atualizar a partir de um repositório de servidor
Atualizar a partir de uma pasta compartilhada
Atualizar utilizando o Kaspersky Update Utility
Atualizar no modo móvel
Iniciar e interromper a tarefa de atualização
Executar a tarefa de atualização usando os direitos de uma conta de usuário diferente
Selecionar o modo de execução da tarefa de atualização
Adicionar uma fonte de atualização
Atualização dos módulos do aplicativo
Usar um servidor proxy para atualizações
Reversão da última atualização

Tecnologia de desinfecção avançada
Desinfecção de ameaças ativas em estações de trabalho
Desinfecção de ameaças ativas em servidores
Eliminação de ameaças não processadas
Proteção do computador
Status da Proteção em Tempo Real
Proteção Contra Ameaças ao Arquivo
Ativar e desativar a Proteção Contra Ameaças ao Arquivo
Pausa automática da Proteção Contra Ameaças ao Arquivo
Alterar a ação executada em arquivos infectados pelo componente Proteção Contra Ameaças ao Arquivo
Formar o escopo de proteção do componente Proteção Contra Ameaças ao Arquivo
Usar métodos de verificação
Usar tecnologias de verificação na operação do componente Proteção Contra Ameaças ao Arquivo
Otimizar a verificação do arquivo
Verificar arquivos compostos
Alterar o modo de verificação
Verificação de contêiner
Prevenção de Intrusão do Host
Ativar e desativar a Prevenção de Intrusão do Host
Gerenciar grupos de confiança de aplicativos
Alterar o grupo de confiança de um aplicativo
Configurando direitos de grupos de confiança
Selecionar um grupo confiável de aplicativos iniciados antes do Kaspersky Endpoint Security
Selecionar um grupo de confiança para aplicativos desconhecidos
Selecionar um grupo de confiança para aplicativos assinados digitalmente
Gerenciar direitos do aplicativo
Proteger os recursos do sistema operacional e dados pessoais
Exclusão de informações sobre aplicativos não utilizados
Monitoramento de Prevenção de Intrusão do Host
Proteção do acesso a áudio e vídeo
Prevenção contra ataque BadUSB
Ativar e desativar Prevenção contra ataque BadUSB
Uso do teclado na tela para a autorização de dispositivos USB
Autorização do leitor de código de barras
Proteção AMSI
Ativar e desativar a proteção AMSI
Otimização da verificação de arquivos pela Proteção AMSI
Proteção Contra Ameaças da Web
Ativar e desativar a Proteção Contra Ameaças da Web
Configurar métodos de detecção de endereços da Web maliciosos
Antiphishing
Criar lista de Endereços da Web confiáveis
Exportar e importar a lista de Endereços da Web confiáveis
Proteção Contra Ameaças ao Correio
Ativar e desativar a Proteção Contra Ameaças ao Correio
Alterar a ação a executar em mensagens de e-mail infectadas
Formar o escopo de proteção do componente Proteção Contra Ameaças ao Correio

Verificar arquivos compostos anexados a mensagens de e-mail
Filtragem de anexos de mensagens de e-mail
Exportar e importar extensões para filtragem de anexos
Verificar e-mails no Microsoft Office Outlook
Verificação de e-mails no Thunderbird, MyOffice e R7-Office
Proteção Contra Ameaças à Rede
Ativar e desativar a Proteção Contra Ameaças à Rede
Bloquear um computador atacante
Configurar endereços de exclusões de bloqueio
Exportar e importar a lista de exclusões do bloqueio
Configurar a Proteção Contra Ameaças à Rede por tipo
Firewall
Ativar ou desativar o Firewall
Alterar o tipo de conexão de rede
Gerenciar regras de pacotes de rede
Criar uma regra de pacote de rede
Ativar ou desativar uma regra de pacotes de rede
Alterar a ação do Firewall para uma regra de pacotes de rede
Alterar a prioridade de uma regra de pacotes de rede
Exportar e importar regras de pacotes de rede
Definição das regras de pacote de rede no XML
Gerenciar as regras de rede de aplicativos
Criar uma nova regra de rede
Ativar e desativar uma regra de rede de aplicativo
Alterar a ação do Firewall para uma regra de rede de um aplicativo
Alterar a prioridade de uma regra de rede de um aplicativo
Monitor de Rede
Prevenção de Exploits
Ativar e desativar a Prevenção de Exploit
Proteção da memória de processos do sistema
Detecção de Comportamento
Anticryptor
Ativar e desativar a proteção de pastas compartilhadas contra criptografia externa
Configurar o período de bloqueio de um computador não confiável
Editar o escopo de proteção
Adicionar computadores confiáveis para criptografia externa de dados
Exportar e importar uma lista de exclusões da proteção de pastas compartilhadas contra criptografia externa
Mecanismo de Remediação
Kaspersky Security Network
Ativar e desativar o uso do Kaspersky Security Network
Limitações da Kaspersky Private Security Network
Ativar e desativar o modo na nuvem para os componentes de proteção
Configurações de proxy da KSN
Verificar a reputação de um arquivo np Kaspersky Security Network
Verificação de conexões criptografadas
Ativar a verificação de conexões criptografadas
Instalação dos certificados raiz confiáveis

Verificar conexões criptografadas com um certificado não confiável
Adicionar o certificado da Kaspersky ao armazenamento de certificados próprio
Excluindo conexões criptografadas da verificação
Bloquear o acesso a domínios com certificados não confiáveis
Limpar dados
Controle do computador
Controle da Web
Adicionar uma regra de acesso a recursos da web
Filtrar por endereços de recursos da Web
Filtrar por conteúdo do recurso da Web
Testar as regras de acesso de recurso da Web
Exportar e importar regras de Controle da Web
Exportar e importar endereços de recursos da Web da regra de Controle da Web
Monitoramento da atividade do usuário na Internet
Editar modelos de mensagens do Controle da Web
Editar máscaras de endereços de recurso da web
Controle da Web para máquinas virtuais
Variáveis nos modelos de mensagem do Controle da Web
Controle de Dispositivos
Sobre as regras de acesso
Obter informações sobre os dispositivos instalados
Gerenciar o acesso a dispositivos por tipo
Gerenciar o acesso a dispositivos por meio de barramento de conexão
Diferenciação dos direitos de acesso do usuário aos dispositivos
Gerenciamento do acesso a dispositivos móveis
Gerenciando o acesso a dispositivos Bluetooth
Controle de impressão
Controle de conexões Wi-Fi
Monitorar o uso de unidades removíveis
Alterar a duração do armazenamento em cache
Ações com dispositivos confiáveis
Adicionar um dispositivo à lista de confiáveis
Exportação e importação da lista de dispositivos confiáveis
Obter acesso a um dispositivo bloqueado
Modo online para conceder acesso
Modo offline para conceder acesso
Editar os modelos de mensagens do Controle de Dispositivo
Antibridging
Ativar o antibridging
Mudar o status de uma regra de conexão
Alterar a prioridade de uma regra de conexão
Controle Adaptativo de Anomalias
Treinamento do Controle Adaptativo de Anomalias
Ativar e desativar uma regra de Controle Adaptativo de Anomalias
Modificar a ação executada quando uma regra de Controle Adaptativo de Anomalias é acionada
Criar uma exclusão para uma regra de Controle Adaptativo de Anomalias
Exportar e importar exclusões para regras de controle adaptativo de anomalias

Aplicar atualizações das regras de Controle Adaptativo de Anomalias
Editar modelos de mensagem de Controle Adaptativo de Anomalias
Monitorando as operações do Controle Adaptativo de Anomalias
Controle de aplicativos
Limitações de funcionalidade do Controle de Aplicativos
Obter informações sobre aplicativos instalados
Como ativar o modo Aplicativos bloqueados
Controle de aplicativos com base em um computador de linha de base
Gerenciar regras de Controle de Aplicativos
Adicionar uma condição de acionamento para a regra de Controle de Aplicativos
Adicionar arquivos executáveis da pasta de Arquivos executáveis à categoria de aplicativos
Adicionar arquivos executáveis relacionados a eventos à categoria de aplicativos
Adicionar uma regra de Controle de aplicativos
Alterar o status de uma regra de Controle de aplicativos usando o Kaspersky Security Center
Exportar e importar regras de Controle de Aplicativos
Exibir eventos resultantes da operação do componente Controle de Aplicativos
Visualização do relatório sobre aplicativos bloqueados
Testar as regras de Controle de Aplicativos
Habilitando e desabilitando o teste de regra de Controle de Aplicativos
Exibir o relatório de aplicativos bloqueados no modo de teste:
Exibir eventos resultantes da operação de teste do componente Controle de Aplicativos
Monitoramento de atividades do aplicativo
Regras para criar máscaras de nome para arquivos ou pastas
Editar modelos de mensagem de Controle de Aplicativos
Variáveis nos modelos de mensagem do Controle de Aplicativos
Práticas recomendadas para realizar um inventário de arquivos executáveis
Melhores práticas para implementar uma lista de aplicativos permitidos
Configurar o modo Lista de permissão para aplicativos
Teste do modo Lista de permissão
Suporte para o modo Lista de permissão
Monitoramento de Portas de rede
Ativar o monitoramento de todas as portas de rede
Criar uma lista de portas de rede monitoradas
Criar uma lista de aplicativos para todas as portas de rede que são monitoradas
Exportar e importar listas de portas monitoradas
Inspeção do Log
Configuração de regras predefinidas
Adição de regras personalizadas
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
Redefinição do status de integridade do sistema
Cloud Discovery

Zona confiável
Criar uma exclusão de verificação
Criação de uma exclusão por tipo de objetos detectados
Editar a lista de aplicativos confiáveis
Criando uma zona confiável local
Exportar e importar a zona confiável
Manipulação de aplicativos com uma assinatura digital confiável
Apêndice. Exclusões de verificação predefinidas e aplicativos confiáveis
Microsoft SQL Server
Microsoft Exchange Server
Microsoft System Center Configuration Manager
Citrix
VMware
Desduplicação de dados no Microsoft Windows Server
Gerenciar o Backup
Configurar o período de armazenamento máximo para arquivos no Backup
Configurar o tamanho máximo de Backup
Restaurar arquivos do Backup
Excluir cópias de backup de arquivos do Backup
Serviço de notificações
Definir as configurações do registro de eventos
Configurar a exibição e entrega de notificações
Configurar a exibição de avisos sobre o status do aplicativo na área de notificação
Mensagens entre usuários e o administrador
Gerenciar relatórios
Visualização de relatórios
Configurar o período máximo de armazenamento de relatórios
Configurar o tamanho máximo do arquivo de relatório
Salvar um relatório em arquivo
Limpando relatórios
Autodefesa do Kaspersky Endpoint Security
Ativar ou desativar a Autodefesa
Ativar e Desativar o suporte ao AM-PPL
Proteção de serviços do aplicativo contra gerenciamento externo
Suportar aplicativos de administração remota
Proteção por senha
Ativar a proteção por senha
Conceder permissões a usuários individuais ou grupos
Usar uma senha temporária para conceder permissões
Revogação da senha temporária
Aspectos especiais das permissões de Proteção por senha
Redefinir a senha do KL Admin
Proteção da conexão do Servidor de Administração
Criptografia de Dados
Limitações de funcionalidades da criptografia
Alteração do comprimento da chave de criptografia (AES56/AES256)

Kaspersky Disk Encryption
Recursos especiais de criptografia de unidade SSD
Iniciar o Kaspersky Disk Encryption
Criar uma lista de discos rígidos excluídos da criptografia
Exportar e importar uma lista de discos rígidos excluídos da criptografia
Ativar a tecnologia de login único (SSO)
Gerenciar contas do Agente de Autenticação
Usar um token ou cartão inteligente com o Agente de Autenticação
Descriptografia de disco rígido
Restaurando o acesso a uma unidade protegida pela tecnologia Kaspersky Disk Encryption
Fazer login com a conta de serviço do Agente de Autenticação
Atualização do sistema operacional
Eliminar erros de atualização da funcionalidade de criptografia
Rastreamento do Agente de Autenticação
Editar as textos de ajuda do Agente de autenticação
A remoção de restos de objetos e dados após testar o funcionamento do Agente de Autenticação
Gerenciamento do BitLocker
Iniciar Criptografia de Unidade de Disco BitLocker
Descriptografando um disco rígido protegido pelo BitLocker
Restauração do acesso a uma unidade protegida pelo BitLocker
Pausa da proteção do BitLocker para atualizar o software
Criptografia a Nível de Arquivo em unidades locais de computador
Criptografia de arquivos em unidades de computadores locais
Formar regras de acesso a arquivos criptografados para aplicativos
Criptografar arquivos que são criados ou modificados por aplicativos específicos
Gerar uma regra de descriptografia
Descriptografar arquivos em unidades de computadores locais
Criar pacotes criptografados
Restaurar acesso aos arquivos criptografados.
Restaurar o acesso a dados criptografados após falha no sistema operacional
Editar modelos de mensagens de acesso a arquivos criptografados
Criptografia de unidades removíveis
Iniciar a criptografia de unidades removíveis
Adicionar uma regra de criptografia para unidades removíveis:
Exportar e importar uma lista de regras de criptografia para unidades removíveis
Modo portátil para acessar arquivos criptografados em unidades removíveis
Descriptografia de unidades removíveis
Exibir os detalhes da criptografia de dados
Exibir o status da criptografia
Visualização das estatísticas de criptografia nos painéis de controle do Kaspersky Security Center
Exibir erros de criptografia de arquivos em unidades de computador locais
Exibir o relatório de criptografia de dados
Trabalhar com dispositivos criptografados quando não há acesso a eles
Recuperar dados usando o Utilitário de restauração FDERT
Criar um disco de recuperação do sistema operacional

Soluções de Detection and Response
Licenciamento MDR e EDR Optimum
Compatibilidade com soluções EDR de terceiros
Kaspersky Endpoint Agent
Migração da configuração [KES+KEA] para [KES+built-in agent]
Migração de políticas e tarefas para o Kaspersky Endpoint Agent
Endpoint Detection and Response Agent (EDR Agent)
Instalando o EDR Agent
Integrando o EDR Agent com MDR
Integrando o EDR Agent com EDR (KATA)
Integrando o EDR Agent com NDR (KATA)
Integração do EDR Agent com EDR Expert (on-premises)
Compatibilidade com aplicativos EPP de terceiros
Managed Detection and Response
Integração do agente integrado com MDR
Guia de migração do KEA para KES para o MDR
Endpoint Detection and Response
Integração do agente integrado com EDR Optimum / EDR Expert
Verificar os indicadores de comprometimento (tarefa padrão)
Telemetria estendida para verificação de IOC
Mover arquivo para a quarentena
Obter arquivo
Excluir arquivo
Início do processo
Encerrar processo
Prevenção de execução
Isolamento do computador em relação à rede
Cloud Sandbox
Guia de migração do KEA para KES para o EDR Optimum
Kaspersky Sandbox
Integração do agente integrado com o Kaspersky Sandbox
Verificar se há indicadores de comprometimento (tarefa autônoma)
Guia de migração do KEA para KES para o Kaspersky Sandbox
Kaspersky Anti Targeted Attack Platform
Integração do agente integrado com EDR / NDR (KATA)
Configuração da telemetria EDR (KATA)
Exclusões de telemetria EDR (KATA)
Exemplo 1. Processos excluídos
Exemplo 2. Comunicações de rede excluídas
Exemplo 3. Operações de arquivo excluídas
Exemplo 4. Modificações de registro excluídas
KATA Sandbox
Integração do agente integrado com o KATA Sandbox
Configuração das ações de resposta a ameaças
Guia de migração do KEA para KES para o EDR (KATA)

Endpoint Detection and Response Expert (on-premises)
Integração do agente integrado com o EDR Expert (on-premises)
Definição das configurações de telemetria do EDR Expert (on-premises)
Exclusões de telemetria do EDR Expert (on-premises)
Exportar e importar filtros de eventos do EDR Expert (on-premises)
Considerações especiais ao usar perfis da política para configurar a integração com o EDR Expert (on-premises) e EDR (KATA)
Endpoint Detection and Response Expert (cloud)
Integração do agente integrado com o EDR Expert (cloud)
Definição das configurações de telemetria do EDR Expert (cloud)
Exclusões de telemetria EDR Expert (cloud)
Como exportar ou importar filtros de eventos do EDR Expert (cloud)
Gerenciamento da Quarentena
Configuração do tamanho máximo da Quarentena
Envio de dados sobre os arquivos em Quarentena para o Kaspersky Security Center
Restauração do arquivo da Quarentena
Monitoramento de ações de EDR
Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Integração do Kaspersky Endpoint Security com a KUMA
Preparação para a integração do KES com o KUMA
Conectar o KES ao KUMA
Filtragem de eventos para serem enviados para a KUMA
Exportar e importar filtros de eventos KUMA
Guia de Migração de KSWS para KES
Correspondência dos componentes do KSWS e KES
Correspondência das configurações do KSWS e do KES
Migração de componentes do KSWS
Migrando tarefas e políticas do KSWS
Migração da zona confiável do KSWS
Migrar regras de Controle de Inicialização de Aplicativos do KSWS
Instalação do KES sobre o KSWS
Migração da configuração [KSWS+KEA] para [KES+built-in agent]
Verifique e confirme se o Kaspersky Security for Windows Server foi removido com êxito
Ativação do KES com uma chave do KSWS
Considerações especiais para migrar servidores de alta carga
Gerenciamento do aplicativo em um servidor no modo Server Core
Migração de [KSWS+KEA] para [KES+agente integrado]
Modo Light Agent para proteger máquinas virtuais
Considerações especiais para o modo Light Agent
Configuração preliminar da máquina virtual
Compatibilidade com a tecnologia Citrix App Layering
Compatibilidade com a tecnologia Citrix Provisioning (Citrix Provisioning Services)
Compatibilidade com a tecnologia Omnissa App Volumes
Instalando o Light Agent
Conectar o Light Agent ao SVM
Descoberta de SVM
Configurar o algoritmo de seleção de SVMs para o Light Agent

Distribuição das conexões de Light Agents com SVMs (tags)
Proteger a conexão entre Light Agent e SVM
Ativar o Light Agent
Guia de migração do KSVLA Light Agent para o KES Light Agent
Instalação do KES Light Agent em vez do KSVLA Light Agent
Correspondência entre os componentes do KSVLA Light Agent e do KES Light Agent
Migração de tarefas e políticas do KSVLA Light Agent
Migração da configuração [KSVLA Light Agent+KEA] para a configuração [KES Light Agent+agente integrado]
Gerenciar o aplicativo a partir da linha de comando
Setup. Instalar o aplicativo
Setup /x. Remoção do aplicativo
msiexec /i. Recuperação do aplicativo
Comandos AVP
SCAN. Verificação de malware
UPDATE. Atualizar bancos de dados e módulos do software aplicativo
ROLLBACK. Reversão da última atualização
TRACES. Tracing
START. Iniciação de um perfil
STOP. Parar um perfil
STATUS. Status do perfil
STATISTICS. Estatísticas de operação de perfil
RESTORE. Restaurar arquivos do Backup
EXPORT. Exportar configurações do aplicativo
IMPORT. Importar configurações do aplicativo
ADDKEY. Aplicar arquivo de chave
LICENSE. Licença
RENEW. Comprar uma licença
PBATESTRESET. Redefinição dos resultados da verificação do disco antes de criptografar o disco
EXIT. Sair do aplicativo
EXITPOLICY. Desativar política
STARTPOLICY. Ativar política
DISABLE. Desativar proteção
SPYWARE. Detectar spyware
KSN. Alternância entre KSN / KPSN
SERVERBINDINGDISABLE. Desativação da proteção da conexão do servidor
Comandos KESCLI
Scan. Verificação de malware
GetScanState. Status de conclusão da verificação
GetLastScanTime. Determinar a hora da conclusão da verificação
GetThreats. Obter dados sobre as ameaças detectadas
UpdateDefinitions. Atualizar bancos de dados e módulos do software aplicativo
GetDefinitionState. Determinação da data e hora da última atualização dos bancos de dados
EnableRTP. Habilitar a proteção
GetRealTimeProtectionState. Status da Proteção Contra Ameaças ao Arquivo
GetEncryptionState. Status da criptografia do disco
Version. Identificar a versão do aplicativo

Comandos de gerenciamento do Detection and Response
SANDBOX. Gerenciamento do Sandbox
PREVENTION. Gerenciamento da prevenção de execução
ISOLATION. Gerenciando o isolamento de rede
RESTORE. Restauração do arquivo da Quarentena
IOCSCAN. Verifica os indicadores de comprometimento (IOC)
MDRLICENSE. Ativação do MDR
EDRKATA. Integração com o EDR (KATA)
EDRExpertOnPrem. Integração com o EDR Expert (on-premises)
KUMA. Integração KUMA
YARA. Execução da Verificação YARA
TELEMETRYFILTERS. Filtragem de eventos para serem enviados para a KUMA
Comandos de gerenciamento do Light Agent
KSVLAINFO. Determinar o modo Light Agent
VIISINFO. Status da conexão do Light Agent com o Servidor de integração
SVMINFO. Status da conexão do Light Agent com o Servidor de proteção
Códigos de erro
Apêndice. Perfis de aplicação
Gerenciar aplicativo usando a API REST
Instalação do aplicativo com a API REST
Trabalhar com a API
Fontes de informação sobre o aplicativo
Entrar em contato com o Suporte Técnico
Conteúdo e armazenamento de arquivos de rastreio
Rastreamento de funcionamento do aplicativo
Rastreamento de desempenho do aplicativo
Armazenar despejos
Protegendo arquivos de despejo e arquivos de rastreamento
Obtenção de dados do SO (Kaspersky Get System Info)
Limitações e avisos
Glossário
Agente de Autenticação
Agente de Rede
Alarme falso
Arquivo compactado
Arquivo infectado
Arquivo infectável
Arquivo IOC
Autenticação Kerberos
Banco de dados de endereços de phishing
Banco de dados de endereços maliciosos
Bancos de dados do Antivírus
Certificado de licença
Chave ativa
Cloud Discovery
Desinfecção
Emissor de certificado

Escopo da verificação
Escopo de proteção
Forma normal de endereço de um recurso da Web
Gerenciador de Arquivos Portátil
Grupo de administração
IOC
Light Agent
Máscara
Módulo de plataforma confiável
Objeto OLE
OpenIOC
Servidor de integração
SVM
Tarefa
Apêndices
Apêndice 1. Configurações do aplicativo
Proteção Contra Ameaças ao Arquivo
Proteção Contra Ameaças da Web
Proteção Contra Ameaças ao Correio
Proteção Contra Ameaças à Rede
Firewall
Prevenção contra ataque BadUSB
Proteção AMSI
Prevenção de Exploits
Detecção de Comportamento
Prevenção de Intrusão do Host
Mecanismo de Remediação
Kaspersky Security Network
Inspeção do Log
Anticryptor
Controle da Web
Controle de Dispositivos
Controle de aplicativos
Controle Adaptativo de Anomalias
Monitor de integridade do sistema
Endpoint Sensor
Sandbox
Managed Detection and Response
Endpoint Detection and Response
Endpoint Detection and Response Expert (on-premises)
Network Detection and Response (KATA)
Integração KUMA
Criptografia Completa do Disco
Criptografia em Nível de Arquivo
Criptografia de unidades removíveis
Modelos (criptografia de dados)
Exclusões

Configurações do aplicativo
Relatórios e armazenamento
Configurações de rede
Interface
Gerenciar configurações
Atualizar bancos de dados e módulos do software aplicativo
Apêndice 2. Grupos de confiança de aplicativos
Apêndice 3. Extensões de arquivo para verificação rápida de unidades removíveis
Apêndice 4. Tipos de arquivos para o filtro de anexos da Proteção Contra Ameaças ao Correio
Apêndice 5. Configurações de rede para interação com serviços externos
Apêndice 6. Eventos do aplicativo
Crítico
Falha funcional
Aviso
Mensagem informativa
Apêndice 7. Extensões de arquivo compatíveis com a prevenção de execução
Apêndice 8. Interpretadores de script compatíveis com a prevenção de execução
Apêndice 9. Escopo da verificação de IOC no registro (RegistryItem)
Apêndice 10. Requisitos de arquivos IOC
Apêndice 11. Resposta a ameaças da API para EDR
Apêndice 12. Contas de usuário em regras de componentes de aplicativos
Informações Legais
Provisão de dados
Provisão de dados segundo o Contrato de Licença do Usuário Final
Fornecimento de dados ao usar a Kaspersky Security Network
Provisão de dados ao usar as soluções de Detection and Response
Kaspersky Endpoint Detection and Response
Kaspersky Sandbox
Kaspersky Endpoint Detection and Response Expert (on-premises)
Kaspersky Network Detection and Response (KATA)
Integração com Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Conformidade com a legislação da União Europeia (GDPR)
Avisos de marcas registradas
Informações sobre código de terceiros

Ajuda do Kaspersky Endpoint Security for Windows

Quais as novidades da versão 14.2?

Foi adicionado suporte à autenticação baseada em token para a Proteção por senha

Novidades de cada versão do Kaspersky Endpoint Security for Windows

Iniciar

Implementação do Kaspersky Endpoint Security for Windows

Configuração inicial do Kaspersky Endpoint Security for Windows

Licenciamento do Kaspersky Endpoint Security for Windows

Provisão de dados

Nos termos do Contrato de Licença do Usuário Final

Ao usar a KSN

GDPR

Eliminar ameaças

Em estações de trabalho

Em servidores

Reagir à detecção de um Indicador de comprometimento (Isolamento de rede → Quarentena → Prevenção de execução)

Práticas recomendadas

Otimização do desempenho do aplicativo

Implementação do modo de negação padrão no Controle de aplicativos

Migração do KEA para o KES com o agente integrado

Usar o KES como parte de outras soluções

Kaspersky EDR

Kaspersky Sandbox

Kaspersky MDR

Novidades

Atualização 14.2

O Kaspersky Endpoint Security 14.2 for Windows apresenta os seguintes recursos e melhorias:

1. Foi alterado o conjunto de componentes instalados por padrão. A configuração padrão do aplicativo agora inclui a Prevenção contra ataque BadUSB, o gerenciamento do BitLocker e o agente integrado do EDR Optimum.

2. Foi adicionado suporte à autenticação baseada em token (Proteção por senha). Agora, para acessar o aplicativo, você pode usar seu nome de usuário e senha, uma senha temporária fornecida pelo administrador ou um token. A autenticação baseada em token pode ser usada, por exemplo, para contas de usuário de serviço que não exigem senha.

3. Foi adicionado um novo critério de segurança de senha para o BitLocker: a verificação do histórico de senhas. O aplicativo impede que os usuários definam uma senha que já tenham usado anteriormente.

4. Foi adicionado suporte à alteração do idioma da interface do Kaspersky Endpoint Security durante a atualização do aplicativo por meio da tarefa *Instalar aplicativo remotamente*. Agora, não é necessário reinstalar o aplicativo caso você tenha escolhido o idioma de interface errado.

5. Foram adicionados novos eventos de telemetria para os usuários das soluções Kaspersky Endpoint Detection and Response: GPO Change, SCCM Local Config Mismatch, SCCM Config Change, SCCM Deployment Task, Smb Connection Open. Esses novos eventos aprimoram os recursos de detecção de ameaças das soluções EDR.

6. Foi adicionado suporte a uma nova ação de resposta a ameaças, *Colocar arquivo*, para os usuários do Kaspersky Endpoint Detection and Response Expert (on-premises). Essa tarefa permite enviar aos computadores arquivos de configuração, scripts de resposta a ameaças, utilitários para mitigar os efeitos de ataques etc. A tarefa *Colocar arquivo* está disponível no console OSMP quando a solução Kaspersky EDR Expert (on-premises) versão 9.0 está implantada.

7. Foi aprimorado o comportamento das ações de resposta a ameaças para os usuários do Kaspersky Endpoint Detection and Response Optimum. Agora, antes de executar a ação (*Excluir arquivo*, *Mover arquivo para a Quarentena* ou *Prevenção de execução*), o aplicativo verifica se o objeto é crítico para o sistema (System Critical Object, SCO) e alerta sobre o possível impacto na estabilidade do sistema. Não é recomendável aplicar essas ações a arquivos de objetos críticos do sistema (SCO).

8. Foi adicionado suporte para que os usuários do Kaspersky Security for Virtualization Light Agent operem o aplicativo como parte de um cluster de alta disponibilidade de Servidores de integração. Um cluster de alta disponibilidade de Servidores de integração fornece proteção ininterrupta ao ambiente virtual graças ao failover das SVMs e dos Light Agents para um Servidor de integração de backup sempre que o Servidor de integração principal falha.

9. Ao desenvolver esta versão do Kaspersky Endpoint Security, incorporamos as alterações dos seguintes patches privados: PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF22065, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF23095, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF24037, PF24043, PF24048, PF25013, PF25016, PF25019, PF25030.

Atualização 14.1

O Kaspersky Endpoint Security 14.1 for Windows apresenta os seguintes recursos e melhorias:

1. O sistema operacional Windows Server 2025 agora é compatível.

2. O limite do número de regras de filtragem de eventos de telemetria para Endpoint Detection and Response Expert (on-premises) e Kaspersky Endpoint Detection and Response Expert (cloud) foi aumentado. O Kaspersky Endpoint Security agora proporciona até 10 mil regras de filtragem de inclusão e exclusão no total.

3. Agora você pode configurar tarefas para execução em dias específicos da semana, com intervalos definidos em semanas. O agendamento está disponível no Kaspersky Security Center 16.1 ou posterior.

4. Para a tarefa *Verificação de malware*, agora é possível definir um período de pausa para reduzir o impacto no desempenho do computador em momentos de maior carga.

5. O desempenho do subsistema de disco rígido do computador protegido foi otimizado com a redução das operações de E/S.

6. Ao desenvolver esta versão do Kaspersky Endpoint Security, incorporamos as alterações dos seguintes patches privados: PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF14071, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF25013, PF25016 e PF25019.

Atualização 14.0

O Kaspersky Endpoint Security 14.0 for Windows apresenta os seguintes recursos e melhorias:

1. Agora, computadores baseados em Arm são compatíveis. Você pode instalar o aplicativo no modo padrão ou no modo Agente EDR. No entanto, o aplicativo tem várias limitações (por exemplo, entre as tecnologias de criptografia de dados, somente o BitLocker é compatível).

2. A auditoria de política estendida é compatível com o Kaspersky Security Center Web Console versão 15.0 ou posterior. Agora você pode visualizar as revisões da política e salvá-las em um arquivo. Uma *revisão* é um conjunto de parâmetros modificados salvos pelo usuário. As revisões permitem comparar e reverter as alterações nos parâmetros da política.

3. Agora, novos eventos de telemetria estão disponíveis para usuários do Kaspersky Endpoint Detection and Response. Esses novos eventos aprimoram os recursos de detecção de ameaças usando as soluções Kaspersky EDR.

4. Ao desenvolver esta versão do Kaspersky Endpoint Security for Windows, incorporamos as alterações dos seguintes patches privados: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Atualização 12.12

O Kaspersky Endpoint Security 12.12 for Windows apresenta os seguintes recursos e melhorias:

1. Agora, a proteção de pastas compartilhadas contra criptografia externa que costumava fazer parte do componente Detecção de Comportamento é um componente separado, o Anticryptor.

2. O suporte para o protocolo Kerberos foi adicionado para autenticar o aplicativo pelo servidor proxy para acesso à Internet.

3. Agora, é possível especificar um hash de arquivo para um aplicativo confiável e não apenas um caminho completo.

4. Mais recursos de tarefa de *Verificação de IOC* estão disponíveis para usuários de soluções de Endpoint Detection and Response (EDR). Agora, a funcionalidade de Verificação retrospectiva IOC está disponível. A *Verificação retrospectiva IOC* é um modo de tarefa de *Verificação de IOC* no qual o Kaspersky Endpoint Security verifica os indicadores de comprometimento com o uso de dados de um determinado período de tempo. Este modo é voltado para a detecção de indicadores de comprometimento nos dados da atividade de rede do computador. O Kaspersky Endpoint Security analisa os dados dos logs do sistema operacional e do navegador no computador.

5. Os usuários do Kaspersky Endpoint Detection and Response (EDR) podem remover o limite de tamanho da quarentena. Talvez isso seja necessário para a verificação YARA, pois o aplicativo pode salvar um arquivo de despejo de memória grande. Agora, é possível usar todo o espaço livre em disco para a quarentena.

6. Agora, a compactação HTTPS é compatível com a otimização da exportação de eventos para a Kaspersky Unified Monitoring and Analysis Platform (KUMA). Isso ajuda a reduzir o tráfego de saída.

7. Ao desenvolver esta versão do Kaspersky Endpoint Security for Windows, incorporamos as alterações dos seguintes patches privados: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Atualização 12.11

O Kaspersky Endpoint Security 12.11 for Windows oferece os seguintes recursos e melhorias:

1. O aplicativo verifica a configuração dos componentes de controle antes de salvar as configurações. A verificação foi adicionada para os componentes controle de aplicativos, controle de dispositivos, 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 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.

2. Suporte adicionado para o envio automático de envio de arquivo para análise do KATA Sandbox. O *KATA Sandbox* é um componente da Kaspersky Anti Targeted Attack Platform que executa arquivos em imagens virtuais de sistemas operacionais. O Sandbox analisa o comportamento do objeto para detectar atividades maliciosas e características de atividades de ataques direcionados à infraestrutura de TI da organização. O Sandbox analisa e verifica objetos em servidores especiais com imagens virtuais implantadas de sistemas operacionais Microsoft Windows (servidores Sandbox). Para o KATA Sandbox funcionar no modo automático, a Kaspersky Anti Targeted Attack Platform 8.0 ou posterior deve ser implementada.

3. Envio otimizado de telemetria EDR. Agora, é possível especificar o comprimento máximo do pacote.

4. Diagnóstico de conexão aprimorada para Kaspersky Security Network. Detalhes do erro de conexão expandido para que a Kaspersky Security Network resolva possíveis problemas.

5. Suporte acrescentado para que as listas de evento de configuração sejam enviadas para a Kaspersky Unified Monitoring and Analysis Platform (KUMA). Agora, além das listas de eventos predefinidas na KUMA, é possível adicionar os eventos manualmente na telemetria ou eventos excluídos por ID nos logs de eventos do Windows.

6. Política da interface atualizada no Web Console. O layout das seções da política foi alterado para garantir o acesso mais rápido aos recursos essenciais.

7. Suporte para Windows 11 25H2.

8. Ao desenvolver esta versão do Kaspersky Endpoint Security for Windows, incorporamos as alterações dos seguintes patches privados: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF22004, PF22008, PF22014.

Atualização 12.10

O Kaspersky Endpoint Security 12.10 for Windows oferece os seguintes recursos e melhorias:

1. Para o componente Prevenção de ataque BadUSB, a opção foi adicionada para autorizar leitores de código de barras por meio da leitura de um código de barras na tela. Você não precisa mais inserir um código utilizando o teclado na tela para autorizar os leitores de código de barras.

2. Os recursos e melhorias a seguir estão disponíveis para usuários das soluções de Endpoint Detection and Response (EDR) da Kaspersky:

   - Agora é possível gerenciar o Isolamento de rede do computador diretamente nos detalhes do alerta. Além disso, nos detalhes do alerta, é possível especificar o período de Isolamento de rede do computador e adicionar exclusões.

   - Preencher os detalhes do alerta com novos dados. Agora, os detalhes do alerta trazem informações mais completas sobre a ameaça, incluindo o comportamento do aplicativo ao responder a ameaças detectadas pelo EDR.

   - O processamento de arquivos IOC foi aprimorado. Agora você pode visualizar e editar o conteúdo dos arquivos IOC na interface do Kaspersky Security Center Web Console. Depois de carregar um arquivo IOC, o aplicativo exibe um relatório sobre o aplicativo de termos IOC.

   - Resposta aprimorada aos IOCs detectados. Agora você pode colocar em quarentena os arquivos detectados pela tarefa *Verificação de IOC* diretamente nos resultados de detecção de IOC, nas propriedades da tarefa. Você também pode isolar computadores da rede nas propriedades da tarefa.

   - Agora é possível criar arquivos IOC diretamente nas propriedades da tarefa *Verificação de IOC*, usando listas de hashes de arquivos, endereços IP ou nomes DNS geradas a partir de um arquivo TXT.

   - Escopo de verificação expandido para a tarefa *Verificação de IOC*. Agora é possível definir um escopo para a Verificação de IOC do registro (**Registro do Windows – RegistryItem**). Nas versões anteriores do aplicativo, só era possível utilizar um escopo de Verificação de IOC predefinido no registro.

3. Nova Permissão de proteção por senha adicionada, *Configurações de exportação*. Por padrão, somente o usuário do KLAdmin pode criar um arquivo de configuração com as configurações do Kaspersky Endpoint Security na interface do aplicativo. Para conceder acesso a outros usuários, será necessário dar permissão a eles.

4. Ao desenvolver esta versão do Kaspersky Endpoint Security for Windows, incorporamos as alterações dos seguintes patches privados: PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF13120, PF13123, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF15062, PF16052, PF16053, PF16055, PF16056, PF16057, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF21007.

Atualização 12.9

O Kaspersky Endpoint Security 12.9 for Windows oferece os seguintes recursos e melhorias:

1. A nova funcionalidade para *gerenciar senhas temporárias* foi adicionada. A senha temporária permite fornecer acesso ao Kaspersky Endpoint Security com a Proteção por Senha ativada para um computador separado. O gerenciamento de senhas temporárias permite salvar o histórico de senhas (até 30 dias), monitorar o status da senha temporária (*Ativo*, *Expirado*, *Revogado*) e revogar senhas temporárias.

2. Foi adicionada a opção de encerrar a conexão com recursos da Web proibidos pelas regras de Controle da Web imediatamente após a aplicação da política. Nas versões anteriores do aplicativo, o Controle da Web restringia somente as novas conexões aos recursos da Web proibidos.

3. Para usuários da Kaspersky Anti Targeted Attack Platform, uma opção para executar a verificação YARA localmente no computador foi adicionada. Para fazer isso, é necessário baixar um arquivo com as regras YARA e executar o comando no CMD.

4. Corrigido o comportamento do aplicativo quando o BitLocker é ativado em computadores nos quais as unidades já estão por ele protegidas com o uso de ferramentas de terceiros. O Kaspersky Endpoint Security inicia o procedimento de recuperação para enviar a chave de recuperação ao Kaspersky Security Center. Assim, o gerenciamento do BitLocker é transferido para o console do Kaspersky Security Center.

5. Uma nova seção, **Histórico de resposta**, está disponível para usuários de soluções Detection and Response da Kaspersky. Esta seção contém informações sobre ações de resposta a ameaças executadas no computador. Tais ações incluem, por exemplo, executar a tarefa *Encerrar processo* ou isolar o computador da rede. O histórico de respostas só está disponível para usuários das seguintes soluções da Kaspersky: MDR, EDR, KATA.

6. Para usuários da Kaspersky Unified Monitoring and Analysis Platform, o suporte para ações de resposta a ameaças EDR já está disponível. Ao responder a ameaças, o KUMA executa scripts que criam tarefas EDR correspondentes. Para executar tarefas EDR, você precisa criar uma regra de resposta para o script personalizado no console KUMA e selecionar eventos.

7. Ao desenvolver esta versão do Kaspersky Endpoint Security for Windows, incorporamos as alterações dos seguintes patches privados: PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF20011, PF20016, PF20017, PF20020, PF20021.

Atualização 12.8

O Kaspersky Endpoint Security 12.8 for Windows oferece os seguintes recursos e melhorias:

1. O aplicativo agora tem suporte ao modo Light Agent para proteger ambientes virtuais. Agora é possível implementar o aplicativo como Light Agent como parte da solução Kaspersky Security for Virtualization Light Agent 6.2.

2. Agora, a Interceptação de operações de arquivo em contêineres do Docker é compatível. O *contêiner* é um ambiente isolado no qual um aplicativo pode ser executado sem interagir diretamente com o sistema operacional. O Kaspersky Endpoint Security verifica os arquivos dentro de contêineres aos quais o usuário obtém acesso. Quando uma ameaça é detectada, os aplicativos bloqueiam essa atividade maliciosa e tentam desinfectar o arquivo dentro do contêiner. Caso o arquivo não possa ser desinfectado, o aplicativo interromperá o contêiner.

3. Agora é possível definir um escopo de proteção de pastas compartilhadas contra criptografia externa (componente Detecção de comportamento). Agora é possível especificar pastas compartilhadas que o aplicativo deve monitorar quanto à atividade de arquivos. Também é possível excluir arquivos do escopo de proteção. Nas versões anteriores do aplicativo, o componente Detecção de Comportamento monitorava todas as pastas compartilhadas quanto à atividade de arquivos.

4. Agora é possível configurar diferentes conjuntos de componentes para diferentes tipos de sistemas operacionais no pacote de instalação. Ou seja, é possível implementar o aplicativo em estações de trabalho e servidores que usam o mesmo pacote de instalação. Os componentes que não estão disponíveis para um determinado tipo de sistema operacional são automaticamente excluídos das propriedades do pacote de instalação.

5. A opção de selecionar exclusões predefinidas de verificação e aplicativos confiáveis foi adicionada. Exclusões de verificação e aplicativos confiáveis predefinidos permitem configurar rapidamente a zona confiável para o aplicativo em um ambiente virtual (Citrix, VMware). Essas exclusões incluem, por exemplo, arquivos de máquina virtual VHD e VHDX. As exclusões podem ser adicionadas ao criar um pacote de instalação de aplicativo, ao criar uma política ou ao instalar o Kaspersky Endpoint Security.

6. A telemetria EDR agora inclui eventos para operações com dispositivos conectados por USB. Também é possível adicionar esses eventos a exclusões da telemetria EDR.

7. A opção de bloquear conexões de rede através do protocolo TLS 1.0 obsoleto foi adicionada. O TLS 1.0 tem um nível de segurança baixo, portanto, é recomendável desativar esse protocolo e usar as versões mais recentes do TLS 1.2 ou TLS 1.3. Por padrão, o Kaspersky Endpoint Security bloqueia conexões TLS 1.0. Após a atualização da versão do aplicativo, a operação de serviços de terceiros que usam o protocolo TLS 1.0 pode falhar. Para evitar problemas na operação de serviços de terceiros, você pode permitir o uso do protocolo TLS 1.0 na política de grupo antes de atualizar a versão do aplicativo.

8. Ao desenvolver esta versão do Kaspersky Endpoint Security for Windows, incorporamos as alterações dos seguintes patches privados: PF10053, PF10054, PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018.

Atualização 12.7

O Kaspersky Endpoint Security 12.7 for Windows oferece os seguintes recursos e melhorias:

1. Agora, é possível limitar o uso de recursos da CPU para as tarefas de *verificação de malware*. Para fazer isso, nas configurações do aplicativo, especifique a porcentagem máxima de carga da CPU para todos os núcleos que podem ser usados durante a verificação do computador.

2. Agora, é possível enviar manualmente os arquivos para verificação no KATA Sandbox. O *KATA Sandbox* é um componente da Kaspersky Anti Targeted Attack Platform que executa arquivos em imagens virtuais de sistemas operacionais. O Sandbox analisa o comportamento do objeto para detectar atividades maliciosas e características de atividades de ataques direcionados à infraestrutura de TI da organização. O Sandbox analisa e verifica objetos em servidores especiais com imagens virtuais implantadas de sistemas operacionais Microsoft Windows (servidores Sandbox). Para enviar um arquivo para verificação ao KATA Sandbox, selecione o comando pertinente no menu de contexto do arquivo.

3. Agora, é possível configurar a integração com a solução que protege a rede local corporativa, *Kaspersky Network Detection and Response*. O Kaspersky Network Detection and Response (NDR) faz parte da Kaspersky Anti Targeted Attack Platform. É possível configurar a interação com o NDR no modo padrão, assim como no modo EDR Agent.

4. O suporte para o cliente de mail Microsoft Office Outlook versão 2021 foi adicionado na extensão da Proteção Contra Ameaças ao Correio. A extensão permite a verificação de mensagens no nível de um cliente de e-mail em vez do nível de protocolo. Além das mensagens, a extensão permite verificar objetos recebidos por meio da interface MAPI dos repositórios do Microsoft Exchange (por exemplo, objetos do calendário). Essa verificação ocorre no cliente de e-mail.

5. Ao desenvolver esta versão do Kaspersky Endpoint Security for Windows, incorporamos as alterações dos seguintes patches privados: PF10049, PF10355, PF12114, PF13109, PF14056, PF15038, PF15045, PF16037, PF16042, PF16047, PF17014, PF17018, PF17021, PF17024, PF18006, PF18007.

Atualização 12.6

O Kaspersky Endpoint Security 12.6 for Windows oferece os seguintes recursos e melhorias:

1. A funcionalidade para integração com a solução Kaspersky SIEM – *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* – foi adicionada. Agora é possível enviar eventos dos logs de eventos do Windows para o coletor da KUMA. Isso permite que a KUMA receba eventos do Windows (um conjunto limitado de EventIDs é compatível) de todos os computadores nos quais o Kaspersky Endpoint Security está instalado, sem instalar os agentes da KUMA nesses computadores.

2. Um novo componente *Monitor de integridade do sistema* foi adicionado para substituir o 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 Endpoint Security gera os eventos correspondentes e alerta o administrador. O monitor de integridade de arquivos não faz mais parte do aplicativo. As configurações do monitor de integridade de arquivos migram automaticamente para o monitor de integridade do sistema quando o aplicativo é atualizado. Para garantir a operação correta do Monitor de integridade do sistema, o aplicativo Kaspersky Endpoint Security e o plug-in de gerenciamento devem ser atualizados para a versão 12.6.

3. O status do EDR Agent (KATA) integrado e instalado foi adicionado nas propriedades do computador no console do Kaspersky Security Center. Agora, caso tenha um EDR Agent (KATA) integrado instalado, a coluna exibirá o componente do status atual do **status do Endpoint Sensor** (por exemplo, *Em execução*, *Interrompido*, *Sem suporte pela licença* etc.).

4. A opção de selecionar exclusões predefinidas de verificação e aplicativos confiáveis foi adicionada. As exclusões predefinidas de verificação e aplicativos confiáveis ajudam a configurar rapidamente a zona confiável ao usar o aplicativo em servidores SQL, Microsoft Exchange e System Center Configuration Manager. Essas exclusões incluem, por exemplo, arquivos de banco de dados MDF e LDF. As exclusões podem ser adicionadas ao criar uma nova política, modificar uma política existente ou instalar o Kaspersky Endpoint Security.

5. A exibição dos detalhes do alerta do Kaspersky Endpoint Detection and Response Optimum foi movida do plug-in de gerenciamento do Kaspersky Endpoint Security para um plug-in de gerenciamento separado do Kaspersky Endpoint Detection and Response. O plug-in de gerenciamento de EDR é um recurso único que trabalha com os agentes nos sistemas operacionais Windows, Mac e Linux. Agora, ao trabalhar com o EDR Optimum, o plug-in de gerenciamento do Kaspersky Endpoint Security será necessário para a criação de tarefas de resposta a ameaças, e o plug-in de gerenciamento do EDR será necessário para a exibição dos detalhes do alerta.

6. Suporte para Windows 11 24H2.

7. Ao desenvolver esta versão do Kaspersky Endpoint Security for Windows, incorporamos as alterações incluídas nos seguintes patches privados: pf10048, pf10353, pf12106, pf12107, pf12108, pf13090, pf13100, pf15031, pf15034, pf15036, pf16021, pf16023, pf16029, pf17002.

Atualização 12.5

O Kaspersky Endpoint Security 12.5 for Windows oferece os seguintes recursos e melhorias:

1. A opção para configurar exclusões de telemetria foi adicionada. *Telemetria* é uma lista de eventos que ocorreram no computador protegido. Os dados de telemetria são usados pela Kaspersky Anti Targeted Attack Platform (EDR) para monitorar e proteger a infraestrutura de TI da organização. A configuração de exclusões de telemetria ajuda a melhorar o desempenho do computador e otimizar a transmissão de dados para o servidor de coleta de telemetria.

2. A interface da zona confiável do aplicativo foi melhorada. Agora, o Kaspersky Endpoint Security oculta os objetos da zona confiável do usuário caso o administrador tenha proibido o usuário de adicionar suas próprias exclusões de verificação (locais) e aplicativos confiáveis. Isso evita o acesso não autorizado à zona confiável por um intruso e aumenta o nível de segurança do computador.

3. A opção de verificar o tráfego dos clientes de e-mail do MyOffice Mail e do R7-Office Organizer foi adicionada. Agora, o componente Proteção Contra Ameaças ao Correio verifica não apenas os anexos de mensagens no download, mas também as mensagens enviadas e recebidas.

4. Uma nova categoria de recursos da Web *Ferramentas de IA Generativa* foi adicionado. É possível configurar o acesso aos sites da nova categoria com o uso do Controle da Web.

5. Agora, você pode selecionar o local de uma regra de pacotes de rede na lista Firewall. A localização de uma regra de pacotes de rede na lista determina a prioridade dela. Nas versões anteriores do aplicativo, uma nova regra só podia ser adicionada ao final da lista e, depois disso, era necessário mover a regra manualmente pela lista para priorizá-la. Agora, ao adicionar uma regra, é possível fazer a escolha entre a regra ser colocada no início, no final da lista ou ao lado da regra selecionada.

6. Nas regras dos componentes do Kaspersky Endpoint Security, agora é possível selecionar usuários não apenas do Active Directory, mas também da lista de usuários no Kaspersky Security Center. Também é possível inserir os dados da conta de usuário local manualmente. Essa possibilidade foi adicionada para as regras dos seguintes componentes: Controle de Aplicativos, Controle de Dispositivos, Controle da Web, Controle Adaptativo de Anomalias e Inspeção de Log.

7. Agora, o relatório de detecção de ataque à rede inclui uma coluna com o endereço MAC do computador atacante (o componente Proteção Contra Ameaças à Rede). Agora, é possível ver o endereço MAC do computador atacante no relatório, além de seu endereço IP. Isso é útil para investigação de incidentes. Relatórios contendo o endereço MAC do computador invasor também estarão disponíveis no Kaspersky Security Center Linux console, versão 15.1 ou posterior.

8. O nível dos requisitos de proteção do computador aumentou. Agora, o alto nível de proteção requer a ativação da proteção de serviços de aplicativo contra gerenciamento externo. Verifique o indicador do nível de segurança na parte superior da janela de política. Caso tenha um nível de segurança médio ou baixo, será possível ativar a proteção de serviços do aplicativo contra gerenciamento externo na janela de recomendação do indicador de nível de segurança.

9. Suporte para novos eventos de detecção de objetos quando o aplicativo está sendo executado na Configuração do Endpoint Detection and Response Agent (EDR Agent), foi adicionado. Esses eventos já eram compatíveis na configuração do [KES+agente integrado].

10. Ao desenvolver esta versão do Kaspersky Endpoint Security for Windows, incorporamos as alterações incluídas nos seguintes patches privados: pf9640, pf9830, pf9831, pf10047, pf10351, pf12102, pf12105, pf13084, pf13089, pf14040, pf14047, pf15026, pf15028, pf16013.

Atualização 12.4

O Kaspersky Endpoint Security 12.4 for Windows oferece os seguintes recursos e melhorias:

1. Adicionada nova funcionalidade para proteger a conexão do computador com o Kaspersky Security Center. A nova tarefa *Proteção da conexão do Servidor de Administração* permite definir uma senha para a conexão com um servidor confiável. Isso significa que não é possível reconectar o computador e executar comandos por outro servidor sem essa senha.

2. Para o componente de Proteção por Senha, a capacidade de selecionar usuários manualmente, e não apenas por meio do Active Directory, foi adicionada. Ou seja, é possível especificar manualmente um nome de usuário e senha e atribuir os direitos de acesso ao Kaspersky Endpoint Security para essa conta. Assim, não é necessário compartilhar a senha do KLAdmin com outros usuários ou criar novas contas no Active Directory para controlar o acesso ao aplicativo.

3. Suporte para Windows 11 23H2.

Atualização 12.3

O Kaspersky Endpoint Security 12.3 for Windows oferece os seguintes recursos e melhorias:

1. Agora, é possível instalar o aplicativo na configuração do Endpoint Detection and Response Agent. Esta configuração permite instalar o aplicativo com um conjunto de componentes requeridos pelas soluções de Detection and Response da Kaspersky: Kaspersky Managed Detection and Response e Kaspersky Anti Targeted Attack Platform (EDR). É possível instalar o aplicativo nesta configuração juntamente com as soluções de terceiros (por exemplo, Dr.Web, Dallas Lock, ESET). Isso viabiliza o uso de ferramentas de segurança de infraestrutura de terceiros juntamente com o Detection and Response da Kaspersky.

2. A operação do Kaspersky Endpoint Security com dispositivos Bluetooth foi aprimorada. Agora, é possível configurar exclusões e restringir o acesso a todos os dispositivos Bluetooth, exceto os dispositivos de entrada (teclados sem fio, mouses, etc.).

3. A operação do componente Controle de Aplicativos com o banco de dados de arquivos executáveis foi otimizada. O Kaspersky Endpoint Security agora remove automaticamente as informações do arquivo de banco de dados caso ele seja excluído do computador. Isso permite manter o banco de dados atualizado, além de economizar os recursos do Kaspersky Security Center.

4. O nível dos requisitos de proteção do computador aumentou. Agora, o nível de proteção alto exige ativar a proteção por senha. Verifique o indicador do nível de segurança na parte superior da janela de política. Caso tenha um nível de proteção médio ou baixo, será possível ativar a proteção por senha na janela de recomendação do indicador de nível de proteção.

5. Adicionada compatibilidade com o protocolo HTTPS para que o aplicativo funcione com a Kaspersky Security Network. Uso do HTTPS ativado pelas propriedades do Servidor de Administração nas configurações do servidor proxy KSN.

Atualização 12.2

O Kaspersky Endpoint Security 12.2 for Windows oferece os seguintes recursos e melhorias:

1. O suporte ao protocolo WPA3 foi adicionado para controlar conexões com redes Wi-Fi (Controle de Dispositivos). Agora é possível selecionar o protocolo WPA3 nas configurações de redes Wi-Fi confiáveis e negar a conexão à rede usando um protocolo menos seguro.

2. Agora você pode escolher um protocolo e portas para exclusões de Proteção Contra Ameaças à Rede. Agora, além de especificar endereços IP de dispositivos confiáveis, você também pode selecionar uma porta e um protocolo. Isso permite que você exclua fluxos de dados individuais e evite ataques de rede de endereços IP confiáveis.

3. Ordem diferente de fontes de atualização para a tarefa de *Atualização de bancos de dados e módulos do aplicativo local* se uma política for aplicada ao computador. O servidor do Kaspersky Security Center agora é usado por padrão como a primeira fonte de atualização em vez dos servidores da Kaspersky. Isso ajuda a economizar tráfego quando o usuário executa a tarefa de *Atualização de bancos de dados e módulos do aplicativo* local.

Atualização 12.1

O Kaspersky Endpoint Security 12.1 for Windows oferece os seguintes recursos e melhorias:

1. Um agente integrado para a solução Kaspersky Anti Targeted Attack Platform foi adicionado. Não é mais preciso ter o Kaspersky Endpoint Agent para poder usar o EDR (KATA). Todas as funções do Kaspersky Endpoint Agent serão executadas pelo Kaspersky Endpoint Security. Para migrar as políticas do Kaspersky Endpoint Agent, use o Assistente de migração. Após atualizar o aplicativo, o Kaspersky Endpoint Security alterna o uso do agente integrado e remove o Kaspersky Endpoint Agent. O Kaspersky Endpoint Agent foi adicionado na lista de software incompatível. O Kaspersky Endpoint Security possui agentes integrados para todas as soluções do Detection and Response, portanto, não é mais necessário instalar o Kaspersky Endpoint Agent para integração com essas soluções.

2. Agora, o modo de compatibilidade do Azure WVD é compatível. Esse recurso garante a exibição correta do estado das máquinas virtuais Azure no console do Kaspersky Anti Targeted Attack Platform. O modo de compatibilidade do Azure WVD permite atribuir um ID do sensor exclusivo e permanente para essas máquinas virtuais.

3. Agora, é possível configurar o acesso do usuário a dispositivos móveis no iTunes ou aplicativos semelhantes. Ou seja, é possível, por exemplo, permitir que o dispositivo móvel seja usado apenas no iTunes e bloquear o uso do dispositivo móvel como uma unidade removível. O aplicativo também é compatível com essas regras para o aplicativo Android Debug Bridge (ADB).

4. Kaspersky Security Center versão 11 não é mais compatível. Atualize o Kaspersky Security Center para a versão mais recente.

Problemas corrigidos

A tabela abaixo lista todos os problemas descobertos em versões anteriores do Kaspersky Endpoint Security e corrigidos na versão atual.

Lista de problemas corrigidos na versão 14.2

Identificador	Descrição
10110351	O componente Controle de Dispositivos permite o acesso a um dispositivo MTD (cartão SD) quando a ação **Bloquear** é selecionada para o tipo de dispositivo **Unidades removíveis**.
10068496	Em um dispositivo protegido, o modo de Proteção contra MAC spoofing pode ser alterado quando as configurações da Proteção Contra Ameaças à Rede estão bloqueadas na política principal.
10095087	Quando a verificação de conexões criptografadas está ativada, o acesso a qualquer site por meio de um Firewall de próxima geração (NGFW) com um certificado revogado aciona uma notificação sobre o redirecionamento para um domínio com um certificado não confiável.
10140912	Com o aplicativo instalado, o computador não detecta o dispositivo PDA BHT1100B que executa o Windows Mobile.
10141009	Se o componente Criptografia de arquivos estiver instalado, o aplicativo Anthropic Claude poderá não ser iniciado.

Identificador	Descrição
10610853	Após a atualização para a nova versão, a política não pode ser aberta porque as configurações do Controle de Dispositivos na nova versão incluem dispositivos que não são compatíveis com a versão anterior.
10720516	Os anexos em arquivos de formatos de aplicativos de escritório podem não abrir quando o aplicativo está instalado.
10421967	Não é possível entrar em uma caixa de correio compartilhada se ela tiver sido adicionada como uma conta separada.

Lista de problemas corrigidos no plug-in da web 14.2.0.8289

Identificador	Descrição
9946286	Ao adicionar o endereço de um site a uma regra do Controle da Web, não é possível usar uma máscara que não contenha um ponto entre o domínio e a zona do domínio.
10054657 10507166	Após a migração para a nova versão, determinados componentes (como Controle de dispositivos e Controle de aplicativos) não podem ser gerenciados por meio da política.
10084390	Nas configurações do componente Controle de dispositivos, o tipo de dispositivo **Disco rígido** está duplicado, o que faz com que os discos rígidos dos usuários sejam bloqueados.
10113718	Em alguns casos, as regras personalizadas do Firewall não são exibidas.
10311613	Nas configurações do componente Prevenção de Intrusão do Host, não é possível adicionar um recurso protegido por máscara usando o caractere `*`.
10391923	No Controle de Aplicativos, ao criar uma categoria de aplicativos com base no hash MD5 de um arquivo, não é exibida nenhuma advertência indicando que essa categoria é inválida e não funcionará.
10571790	No componente Controle de aplicativos, foi corrigido o título da lista de regras de bloqueio no modo **Permitir tudo, exceto a lista de regras**.
10592891 10689065	Na Zona confiável, o campo **Comentário** não é exibido para exclusões na seção **Exclusões de Verificação de malware**.
10613015 10689049 10592534	No componente Controle de dispositivos, o campo **Comentário** não é exibido para dispositivos confiáveis.
10645068 10689057	A tarefa *Remover a chave* não é executada se um arquivo de chave de licença no formato KEY estiver selecionado.
10685370 10685422	No componente Controle de dispositivos, não é possível adicionar um novo dispositivo à lista de dispositivos confiáveis se já houver um dispositivo com esse nome na lista.
10721136	As tarefas de grupo não podem ser salvas se nenhuma data de conclusão for especificada nas configurações de agendamento.
10753509	Modificar a lista de usuários e grupos de dispositivos confiáveis no componente Controle de dispositivos pode alterar os tipos de registro, fazendo com que as configurações deixem de ser aplicadas ao dispositivo.
10773402	Em alguns casos, as alterações nas configurações da política podem não ser salvas devido a perfis corrompidos.
10822620	As configurações do componente Anticryptor não são exibidas na política, e as alterações nas configurações de notificação não são salvas.
10817035	Em uma política secundária, é possível adicionar um dispositivo confiável mesmo que essa configuração esteja desativada na política principal ("cadeado" fechado). No entanto, o dispositivo adicionado não é salvo.
10678009	No plug-in da web do Kaspersky Endpoint Security, não é possível adicionar uma nova regra do Firewall a uma política se uma regra tiver sido criada anteriormente usando um intervalo de endereços IP.

Lista de problemas corrigidos na versão 14.1

Identificador	Descrição
10140523	Ativar o NVMe Nativo no Windows 11 pode resultar em comportamento instável do aplicativo.
9340076	Em um dispositivo com o aplicativo instalado e o componente Criptografia de Arquivos ativado, o Windows Explorer não atualiza automaticamente o conteúdo de uma pasta de rede depois que ela é modificada a partir de outro dispositivo.
9722863	O relatório Controle de Dispositivos não inclui o evento de desconexão de token USB.
10006481	Depois de aplicar uma regra que nega o tráfego de entrada, as conexões TCP ativas com serviços externos podem ser encerradas prematuramente devido ao cálculo incorreto do tempo limite.
10140912	O aplicativo não detecta o dispositivo PDA BHT1100B.
10157563	Folder Redirection pode não funcionar após uma reinicialização em estações de trabalho VDI.
10158494	O Controle de Dispositivos registra vários eventos de conexão e desconexão de um dispositivo removível sem que ele seja fisicamente reconectado.

Perguntas frequentes

GERAL

Em quais computadores o Kaspersky Endpoint Security pode operar?

O que mudou desde a última versão?

Com quais outros aplicativos da Kaspersky o Kaspersky Endpoint Security pode operar?

Como posso conservar os recursos do computador durante a operação do Kaspersky Endpoint Security?

IMPLEMENTAÇÃO

Como instalar o Kaspersky Endpoint Security em todos os computadores de uma organização?

Quais configurações de instalação podem ser configuradas na linha de comando?

Como desinstalar remotamente o Kaspersky Endpoint Security?

UPDATE

Quais são os métodos disponíveis para atualizar os bancos de dados?

O que fazer se surgirem problemas após uma atualização?

Como atualizar bancos de dados fora da rede corporativa?

É possível usar um servidor proxy para atualizações?

SEGURANÇA

Como o Kaspersky Endpoint Security verifica os e-mails?

Como excluir um arquivo confiável das verificações?

Como proteger um computador contra vírus de unidades flash?

Como executar uma verificação de malware ocultado do usuário?

Como pausar temporariamente a proteção do Kaspersky Endpoint Security?

Como restaurar um arquivo que o Kaspersky Endpoint Security excluiu erroneamente?

Como proteger o Kaspersky Endpoint Security contra a desinstalação por um usuário?

INTERNET

O Kaspersky Endpoint Security verifica conexões criptografadas (HTTPS)?

Como permitir que os usuários se conectem apenas às redes Wi-Fi confiáveis?

Como bloquear redes sociais?

APLICATIVO

Como saber quais aplicativos estão instalados no computador do usuário (inventário)?

Como eu evito que jogos de computador sejam executados?

Como verificar se o Controle de Aplicativos foi configurado corretamente?

Como adicionar um aplicativo à lista confiável?

DISPOSITIVOS

Como bloquear o uso de unidades flash?

Como adicionar um dispositivo à lista confiável?

É possível obter acesso a um dispositivo bloqueado?

CRIPTOGRAFIA

Em quais condições a criptografia é impossível?

Como usar uma senha para restringir o acesso a um arquivo?

É possível usar cartões inteligentes e tokens com criptografia?

É possível obter acesso a dados criptografados se não houver conexão com o Kaspersky Security Center?

O que fazer se o sistema operacional do computador falhar, mas os dados permanecerem criptografados?

SUPORTE

Onde o arquivo de relatório está armazenado?

Como criar um arquivo de rastreamento?

Como ativar a gravação do dump?

Kaspersky Endpoint Security for Windows

O Kaspersky Endpoint Security for Windows (doravante também referido como Kaspersky Endpoint Security) fornece ampla proteção de computadores contra vários tipos de ameaças e ataques de rede e de phishing.

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

Tecnologias de detecção de ameaças

Aprendizado de máquina

O Kaspersky Endpoint Security usa um modelo baseado em aprendizado de máquina. O modelo foi desenvolvido por especialistas da Kaspersky. Posteriormente, o modelo é continuamente alimentado com dados de ameaças da KSN (treinamento do modelo).

Análise na nuvem

O Kaspersky Endpoint Security recebe os dados de ameaças da Kaspersky Security Network. *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.

Análise especializada

O Kaspersky Endpoint Security usa dados de ameaças adicionados por analistas de vírus da Kaspersky. Os analistas de vírus verificam manualmente os objetos caso a reputação de um objeto não possa ser determinada automaticamente.

Análise de comportamento

O Kaspersky Endpoint Security analisa a atividade de um objeto em tempo real.

Análise automática

O Kaspersky Endpoint Security recebe dados de um sistema automático de análise de objetos. O sistema processa todos os objetos enviados para a Kaspersky. O sistema então determina a reputação do objeto e adiciona os dados aos bancos de dados do antivírus. Caso o sistema não possa determinar a reputação do objeto, ele consultará os analistas de vírus da Kaspersky.

Sandbox

O Kaspersky Endpoint Security processa os objetos em uma máquina virtual. O Kaspersky Sandbox analisa o comportamento de um objeto e toma uma decisão sobre a reputação. A tecnologia estará disponível apenas se a solução Kaspersky Sandbox estiver em uso.

Cloud Sandbox

O Kaspersky Endpoint Security verifica objetos em um ambiente isolado fornecido pela Kaspersky. A tecnologia Cloud Sandbox está habilitada permanentemente e disponível para todos os usuários da Kaspersky Security Network, independentemente do tipo de licença em uso. Caso já tenha implantado a solução Endpoint Detection and Response, é possível habilitar um contador separado para as ameaças detectadas pelo Cloud Sandbox.

Árvore de seleção

Cada tipo de ameaça é processada por um componente exclusivo. É possível ativar e desativar os componentes de modo independente, como também configurá-los.

Seção	Componente
Proteção Essencial Contra Ameaças	**Proteção Contra Ameaças ao Arquivo** O componente Proteção Contra Ameaças ao Arquivo permite evitar infecção do sistema de arquivos do computador. Por padrão, o componente Proteção Contra Ameaças ao Arquivo está localizado de forma permanente na RAM do computador e verifica todos os arquivos abertos, salvos ou executados em tempo real. O componente verifica os arquivos em todas as unidades do computador, inclusive unidades conectadas. O componente fornece proteção ao computador com a ajuda de bancos de dados de antivírus, o serviço na nuvem Kaspersky Security Network e análise heurística. **Proteção Contra Ameaças da Web** O componente Proteção Contra Ameaças da Web impede o download de arquivos maliciosos da Internet e também bloqueia a conexão com sites maliciosos e de phishing. O componente fornece proteção ao computador com a ajuda de bancos de dados de antivírus, o serviço na nuvem Kaspersky Security Network e análise heurística. **Proteção Contra Ameaças ao Correio** O componente Proteção contra ameaças de correio verifica os anexos das mensagens de e-mail recebidas e enviadas para detectar vírus e outras ameaças. O componente fornece proteção ao computador com a ajuda de bancos de dados de antivírus, o serviço na nuvem Kaspersky Security Network e análise heurística. A Proteção Contra Ameaças ao Correio pode verificar as mensagens recebidas e enviadas. O aplicativo é compatível com POP3, SMTP, IMAP e NNTP nos seguintes clientes de e-mail: • Microsoft Office Outlook • Mozilla Thunderbird • Windows Mail • Correio do MyOffice • R7-Office Organizer Para verificar o tráfego nos programas de e-mail Mozilla Thunderbird, MyOffice Mail e R7-Office Organizer, é necessário adicionar o certificado da Kaspersky ao armazenamento de certificados e selecionar o armazenamento de certificados próprio. A Proteção Contra Ameaças ao Correio não oferece suporte a outros protocolos e clientes de e-mail. A Proteção Contra Ameaças ao Correio pode nem sempre ser capaz de obter acesso a mensagens no *nível de protocolo* (por exemplo, ao usar a solução Microsoft Exchange). Por essa razão, a Proteção Contra Ameaças ao Correio inclui uma extensão para Microsoft Office Outlook. A extensão permite verificar mensagens no *nível do cliente de e-mail*. A extensão Proteção Contra Ameaças ao Correio é compatível com as versões de 32 e 64 bits do Outlook 2010, 2013, 2016, 2019, 2021, 2024 e 365. Em computadores baseados em Arm, a extensão Proteção Contra Ameaças ao Correio é compatível com as versões de 32 e 64 bits do Outlook 2016, Outlook 2021, Outlook 2024 e Outlook 365 para Arm64. **Proteção Contra Ameaças à Rede** O componente *Proteção Contra Ameaças à Rede* (também chamado de Intrusion Detection System, IDS) monitora o tráfego de rede de entrada em busca de atividades com características de ataques de rede. Quando o aplicativo detecta uma tentativa de ataque de rede no computador do usuário, ele bloqueia a conexão de rede com o computador atacante. 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. **Firewall** O componente Firewall bloqueia conexões não autorizadas ao computador enquanto conectado na Internet ou na rede local. O Firewall também controla a atividade de rede dos aplicativos no computador. Isso permite proteger sua LAN contra roubo de identidade e outros ataques. O componente fornece proteção ao computador com a ajuda de bancos de dados antivírus, o serviço na nuvem da Kaspersky Security Network e *regras de rede* predefinidas. **Prevenção contra ataque BadUSB** O componente Prevenção contra ataque BadUSB previne dispositivos de USB infectados que emulam um teclado de unir-se ao computador. **Proteção AMSI** O componente de Proteção AMSI 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 Endpoint Security para uma verificação adicional e receber os resultados da verificação desses objetos.

Seção	Componente
Proteção Avançada Contra Ameaças	**Kaspersky Security Network** *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 Endpoint Security a novas ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos positivos. Caso participe da Kaspersky Security Network, os serviços da KSN fornecem à Kaspersky Endpoint Security informações sobre a reputação dos endereços da Web verificados, além de informações sobre a categoria e a reputação dos arquivos verificados. **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 Endpoint Security executará a ação de resposta selecionada. A funcionalidade do Kaspersky Endpoint Security com base em padrões de atividades perigosas fornece defesa proativa ao computador. O componente Detecção de Comportamento também monitora as portas de rede quanto aos processos de aplicativos que possam ameaçar a segurança do computador. O aplicativo obtém informações sobre esses processos em bancos de dados de antivírus. **Anticryptor** O componente Anticryptor analisa a atividade em pastas compartilhadas. Se esta atividade combinar com uma assinatura de fluxo de comportamento que é típica para a criptografia externa, o Kaspersky Endpoint Security executa a ação selecionada. **Prevenção de 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, os exploits podem utilizar um ataque de estouro de buffer. Para isso, o exploit envia uma grande quantidade de dados para um aplicativo vulnerável. Ao processar esses dados, o aplicativo vulnerável executa um código malicioso. Como resultado desse ataque, o exploit pode iniciar uma instalação não autorizada de malware. Quando há uma tentativa de executar um arquivo executável de um aplicativo vulnerável que não foi realizada pelo usuário, o Kaspersky Endpoint Security bloqueia a execução do arquivo ou notifica o usuário. O componente Prevenção de Exploits também monitora as portas de rede quanto a processos de aplicativos que possam ameaçar a segurança do computador. O aplicativo obtém informações sobre esses processos em bancos de dados de antivírus. **Prevenção de Intrusão do Host** O componente Prevenção de Intrusão do Host impede que os aplicativos executem ações perigosas para o sistema, e garante o controle de acesso aos recursos do sistema operacional e aos dados pessoais. O componente fornece proteção ao computador com a ajuda de bancos de dados antivírus e o serviço na nuvem Kaspersky Security Network. **Mecanismo de Remediação** O componente Mecanismo de Remediação permite que o Kaspersky Endpoint Security desfaça ações executadas por Malwares no sistema operacional.

Seção	Componente
Controles de segurança	**Controle de aplicativos** O Controle de aplicativos gerencia a inicialização de aplicativos nos computadores dos usuários. Isso permite que você implemente uma política de segurança corporativa ao usar aplicativos. O Controle de aplicativos também reduz o risco de infecção do computador, restringindo o acesso aos 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. **Controle da Web** O Controle da Web gerencia o acesso dos usuários aos recursos da Web. Isso ajuda a reduzir o tráfego e o uso inadequado do tempo de trabalho. Quando um usuário tenta abrir um site restrito pelo Controle da Web, o Kaspersky Endpoint Security bloqueará o acesso ou exibirá um aviso. **Controle Adaptativo de Anomalias** O componente de Controle Adaptativo de Anomalias monitora e bloqueia ações suspeitas que não são típicas dos computadores em uma rede empresarial. O Controle Adaptativo de Anomalias usa um conjunto de regras para rastrear comportamentos incomuns (por exemplo, a regra *Inicialização do Microsoft PowerShell pelo aplicativo Office*). As regras são criadas pelos especialistas da Kaspersky com base em cenários típicos de atividade maliciosa. Você pode configurar como o Controle Adaptativo de Anomalias manipula cada regra e, por exemplo, permitir a execução de scripts do PowerShell que automatizam determinadas tarefas de fluxo de trabalho. Kaspersky Endpoint Security atualiza o conjunto de regras junto com os bancos de dados do aplicativo. **Inspeção de 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. **Monitor de integridade do sistema** 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 Endpoint Security gera os eventos correspondentes e alerta o administrador.
Tarefas	**Verificação de malware** O Kaspersky Endpoint Security verifica o computador quanto à presença de vírus e outras ameaças. A Verificação de malware ajuda a descartar a possibilidade de disseminação de malwares que não foram detectados pelos componentes de proteção devido a um baixo nível de segurança, por exemplo. **Atualização de bancos de dados e módulos do aplicativo** O Kaspersky Endpoint Security baixa bancos de dados e módulos do aplicativo atualizados. A atualização mantém o computador protegido contra os últimos vírus e outras ameaças. O aplicativo é atualizado automaticamente por padrão, mas também é possível atualizar os bancos de dados e módulos do aplicativo manualmente se preferir. **Reversão da última atualização** O Kaspersky Endpoint Security reverte a última atualização de bancos de dados e módulos. Isso permite reverter os bancos de dados e os módulos do aplicativo para as versões anteriores quando necessário, por exemplo, quando a nova versão do banco de dados contém uma assinatura inválida que faz com que o Kaspersky Endpoint Security bloqueie um aplicativo seguro. **Verificação de integridade do aplicativo** O Kaspersky Endpoint Security verifica os módulos do aplicativo na pasta de instalação do aplicativo para detectar corrupção ou modificações. Se um módulo do aplicativo tiver uma assinatura digital incorreta, o módulo é considerado corrompido.
Criptografia de dados	**Criptografia em Nível de Arquivo** O componente permite a criação de regras de criptografia de arquivos. É possível selecionar as pastas predefinidas para criptografia, selecionar uma pasta manualmente ou selecionar os arquivos individuais por extensão. **Criptografia completa do disco** O componente permite criptografar o disco rígido usando Kaspersky Disk Encryption ou a Criptografia de Unidade de Disco BitLocker. **Criptografia de unidades removíveis** O componente permite proteger os dados em unidades removíveis. É possível usar criptografia completa do disco (FDE) ou criptografia em nível de arquivo (FLE).

Seção	Componente
Detection and Response	**Endpoint Detection and Response Optimum** Agente integrado para a solução Kaspersky Endpoint Detection and Response Optimum (doravante também "EDR Optimum"). O *Kaspersky Endpoint Detection and Response* é uma solução para proteger a infraestrutura corporativa de TI contra ameaças cibernéticas avançadas. A funcionalidade da solução combina a detecção automática de ameaças com a capacidade de reagir a essas ameaças para neutralizar ataques avançados, incluindo novos exploits, ransomwares, ataques sem arquivo, bem como métodos que usam ferramentas de sistema legítimas. Para obter mais informações sobre a solução, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum. **Endpoint Detection and Response Expert** Agente integrado da solução Kaspersky Endpoint Detection and Response Expert (doravante também "EDR Expert"). O EDR Expert oferece mais monitoramento de ameaças e funcionalidade de resposta do que o EDR Optimum. Para obter mais informações sobre a solução, consulte a Ajuda do Kaspersky Endpoint Detection and Response Expert. **Endpoint Detection and Response Expert (on-premises)** e **Network Detection and Response (KATA)** Agentes integrados para gerenciar os componentes Endpoint Detection and Response e o Network Detection and Response que fazem parte da solução Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* é uma solução projetada para a detecção oportuna de ameaças sofisticadas, como ataques direcionados, ameaças persistentes avançadas (APT) e ataques de dia zero, entre outros. A Kaspersky Anti Targeted Attack Platform inclui três unidades funcionais: • Kaspersky Anti Targeted Attack Platform (*KATA*) • Kaspersky Endpoint Detection and Response (*EDR (KATA)*) • Network Detection and Response (*NDR (KATA)*) É possível adquirir todas as unidades funcionais ou unidades individuais separadamente. Para obter informações detalhadas sobre a solução, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform. **Sandbox** Agente integrado para Sandbox. O componente *Sandbox* detecta e bloqueia automaticamente ameaças avançadas em computadores. O Sandbox analisa o comportamento do objeto para detectar atividades maliciosas e características de atividades de ataques direcionados à infraestrutura de TI da organização. O Sandbox analisa e verifica objetos em servidores especiais com imagens virtuais implantadas de sistemas operacionais Microsoft Windows (servidores Sandbox). Para obter informações detalhadas sobre a solução, consulte a ajuda do Kaspersky Sandbox e a ajuda da Kaspersky Anti Targeted Attack Platform. **Managed Detection and Response** Agente integrado para compatibilizar a operação da solução Kaspersky Managed Detection and Response. A solução *Kaspersky Managed Detection and Response (MDR)* detecta e analisa automaticamente os incidentes de segurança em sua infraestrutura. Para isso, o MDR usa dados de telemetria recebidos de terminais 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.

Modos do aplicativo: Standard, EDR Agent, Light Agent

O Kaspersky Endpoint Security for Windows faz parte de muitas soluções da Kaspersky. Dependendo da solução, é necessário selecionar um modo para o aplicativo.

Modo Standard

Esse é o modo principal e padrão do aplicativo. É possível instalar o aplicativo nesse modo como parte das soluções do Kaspersky EPP (Endpoint Protection Platform). Por exemplo, o Kaspersky Endpoint Security no modo Standard faz parte do Kaspersky Endpoint Security for Business. O Kaspersky Endpoint Security fornece proteção abrangente de estações de trabalho e servidores contra várias ameaças, ataques de rede e golpes. No modo Standard, os agentes integrados também estão disponíveis para integração com as soluções Kaspersky Detection and Response, incluindo EDR, MDR, KUMA e outros.

EDR Agent

Esse modo permite implementar as soluções do Kaspersky Detection and Response com soluções EPP de terceiros. As soluções de Detection and Response incluem o Kaspersky Managed Detection and Response (MDR) e a Kaspersky Anti Targeted Attack Platform (KATA). O EDR Agent também é compatível com a solução Kaspersky SIEM e a Kaspersky Unified Monitoring and Analysis Platform (KUMA).

Nesse modo, os componentes de proteção padrão, como a Proteção Contra Ameaças ao Arquivo ou a Proteção Contra Ameaças da Web, não estão disponíveis. A proteção padrão do computador é fornecida pela solução EPP de terceiros. O EDR Agent monitora continuamente os processos em execução nesses computadores, conexões de rede abertas e arquivos sendo modificados, além de interagir com as soluções de Detection and Response.

Light Agent

Esse modo é usado para proteger ambientes virtuais. O Kaspersky Endpoint Security no modo Light Agent faz parte da solução Kaspersky Hybrid Cloud Security. O Light Agent protege máquinas virtuais com sistemas operacionais convidados para estações de trabalho e servidores. Os mesmos componentes de proteção e controle estão disponíveis nesse modo e no modo Standard. A diferença é que os objetos são verificados quanto a vírus e outros malwares por um componente de solução especial instalado em uma máquina virtual separada, SVM (Secure Virtual Machine). Assim, o Light Agent usa os recursos do SVM para garantir a segurança da infraestrutura em vez dos recursos da máquina virtual.

Kit de distribuição

O kit de distribuição inclui os seguintes pacotes de distribuição:

- **AES256**

  Esse pacote de distribuição se destina à instalação em computadores com arquitetura x86/x64. Esse pacote de distribuição contém ferramentas criptográficas que implementam o algoritmo de criptografia AES (Advanced Encryption Standard), com um comprimento de chave efetivo de 256 bits.

- **AES56**

  Esse pacote de distribuição se destina à instalação em computadores com arquitetura x86/x64. Esse pacote de distribuição contém ferramentas criptográficas que implementam o algoritmo de criptografia AES, com um comprimento de chave efetivo de 56 bits.

- **Arm64**

  Este pacote de distribuição está destinado à instalação em computadores baseados em Arm. Esse pacote de distribuição não se destina à instalação em servidores.

Antes da instalação, verifique e confirme se o pacote de distribuição corresponde à arquitetura de seu processador. Se o pacote de distribuição não corresponder à arquitetura do processador, o instalador encerrará a instalação com um erro.

O pacote de distribuição é um arquivo compactado de extração automática no formato EXE. Para visualizar o conteúdo do pacote de distribuição, é necessário extrair o arquivo compactado para uma pasta separada. Cada pacote de distribuição contém os seguintes arquivos:

`kes_win.msi`	Pacote de instalação do Kaspersky Endpoint Security.
`setup_kes.exe`	Os arquivos necessários para a instalação do aplicativo usando diversos métodos disponíveis.
`kes_win.kud`	Arquivo para criar pacotes de instalação do Kaspersky Endpoint Security.
`klcfginst.msi`	Pacote de instalação do plug-in de gerenciamento de aplicativos no Console de Administração do Kaspersky Security Center.
`bases.cab`	Arquivos de pacote de atualização que são usados durante a instalação.
`cleaner_v2.cab` `cleanerapi_v2.cab`	Arquivos para remover o software incompatível.
`incompatible.txt`	Arquivo que contém a lista de softwares que podem causar problemas de compatibilidade com o Kaspersky Endpoint Security. A Kaspersky não garante a compatibilidade do Kaspersky Endpoint Security com o software da lista.
`ksn_<language ID>.txt`	Arquivo onde é possível ler os termos de participação na Kaspersky Security Network.
`license.txt`	Arquivo onde é possível ler o Contrato de Licença do Usuário Final e a Política de Privacidade.
`installer.ini`	Arquivo que contém as configurações internas do kit de distribuição.
`kes.cab`	Arquivos para a interface gráfica do aplicativo.
`aes256.cab` / `aes56.cab`	Arquivos para o algoritmo criptográfico AES (não incluídos no pacote de distribuição Arm64).
`package.kcat`	Arquivo com assinaturas do kit de distribuição do aplicativo. A assinatura digital garante a autenticidade e integridade do kit de distribuição do aplicativo.

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

Requisitos de hardware e software

Este artigo lista as versões de software nas quais o aplicativo foi testado e para as quais seu funcionamento correto é garantido. O aplicativo também pode funcionar com outras versões de software, mas essas configurações não passaram por um ciclo de testes completo e não estão incluídas na lista de versões com suporte garantido.

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

Para instalar o aplicativo, é necessário ter direitos administrativos no computador.

Requisitos gerais mínimos

Requisitos mínimos	Estação de trabalho (x86/x64)	Servidor (x86/x64)	Arm
Armazenamento	2 GB	2 GB	2 GB
CPU	1 GHz, com suporte a instruções SSE2	1,4 GHz, com suporte a instruções SSE2	1 GHz, arquitetura Armv8.1
RAM	Estação de trabalho (x86): 1 GB Estação de trabalho (x64): 2 GB	2 GB Nota: o servidor requer 8 GB de memória para instalar o aplicativo com o agente integrado para o Kaspersky Anti Targeted Attack Platform.	4 GB
Microsoft .NET Framework	4 ou posterior	4 ou posterior	4,8 ou posterior

Estações de trabalho

Sistemas operacionais para estações de trabalho com suporte:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multisessão
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multisessão
- Windows 11 for Arm64 Home / Pro / Pro for Workstations / Education / Enterprise

Os sistemas operacionais Windows, a partir da versão 11 24H2, são compatíveis com a tecnologia UDP Receive Segment Coalescing Offload (URO). A tecnologia é ativada por padrão se uma placa de rede e drivers compatíveis estiverem instalados no computador. Desativar o URO no computador de um usuário pode reduzir significativamente o desempenho do aplicativo.

Para o funcionamento correto do Kaspersky Endpoint Security, o serviço Windows Security Center (wscsvc) deve estar em execução no computador do usuário.

O Kaspersky Endpoint Security não pode ser instalado no Microsoft Windows 7 sem que as atualizações do sistema operacional estejam instaladas: KB4490628 (12 de março de 2019) e KB4474419 (23 de setembro de 2019). Para obter informações detalhadas, consulte a Base de Conhecimento do Suporte Técnico.

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

Para obter detalhes sobre o suporte do sistema operacional Microsoft Windows 11, consulte a Base de Conhecimento do Suporte Técnico.

Servidores

O Kaspersky Endpoint Security é compatível com os componentes principais do aplicativo em computadores que executam o sistema operacional Windows para servidores. É possível usar o Kaspersky Endpoint Security for Windows em vez do Kaspersky Security for Windows Server nos servidores e clusters da sua organização (Cluster Mode). O aplicativo também é compatível com o Server Core Mode (consulte os problemas conhecidos).

Suporte aos sistemas operacionais para servidores:

- Windows Small Business Server 2011 Essentials / Standard (64 bits);

  O Microsoft Small Business Server 2011 Standard (64 bits) é compatível apenas se o Service Pack 1 para Microsoft Windows Server 2008 R2 estiver instalado

- Windows MultiPoint Server 2011 (64 bits);
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1
- Windows Web Server 2008 R2 Service Pack 1
- Windows Server 2012 / Essentials / Standard / Datacenter (incluindo o modo Server Core)
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (incluindo o modo Server Core)
- Windows Server 2016 Essentials / Standard / Datacenter (incluindo o modo Server Core)
- Windows Server 2019 Essentials / Standard / Datacenter (incluindo o modo Server Core)

- Windows Server 2022 Standard / Datacenter / Datacenter Azure Edition (incluindo o modo Server Core)
- Windows Server 2025 Standard / Datacenter

O Kaspersky Endpoint Security não pode ser instalado no Microsoft Windows Server 2008 R2 sem que as atualizações do sistema operacional estejam instaladas: KB4490628 (12 de março de 2019) e KB4474419 (23 de setembro de 2019).

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

Para obter detalhes sobre o suporte do sistema operacional Microsoft Windows Server 2022, consulte a Base de Conhecimento do Suporte Técnico.

Sistemas operacionais incompatíveis para servidores:

- Windows Server 2003 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Core Standard / Enterprise / Datacenter Service Pack 2
- Microsoft Small Business Server 2008 Standard / Premium Service Pack 2

Plataformas virtuais

Plataformas virtuais compatíveis com a operação do aplicativo no modo padrão:

- Estações de trabalho VMware Pro 15.5.2;
- VMware ESXi 7.0 Patch Release ESXi 7.0b
- Windows Hyper-V Server 2019
- Citrix Virtual Apps and Desktops 7 2009;
- Citrix Provisioning 2009;
- Citrix Hypervisor 8.2 LTSR

O aplicativo é compatível com máquinas virtuais, criadas usando o Hyper-V, que executam o Windows 11 Pro Arm64.

Máquinas virtuais para instalação do Light Agent

A instalação do Kaspersky Endpoint Security no Modo Light Agent em máquinas virtuais baseadas em Arm não é compatível.

O BIOS das máquinas virtuais deve ser compatível com a especificação SMBIOS versão 2.1 ou superior.

Os seguintes pacotes e utilitários devem estar instalados nas máquinas virtuais:

- Ao usar o Microsoft Hyper-V – pacote Integration Services.
- Ao usar o VMware vSphere – pacote VMware Tools.
- Ao usar o XenServer – pacote XenTools.
- Ao usar o HUAWEI FusionSphere – pacote HUAWEI Tools.
- Ao usar hipervisores baseados em KVM – QEMU Guest Agent.

Consulte os requisitos virtuais de infraestrutura na seção ajuda do Kaspersky Security for Virtualization Light Agent para executar o aplicativo no modo Light Agent.

Para o funcionamento correto do aplicativo, utilize uma interface de rede virtualizada com largura de banda de pelo menos 100 Mbit/s.

Servidores de terminal

Tipos de servidores de terminal compatíveis:

- Microsoft Remote Desktop Services para Windows Server 2008 R2 SP1;
- Microsoft Remote Desktop Services com base no Windows Server 2012.
- Microsoft Remote Desktop Services para Windows Server 2012 R2;
- Microsoft Remote Desktop Services com base no Windows Server 2016.
- Microsoft Remote Desktop Services com base no Windows Server 2019.
- Microsoft Remote Desktop Services com base no Windows Server 2022.
- Microsoft Remote Desktop Services com base no Windows Server 2025.
- Citrix RDSH do Citrix Virtual Apps and Desktops 7 2507 LTSR

Suporte ao Kaspersky Security Center

O Kaspersky Endpoint Security tem suporte à operação com as seguintes versões do Kaspersky Security Center:

- Kaspersky Security Center 14.2
- Kaspersky Security Center Linux 14.2
- Kaspersky Security Center Linux 15
- Kaspersky Security Center Windows 15.1
- Kaspersky Security Center Linux 15.1
- Kaspersky Security Center Linux 15.2
- Kaspersky Security Center Linux 15.3
- Kaspersky Security Center Linux 15.4
- Kaspersky Security Center Linux 16
- Kaspersky Security Center Linux 16.1
- Kaspersky Security Center Linux 16.2
- Kaspersky Security Center Linux 16.3
- Kaspersky Security Center Linux 17

Comparação de recursos de aplicativo disponíveis dependendo do tipo de sistema operacional

O conjunto de recursos disponíveis do Kaspersky Endpoint Security depende do tipo do sistema operacional: estação de trabalho ou servidor (veja a tabela a seguir).

A partir do Kaspersky Endpoint Security12.8 for Windows, é possível configurar diferentes conjuntos de componentes para diferentes tipos de sistema operacional no pacote de instalação. Ou seja, é possível implementar o aplicativo em estações de trabalho e servidores usando o mesmo pacote de instalação.

A instalação do Kaspersky Endpoint Security no Modo Light Agent em máquinas virtuais baseadas em Arm não é compatível.

Comparação de recursos do Kaspersky Endpoint Security

Recurso	Estação de trabalho	Estação de trabalho baseada em Arm	Servidor	Modo Server Core
Proteção Avançada Contra Ameaças				
Kaspersky Security Network	✓	✓	✓	✓

Recurso	Estação de trabalho	Estação de trabalho baseada em Arm	Servidor	Modo Server Core
Detecção de Comportamento	✓	✓	✓	✓
Anticryptor	✓	✓	✓	✓
Prevenção de Exploits	✓	✓	✓	✓
Prevenção de Intrusão do Host	✓	✓	–	–
Mecanismo de Remediação	✓	✓	✓	✓
Proteção Essencial Contra Ameaças				
Proteção Contra Ameaças ao Arquivo	✓	✓	✓	✓
Proteção Contra Ameaças da Web	✓	✓	✓	–
Proteção Contra Ameaças ao Correio	✓	✓	✓	–
Firewall	✓	✓	✓	✓
Proteção Contra Ameaças à Rede	✓	✓	✓	✓
Prevenção contra ataque BadUSB	✓	✓	✓	–
Proteção AMSI	✓	✓	✓	✓
Controles de Segurança				
Inspeção de log	–	–	✓	–
Controle de aplicativos	✓	✓	✓	✓
Controle de dispositivos	✓	✓	✓	✓
Controle da Web	✓	✓	✓	–
Controle Adaptativo de Anomalias	✓	✓	–	–
Monitor de integridade do sistema	–	–	✓	–
Cloud Discovery	✓	✓	–	–
Criptografia de dados				
Kaspersky Disk Encryption	✓	–	–	–
Criptografia de unidade de disco BitLocker	✓	✓	✓	✓
Criptografia em Nível de Arquivo	✓	–	–	–
Criptografia de unidades removíveis	✓	–	–	–
Detection and Response				
Endpoint Detection and Response Optimum	✓	✓	✓	✓
Endpoint Detection and Response Expert (cloud)	✓	✓	✓	✓
Endpoint Detection and Response (KATA)	✓	✓	✓	✓
Network Detection and Response (KATA)	✓	✓	✓	✓
Sandbox	✓	✓	✓	✓
Managed Detection and Response (MDR)	✓	✓	✓	✓
Integração KUMA	✓	✓	✓	✓

Comparação de funções de aplicativo, dependendo das ferramentas de gerenciamento

O conjunto de funções disponíveis no Kaspersky Endpoint Security depende das ferramentas de gerenciamento (consulte a tabela abaixo).

É possível gerenciar o aplicativo usando os seguintes consoles do Kaspersky Security Center:

- Console de Administração. Snap-in do Console de Gerenciamento Microsoft (MMC) instalado na estação de trabalho do administrador.

- Web Console. Componente do Kaspersky Security Center que está instalado no Servidor de Administração. Você pode trabalhar no Web Console usando um navegador em qualquer computador.

Você pode gerenciar o aplicativo usando o Kaspersky Security Center Cloud Console. O *Console na nuvem do Kaspersky Security Center* é a versão na nuvem do Kaspersky Security Center. Isso significa que o Servidor de Administração e outros componentes do Kaspersky Security Center estão instalados na infraestrutura na nuvem do Kaspersky. Para obter informações detalhadas sobre o gerenciamento do aplicativo por meio do Kaspersky Security Center Cloud Console, consulte a Ajuda do Kaspersky Security Center Cloud Console.

O Kaspersky Endpoint Security faz parte da solução Kaspersky Next Pro View. Para obter mais informações sobre os recursos do aplicativo disponíveis quando ele funciona como parte desta solução, consulte a Ajuda do Kaspersky Next.

Comparação de recursos do Kaspersky Endpoint Security

Recurso	Kaspersky Security Center		Kaspersky Security Center
	Console de administração	Web Console	Console na nuvem
Proteção Avançada Contra Ameaças			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Detecção de Comportamento	✓	✓	✓
Anticryptor			
Prevenção de Exploits	✓	✓	✓
Prevenção de Intrusão do Host	✓	✓	✓
Mecanismo de Remediação	✓	✓	✓
Proteção Essencial Contra Ameaças			
Proteção Contra Ameaças ao Arquivo	✓	✓	✓
Proteção Contra Ameaças da Web	✓	✓	✓
Proteção Contra Ameaças ao Correio	✓	✓	✓
Firewall	✓	✓	✓
Proteção Contra Ameaças à Rede	✓	✓	✓
Prevenção contra ataque BadUSB	✓	✓	✓
Proteção AMSI	✓	✓	✓
Controles de Segurança			
Inspeção de log	✓	✓	✓
Controle de aplicativos	✓	✓	✓
Controle de dispositivos	✓	✓	✓
Controle da Web	✓	✓	✓
Controle Adaptativo de Anomalias	✓	✓	✓
Monitor de integridade do sistema	✓	✓	✓
Cloud Discovery	–	–	✓

Recurso	Kaspersky Security Center		Kaspersky Security Center
	Console de administração	Web Console	Console na nuvem
Criptografia de dados			
Kaspersky Disk Encryption	✓	✓	–
Criptografia de unidade de disco BitLocker	✓	✓	✓
Criptografia em Nível de Arquivo	✓	✓	–
Criptografia de unidades removíveis	✓	✓	–
Detection and Response			
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert (cloud)	–	–	✓
Endpoint Detection and Response (KATA)	✓	✓	–
Network Detection and Response (KATA)	✓	✓	–
Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
Integração KUMA	✓	✓	✓
Tarefas			
Adicionar chave	✓	✓	✓
Alterar componentes do aplicativo	✓	✓	✓
Inventário	✓	✓	✓
Atualização	✓	✓	✓
Reversão de atualização	✓	✓	✓
Verificação de malware	✓	✓	✓
Verificação de integridade do aplicativo	✓	✓	–
Limpar dados	✓	✓	✓
Gerenciar contas do Agente de Autenticação (Kaspersky Disk Encryption)	✓	✓	–
Verificação de IOC (EDR)	–	✓	✓
Mover arquivo para a Quarentena (EDR)	–	✓	✓
Obter o arquivo (EDR)	–	✓	✓
Excluir arquivo (EDR)	–	✓	✓
Iniciar processo (EDR)	–	✓	✓
Encerrar processo (EDR)	–	✓	✓

Compatibilidade com outros aplicativos

O Kaspersky Endpoint Security é incompatível com alguns aplicativos da Kaspersky e com alguns aplicativos de terceiros. Portanto, antes de instalar, atualizar a versão do aplicativo e alterar os componentes do aplicativo, o Kaspersky Endpoint Security verificará o computador para confirmar se algum desses aplicativos está presente.

Compatibilidade com aplicativos de terceiros

O Kaspersky Endpoint Security é incompatível com aplicativos que fazem parte de sistemas de proteção de endpoints de terceiros (Endpoint Protection Platform, EPP). O Kaspersky Endpoint Security também pode ter problemas de compatibilidade com outros aplicativos. Para determinar a compatibilidade, o Kaspersky Endpoint 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.

A Kaspersky não garante a compatibilidade do Kaspersky Endpoint Security com o software da lista. Caso um aplicativo da lista seja descoberto, o instalador interromperá a implementação do Kaspersky Endpoint Security. O instalador pode excluir automaticamente alguns aplicativos da lista. Caso esteja disposto a desconsiderar os riscos e caso queira instalar o Kaspersky Endpoint Security com um software da lista no mesmo computador, será possível ignorar a verificação do computador (consulte as instruções abaixo).

DOWNLOAD DO ARQUIVO INCOMPATIBLE.TXT

Compatibilidade com aplicativos da Kaspersky

O Kaspersky Endpoint Security é incompatível com os seguintes aplicativos da Kaspersky:

- Kaspersky Standard | Plus | Premium.
- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Endpoint Sensor como parte das soluções Kaspersky Anti Targeted Attack Platform e Kaspersky Endpoint Detection and Response.
- Kaspersky Endpoint Agent como parte das soluções de Detection and Response da Kaspersky.

  A Kaspersky está mudando toda a Detection and Response para trabalhar com o agente integrado do Kaspersky Endpoint Security em vez do Kaspersky Endpoint Agent. A partir da versão 12.1, o aplicativo é compatível com todas as soluções de Detection and Response.

- Kaspersky Security for Virtualization Light Agent.
- Kaspersky Fraud Prevention for Endpoint.

- Kaspersky Security for Windows Server

  Desde o Kaspersky Endpoint Security 12.0, é possível migrar do Kaspersky Security for Windows Server para o Kaspersky Endpoint Security for Windows e usar a mesma solução para a proteção de estações de trabalho e servidores.

- Kaspersky Embedded Systems Security.

Se os aplicativos da Kaspersky dessa lista estiverem instalados no computador, o Kaspersky Endpoint Security os removerá. Aguarde a conclusão desse processo antes de continuar com a instalação do Kaspersky Endpoint Security.

Exclusão da verificação de software que pode causar problemas de compatibilidade

Caso o Kaspersky Endpoint Security detecte um software da lista incompatible.txt, a instalação do aplicativo será encerrada. Para continuar a instalação, é necessário remover esse aplicativo. No entanto, caso o fornecedor do software de terceiros tenha indicado na sua documentação que o software é compatível com a Endpoint Protection Platform (EPP), será possível instalar o Kaspersky Endpoint Security em um computador que contenha um aplicativo desse fornecedor. Por exemplo, o provedor de soluções do Endpoint Detection and Response (EDR) pode declarar a compatibilidade com sistemas EPP de terceiros. Se esse for o caso, é preciso iniciar a instalação do Kaspersky Endpoint Security sem executar uma verificação de software instalado. Para isso, forneça os seguintes parâmetros para o instalador:

- `SKIPPRODUCTCHECK=1` Desative a verificação de software instalado. A lista de softwares que podem causar problemas de compatibilidade está disponível no arquivo incompatible.txt do kit de distribuição. Se nenhum valor for definido para este parâmetro e um software da lista for detectado, a instalação do Kaspersky Endpoint Security será interrompida.

- `SKIPPRODUCTUNINSTALL=1` Desative a remoção automática do software detectado da lista incompatible.txt. Se nenhum valor for definido para este parâmetro, o Kaspersky Endpoint Security tentará remover o software que pode causar problemas de compatibilidade.

- `CLEANERSIGNCHECK=0` Desative a verificação de assinatura digital de aplicativos encontrados pela verificação. Caso o parâmetro não seja definido, a verificação de assinaturas digitais será desativada com a implantação do aplicativo por meio do Kaspersky Security Center. Quando o aplicativo é instalado localmente, a verificação de assinatura digital é ativada por padrão.

É possível fornecer os parâmetros na linha de comando quando estiver instalando o aplicativo localmente.

Se durante o processo de instalação você pulou a verificação de componentes de software que podem causar problemas de compatibilidade, o Kaspersky Endpoint Security pode realizar essa verificação novamente quando os componentes do aplicativo forem alterados. Para ignorar a verificação do software instalado, é necessário configurar a tarefa *Alterar componentes do aplicativo*.

Exemplo:
```
C:\KES\setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0 /s
```

Para instalar remotamente o Kaspersky Endpoint Security, é preciso adicionar os parâmetros apropriados ao arquivo de geração do pacote de instalação chamado `kes_win.kud` dentro de `[Setup]` (veja abaixo). O arquivo `kes_win.kud` está incluído no kit de distribuição.

kes_win.kud

```
[Setup]
UseWrapper=1
ExecutableRelPath=EXEC
Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0
Executable=setup_kes.exe
RebootDelegated = 1
RebootAllowed=1
ConfigFile=installer.ini
RelPathsToExclude=klcfginst.msi
```

Instalar e remover o aplicativo

O Kaspersky Endpoint Security pode ser instalado em um computador de vários modos:

- localmente, usando o Assistente de configuração.
- localmente a partir da linha de comando.
- Uso remoto do Kaspersky Security Center.
- remotamente, por meio do Editor de Gerenciamento de Política de Grupo do Microsoft Windows (para obter mais detalhes, consulte o site do Suporte Técnico da Microsoft).
- remotamente, usando o System Center Configuration Manager.

Você pode definir as configurações do aplicativo de várias maneiras. Se você usar simultaneamente vários métodos para definir as configurações, o Kaspersky Endpoint Security aplicará as configurações com a prioridade mais alta. O Kaspersky Endpoint Security usa a seguinte ordem de prioridades:

1. Configurações recebidas do arquivo setup.ini.
2. Configurações recebidas do arquivo installer.ini.
3. Configurações recebidas da linha de comando.
4. Configurações recebidas do arquivo de configuração (install.cfg).

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

Ao instalar o Kaspersky Endpoint Security, o sistema operacional poderá exibir suas próprias mensagens. As conexões de rede e de Internet também podem ser interrompidas durante a instalação do aplicativo.

Ao instalar, atualizar ou desinstalar o Kaspersky Endpoint Security, podem ocorrer erros. Para obter mais informações sobre como solucionar esses erros, consulte a Base de Conhecimento do Suporte Técnico.

Implementação por meio do Kaspersky Security Center

O Kaspersky Endpoint Security pode ser implementado em computadores dentro de uma rede corporativa de vários modos. Você pode selecionar o cenário de implementação mais conveniente para a sua organização ou combinar vários cenários de implementação ao mesmo tempo. Antes de instalar o aplicativo, é necessário certificar-se de que o Agente de Rede do Kaspersky Security Center esteja instalado no computador. O *Agente de Rede* facilita a interação entre o Servidor de Administração e um computador cliente.

O Kaspersky Security Center é compatível com os principais métodos de implementação a seguir:

- Instalação do aplicativo usando o Assistente de Implementação de Proteção.

  O método de instalação padrão é conveniente se você estiver satisfeito com as configurações padrão do Kaspersky Endpoint Security e se a sua organização tiver uma infraestrutura simples que não exija configurações especiais.

- Instalação do aplicativo usando a tarefa de instalação remota.

  Método de instalação universal, o qual permite definir as configurações do Kaspersky Endpoint Security e gerenciar com flexibilidade tarefas de instalação remota. A instalação do Kaspersky Endpoint Security consiste nas seguintes etapas:

  1. Criar um pacote de instalação.
  2. Criar uma tarefa de instalação remota.

O Kaspersky Security Center também oferece suporte a outros métodos de instalação do Kaspersky Endpoint Security, como a implementação em uma imagem do sistema operacional. Para obter detalhes sobre outros métodos de implementação, consulte a Ajuda do Kaspersky Security Center.

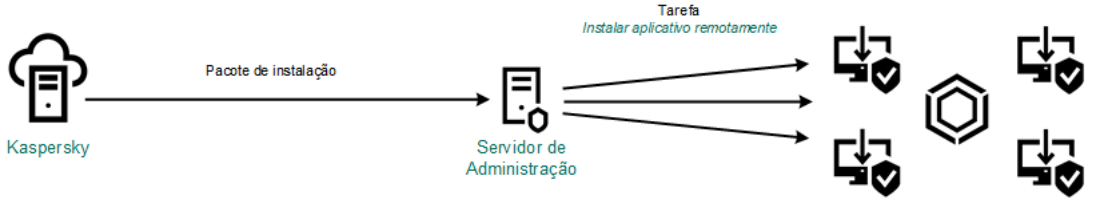
Instalação padrão do aplicativo

O Kaspersky Security Center fornece um Assistente de implementação de proteção para instalar o aplicativo em computadores corporativos. O Assistente de Implementação de Proteção inclui as seguintes ações principais:

1. Seleção do pacote de instalação do Kaspersky Endpoint Security.

   Um *pacote de instalação* é um grupo de arquivos criados para instalação remota de um aplicativo da Kaspersky por meio do Kaspersky Security Center. O pacote de instalação contém várias configurações necessárias para instalar o aplicativo e executá-lo imediatamente após a instalação. O pacote de instalação é criado usando arquivos com as extensões .kpd e .kud incluídas no kit de distribuição do aplicativo. O pacote de instalação do Kaspersky Endpoint Security é comum para todas as versões do Windows que têm suporte e tipos de arquitetura de processador.

2. Criação da tarefa *Instalar o aplicativo remotamente* do Servidor de Administração do Kaspersky Security Center.



Implementação do Kaspersky Endpoint Security

Como executar o Assistente de implantação de proteção no Console de administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Avançado** → **Instalação remota**.
3. Clique no link **Implementar o pacote de instalação nos dispositivos gerenciados (estações de trabalho)**.

O Assistente de Implementação de Proteção será iniciado. Siga as instruções do Assistente.

As portas TCP 139 e 445 e as portas UDP 137 e 138 devem ser abertas em um computador cliente.

Etapa 1. Selecionar um pacote de instalação

Selecione o pacote de instalação do Kaspersky Endpoint Security na lista. Se a lista não tiver o pacote de instalação do Kaspersky Endpoint Security, você poderá criar o pacote clicando no Assistente.

Você pode definir as configurações do pacote de instalação no Kaspersky Security Center. Por exemplo, você pode selecionar os componentes do aplicativo que serão instalados em um computador.

O Agente de rede também será instalado junto com o Kaspersky Endpoint Security. O *Agente de Rede* facilita a interação entre o Servidor de Administração e um computador cliente. Se o Agente de Rede já estiver instalado no computador, ele não será instalado novamente.

Etapa 2. Selecionar a fonte do pacote de instalação

Selecione a fonte **Implementar o pacote do Kaspersky Security Center**.

Etapa 3. Selecionar dispositivos para instalação

Selecione os computadores para instalar o Kaspersky Endpoint Security. 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*. O Agente de Rede não é instalado em dispositivos não atribuídos. Neste caso, a tarefa é atribuída a dispositivos específicos. 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. Definir configurações da tarefa de instalação remota

Defina as seguintes configurações adicionais do aplicativo:

- **Forçar download do pacote de instalação**. Selecione o método de instalação do aplicativo:

  - **Usando o Agente de Rede**. O Agente de Rede é responsável por entregar o pacote de instalação do Kaspersky Endpoint Security aos computadores cliente. Se o Agente de Rede não está instalado, a tarefa terminará com um erro. Nesse caso, adicione o pacote de instalação do Agente de Rede à tarefa *Instalar o aplicativo remotamente* e ative a entrega de arquivos por meio dos recursos do sistema operacional. Em seguida, o Agente de Rede será instalado usando os recursos do sistema operacional. Em seguida, o Kaspersky Endpoint Security será instalado pelas ferramentas do Agente de Rede.

  - **Usando recursos do sistema operacional através de pontos de distribuição**. O pacote de instalação é entregue aos computadores clientes usando recursos do sistema operacional por meio de pontos de distribuição. Você poderá selecionar esta opção se houver pelo menos um ponto de distribuição na rede. Para obter mais detalhes sobre os pontos de distribuição, consulte a ajuda do Kaspersky Security Center.

  - **Usando recursos do sistema operacional através do Servidor de Administração**. Os arquivos serão entregues a computadores clientes usando recursos do sistema operacional por meio do Servidor de Administração. Você pode selecionar esta opção se o Agente de Rede não estiver instalado no computador cliente, mas o computador cliente estiver na mesma rede que o Servidor de Administração.

- **Comportamento para dispositivos gerenciados por meio de outros Servidores de Administração**. Selecione o método de instalação do Kaspersky Endpoint Security. Se a rede tiver mais de um Servidor de Administração instalado, esses Servidores de Administração poderão ver os mesmos computadores clientes. Isso pode fazer com que, por exemplo, um aplicativo seja instalado remotamente no mesmo computador cliente várias vezes por meio de diferentes Servidores de Administração, ou outros conflitos.

- **Não reinstalar o aplicativo se ele já estiver instalado**. Desmarque esta caixa de seleção se você quiser instalar uma versão anterior do aplicativo, por exemplo.

- **Atribuir a instalação do Agente de Rede em políticas de grupo do Active Directory**. Instalação manual do Agente de rede usando os recursos do Active Directory. Para instalar o Agente de Rede, a tarefa de instalação remota deve ser executada com privilégios de administrador de domínio.

Etapa 5. Selecionar uma chave de licença

Adicione uma chave ao pacote de instalação para ativar o aplicativo. Esta etapa é opcional. Se o Servidor de Administração tiver uma chave de licença com a funcionalidade de distribuição, a chave será adicionada automaticamente depois. Também é possível ativar o aplicativo posteriormente com o uso da tarefa *Adicionar chave*.

Etapa 6. Selecionar a configuração de reinicialização do sistema operacional

Selecione a ação a ser executada se for necessário reiniciar o computador. Não é necessário reiniciar ao instalar o Kaspersky Endpoint Security. A reinicialização será necessária apenas se você precisar remover aplicativos incompatíveis antes da instalação. A reinicialização também poderá ser necessária quando a versão do aplicativo for atualizada.

Etapa 7. Remover aplicativos incompatíveis antes de instalar o aplicativo

Leia atentamente a lista de aplicativos incompatíveis e permita a remoção desses aplicativos. Se houver aplicativos incompatíveis instalados no computador, a instalação do Kaspersky Endpoint Security terminará com um erro.

Etapa 8. Selecionar uma conta para acessar dispositivos

Selecione a conta para instalar o Agente de rede usando as ferramentas do sistema operacional. Neste caso, os direitos de administrador são necessários para acessar o computador. Você pode adicionar várias contas. Se uma conta não tiver direitos suficientes, o Assistente de Instalação usará a próxima conta. Se você instalar o Kaspersky Endpoint Security usando as ferramentas do Agente de Rede, não precisará selecionar uma conta.

Etapa 9. Iniciando a instalação

Conclua o 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 iniciar o Assistente de implementação de proteção no Web Console e no Cloud Console

Na janela principal do Web Console, selecione **Descoberta e implementação** → **Implementação e atribuição** → **Assistente de Implementação da Proteção**.

O Assistente de Implementação de Proteção será iniciado. Siga as instruções do Assistente.

> As portas TCP 139 e 445 e as portas UDP 137 e 138 devem ser abertas em um computador cliente.

Etapa 1. Selecionar um pacote de instalação

Selecione o pacote de instalação do Kaspersky Endpoint Security na lista. Se a lista não tiver o pacote de instalação do Kaspersky Endpoint Security, você poderá criar o pacote clicando no Assistente. Para criar o pacote de instalação, você não precisa procurar o pacote de distribuição e salvá-lo na memória do computador. No Kaspersky Security Center, você pode exibir a lista dos pacotes de distribuição que residem nos servidores da Kaspersky, e o pacote de instalação é criado automaticamente. A Kaspersky atualiza a lista após o lançamento de novas versões de aplicativos.

Você pode definir as configurações do pacote de instalação no Kaspersky Security Center. Por exemplo, você pode selecionar os componentes do aplicativo que serão instalados em um computador.

Etapa 2. Selecionar uma chave de licença

Adicione uma chave ao pacote de instalação para ativar o aplicativo. Esta etapa é opcional. Se o Servidor de Administração tiver uma chave de licença com a funcionalidade de distribuição, a chave será adicionada automaticamente depois. Também é possível ativar o aplicativo posteriormente com o uso da tarefa *Adicionar chave*.

Etapa 3. Selecionar um Agente de rede

Selecione a versão do Agente de rede que será instalado em conjunto com o Kaspersky Endpoint Security. O *Agente de Rede* facilita a interação entre o Servidor de Administração e um computador cliente. Se o Agente de Rede já estiver instalado no computador, ele não será instalado novamente.

Etapa 4. Selecionar dispositivos para instalação

Selecione os computadores para instalar o Kaspersky Endpoint Security. 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*. O Agente de Rede não é instalado em dispositivos não atribuídos. Neste caso, a tarefa é atribuída a dispositivos específicos. 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 5. Definir as configurações avançadas

Defina as seguintes configurações adicionais do aplicativo:

- **Forçar download do pacote de instalação**. Selecione o método de instalação do aplicativo:

  - **Usando o Agente de Rede**. O Agente de Rede é responsável por entregar o pacote de instalação do Kaspersky Endpoint Security aos computadores cliente. Se o Agente de Rede não está instalado, a tarefa terminará com um erro. Nesse caso, adicione o pacote de instalação do Agente de Rede à tarefa *Instalar o aplicativo remotamente* e ative a entrega de arquivos por meio dos recursos do sistema operacional. Em seguida, o Agente de Rede será instalado usando os recursos do sistema operacional. Em seguida, o Kaspersky Endpoint Security será instalado pelas ferramentas do Agente de Rede.

  - **Usando recursos do sistema operacional através de pontos de distribuição**. O pacote de instalação é entregue aos computadores clientes usando recursos do sistema operacional por meio de pontos de distribuição. Você poderá selecionar esta opção se houver pelo menos um ponto de distribuição na rede. Para obter mais detalhes sobre os pontos de distribuição, consulte a ajuda do Kaspersky Security Center.

  - **Usando recursos do sistema operacional através do Servidor de Administração**. Os arquivos serão entregues a computadores clientes usando recursos do sistema operacional por meio do Servidor de Administração. Você pode selecionar esta opção se o Agente de Rede não estiver instalado no computador cliente, mas o computador cliente estiver na mesma rede que o Servidor de Administração.

- **Não reinstalar o aplicativo se ele já estiver instalado**. Desmarque esta caixa de seleção se você quiser instalar uma versão anterior do aplicativo, por exemplo.

- **Atribuir a instalação do pacote em políticas de grupo do Active Directory**. O Kaspersky Endpoint Security é instalado por meio do Agente de Rede ou manualmente por meio do Active Directory. Para instalar o Agente de Rede, a tarefa de instalação remota deve ser executada com privilégios de administrador de domínio.

Etapa 6. Selecionar a configuração de reinicialização do sistema operacional

Selecione a ação a ser executada se for necessário reiniciar o computador. Não é necessário reiniciar ao instalar o Kaspersky Endpoint Security. A reinicialização será necessária apenas se você precisar remover aplicativos incompatíveis antes da instalação. A reinicialização também poderá ser necessária quando a versão do aplicativo for atualizada.

Etapa 7. Remover aplicativos incompatíveis antes de instalar o aplicativo

Leia atentamente a lista de aplicativos incompatíveis e permita a remoção desses aplicativos. Se houver aplicativos incompatíveis instalados no computador, a instalação do Kaspersky Endpoint Security terminará com um erro.

Etapa 8. Atribuir a um grupo de administração

Selecione o grupo de administração para o qual os computadores serão movidos após a instalação do Agente de rede. Os computadores precisam ser movidos para um grupo de administração para que políticas e tarefas de grupo possam ser aplicadas. Se um computador já estiver em qualquer grupo de administração, o computador não será movido. Se você não selecionar um grupo de administração, os computadores serão adicionados ao grupo **Dispositivos não atribuídos**.

Etapa 9. Selecionar uma conta para acessar dispositivos

Selecione a conta para instalar o Agente de rede usando as ferramentas do sistema operacional. Neste caso, os direitos de administrador são necessários para acessar o computador. Você pode adicionar várias contas. Se uma conta não tiver direitos suficientes, o Assistente de Instalação usará a próxima conta. Se você instalar o Kaspersky Endpoint Security usando as ferramentas do Agente de Rede, não precisará selecionar uma conta.

Etapa 10. Iniciar instalação

Conclua o 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.

Criar um pacote de instalação

Um *pacote de instalação* é um grupo de arquivos criados para instalação remota de um aplicativo da Kaspersky por meio do Kaspersky Security Center. O pacote de instalação contém várias configurações necessárias para instalar o aplicativo e executá-lo imediatamente após a instalação. O pacote de instalação é criado usando arquivos com as extensões .kpd e .kud incluídas no kit de distribuição do aplicativo. O pacote de instalação do Kaspersky Endpoint Security é comum para todas as versões do Windows que têm suporte e tipos de arquitetura de processador.

Como criar um pacote de instalação no Console de administração (MMC)

1. No Console de Administração, acesse a pasta **Servidor de Administração** → **Avançado** → **Instalação remota** → **Pacotes de instalação**.

   Isso abre uma lista de pacotes de instalação que foram baixados no Kaspersky Security Center.

2. Clique **Criar pacote de instalação**.

O Assistente de novo pacote é iniciado. Siga as instruções do Assistente.

Etapa 1. Selecionar o tipo de pacote de instalação

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

Etapa 2. Definir nome do pacote de instalação

Insira o nome do pacote de instalação, por exemplo, *Kaspersky Endpoint Security for Windows 14.2*.

Etapa 3. Selecionar o pacote de distribuição para instalação

Clique no botão **Procurar** e selecione o arquivo `kes_win.kud` que está incluído no kit de distribuição.

Se necessário, atualize os bancos de dados de antivírus no pacote de instalação usando a caixa de seleção **Copiar atualizações do repositório para o pacote de instalação**.

Etapa 4. Contrato de Licença do Usuário Final e Política de Privacidade

Leia e aceite os termos do Contrato de Licença do Usuário Final e da Política de Privacidade.

O pacote de instalação será criado e adicionado ao Kaspersky Security Center. Usando o pacote de instalação, você pode instalar o Kaspersky Endpoint Security em computadores da rede corporativa ou atualizar a versão do aplicativo.

Nas configurações do pacote de instalação, é possível selecionar componentes do aplicativo para diferentes tipos de sistema operacional. Ou seja, o pacote de instalação inclui dois conjuntos de componentes: para estações de trabalho e servidores. Antes de implementar o pacote de instalação, o instalador detecta o tipo de sistema operacional e instala somente os componentes do aplicativo selecionados para esse tipo de sistema operacional. Dessa forma, pode-se usar o mesmo pacote de instalação para estações de trabalho e servidores.

O pacote de instalação contém bancos de dados de antivírus do Repositório do servidor de administração. Você pode atualizar os bancos de dados no pacote de instalação para reduzir o consumo de tráfego ao atualizar os bancos de dados após a instalação do Kaspersky Endpoint Security.

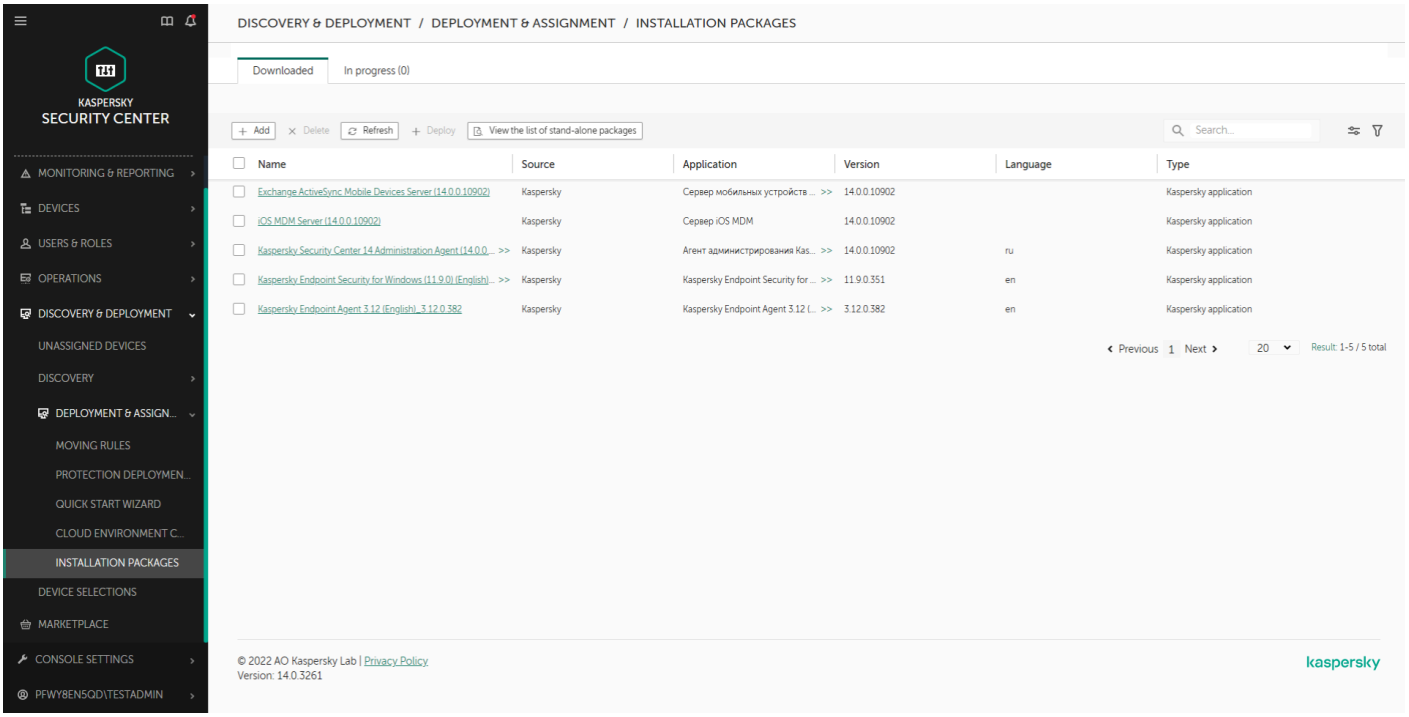
Como criar um pacote de instalação no Web Console

1. Na janela principal do Web Console, selecione **Descoberta e implementação** → **Implementação e atribuição** → **Pacotes de instalação**.

   Isso abre uma lista de pacotes de instalação que foram baixados no Kaspersky Security Center.

2. Clique **Adicionar**.

O Assistente de novo pacote é iniciado. Siga as instruções do Assistente.



Lista de pacotes de instalação

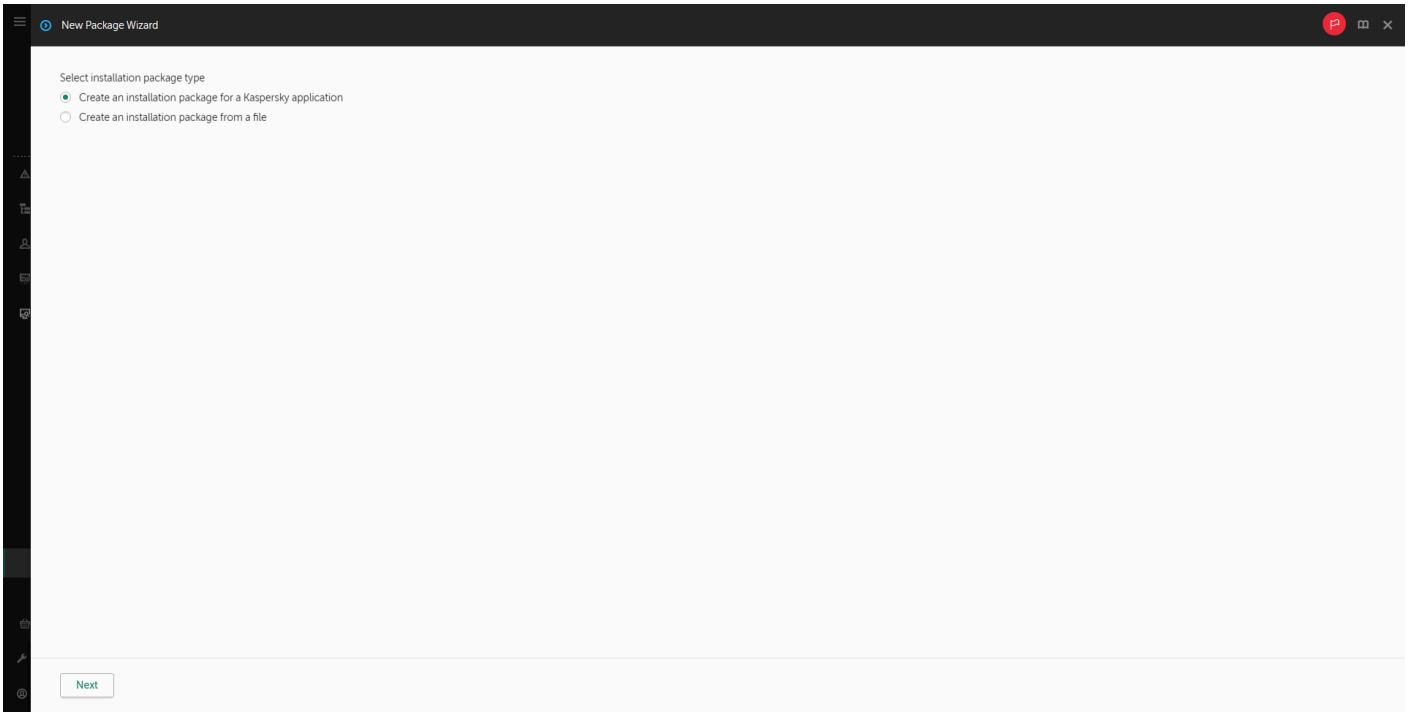
Etapa 1. Selecionar o tipo de pacote de instalação

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

O Assistente criará um pacote de instalação a partir do pacote de distribuição localizado nos servidores da Kaspersky. A lista é atualizada automaticamente conforme novas versões de aplicativos são lançadas. É recomendável selecionar esta opção para a instalação do Kaspersky Endpoint Security.

Você também pode criar um pacote de instalação a partir de um arquivo.

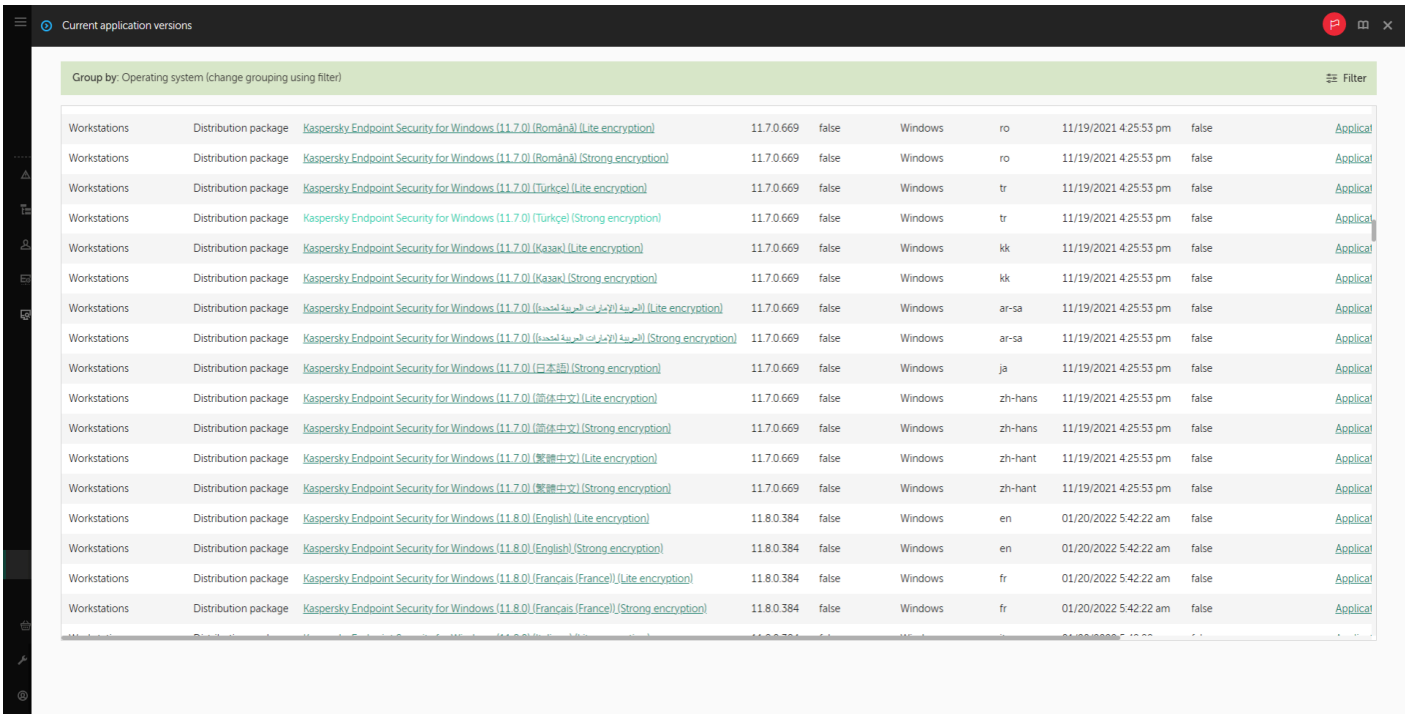
A criação de um pacote de instalação do Kaspersky Endpoint Security a partir de um arquivo só está disponível no Kaspersky Security Center Web Console.



Tipos de pacotes de instalação

Etapa 2. Pacotes de instalação

Selecione o pacote de instalação do Kaspersky Endpoint Security for Windows. O processo de criação do pacote de instalação é iniciado. Durante a criação do pacote de instalação, você deve aceitar os termos do Contrato de Licença do Usuário Final e da Política de Privacidade.



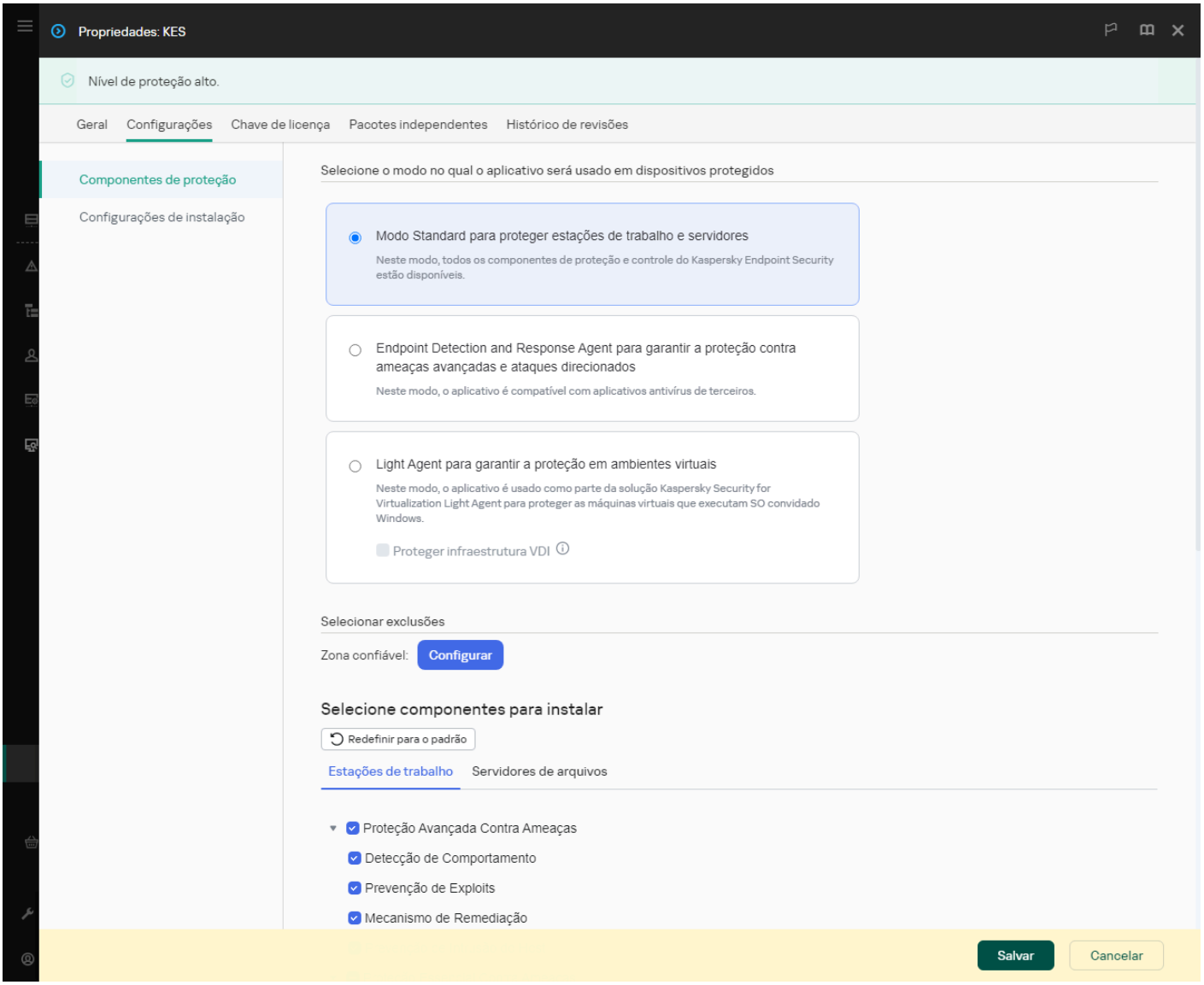
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Română) (Lite encryption)	11.7.0.669	false	Windows	ro	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Română) (Strong encryption)	11.7.0.669	false	Windows	ro	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Türkçe) (Lite encryption)	11.7.0.669	false	Windows	tr	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Türkçe) (Strong encryption)	11.7.0.669	false	Windows	tr	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Казак) (Lite encryption)	11.7.0.669	false	Windows	kk	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Казак) (Strong encryption)	11.7.0.669	false	Windows	kk	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) ((العربية (الإمارات العربية المتحدة)) (Lite encryption)	11.7.0.669	false	Windows	ar-sa	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) ((العربية (الإمارات العربية المتحدة)) (Strong encryption)	11.7.0.669	false	Windows	ar-sa	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (日本語) (Strong encryption)	11.7.0.669	false	Windows	ja	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (简体中文) (Lite encryption)	11.7.0.669	false	Windows	zh-hans	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (简体中文) (Strong encryption)	11.7.0.669	false	Windows	zh-hans	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (繁體中文) (Lite encryption)	11.7.0.669	false	Windows	zh-hant	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (繁體中文) (Strong encryption)	11.7.0.669	false	Windows	zh-hant	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.8.0) (English) (Lite encryption)	11.8.0.384	false	Windows	en	01/20/2022 5:42:22 am	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.8.0) (English) (Strong encryption)	11.8.0.384	false	Windows	en	01/20/2022 5:42:22 am	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.8.0) (Français (France)) (Lite encryption)	11.8.0.384	false	Windows	fr	01/20/2022 5:42:22 am	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.8.0) (Français (France)) (Strong encryption)	11.8.0.384	false	Windows	fr	01/20/2022 5:42:22 am	false	Applicat

Lista de pacotes de instalação em servidores da Kaspersky

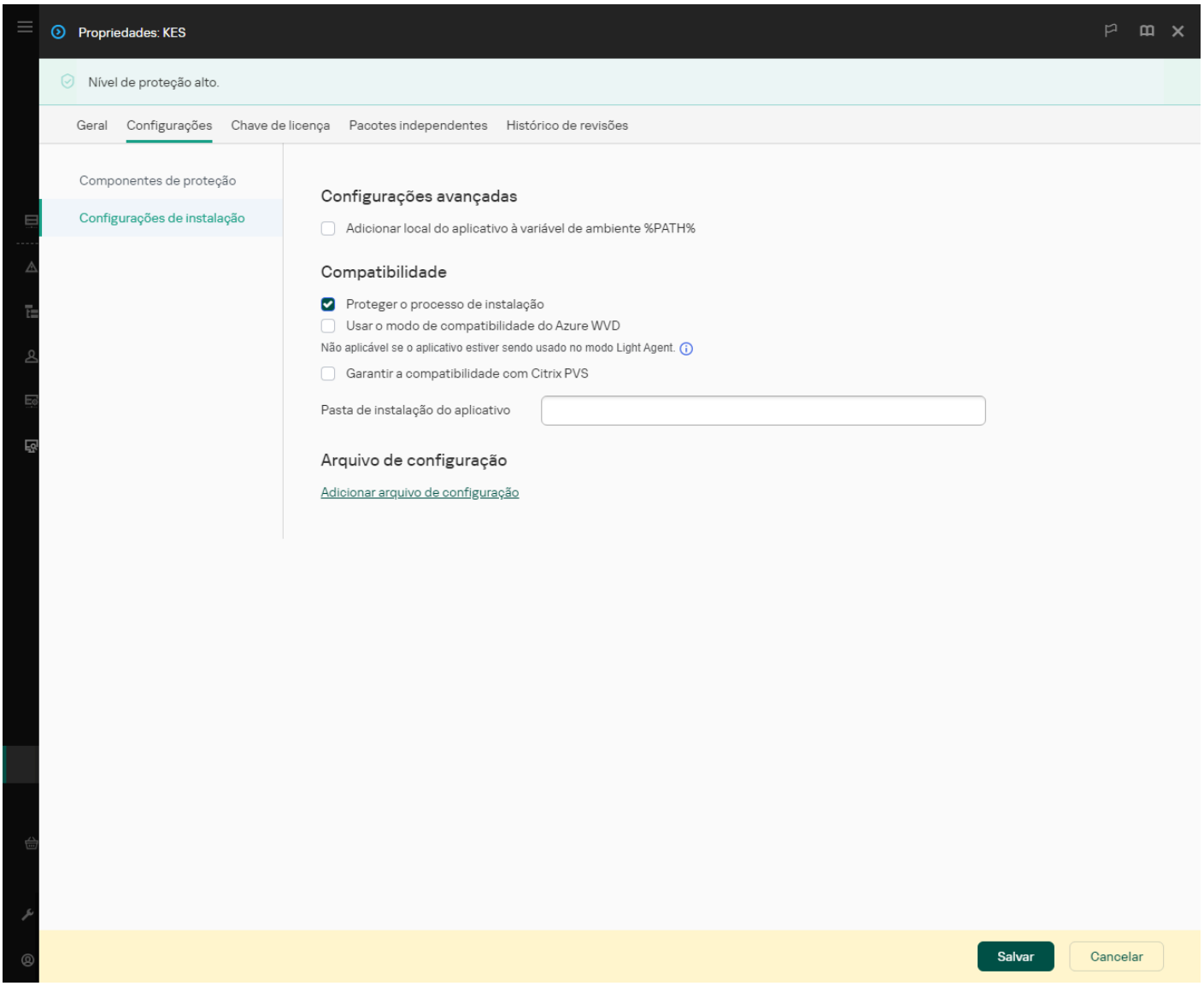
O pacote de instalação será criado e adicionado ao Kaspersky Security Center. Usando o pacote de instalação, você pode instalar o Kaspersky Endpoint Security em computadores da rede corporativa ou atualizar a versão do aplicativo.

Nas configurações do pacote de instalação, é possível selecionar componentes do aplicativo para diferentes tipos de sistema operacional. Ou seja, o pacote de instalação inclui dois conjuntos de componentes: para estações de trabalho e servidores. Antes de implementar o pacote de instalação, o instalador detecta o tipo de sistema operacional e instala somente os componentes do aplicativo selecionados para esse tipo de sistema operacional. Dessa forma, pode-se usar o mesmo pacote de instalação para estações de trabalho e servidores.

O pacote de instalação contém bancos de dados de antivírus do Repositório do servidor de administração. Você pode atualizar os bancos de dados no pacote de instalação para reduzir o consumo de tráfego ao atualizar os bancos de dados após a instalação do Kaspersky Endpoint Security.



Componentes incluídos no pacote de instalação



Configurações de instalação do pacote de instalação

Configurações do pacote de instalação

Seção	Descrição
Componentes de proteção	**Modo Standard**. A configuração padrão. Essa configuração permite usar todos os componentes do aplicativo, inclusive os componentes que fornecem suporte para as soluções de Detection and Response. Essa configuração é usada para a proteção abrangente do computador contra diversas ameaças, ataques de rede e fraudes. **Endpoint Detection and Response Agent**. Nesta configuração, é possível instalar apenas os componentes que fornecem suporte para as soluções Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), assim como KUMA. Essa configuração será necessária caso uma Endpoint Protection Platform (EPP) de terceiros seja implantada na sua organização juntamente com uma solução Kaspersky Detection and Response. Isso torna o Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent compatível com os aplicativos EPP de terceiros. **Light Agent para garantir a proteção em ambientes virtuais**. Essa configuração destina-se ao aplicativo usado como parte da solução do Kaspersky Security for Virtualization Light Agent. O Light Agent deve ser instalado em cada máquina virtual que precisa ser protegida pela solução. Nessa configuração, não é possível usar componentes de criptografia de dados ou o Controle Adaptativo de Anomalias. Se estiver instalando o Light Agent em um modelo de máquina virtual que será usado para criar *máquinas virtuais não persistentes*, marque a caixa de seleção **Proteger infraestrutura VDI** (VDI significa Virtual Desktop Infrastructure). O modo de proteção VDI ajuda a otimizar o desempenho do Kaspersky Endpoint Security em máquinas virtuais não persistentes. Nesse modo, o Light Agent recusa as atualizações do aplicativo que exigem a reinicialização da máquina virtual. Ao receber atualizações do aplicativo que exijam uma reinicialização, o Light Agent gerará um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas.
Exclusões	A partir do Kaspersky Endpoint Security 12.6 for Windows, as exclusões de verificação e aplicativos confiáveis são adicionadas na zona confiável. As exclusões predefinidas de verificação e aplicativos confiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, Microsoft Exchange e System Center Configuration Manager. Isso significa que não será necessário configurar manualmente uma zona confiável para o aplicativo nos servidores. A partir do Kaspersky Endpoint Security 12.8 for Windows, é possível instalar o aplicativo no modo Light Agent para proteger ambientes virtuais. Exclusões de verificação e aplicativos confiáveis predefinidos podem ajudar a configurar rapidamente o Kaspersky Endpoint Security em ambientes virtuais Citrix e VMware. Também é possível configurar a zona confiável mais tarde nas propriedades da política: exclusões de verificação e aplicativos confiáveis.

Seção	Descrição
Selecione componentes para instalar	Nesta seção, você pode selecionar os componentes do aplicativo que serão disponibilizados. É possível alterar a configuração de componentes do aplicativo posteriormente, usando a tarefa *Alterar componentes do aplicativo*. É possível criar conjuntos separados de componentes para estações de trabalho e servidores. Antes de implementar o pacote de instalação, o instalador detecta o tipo de sistema operacional e instala somente os componentes do aplicativo selecionados para esse tipo de sistema operacional. Dessa forma, pode-se usar o mesmo pacote de instalação para estações de trabalho e servidores. O conjunto de componentes disponíveis depende da configuração do aplicativo: **Modo Standard** O Kaspersky Data Encryption, a Criptografia em Nível de Arquivo e todos os agentes integrados, exceto o EDR Optimum, não são instalados por padrão. Eles podem ser adicionados nas configurações do pacote de instalação. **Endpoint Detection and Response Agent** Nessa configuração, somente os agentes integrados para as soluções Kaspersky Detection and Response estão disponíveis. **Light Agent para garantir a proteção em ambientes virtuais** Nessa configuração, é possível usar quase todos os componentes do aplicativo disponíveis na configuração **Modo Standard**, exceto componentes de criptografia de dados e o Controle Adaptativo de Anomalias.
Chave de licença	Nesta seção, é possível ativar o aplicativo. Para ativar o aplicativo, é necessário selecionar uma chave de licença. Antes de fazer isso, é necessário adicionar a chave ao Servidor de Administração. Para obter mais informações sobre como adicionar chaves ao Servidor de Administração do Kaspersky Security Center, consulte a Ajuda do Kaspersky Security Center.
Aplicativos incompatíveis	Leia atentamente a lista de aplicativos incompatíveis e permita a remoção desses aplicativos. Se houver aplicativos incompatíveis instalados no computador, a instalação do Kaspersky Endpoint Security terminará com um erro.
Configurações de instalação	**Adicionar o caminho para o arquivo avp.com à variável do sistema %PATH%**. É possível adicionar o caminho de instalação à variável %PATH% para uso adequado da interface da linha de comando. **Proteger o processo de instalação**. 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 Endpoint Security e bloqueio do acesso à seção de registro do sistema que contém chaves do aplicativo. Contudo, 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. **Garantir a compatibilidade com Citrix PVS**. É possível ativar o suporte ao Citrix Provisioning Services para instalar o Kaspersky Endpoint Security em uma máquina virtual. **Usar o modo de compatibilidade do Azure WVD**. Esse recurso garante a exibição correta do estado das máquinas virtuais Azure no console do Kaspersky Anti Targeted Attack Platform. Para monitorar o desempenho do computador, o Kaspersky Endpoint Security envia telemetria aos servidores da KATA. A telemetria inclui um ID do computador (Sensor ID). O modo de compatibilidade do Azure WVD permite atribuir um Sensor ID exclusivo e permanente para essas máquinas virtuais. Caso o modo de compatibilidade esteja desativado, o Sensor ID poderá mudar depois que o computador for reiniciado devido ao funcionamento das máquinas virtuais do Azure. Isso pode fazer com que máquinas virtuais duplicadas apareçam no console. **Pasta de instalação do aplicativo**. Você pode alterar o caminho de instalação do Kaspersky Endpoint Security em um computador cliente. Por padrão, o aplicativo é instalado na pasta `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.2`. **Arquivo de configuração**. Instalação do aplicativo com configurações predefinidas. Para fazer isso, você precisa carregar um arquivo que define as configurações do Kaspersky Endpoint Security. Você pode criar um arquivo de configuração na interface local do aplicativo. O Assistente de Novo Pacote não oferece suporte a arquivos de configuração criptografados. Ao exportar o arquivo de configuração, ignore a etapa de criptografia do arquivo.

Atualização de bancos de dados no pacote de instalação

O pacote de instalação contém bancos de dados antivírus do repositório do Servidor de Administração atualizados quando o pacote de instalação é criado. Após criar o pacote de instalação, você pode atualizar os bancos de dados antivírus no pacote de instalação. Isso permite reduzir o consumo de tráfego ao atualizar bancos de dados antivírus após a instalação do Kaspersky Endpoint Security.

Para atualizar os bancos de dados do antivírus no repositório do Servidor de Administração, use a tarefa *Baixar atualizações no repositório do Servidor de Administração* do Servidor de Administração. Para obter mais informações sobre a atualização dos bancos de dados antivírus no repositório do Servidor de Administração, consulte a Ajuda do Kaspersky Security Center.

Você pode atualizar os bancos de dados no pacote de instalação apenas no Console de administração e no Kaspersky Security Center Web Console. Não é possível atualizar os bancos de dados no pacote de instalação no Kaspersky Security Center Cloud Console.

Como atualizar os bancos de dados antivírus no pacote de instalação por meio do Console de administração (MMC)

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

2. Na árvore do console, selecione a pasta **Avançado** → **Instalação remota** → **Pacotes de instalação**.

   Isso abre uma lista de pacotes de instalação que foram baixados no Kaspersky Security Center.

3. Abra as propriedades do pacote de instalação.

4. Na seção **Geral**, clique no botão **Atualizar bancos de dados**.

Como resultado, os bancos de dados antivírus no pacote de instalação serão atualizados no repositório do Servidor de Administração. O arquivo `bases.cab` incluído no kit de distribuição será substituído pela pasta `bases`. Os arquivos do pacote de atualização estarão dentro da pasta.

Como atualizar bancos de dados antivírus em um pacote de instalação por meio do Web Console

1. Na janela principal do Web Console, selecione **Descoberta e implementação** → **Implementação e atribuição** → **Pacotes de instalação**.

   É exibida uma lista dos pacotes de instalação baixados no Web Console.

2. Clique no nome do pacote de instalação do Kaspersky Endpoint Security no qual você deseja atualizar os bancos de dados antivírus.

   A janela de propriedades do pacote de instalação é exibida.

3. Na guia **Informações gerais**, clique no link **Atualizar bancos de dados**.

Como resultado, os bancos de dados antivírus no pacote de instalação serão atualizados no repositório do Servidor de Administração. O arquivo `bases.cab` incluído no kit de distribuição será substituído pela pasta `bases`. Os arquivos do pacote de atualização estarão dentro da pasta.

Criar uma tarefa de instalação remota

A tarefa *Instalar o aplicativo remotamente* foi desenvolvida para a instalação remota do Kaspersky Endpoint Security. A tarefa *Instalar o aplicativo remotamente* permite implementar o pacote de instalação do aplicativo em todos os computadores da organização. Antes de implantar o pacote de instalação, você pode atualizar os bancos de dados de antivírus dentro do pacote e selecionar os componentes de aplicativos disponíveis nas propriedades do pacote de instalação.

Como criar uma tarefa de instalação remota no console de administração (MMC)

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

2. Na árvore do console, selecione **Tarefas**.

   A lista de tarefas é aberta.

3. Clique **Nova tarefa**.

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

Etapa 1. Selecionar o tipo de tarefa

Selecione **Servidor de Administração do Kaspersky Security Center → Instalar o aplicativo remotamente**.

Etapa 2. Selecionar um pacote de instalação

Selecione o pacote de instalação do Kaspersky Endpoint Security na lista. Se a lista não tiver o pacote de instalação do Kaspersky Endpoint Security, você poderá criar o pacote clicando no Assistente.

Você pode definir as configurações do pacote de instalação no Kaspersky Security Center. Por exemplo, você pode selecionar os componentes do aplicativo que serão instalados em um computador.

O Agente de rede também será instalado junto com o Kaspersky Endpoint Security. O *Agente de Rede* facilita a interação entre o Servidor de Administração e um computador cliente. Se o Agente de Rede já estiver instalado no computador, ele não será instalado novamente.

Etapa 3. Adicional

Selecione o pacote de instalação do Agente de Rede. A versão selecionada do Agente de rede será instalada em conjunto com o Kaspersky Endpoint Security.

Etapa 4. Configurações

Defina as seguintes configurações adicionais do aplicativo:

- **Forçar download do pacote de instalação**. Selecione o método de instalação do aplicativo:
  - **Usando o Agente de Rede**. O Agente de Rede é responsável por entregar o pacote de instalação do Kaspersky Endpoint Security aos computadores cliente. Se o Agente de Rede não está instalado, a tarefa terminará com um erro. Nesse caso, adicione o pacote de instalação do Agente de Rede à tarefa *Instalar o aplicativo remotamente* e ative a entrega de arquivos por meio dos recursos do sistema operacional. Em seguida, o Agente de Rede será instalado usando os recursos do sistema operacional. Em seguida, o Kaspersky Endpoint Security será instalado pelas ferramentas do Agente de Rede.
  - **Usando recursos do sistema operacional através de pontos de distribuição**. O pacote de instalação é entregue aos computadores clientes usando recursos do sistema operacional por meio de pontos de distribuição. Você poderá selecionar esta opção se houver pelo menos um ponto de distribuição na rede. Para obter mais detalhes sobre os pontos de distribuição, consulte a ajuda do Kaspersky Security Center.
  - **Usando recursos do sistema operacional através do Servidor de Administração**. Os arquivos serão entregues a computadores clientes usando recursos do sistema operacional por meio do Servidor de Administração. Você pode selecionar esta opção se o Agente de Rede não estiver instalado no computador cliente, mas o computador cliente estiver na mesma rede que o Servidor de Administração.

- **Comportamento para dispositivos gerenciados por meio de outros Servidores de Administração**. Selecione o método de instalação do Kaspersky Endpoint Security. Se a rede tiver mais de um Servidor de Administração instalado, esses Servidores de Administração poderão ver os mesmos computadores clientes. Isso pode fazer com que, por exemplo, um aplicativo seja instalado remotamente no mesmo computador cliente várias vezes por meio de diferentes Servidores de Administração, ou outros conflitos.

- **Não reinstalar o aplicativo se ele já estiver instalado**. Desmarque esta caixa de seleção se você quiser instalar uma versão anterior do aplicativo, por exemplo.

Etapa 5. Selecionar a configuração de reinicialização do sistema operacional

Selecione a ação a ser executada se for necessário reiniciar o computador. Não é necessário reiniciar ao instalar o Kaspersky Endpoint Security. A reinicialização será necessária apenas se você precisar remover aplicativos incompatíveis antes da instalação. A reinicialização também poderá ser necessária quando a versão do aplicativo for atualizada.

Etapa 6. Selecionar os dispositivos aos quais a tarefa será atribuída

Selecione os computadores para instalar o Kaspersky Endpoint Security. 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*. O Agente de Rede não é instalado em dispositivos não atribuídos. Neste caso, a tarefa é atribuída a dispositivos específicos. 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 7. Seleção da conta para executar a tarefa

Selecione a conta para instalar o Agente de rede usando as ferramentas do sistema operacional. Neste caso, os direitos de administrador são necessários para acessar o computador. Você pode adicionar várias contas. Se uma conta não tiver direitos suficientes, o Assistente de Instalação usará a próxima conta. Se você instalar o Kaspersky Endpoint Security usando as ferramentas do Agente de Rede, não precisará selecionar uma conta.

Etapa 8. Configurar um agendamento de início de tarefa

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

Etapa 9. Definir o nome da tarefa

Insira um nome para a tarefa, por exemplo, *Instalar o Kaspersky Endpoint Security for Windows 14.2*.

Etapa 10. Encerrar a criação da tarefa

Conclua o 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. O aplicativo será instalado no modo silencioso. Após a instalação, o ícone será adicionado à área de notificação do computador do usuário. Se o ícone estiver assim , verifique se você ativou o aplicativo.

Como criar uma tarefa de instalação remota no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **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 Security Center**.

2. Na lista suspensa **Tipo de tarefa**, selecione **Instalar o aplicativo remotamente**.

3. No campo **Nome da tarefa**, insira uma breve descrição, como *Instalação do Kaspersky Endpoint Security para gerentes*.

4. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

Etapa 2. Selecionar computadores para instalação

Nesta etapa, selecione os computadores para instalar o Kaspersky Endpoint Security de acordo com a opção de escopo da tarefa selecionada.

Etapa 3. Configurar um pacote de instalação

Nesta etapa, configure o pacote de instalação:

1. Selecione o pacote de instalação do Kaspersky Endpoint Security for Windows (14.2).

2. Selecione o pacote de instalação do Agente de Rede.

   A versão selecionada do Agente de rede será instalada em conjunto com o Kaspersky Endpoint Security. O *Agente de Rede* facilita a interação entre o Servidor de Administração e um computador cliente. Se o Agente de Rede já estiver instalado no computador, ele não será instalado novamente.

3. No bloco **Forçar download do pacote de instalação**, selecione o método de instalação do aplicativo:

   - **Usando o Agente de Rede**. O Agente de Rede é responsável por entregar o pacote de instalação do Kaspersky Endpoint Security aos computadores cliente. Se o Agente de Rede não está instalado, a tarefa terminará com um erro. Nesse caso, adicione o pacote de instalação do Agente de Rede à tarefa *Instalar o aplicativo remotamente* e ative a entrega de arquivos por meio dos recursos do sistema operacional. Em seguida, o Agente de Rede será instalado usando os recursos do sistema operacional. Em seguida, o Kaspersky Endpoint Security será instalado pelas ferramentas do Agente de Rede.

   - **Usando recursos do sistema operacional através de pontos de distribuição**. O pacote de instalação é entregue aos computadores clientes usando recursos do sistema operacional por meio de pontos de distribuição. Você poderá selecionar esta opção se houver pelo menos um ponto de distribuição na rede. Para obter mais detalhes sobre os pontos de distribuição, consulte a ajuda do Kaspersky Security Center.

   - **Usando recursos do sistema operacional através do Servidor de Administração**. Os arquivos serão entregues a computadores clientes usando recursos do sistema operacional por meio do Servidor de Administração. Você pode selecionar esta opção se o Agente de Rede não estiver instalado no computador cliente, mas o computador cliente estiver na mesma rede que o Servidor de Administração.

4. No campo **Número máximo de downloads concomitantes**, defina um limite para o número de solicitações de download do pacote de instalação enviadas ao Servidor de Administração. Um limite para o número de solicitações ajudará a impedir sobrecarga da rede.

5. No campo **Número máximo de tentativas de instalação**, defina um limite para o número de tentativas de instalação do aplicativo. Se a instalação do Kaspersky Endpoint Security terminar com um erro, a tarefa reiniciará automaticamente a instalação.

6. Caso seja necessário, desmarque a caixa de seleção **Não reinstalar o aplicativo se ele já estiver instalado**. Ele permite, por exemplo, instalar uma das versões anteriores do aplicativo.

7. Caso seja necessário, desmarque a caixa de seleção **Verificar o tipo do sistema operacional antes de baixar**. Isso permite que você impeça o download de um pacote de distribuição de aplicativos se o sistema operacional do computador não atender aos requisitos de software. Se tiver certeza de que o sistema operacional do computador atende aos requisitos de software, você pode ignorar essa verificação.

8. Caso seja necessário, marque a caixa de seleção **Atribuir a instalação do pacote em políticas de grupo do Active Directory**. O Kaspersky Endpoint Security é instalado por meio do Agente de Rede ou manualmente por meio do Active Directory. Para instalar o Agente de Rede, a tarefa de instalação remota deve ser executada com privilégios de administrador de domínio.

9. Caso seja necessário, marque a caixa de seleção **Solicitar aos usuários o fechamento de aplicativos em execução**. A instalação do Kaspersky Endpoint Security utiliza recursos do computador. Para a conveniência do usuário, o Assistente de Instalação do Aplicativo solicita que você feche os aplicativos em execução antes de iniciar a instalação. Isso ajuda a evitar interrupções na operação de outros aplicativos e evita possíveis avarias do computador.

10. No bloco **Comportamento para dispositivos gerenciados por meio de outros Servidores de Administração**, selecione o método de instalação do Kaspersky Endpoint Security. Se a rede tiver mais de um Servidor de Administração instalado, esses Servidores de Administração poderão ver os mesmos computadores clientes. Isso pode fazer com que, por exemplo, um aplicativo seja instalado remotamente no mesmo computador cliente várias vezes por meio de diferentes Servidores de Administração, ou outros conflitos.

Etapa 4. Seleção da conta para executar a tarefa

Selecione a conta para instalar o Agente de rede usando as ferramentas do sistema operacional. Neste caso, os direitos de administrador são necessários para acessar o computador. Você pode adicionar várias contas. Se uma conta não tiver direitos suficientes, o Assistente de Instalação usará a próxima conta. Se você instalar o Kaspersky Endpoint Security usando as ferramentas do Agente de Rede, não precisará selecionar uma conta.

Etapa 5. Concluir a criação da tarefa

Finalize o assistente, clicando no botão **Concluir**. Uma nova tarefa será exibida na lista de tarefas. Para executar uma tarefa, marque a caixa de seleção ao lado da tarefa e clique no botão **Iniciar**. O aplicativo será instalado no modo silencioso. Após a instalação, o ícone será adicionado à área de notificação do computador do usuário. Se o ícone estiver assim , verifique se você ativou o aplicativo.

Instalar o aplicativo localmente usando o assistente de instalação

A interface do aplicativo Assistente de Instalação consiste em uma sequência de janelas que correspondem às etapas de instalação do aplicativo. Verifique e confirme se a conta de usuário na qual o assistente de configuração está sendo executado está no grupo de administradores.

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

1. Copie a pasta Kit de distribuição no computador do usuário.

2. Execute setup_kes.exe.

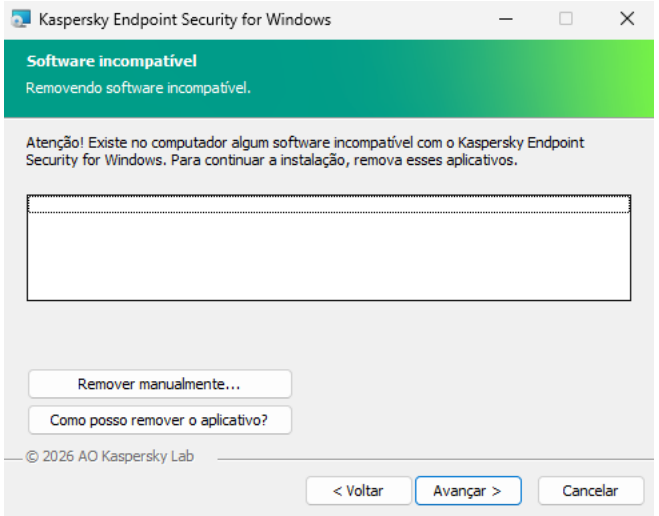
O assistente de Instalação é iniciado.

Preparando para instalação

Antes de instalar o Kaspersky Endpoint Security em um computador, ou de atualizá-lo a partir de uma versão anterior, as seguintes condições são verificadas:

- Se houver qualquer software instalado que possa ter problemas de compatibilidade com o Kaspersky Endpoint Security (a lista de software está disponível no arquivo incompatible.txt incluído no kit de distribuição).
- Se os requisitos de software foram atendidos.
- Se o Microsoft .NET Framework estiver presente.
- Se o usuário tem direitos para instalar o produto de software.

Caso um destes requisitos não seja cumprido, uma notificação é exibida na tela. Por exemplo, uma notificação sobre softwares incompatíveis (veja a figura abaixo).



Remoção de softwares incompatíveis

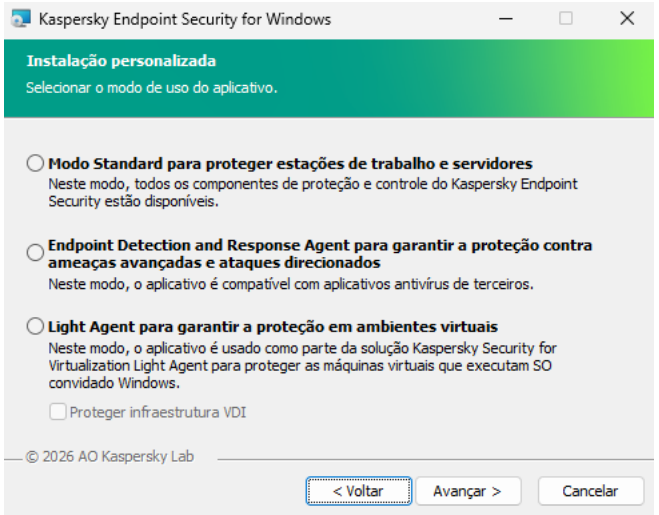
Se o computador cumprir os requisitos citados, o Assistente de Instalação busca os aplicativos da Kaspersky que poderiam acarretar conflitos quando executados no mesmo tempo em que o aplicativo é instalado. Caso sejam encontrados tais aplicativos, é solicitado ao usuário que os remova manualmente.

Caso os aplicativos detectados incluíam versões anteriores do Kaspersky Endpoint Security, todos os dados que puderem ser migrados (como dados de ativação e configurações do aplicativo) serão conservados e usados durante a instalação do Kaspersky Endpoint Security 14.2 for Windows, e a versão anterior do aplicativo será automaticamente removida. Isto se aplica às seguintes versões do aplicativo:

- Kaspersky Endpoint Security 12.3 for Windows (compilação 12.3.0.493)
- Kaspersky Endpoint Security 12.4 for Windows (compilação 12.4.0.467)
- Kaspersky Endpoint Security 12.5 for Windows (compilação 12.5.0.539)
- Kaspersky Endpoint Security 12.6 for Windows (compilação 12.6.0.438)
- Kaspersky Endpoint Security 12.7 for Windows (compilação 12.7.0.533)
- Kaspersky Endpoint Security 12.8 for Windows (compilação 12.8.0.505)

- Kaspersky Endpoint Security 12.9 for Windows (compilação 12.9.0.384)
- Kaspersky Endpoint Security 12.10 for Windows (compilação 12.10.0.466)
- Kaspersky Endpoint Security 12.11 for Windows (compilação 12.11.0.637)
- Kaspersky Endpoint Security 12.12 for Windows (compilação 12.12.0.522)
- Kaspersky Endpoint Security 14.0 for Windows (compilação 14.0.0.504)
- Kaspersky Endpoint Security 14.1 for Windows (compilação 14.1.0.423)

Configuração do Kaspersky Endpoint Security



Escolhendo a configuração do aplicativo

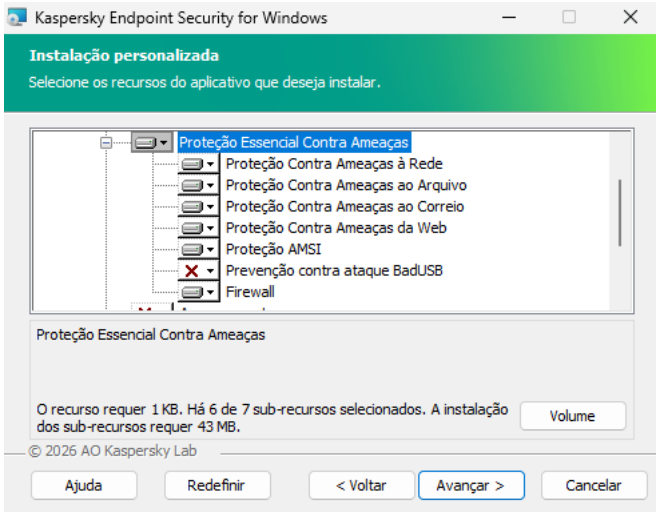
Modo Standard. A configuração padrão. Essa configuração permite usar todos os componentes do aplicativo, inclusive os componentes que fornecem suporte para as soluções de Detection and Response. Essa configuração é usada para a proteção abrangente do computador contra diversas ameaças, ataques de rede e fraudes.

Endpoint Detection and Response Agent. Nesta configuração, é possível instalar apenas os componentes que fornecem suporte para as soluções Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), assim como KUMA. Essa configuração será necessária caso uma Endpoint Protection Platform (EPP) de terceiros seja implantada na sua organização juntamente com uma solução Kaspersky Detection and Response. Isso torna o Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent compatível com os aplicativos EPP de terceiros.

Light Agent para garantir a proteção em ambientes virtuais. Essa configuração destina-se ao aplicativo usado como parte da solução do Kaspersky Security for Virtualization Light Agent. O Light Agent deve ser instalado em cada máquina virtual que precisa ser protegida pela solução. Nessa configuração, não é possível usar componentes de criptografia de dados ou o Controle Adaptativo de Anomalias. Se estiver instalando o Light Agent em um modelo de máquina virtual que será usado para criar *máquinas virtuais não persistentes*, marque a caixa de seleção **Proteger infraestrutura VDI** (VDI significa Virtual Desktop Infrastructure). O modo de proteção VDI ajuda a otimizar o desempenho do Kaspersky Endpoint Security em máquinas virtuais não persistentes. Nesse modo, o Light Agent recusa as atualizações do aplicativo que exigem a reinicialização da máquina virtual. Ao receber atualizações do aplicativo que exijam uma reinicialização, o Light Agent gerará um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas.

Componentes do Kaspersky Endpoint Security

Durante o processo de instalação, você pode selecionar os componentes do Kaspersky Endpoint Security que você quer instalar (veja a figura abaixo). O componente Proteção Contra Ameaças ao Arquivo é um componente obrigatório que deve ser instalado. Não é possível cancelar a sua instalação.



Seleção de componentes do aplicativo para instalação

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

- Kaspersky Disk Encryption
- Criptografia em Nível de Arquivo
- Endpoint Detection and Response Expert (on-premises)
- Endpoint Detection and Response Expert (cloud)
- Sandbox
- Managed Detection and Response
- Network Detection and Response (KATA)
- Integração com KUMA

Você pode alterar os componentes disponíveis do aplicativo depois de concluir a instalação do aplicativo. Para isso, você precisa executar o Assistente de instalação novamente e optar por alterar os componentes disponíveis.

Caso necessite instalar componentes Detection and Response, o Kaspersky Endpoint Security dá suporte às configurações:

- Somente Endpoint Detection and Response Optimum
- Somente Endpoint Detection and Response Expert (cloud)
- Somente Endpoint Detection and Response Expert (on-premises)

- Somente Network Detection and Response (KATA)
- Somente Sandbox
- Endpoint Detection and Response Optimum e Sandbox
- Endpoint Detection and Response Expert (cloud) e Sandbox
- Endpoint Detection and Response Expert (on-premises) e Sandbox
- Network Detection and Response (KATA) e Endpoint Detection and Response Expert (on-premises)
- Network Detection and Response (KATA) e Managed Detection and Response

O Kaspersky Endpoint Security verifica a seleção de componentes antes de instalar o aplicativo. Se a configuração selecionada de componentes Detection and Response não for compatível, o Kaspersky Endpoint Security não pode ser instalado.

Seleção da pasta para instalação do aplicativo

Você pode alterar o caminho de instalação do Kaspersky Endpoint Security em um computador cliente. Por padrão, o aplicativo é instalado na pasta `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.2`.

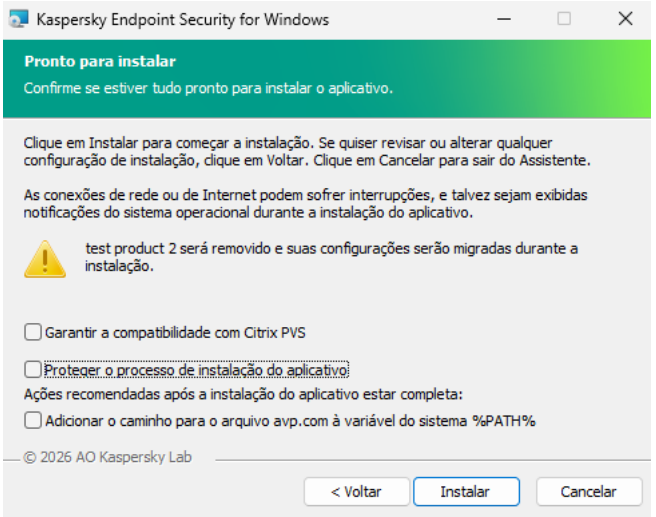
Configuração da zona confiável

A partir do Kaspersky Endpoint Security 12.6 for Windows, as exclusões de verificação e aplicativos confiáveis são adicionadas na zona confiável. As exclusões predefinidas de verificação e aplicativos confiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, Microsoft Exchange e System Center Configuration Manager. Isso significa que não será necessário configurar manualmente uma zona confiável para o aplicativo nos servidores.

A partir do Kaspersky Endpoint Security 12.8 for Windows, é possível instalar o aplicativo no modo Light Agent para proteger ambientes virtuais. Exclusões de verificação e aplicativos confiáveis predefinidos podem ajudar a configurar rapidamente o Kaspersky Endpoint Security em ambientes virtuais Citrix e VMware.

Também é possível configurar a zona confiável mais tarde nas propriedades da política: exclusões de verificação e aplicativos confiáveis.

Configurações avançadas



Configurações avançadas de instalação do aplicativo

Proteger o processo de instalação do aplicativo. 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 Endpoint Security e bloqueio do acesso à seção de registro do sistema que contém chaves do aplicativo. Contudo, 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.

Garantir a compatibilidade com Citrix PVS. É possível ativar o suporte ao Citrix Provisioning Services para instalar o Kaspersky Endpoint Security em uma máquina virtual.

Adicionar o caminho para o arquivo avp.com à variável do sistema %PATH%. É possível adicionar o caminho de instalação à variável %PATH% para uso adequado da interface da linha de comando.

Instalar remotamente o aplicativo usando o System Center Configuration Manager

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

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

1. Abra o console do Configuration Manager.

2. Na parte direita do console, no bloco **Gerenciamento de aplicativos**, selecione **Pacotes**.

3. Na parte superior do console, no painel de comando, clique no botão **Criar pacote**.

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

4. No Novo Assistente de Aplicativos e Pacotes:

   a. Na seção **Pacote**:

      - No campo **Nome**, insira o nome do pacote de instalação.

      - No campo **Pasta de origem**, especifique o caminho para a pasta contendo o pacote de distribuição do Kaspersky Endpoint Security.

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

   c. Na seção **Programa padrão**:

      - No campo **Nome**, digite o nome exclusivo do pacote de instalação (por exemplo, o nome do aplicativo inclusive a versão).

      - No campo **Linha de comando**, especifique as opções de instalação do Kaspersky Endpoint Security na linha de comando.

      - Clique no botão **Procurar** para especificar o caminho para o arquivo executável do aplicativo.

      - Certifique-se de que a lista **Modo de execução** tenha o item **Executar com direitos administrativos** selecionado.

   d. Na seção **Requisitos**:

      - Marque a caixa de seleção **Executa outro programa primeiro** caso queira que um aplicativo diferente seja iniciado antes de instalar o Kaspersky Endpoint Security.

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

      - Selecione a opção **Este programa pode ser executado somente em plataformas especificadas** no bloco **Requisitos da plataforma**, caso deseje que o aplicativo seja instalado somente nos sistemas operacionais especificados.

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

      Esta etapa é opcional.

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

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

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

   Isto inicia o *Assistente de Implementação*.

6. No Assistente de Implementação:

   a. Na seção **Geral**:

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

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

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

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

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

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

Descrição das configurações de instalação do arquivo setup.ini

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

Use o arquivo setup.ini somente ao instalar o aplicativo no modo silencioso.

Não é possível adicionar um caminho ao arquivo de configuração install.cfg no arquivo setup.ini. O aplicativo também ignora o arquivo de configuração install.cfg, caso ele seja colocado na mesma pasta do kit de distribuição do Kaspersky Endpoint Security. Para aplicar as configurações do arquivo de configuração install.cfg, você precisa especificar o caminho para o arquivo no seguinte comando de instalação do aplicativo: `CONFIGPATH=<path to the configuration file>`.

DOWNLOAD DO ARQUIVO SETUP.INI

O arquivo setup.ini consiste nas seguintes seções:

- `[Setup]` – configurações gerais da instalação do aplicativo.
- `[Components]` – seleção dos componentes do aplicativo a serem instalados no modo Standard. Se nenhum dos componentes for especificado, todos os componentes que estão disponíveis para o sistema operacional são instalados. A Proteção Contra Ameaças ao Arquivo é um componente obrigatório instalado no computador, independentemente das configurações indicadas nesta seção.
- `[Tasks]` – seleção de tarefas a serem incluídas na lista de tarefas do Kaspersky Endpoint Security. Se nenhuma tarefa for especificada, todas as tarefas serão incluídas na lista de tarefas do Kaspersky Endpoint Security.

Em alternativa ao valor `1`, é possível usar os valores `yes`, `on`, `enable`, `enabled` e `true`. Em alternativa ao valor `0`, é possível usar os valores `no`, `off`, `disable`, `disabled` e `false`.

Seção	Parâmetro	Descrição
`[Setup]`	`InstallDir`	Caminho até a pasta de instalação do aplicativo.
	`ActivationCode`	Código de ativação do Kaspersky Endpoint Security.
	`Eula`	A aceitação dos termos do Contrato de Licença do Usuário Final. O texto do Contrato de Licença está incluído no kit de distribuição do Kaspersky Endpoint Security. A aceitação dos termos do Contrato de Licença de Usuário Final é necessária para instalar o aplicativo ou para atualizar uma versão do aplicativo.
	`PrivacyPolicy`	Aceitação da Política de Privacidade. O texto da Política de Privacidade está incluído no kit de distribuição do Kaspersky Endpoint Security. Para instalar o aplicativo ou atualizar a versão do aplicativo, aceite a Política de Privacidade.
	`KSN`	Acordo ou recusa em participar da Kaspersky Security Network (KSN). Se nenhum valor for definido para este parâmetro, o Kaspersky Endpoint Security solicitará a confirmação do seu consentimento ou recusa em participar da KSN quando o Kaspersky Endpoint Security for iniciado pela primeira vez. Valores disponíveis: • `1` – concordo em participar da KSN. • `0` – não aceito participar da KSN (valor padrão). O pacote de distribuição do Kaspersky Endpoint Security é otimizado para uso com a Kaspersky Security Network. Se você optar por não participar da Kaspersky Security Network, atualize o Kaspersky Endpoint Security assim que a instalação for concluída.
	`CLEANERSIGNCHECK`	Verificação das assinaturas digitais dos arquivos de software detectados na lista incompatible.txt. Para remover o software, o Kaspersky Endpoint Security executa o arquivo do instalador do software. Se o arquivo do instalador não tiver assinatura digital, o Kaspersky Endpoint Security considera o arquivo não confiável e interrompe a remoção do software para evitar a execução de um possível código malicioso. Se o aplicativo não puder verificar a assinatura digital do arquivo de software detectado, a instalação do Kaspersky Endpoint Security é interrompida com um erro. O valor padrão é diferente dependendo do método de instalação do software: • `0` significa que a verificação de assinatura digital está desativada (valor padrão caso tenha sido implantado pelo Kaspersky Security Center). • `1` significa que a verificação de assinatura digital está ativada (valor padrão caso o aplicativo seja instalado localmente).
	`Login`	Defina o nome de usuário para acessar os recursos e configurações do Kaspersky Endpoint Security (o componente Proteção por senha). O nome de usuário é definido junto com as configurações `Password` e `PasswordArea`. O nome de usuário KLAdmin é usado por padrão.
	`Password`	Especifique uma senha para acessar os recursos e as configurações do Kaspersky Endpoint Security (a senha é especificada em conjunto com os parâmetros de `Login` e `PasswordArea`). Se você especificou uma senha mas não especificou um nome de usuário com o parâmetro `Login`, o nome de usuário KLAdmin é usado por padrão.

Seção	Parâmetro	Descrição
	`PasswordArea`	Especifique o escopo da senha para acessar os recursos e as configurações do Kaspersky Endpoint Security. Quando um usuário tenta executar uma ação incluída nesse escopo, o Kaspersky Endpoint Security solicita as credenciais da conta do usuário (os parâmetros `Login` e `Password`). Use o caractere `;` para especificar vários valores. Valores disponíveis: • `SET` – modificar as configurações do aplicativo. • `EXIT` – sair do aplicativo. • `DISPROTECT` – desativar componentes de proteção e interromper tarefas de verificação. • `DISPOLICY` – desativar a política do Kaspersky Security Center. • `UNINST` – remover o aplicativo do computador. • `DISCTRL` – desativar componentes de controle. • `REMOVELIC` – remover a chave. • `REPORTS` – visualizar relatórios. • `EXPORT` – exportar as configurações do aplicativo. Por exemplo, `PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`.
	`SelfProtection`	Ativar ou desativar o mecanismo de proteção da instalação do aplicativo. Valores disponíveis: • `1` – o mecanismo de proteção da instalação do aplicativo é ativado (valor padrão). • `0` – o mecanismo de proteção da instalação do aplicativo é desativado. 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 Endpoint Security e bloqueio do acesso à seção de registro do sistema que contém chaves do aplicativo. Contudo, 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.
	`PROTECTOSSERVICES`	Proteção da funcionalidade dos serviços do sistema operacional. A proteção dos serviços do sistema operacional impede que aplicativos de terceiros interfiram no funcionamento desses serviços. Esses serviços incluem, por exemplo, o serviço de inicialização automática de aplicativos. • `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.
	`EnableAzureSupport`	Ativação ou desativação do modo de compatibilidade Azure WVD. Valores disponíveis: • `1`: o modo de compatibilidade do Azure WVD está ativado. • `0`: o modo de compatibilidade do Azure WVD está desativado (valor padrão). Esse recurso garante a exibição correta do estado das máquinas virtuais Azure no console do Kaspersky Anti Targeted Attack Platform. Para monitorar o desempenho do computador, o Kaspersky Endpoint Security envia telemetria aos servidores da KATA. A telemetria inclui um ID do computador (Sensor ID). O modo de compatibilidade do Azure WVD permite atribuir um Sensor ID exclusivo e permanente para essas máquinas virtuais. Caso o modo de compatibilidade esteja desativado, o Sensor ID poderá mudar depois que o computador for reiniciado devido ao funcionamento das máquinas virtuais do Azure. Isso pode fazer com que máquinas virtuais duplicadas apareçam no console.
	`Reboot`	Reinício automático do computador, se necessário após a instalação ou atualização do aplicativo. Se nenhum valor for definido para esse parâmetro, a reinicialização automática do computador é bloqueada. Não é necessário reiniciar ao instalar o Kaspersky Endpoint Security. A reinicialização será necessária apenas se você precisar remover aplicativos incompatíveis antes da instalação. A reinicialização também poderá ser necessária quando a versão do aplicativo for atualizada.
	`AddEnvironment`	Na variável do sistema %PATH%, adicione o caminho para os arquivos executáveis que estão localizados na pasta de configuração do Kaspersky Endpoint Security. Valores disponíveis: • `1` – a variável de sistema %PATH% é complementada com o caminho para os arquivos executáveis localizados na pasta de configuração do Kaspersky Endpoint Security. • `0` – a variável de sistema %PATH% não é complementada com o caminho para arquivos executáveis localizados na pasta de configuração do Kaspersky Endpoint Security.

Seção	Parâmetro	Descrição
	AMPPL	Ativa ou desativa a proteção do serviço Kaspersky Endpoint Security usando a tecnologia AM-PPL (Antimalware Protected Process Light). Para obter mais detalhes sobre a tecnologia AM-PPL, visite o site da Microsoft. A tecnologia AM-PPL está disponível para os sistemas operacionais Windows 10 versão 1703 (RS2) ou posterior e Windows Server 2019. Valores disponíveis: • 1 – Proteção do serviço Kaspersky Endpoint Security usando a tecnologia AM-PPL ativada. • 0 – Proteção do serviço Kaspersky Endpoint Security usando a tecnologia AM-PPL desativada.
	UPGRADEMODE	Modo de atualização do aplicativo: • Seamless atualização do aplicativo com a reinicialização do computador (padrão). • Force atualização do aplicativo sem a reinicialização do computador. É possível atualizar o aplicativo sem reiniciar a partir da versão 11.10.0. Para atualizar uma versão anterior do aplicativo, é necessário reiniciar o computador. Também é possível instalar patches sem reiniciar a partir da versão 11.11.0. Não é necessário reiniciar ao instalar o Kaspersky Endpoint Security. Portanto, o modo de atualização do aplicativo será especificado nas configurações do aplicativo. É possível alterar este parâmetro nas configurações ou na política do aplicativo. Ao atualizar um aplicativo já instalado, a prioridade do parâmetro especificado no arquivo setup.ini será mais elevada do que aquela do parâmetro especificado nas configurações do aplicativo ou na linha de comando. Por exemplo, se o modo de atualização Force estiver especificado no arquivo setup.ini e o modo Seamless estiver especificado nas configurações do aplicativo, a atualização será instalada sem reinicialização (Force). Se estiver usando o arquivo setup.ini, no qual o parâmetro UPGRADEMODE não está especificado, o instalador vai utilizar um valor padrão (Seamless) e instalará a atualização com reinicialização do computador.
	SetupReg	Ativa a gravação das chaves de registro do arquivo setup.reg para o registro. Valor do parâmetro SetupReg: setup.reg.
	EnableTraces	Ativar ou desativar rastreamentos de aplicativos. Após o Kaspersky Endpoint Security ser iniciado, os arquivos de rastreamento serão salvos na pasta %ProgramData%\Kaspersky Lab\KES.14.2\Traces. Valores disponíveis: • 1 – rastreamentos ativados. • 0 – rastreamentos desativados (valor padrão).
	TracesLevel	Nível de detalhe dos rastreamentos. Valores disponíveis: • 100 (crítico). Apenas mensagens sobre erros fatais. • 200 (alto). Mensagens sobre todos os erros, incluindo erros fatais. • 300 (diagnóstico). Mensagens sobre todos os erros, bem como avisos. • 400 (importante). Todas as mensagens de erro, avisos e informações adicionais. • 500 (normal). Mensagens sobre todos os erros e avisos, bem como informações detalhadas sobre a operação do aplicativo no modo normal (padrão). • 600 (baixo). Todas as mensagens.
	RESTAPI	Gerenciamento do aplicativo por meio da API REST. Para gerenciar o aplicativo por meio da API REST, você deve especificar o nome do usuário (parâmetro RESTAPI_User). Valores disponíveis: • 1 – Gerenciamento via API REST permitido. • 0 – Gerenciamento via API REST bloqueado (valor padrão). Para gerenciar o aplicativo por meio da API REST, o gerenciamento usando sistemas administrativos deve ser permitido. Para fazer isso, defina o parâmetro AdminKitConnector=1. Se você gerencia o aplicativo por meio da API REST, é impossível gerenciar o aplicativo usando os sistemas de administração da Kaspersky.
	RESTAPI_User	Nome de usuário da conta de domínio do Windows usada para gerenciar o aplicativo por meio da API REST. O gerenciamento do aplicativo por meio da API REST está disponível apenas para este usuário. Digite o nome do usuário no formato <DOMAIN>\<UserName> (por exemplo, RESTAPI_User=COMPANY\Administrator). Você pode selecionar apenas um usuário para trabalhar com a API REST. Adicionar um nome de usuário é um pré-requisito para gerenciar o aplicativo por meio da API REST.
	RESTAPI_Port	Porta usada para gerenciar o aplicativo por meio da API REST. A porta 6782 é usada por padrão. Certifique-se de que a porta está livre.

Seção	Parâmetro	Descrição
	`RESTAPI_Certificate`	Certificado de identificação de solicitações (por exemplo, `RESTAPI_Certificate=C:\cert.pem`). A interação segura do Kaspersky Endpoint Security com o cliente REST requer a configuração da identificação da solicitação. Para fazer isso, é necessário instalar um certificado e, posteriormente, assinar a carga útil de cada solicitação.
	`StandaloneMode`	Instalação do aplicativo no modo Endpoint Detection and Response Agent (EDR Agent). O *Endpoint Detection and Response Agent* é um aplicativo instalado em estações de trabalho e servidores individuais na infraestrutura de TI da organização para oferecer suporte às soluções Kaspersky Managed Detection and Response e Kaspersky Anti Targeted Attack Platform. O EDR Agent é compatível com aplicativos EPP de terceiros. Isso viabiliza o uso de ferramentas de segurança de infraestrutura de terceiros juntamente com o Detection and Response da Kaspersky. Para instalar o EDR Agent, na seção `[Components]`, selecione os componentes `StandaloneKATA`, `StandaloneNDR` ou `StandaloneMDR`. O EDR Agent não é compatível com outros componentes do aplicativo. Valores disponíveis: • `1` para instalar o aplicativo no modo EDR Agent. • `0` para instalar o aplicativo no modo Padrão (padrão).
	`KSVLAMode`	Instalar o aplicativo no modo Light Agent. Essa configuração destina-se ao aplicativo usado como parte da solução do Kaspersky Security for Virtualization Light Agent. O Light Agent deve ser instalado em cada máquina virtual que precisa ser protegida pela solução. Valores disponíveis: • `1` para instalar o aplicativo no modo Light Agent. • `0` para instalar o aplicativo no modo Padrão (padrão).
	`InstallOnVDI`	Ativar o modo de proteção VDI ao instalar o aplicativo no modo Light Agent (`KSVLAMode=1`). O modo de proteção VDI ajuda a otimizar o desempenho do Kaspersky Endpoint Security em máquinas virtuais não persistentes. Nesse modo, o Light Agent recusa as atualizações do aplicativo que exigem a reinicialização da máquina virtual. Ao receber atualizações do aplicativo que exijam uma reinicialização, o Light Agent gerará um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas. Valores disponíveis: • `1` para ativar o modo de proteção VDI. • `0` para desativar o modo de proteção VDI (padrão).
	`KESExclusions`	Adicionar predefinições de exclusões de verificação e aplicativos confiáveis ao instalar o aplicativo no servidor. As exclusões predefinidas de verificação e aplicativos confiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, Microsoft Exchange e System Center Configuration Manager. Por exemplo, as exclusões predefinidas de verificação para servidores SQL incluem arquivos de banco de dados MDF e LDF. Isso significa que não será necessário configurar manualmente uma zona confiável para o aplicativo nos servidores. Valores disponíveis: • `1` ativa exclusões de verificação e aplicativos confiáveis predefinidos. • `0` desativa exclusões de verificação e aplicativos confiáveis predefinidos (padrão).
	`LAExclusions`	Adicionar exclusões de verificação e aplicativos confiáveis predefinidos ao instalar o aplicativo em uma máquina virtual (modo Light Agent). Exclusões de verificação e aplicativos confiáveis predefinidos podem ajudar a configurar rapidamente o Kaspersky Endpoint Security em ambientes virtuais Citrix e VMware. Valores disponíveis: • `1` ativa exclusões de verificação e aplicativos confiáveis predefinidos. • `0` desativa exclusões de verificação e aplicativos confiáveis predefinidos (padrão).

Seção	Parâmetro	Descrição
	`EnableUniqueSensorID`	Criar um identificador exclusivo do computador (Sensor ID) durante a instalação ou a atualização do aplicativo. O Sensor ID é usado na solução Kaspersky Anti Targeted Attack Platform para identificar computadores que enviam telemetria ao servidor. Ao criar o Sensor ID, o aplicativo usa um algoritmo que leva em consideração a configuração do computador, como o número de série da placa-mãe. Em alguns casos, por exemplo, ao usar o aplicativo em um ambiente virtual, o Sensor ID pode ser duplicado. Como resultado, a Kaspersky Anti Targeted Attack Platform não consegue identificar o computador do qual a telemetria é enviada. Para criar um Sensor ID exclusivo, é necessário definir o parâmetro `EnableUniqueSensorID=1`. Como resultado, o aplicativo usará um algoritmo diferente para criar o Sensor ID, que leva em consideração outros dados sobre o computador. Isso garante um Sensor ID exclusivo. Por padrão, o parâmetro não é definido. O aplicativo herda o Sensor ID nos seguintes casos: • Atualizar a versão do aplicativo; • migração da configuração [KES+KEA] para [KES+built-in agent]. Como parte do seu reparo, o instalador tenta herdar o Sensor ID. Se o Sensor ID não puder ser restaurado, o aplicativo criará um novo Sensor ID.
	`CitrixCompatibility`	Ativação do suporte para Citrix Provisioning Services para instalação do Kaspersky Endpoint Security em uma máquina virtual.
`[Components]`	`ALL`	Instalação de todos os componentes. Se o valor de parâmetro `1` for especificado, todos os componentes serão instalados apesar das configurações de instalação de componentes individuais. Devido à forma como as soluções Detection and Response são compatíveis, os componentes Endpoint Detection and Response Optimum and Sandbox são instalados no computador. O componente Endpoint Detection and Response Expert (cloud) não é compatível com essa configuração.
	`MailThreatProtection`	Proteção Contra Ameaças ao Correio.
	`WebThreatProtection`	Proteção Contra Ameaças da Web.
	`AMSI`	Proteção AMSI.
	`HostIntrusionPrevention`	Prevenção de Intrusão do Host.
	`BehaviorDetection`	Detecção de Comportamento.
	`ExploitPrevention`	Prevenção de Exploit.
	`RemediationEngine`	Mecanismo de Remediação.
	`Firewall`	Firewall.
	`NetworkThreatProtection`	Proteção Contra Ameaças à Rede.
	`WebControl`	Controle da Web.
	`DeviceControl`	Controle de Dispositivos.
	`ApplicationControl`	Controle de Aplicativos.
	`AdaptiveAnomaliesControl`	Controle Adaptativo de Anomalias.
	`CloudDiscovery`	Cloud Discovery.
	`LogInspector`	Inspeção do Log
	`AntiCryptor`	Anticryptor
	`FileThreatProtection`	Proteção Contra Ameaças ao Arquivo.
	`SystemIntegrityMonitor`	Monitor de integridade do sistema.
	`FileEncryption`	Bibliotecas de Criptografia a Nível de Arquivo.
	`DiskEncryption`	Bibliotecas de Criptografia completa do disco.
	`MSBitLocker`	Bibliotecas de gerenciamento de Criptografia do BitLocker.
	`BadUSBAttackPrevention`	Prevenção contra ataque BadUSB.

Seção	Parâmetro	Descrição
	`EDR`	Endpoint Detection and Response Optimum O componente não é compatível com os componentes Endpoint Detection and Response Expert (cloud) (`EDRCloud`) e Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`EDRCloud`	Endpoint Detection and Response Expert (cloud) O componente não é compatível com os componentes Endpoint Detection and Response Optimum (`EDR`) e Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`AntiAPT`	Endpoint Detection and Response Expert (on-premises) O componente não é compatível com os componentes Endpoint Detection and Response Expert (cloud) (`EDRCloud`) e Endpoint Detection and Response Optimum (`EDR`).
	`SB`	Kaspersky Sandbox ou KATA Sandbox. O *Kaspersky Sandbox* é uma solução independente de Detection and Response da Kaspersky. O *KATA Sandbox* é um componente da solução Kaspersky Anti Targeted Attack Platform.
	`MDR`	Managed Detection and Response
	`NDR`	Network Detection and Response (KATA) O componente não é compatível com os componentes Endpoint Detection and Response Expert (cloud) (`EDRCloud`) e Endpoint Detection and Response Optimum (`EDR`).
	`AdminKitConnector`	Gerenciamento de aplicativos usando sistemas de administração. Os sistemas de administração incluem, por exemplo, o Kaspersky Security Center. Além dos sistemas de administração da Kaspersky, você pode usar soluções de terceiros. O Kaspersky Endpoint Security fornece uma API para essa finalidade. Valores disponíveis: • `1` – Gerenciamento de aplicativos com a ajuda de sistemas de administração permitido (valor padrão). • `0` – Gerenciamento de aplicativos permitido apenas pela interface local.
	`KUMAIntegration`	Integração com KUMA.
	`StandaloneKATA`	Instalando o aplicativo no modo Endpoint Detection and Response Agent (EDR Agent) para integração com o Kaspersky Anti Targeted Attack Platform (EDR).
	`StandaloneMDR`	Instalando o aplicativo no modo Endpoint Detection and Response Agent (EDR Agent) para integração com o Kaspersky Managed Detection and Response.
	`StandaloneNDR`	Instalando o aplicativo no modo Endpoint Detection and Response Agent (EDR Agent) para integração com o Kaspersky Anti Targeted Attack Platform (NDR).
	`StandaloneSiemTelemetry`	Instalação do aplicativo no modo Endpoint Detection and Response Agent (EDR Agent) para integração com o KUMA.
`[Tasks]`	`ScanMyComputer`	Tarefa de Verificação Completa. Valores disponíveis: • `1` – a tarefa está incluída na lista de tarefas do Kaspersky Endpoint Security. • `0` – a tarefa não está incluída na lista de tarefas do Kaspersky Endpoint Security.
	`ScanCritical`	Tarefa de Verificação de Áreas Críticas. Valores disponíveis: • `1` – a tarefa está incluída na lista de tarefas do Kaspersky Endpoint Security. • `0` – a tarefa não está incluída na lista de tarefas do Kaspersky Endpoint Security.

Seção	Parâmetro	Descrição
	`Updater`	Tarefa de atualização. Valores disponíveis: • `1` – a tarefa está incluída na lista de tarefas do Kaspersky Endpoint Security. • `0` – a tarefa não está incluída na lista de tarefas do Kaspersky Endpoint Security.

Processos do Kaspersky Endpoint Security for Windows

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

Processos do Kaspersky Endpoint Security for Windows

Nome do arquivo	Finalidade
avp.exe	Processo de funcionamento do Kaspersky Endpoint Security for Windows.
avpsus.exe	Esse processo permite instalar e reverter atualizações críticas e aprovadas de módulos do aplicativo.

Alterar componentes do aplicativo

Durante a instalação do aplicativo, você pode selecionar os componentes que estarão disponíveis. Você pode alterar os componentes de aplicativos disponíveis das seguintes maneiras:

- Localmente, usando o Assistente de configuração.

  Componentes do aplicativo são modificados usando o método normal de um sistema operativo Windows, que é feito através do Painel de Controle. Execute o Assistente de configuração de aplicativos e selecione a opção para alterar os componentes de aplicativos disponíveis. Siga as instruções na tela.

  > Este método não estará disponível se o aplicativo tiver sido instalado por meio do Kaspersky Security Center. É possível alterar a seleção de componentes do aplicativo no Painel de Controle somente após instalar o aplicativo localmente.

- Uso remoto do Kaspersky Security Center.

  A tarefa *Alterar componentes do aplicativo* permite alterar os componentes do Kaspersky Endpoint Security depois que o aplicativo é instalado.

Leve em conta as seguintes considerações especiais ao alterar os componentes do aplicativo:

- Em computadores executando o Windows Server, você não pode instalar todos os componentes do Kaspersky Endpoint Security (por exemplo, o componente Controle Adaptativo de Anomalias não está disponível).

- Se os discos rígidos do seu computador estiverem protegidos pelo Criptografia completa do disco (FDE), você não poderá remover o componente Criptografia completa do disco. Para remover o componente Criptografia completa do disco, descriptografe todos os discos rígidos do computador.

- Se o computador tiver arquivos criptografados (FLE) ou se o usuário utilizar unidades removíveis criptografadas (FDE ou FLE), será impossível acessar os arquivos e as unidades removíveis depois que os componentes de Criptografia de dados forem removidos. Você pode acessar os arquivos e as unidades removíveis reinstalando os componentes de Criptografia de dados.

- Se o aplicativo for instalado no modo Light Agent em uma infraestrutura VDI, não há suporte para a alteração dos componentes do conjunto.

Como adicionar ou remover componentes de aplicativos no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **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

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Selecione componentes para instalar**.

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

Selecionar as configurações do aplicativo:

- **Modo Standard para proteger hosts**. A configuração padrão. Essa configuração permite usar todos os componentes do aplicativo, inclusive os componentes que fornecem suporte para as soluções de Detection and Response. Essa configuração é usada para a proteção abrangente do computador contra diversas ameaças, ataques de rede e fraudes.

- **Endpoint Detection and Response Agent para garantir a proteção contra ameaças avançadas e ataques direcionados**. Nesta configuração, é possível instalar apenas os componentes que fornecem suporte para as soluções Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), assim como KUMA. Essa configuração será necessária caso uma Endpoint Protection Platform (EPP) de terceiros seja implantada na sua organização juntamente com uma solução Kaspersky Detection and Response. Isso torna o Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent compatível com os aplicativos EPP de terceiros.

  Ao alterar a configuração do aplicativo para que o EDR Agent funcione com o MDR, certifique-se de que os componentes responsáveis pelo recebimento de telemetria estejam ativados.

- **Light Agent para garantir a proteção em ambientes virtuais**. Essa configuração destina-se ao aplicativo usado como parte da solução do Kaspersky Security for Virtualization Light Agent. O Light Agent deve ser instalado em cada máquina virtual que precisa ser protegida pela solução. Nessa configuração, não é possível usar componentes de criptografia de dados ou o Controle Adaptativo de Anomalias. Se estiver instalando o Light Agent em um modelo de máquina virtual que será usado para criar *máquinas virtuais não persistentes*, marque a caixa de seleção **Proteger infraestrutura VDI** (VDI significa Virtual Desktop Infrastructure). O modo de proteção VDI ajuda a otimizar o desempenho do Kaspersky Endpoint Security em máquinas virtuais não persistentes. Nesse modo, o Light Agent recusa as atualizações do aplicativo que exigem a reinicialização da máquina virtual. Ao receber atualizações do aplicativo que exijam uma reinicialização, o Light Agent gerará um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas.

Selecione os componentes do aplicativo que estarão disponíveis no computador do usuário.

Etapa 3. Configurações avançadas

Defina as configurações avançadas para a tarefa (consulte a tabela abaixo).

Etapa 4. 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 5. Configurar um agendamento de início de tarefa

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

Etapa 6. Definir o nome da tarefa

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

Etapa 7. Concluir a criação da tarefa

Conclua o 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 adicionar ou remover componentes de aplicativos no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2.0**.
2. Na lista suspensa **Tipo de tarefa**, selecione **Alterar componentes do aplicativo**.
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

Marque a caixa de seleção **Abrir detalhes da tarefa quando a criação for concluída** e conclua o assistente.

Nas propriedades da tarefa, selecione a guia **Configurações do aplicativo**. Em seguida, selecione a configuração do aplicativo:

- **Modo Standard para proteger estações de trabalho e servidores**. A configuração padrão. Essa configuração permite usar todos os componentes do aplicativo, inclusive os componentes que fornecem suporte para as soluções de Detection and Response. Essa configuração é usada para a proteção abrangente do computador contra diversas ameaças, ataques de rede e fraudes.

- **Endpoint Detection and Response Agent para garantir a proteção contra ameaças avançadas e ataques direcionados**. Nesta configuração, é possível instalar apenas os componentes que fornecem suporte para as soluções Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), assim como KUMA. Essa configuração será necessária caso uma Endpoint Protection Platform (EPP) de terceiros seja implantada na sua organização juntamente com uma solução Kaspersky Detection and Response. Isso torna o Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent compatível com os aplicativos EPP de terceiros.

  Ao alterar a configuração do aplicativo para que o EDR Agent funcione com o MDR, certifique-se de que os componentes responsáveis pelo recebimento de telemetria estejam ativados.

- **Light Agent para garantir a proteção em ambientes virtuais**. Essa configuração destina-se ao aplicativo usado como parte da solução do Kaspersky Security for Virtualization Light Agent. O Light Agent deve ser instalado em cada máquina virtual que precisa ser protegida pela solução. Nessa configuração, não é possível usar componentes de criptografia de dados ou o Controle Adaptativo de Anomalias. Se estiver instalando o Light Agent em um modelo de máquina virtual que será usado para criar *máquinas virtuais não persistentes*, marque a caixa de seleção **Proteger infraestrutura VDI** (VDI significa Virtual Desktop Infrastructure). O modo de proteção VDI ajuda a otimizar o desempenho do Kaspersky Endpoint Security em máquinas virtuais não persistentes. Nesse modo, o Light Agent recusa as atualizações do aplicativo que exigem a reinicialização da máquina virtual. Ao receber atualizações do aplicativo que exijam uma reinicialização, o Light Agent gerará um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas.

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 Endpoint Security nos computadores dos usuários será modificado no modo silencioso. As configurações dos componentes disponíveis serão exibidas na interface local do aplicativo. Os componentes que não estiverem incluídos no aplicativo estão desativados e as configurações desses componentes não estão disponíveis.

Ao instalar, atualizar ou desinstalar o Kaspersky Endpoint Security, podem ocorrer erros. Para obter mais informações sobre como solucionar esses erros, consulte a Base de Conhecimento do Suporte Técnico.

Parâmetro	Descrição
Configurações da tarefa	**Verificar se há aplicativos incompatíveis de terceiros**. Por padrão, o Kaspersky Endpoint Security verifica a compatibilidade dos aplicativos instalados. A lista de software que pode causar problemas de compatibilidade está disponível no arquivo incompatible.txt. O arquivo está incluído no kit de distribuição. Caso a verificação do software instalado esteja ativada, quando um aplicativo da lista for detectado, o Kaspersky Endpoint Security interromperá a tarefa. É possível desativar a verificação do software instalado se a documentação do fornecedor do software de terceiros solicitar compatibilidade com a Endpoint Protection Platform (EPP). **Remover aplicativos incompatíveis de terceiros**. Remoção automática de aplicativos da lista incompatible.txt antes de alterar o conjunto de componentes. Caso esta funcionalidade esteja ativada, o Kaspersky Endpoint Security tentará remover os aplicativos que podem causar problemas de compatibilidade para continuar a tarefa. **Usar o modo de compatibilidade do Azure WVD**. Esse recurso garante a exibição correta do estado das máquinas virtuais Azure no console do Kaspersky Anti Targeted Attack Platform. Para monitorar o desempenho do computador, o Kaspersky Endpoint Security envia telemetria aos servidores da KATA. A telemetria inclui um ID do computador (Sensor ID). O modo de compatibilidade do Azure WVD permite atribuir um Sensor ID exclusivo e permanente para essas máquinas virtuais. Caso o modo de compatibilidade esteja desativado, o Sensor ID poderá mudar depois que o computador for reiniciado devido ao funcionamento das máquinas virtuais do Azure. Isso pode fazer com que máquinas virtuais duplicadas apareçam no console.
Exclusões	A partir do Kaspersky Endpoint Security 12.6 for Windows, as exclusões de verificação e aplicativos confiáveis são adicionadas na zona confiável. As exclusões predefinidas de verificação e aplicativos confiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, Microsoft Exchange e System Center Configuration Manager. Isso significa que não será necessário configurar manualmente uma zona confiável para o aplicativo nos servidores. A partir do Kaspersky Endpoint Security 12.8 for Windows, é possível instalar o aplicativo no modo Light Agent para proteger ambientes virtuais. Exclusões de verificação e aplicativos confiáveis predefinidos podem ajudar a configurar rapidamente o Kaspersky Endpoint Security em ambientes virtuais Citrix e VMware. Também é possível configurar a zona confiável mais tarde nas propriedades da política: exclusões de verificação e aplicativos confiáveis.
Modo separado / Modo combinado	É possível criar conjuntos separados de componentes para estações de trabalho e servidores: **Modo separado**. Antes de implementar o pacote de instalação, o instalador detecta o tipo de sistema operacional e instala somente os componentes do aplicativo selecionados para esse tipo de sistema operacional. Dessa forma, pode-se usar o mesmo pacote de instalação para estações de trabalho e servidores. O **Modo combinado** oferece uma lista comum de componentes para estações de trabalho e servidores. A disponibilidade de componentes individuais depende do tipo de sistema operacional. Nesse modo, recomendamos criar um pacote de instalação separado para estações de trabalho e um pacote de instalação separado para servidores. É possível configurar a lista comum de componentes no pacote de instalação somente no modo Standard.
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 Endpoint 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.
Use a senha para desinstalar o Kaspersky Endpoint Agent e o Kaspersky Security for Windows Server	Geralmente, os administradores ativam a proteção por senha nas configurações dessas tarefas para restringir o acesso ao Kaspersky Endpoint Agent (KEA) e Kaspersky Security for Windows Server (KSWS). Ou seja, caso esteja migrando da configuração [KES+KEA] para [KES+agente integrado] ou caso esteja migrando de KSWS para KES, será necessário inserir uma senha para remover esses aplicativos.

Upgrade de uma versão anterior do aplicativo

Quando você atualiza uma versão anterior do aplicativo para uma versão mais recente, considere o seguinte:

- Recomendamos que você encerre todos os aplicativos ativos antes de iniciar a atualização.
- Antes de atualizar, o Kaspersky Endpoint Security bloqueia a funcionalidade de Criptografia Completa do Disco. Se não for possível bloquear a Criptografia Completa do Disco, a instalação da atualização não será inicializada. Depois de atualizar o aplicativo, a funcionalidade de Criptografia Completa do Disco será restaurada.
- Para alterar o idioma do aplicativo, na tarefa *Instalar o aplicativo remotamente*, selecione o pacote de instalação com a localização desejada e atualize o aplicativo. A opção de alterar o idioma do aplicativo foi disponibilizada pela primeira vez no Kaspersky Endpoint Security for Windows 14.2.

O Kaspersky Endpoint Security suporta atualizações para as seguintes versões do aplicativo:

- Kaspersky Endpoint Security 12.3 for Windows (compilação 12.3.0.493)
- Kaspersky Endpoint Security 12.4 for Windows (compilação 12.4.0.467)
- Kaspersky Endpoint Security 12.5 for Windows (compilação 12.5.0.539)
- Kaspersky Endpoint Security 12.6 for Windows (compilação 12.6.0.438)
- Kaspersky Endpoint Security 12.7 for Windows (compilação 12.7.0.533)
- Kaspersky Endpoint Security 12.8 for Windows (compilação 12.8.0.505)
- Kaspersky Endpoint Security 12.9 for Windows (compilação 12.9.0.384)
- Kaspersky Endpoint Security 12.10 for Windows (compilação 12.10.0.466)
- Kaspersky Endpoint Security 12.11 for Windows (compilação 12.11.0.637)
- Kaspersky Endpoint Security 12.12 for Windows (compilação 12.12.0.522)
- Kaspersky Endpoint Security 14.0 for Windows (compilação 14.0.0.504)
- Kaspersky Endpoint Security 14.1 for Windows (compilação 14.1.0.423)

Ao instalar, atualizar ou desinstalar o Kaspersky Endpoint Security, podem ocorrer erros. Para obter mais informações sobre como solucionar esses erros, consulte a Base de Conhecimento do Suporte Técnico.

Métodos de atualização do aplicativo

O Kaspersky Endpoint Security pode ser atualizado no computador de vários modos:

- Uso do serviço de atualização da Kaspersky (Seamless Update – SMU).
- localmente, usando o Assistente de configuração.
- localmente a partir da linha de comando.
- Uso remoto do Kaspersky Security Center.
- remotamente, por meio do Editor de Gerenciamento de Política de Grupo do Microsoft Windows (para obter mais detalhes, consulte o site do Suporte Técnico da Microsoft).
- remotamente, usando o System Center Configuration Manager.

Se o aplicativo implantado na rede corporativa tiver um conjunto de componentes diferente do conjunto padrão, a atualização do aplicativo por meio do Console de Administração (MMC) será diferente da atualização por meio do Web Console. Ao atualizar o Kaspersky Endpoint Security, considere o seguinte:

- Kaspersky Security Center Web Console.

  Se você criou um pacote de instalação para a nova versão do aplicativo com o conjunto de componentes padrão, o conjunto de componentes no computador do usuário não será alterado. Para usar o Kaspersky Endpoint Security com o conjunto de componentes padrão, é necessário abrir as propriedades do pacote de instalação, alterar o conjunto de componentes e reverter para o conjunto original de componentes e salvar as alterações.

- Console de Administração do Kaspersky Security Center.

  O conjunto de componentes do aplicativo após a atualização corresponderá ao conjunto de componentes no pacote de instalação. Ou seja, se a nova versão do aplicativo tiver o conjunto padrão de componentes, por exemplo, o agente integrado do MDR será removido do computador, pois esse componente não faz parte do conjunto padrão. Para continuar usando o aplicativo com o mesmo conjunto de componentes que antes da atualização, selecione os componentes necessários nas configurações do pacote de instalação.

Atualizar o aplicativo sem reiniciar

A atualização do aplicativo sem reiniciar fornece operação ininterrupta do servidor quando a versão do aplicativo é atualizada.

A atualização do aplicativo sem reinicialização tem as seguintes limitações:

- É possível atualizar o aplicativo sem reiniciar a partir da versão 11.10.0. Para atualizar uma versão anterior do aplicativo, é necessário reiniciar o computador.

- É possível instalar patches sem reiniciar a partir da versão 11.11.0. Para instalar patches para as versões anteriores do aplicativo, pode ser necessário reiniciar o computador.

- A atualização do aplicativo sem reinicialização não está disponível em computadores com criptografia de dados habilitada (criptografia Kaspersky (FDE), BitLocker, Criptografia em Nível de Arquivo (FLE)). Para atualizar o aplicativo em computadores com criptografia de dados habilitada, o computador deve ser reiniciado.

- O aplicativo não pode ser atualizado em uma máquina virtual sem reinicialização. Para atualizar o aplicativo em uma máquina virtual, é necessário reiniciar a máquina virtual.

Depois de atualizar o aplicativo, instalar um patch, alterar o conjunto de componentes de aplicativos ou restaurar, o Kaspersky Endpoint Security será reiniciado para começar a usar a nova versão. A reinicialização do Kaspersky Endpoint Security pode levar até um minuto. Durante este tempo, o nível da proteção do computador é reduzido. A reinicialização do aplicativo restaura o nível de proteção do computador.

Como selecionar o modo de atualização do aplicativo no Console de administração (MMC)

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

2. Na árvore do console, selecione **Políticas**.

3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

4. Na janela da política, selecione **Configurações gerais** → **Configurações de aplicativos**.

5. No bloco **Configurações avançadas**, selecione ou limpe a caixa de seleção **Instalar atualizações do aplicativo sem reinicialização** para configurar o modo de atualização do aplicativo.

6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como selecionar o modo de atualização do aplicativo no Web Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Interação com o usuário**.

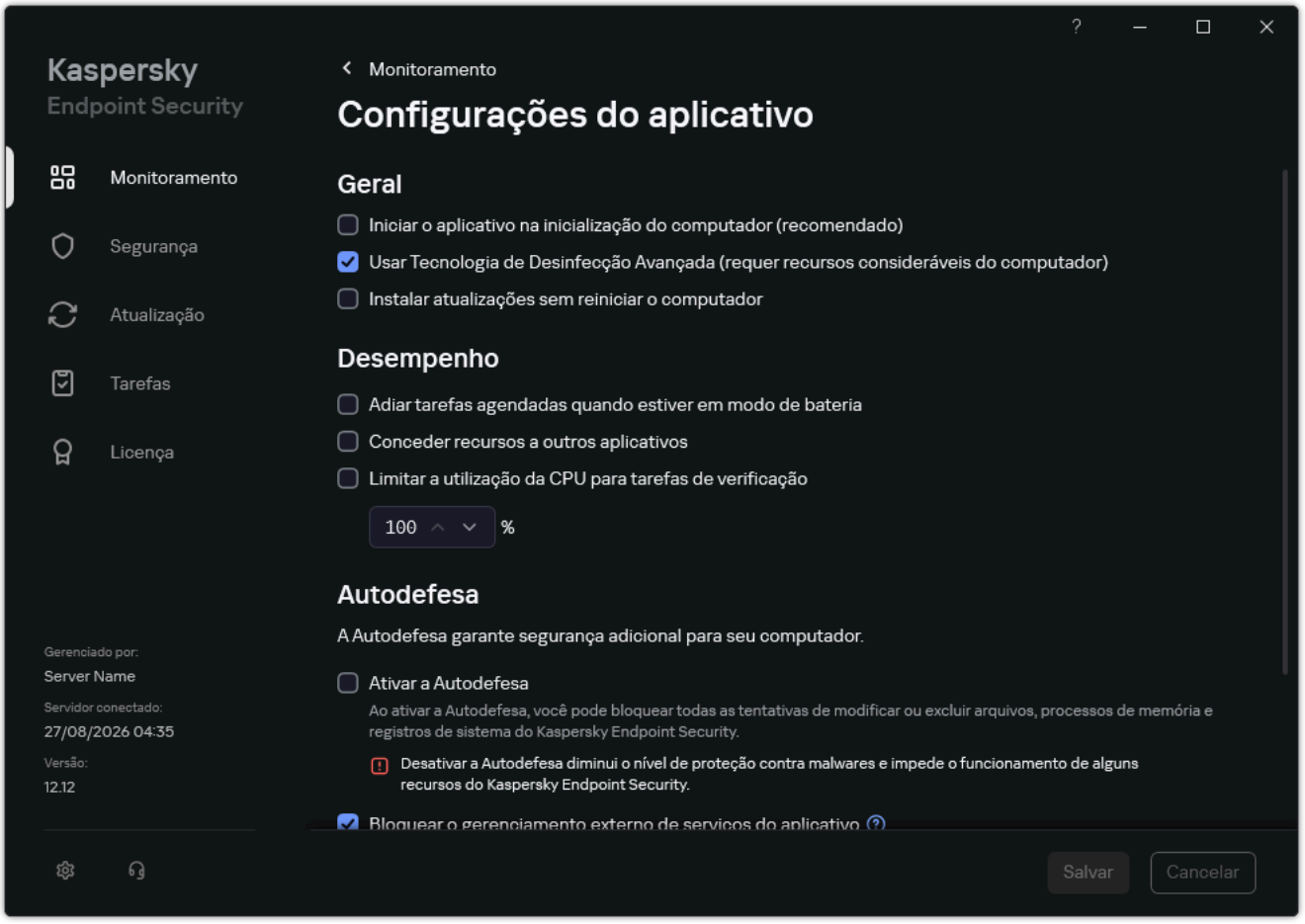
5. No bloco **Configurações de atualização do aplicativo**, selecione ou limpe a caixa de seleção **Instalar atualizações do aplicativo sem reinicialização** para configurar o modo de atualização do aplicativo.

6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como selecionar o modo de atualização do aplicativo na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações do aplicativo**.



Configurações do Kaspersky Endpoint Security for Windows

3. No bloco **Geral**, selecione ou limpe a caixa de seleção **Instalar atualizações sem reiniciar o computador** para configurar o modo de atualização do aplicativo.

4. Salvar alterações.

Você também pode selecionar o modo de atualização do aplicativo ao instalar o aplicativo pela linha de comando (usando a opção `UPGRADEMODE`).

Após a conclusão do procedimento de atualização do aplicativo sem reinicialização, a nova versão do Kaspersky Endpoint Security estará instalada no computador. A versão anterior do aplicativo será excluída automaticamente.

Não é possível iniciar uma atualização de aplicativo antes da conclusão completa da atualização anterior.

É possível verificar o status da atualização do Kaspersky Endpoint Security usando o relatório de versão do aplicativo da Kaspersky, no console do Kaspersky Security Center.

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 Endpoint Security recebe a nova versão do aplicativo junto com os bancos de dados 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.

Você pode gerenciar a atualização do SMU do aplicativo usando a 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 antivírus, você deve permitir a atualização dos *módulos do aplicativo* nas configurações da tarefa *Atualização de bancos de dados e módulos do aplicativo*. Também nas configurações da tarefa *Atualização de bancos de dados e módulos do aplicativo*, você pode permitir a atualização do aplicativo sem reiniciar.

Etapas de uma atualização do SMU do aplicativo

1. **Após o lançamento de uma nova versão do aplicativo, a Kaspersky distribui a atualização.**

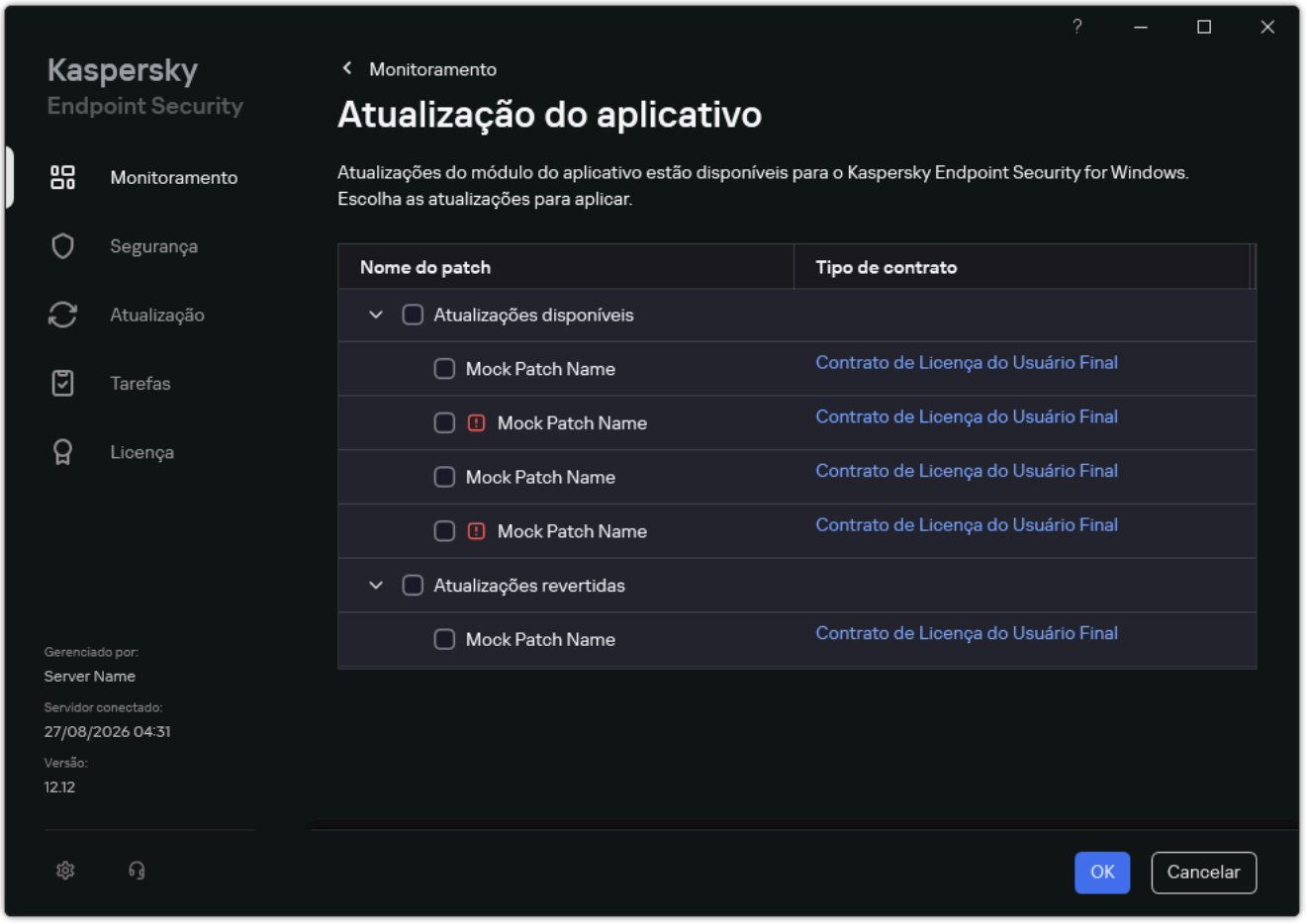
2. **O usuário aprova a atualização do aplicativo.**

   Se o computador estiver conectado ao Kaspersky Security Center, a atualização estará disponível no Kaspersky Security Center, na seção **Atualização de bancos de dados e módulos de aplicativos Kaspersky**. Para obter mais detalhes sobre como aprovar atualizações, consulte a Ajuda do Kaspersky Security Center.

   Se o computador não estiver conectado ao Kaspersky Security Center, a atualização estará disponível na seção de notificação da interface do aplicativo: . Para aprovar a atualização, selecione uma versão do aplicativo e aceite os termos e condições dos acordos (consulte a figura abaixo).

3. **O Kaspersky Endpoint Security executa a tarefa *Atualização de bancos de dados e módulos do aplicativo* de acordo com o agendamento configurado.**

Como resultado, o Kaspersky Endpoint Security atualiza o aplicativo no modo "silencioso".



Atualizações de aplicativos disponíveis

Remoção do aplicativo

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

Ao instalar, atualizar ou desinstalar o Kaspersky Endpoint Security, podem ocorrer erros. Para obter mais informações sobre como solucionar esses erros, consulte a Base de Conhecimento do Suporte Técnico.

Removendo o aplicativo remotamente pelo Kaspersky Security Center

Você pode desinstalar remotamente o aplicativo usando a tarefa *Desinstalar aplicativo remotamente*. Ao executar a tarefa, o Kaspersky Endpoint Security baixa o utilitário de desinstalação do aplicativo para o computador do usuário. Após concluir a desinstalação do aplicativo, o utilitário será removido automaticamente.

Como remover o aplicativo através do Console de administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Tarefas**.

   A lista de tarefas é aberta.
3. Clique **Nova tarefa**.

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

Etapa 1. Selecionar o tipo de tarefa

Selecione **Servidor de Administração do Kaspersky Security Center** → **Avançado** → **Desinstalar aplicativo remotamente**.

Etapa 2. Seleção do aplicativo a ser removido

Selecione **Desinstalar o aplicativo compatível com o Kaspersky Security Center**.

Etapa 3. Configurações da tarefa para desinstalação do aplicativo

Selecione **Kaspersky Endpoint Security for Windows (14.2)**.

Etapa 4. Desinstalar configurações do utilitário

Defina as seguintes configurações adicionais do aplicativo:

- **Forçar download do utilitário de desinstalação**. Selecione o método de entrega do utilitário:
  - **Usando o Agente de Rede**. Se o Agente de Rede não tiver sido instalado no computador, o primeiro Agente de Rede será instalado usando as ferramentas do sistema operacional. Em seguida, o Kaspersky Endpoint Security será desinstalado pelas ferramentas do Agente de Rede.
  - **Usando recursos do sistema operacional através do Servidor de Administração**. O utilitário será entregue aos computadores clientes usando recursos do sistema operacional através do servidor de administração. Você pode selecionar esta opção se o Agente de Rede não estiver instalado no computador cliente, mas o computador cliente estiver na mesma rede que o Servidor de Administração.
  - **Usando recursos do sistema operacional através de pontos de distribuição**. O utilitário é entregue aos computadores clientes usando recursos do sistema operacional através de pontos de distribuição. Você poderá selecionar esta opção se houver pelo menos um ponto de distribuição na rede. Para obter mais detalhes sobre os pontos de distribuição, consulte a ajuda do Kaspersky Security Center.
- **Verificar o tipo do sistema operacional antes de baixar**. Se necessário, desmarque esta caixa de seleção. Isso permite que você impeça o download do utilitário de desinstalação se o sistema operacional do computador não atender aos requisitos de software. Se tiver certeza de que o sistema operacional do computador atende aos requisitos de software, você pode ignorar essa verificação.

Se a operação de desinstalação do aplicativo estiver protegida por senha, faça o seguinte:

1. Marque a caixa de seleção **Usar senha de desinstalação**.
2. Clique no botão **Editar**.
3. Digite a senha da conta KLAdmin.

Etapa 5. Selecionar a configuração de reinicialização do sistema operacional

Após a desinstalação do aplicativo, é necessário reiniciar. Selecione a ação que será executada para reiniciar o computador.

Etapa 6. 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 7. Seleção da conta para executar a tarefa

Selecione a conta para instalar o Agente de rede usando as ferramentas do sistema operacional. Neste caso, os direitos de administrador são necessários para acessar o computador. Você pode adicionar várias contas. Se uma conta não tiver direitos suficientes, o Assistente de Instalação usará a próxima conta. Se você desinstalar o Kaspersky Endpoint Security usando as ferramentas do Agente de Rede, não precisará selecionar uma conta.

Etapa 8. Configurar um agendamento de início de tarefa

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

Etapa 9. Definir o nome da tarefa

Digite um nome para a tarefa, por exemplo, *Remover Kaspersky Endpoint Security 14.2*.

Etapa 10. Encerrar a criação da tarefa

Conclua o 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.

A aplicação será desinstalada no modo silencioso.

Como remover aplicativos por meio do Web Console e do Cloud Console

1. Na janela principal do Web Console, selecione **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 Security Center**.

2. Na lista suspensa **Tipo de tarefa**, selecione **Desinstalar aplicativo remotamente**.

3. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Desinstalar o Kaspersky Endpoint Security dos computadores de suporte técnico*.

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. Definir as configurações de desinstalação do aplicativo

Nesta etapa, defina as configurações de desinstalação do aplicativo:

1. Selecione o tipo de **Desinstalar o aplicativo gerenciado**.

2. Selecione **Kaspersky Endpoint Security for Windows**.

3. **Forçar download do utilitário de desinstalação**. Selecione o método de entrega do utilitário:

   - **Usando o Agente de Rede**. Se o Agente de Rede não tiver sido instalado no computador, o primeiro Agente de Rede será instalado usando as ferramentas do sistema operacional. Em seguida, o Kaspersky Endpoint Security será desinstalado pelas ferramentas do Agente de Rede.

   - **Usando recursos do sistema operacional através do Servidor de Administração**. O utilitário será entregue aos computadores clientes usando recursos do sistema operacional através do servidor de administração. Você pode selecionar esta opção se o Agente de Rede não estiver instalado no computador cliente, mas o computador cliente estiver na mesma rede que o Servidor de Administração.

   - **Usando recursos do sistema operacional através de pontos de distribuição**. O utilitário é entregue aos computadores clientes usando recursos do sistema operacional através de pontos de distribuição. Você poderá selecionar esta opção se houver pelo menos um ponto de distribuição na rede. Para obter mais detalhes sobre os pontos de distribuição, consulte a ajuda do Kaspersky Security Center.

4. No campo **Número máximo de downloads concomitantes**, defina um limite para o número de solicitações enviadas ao Servidor de administração para baixar o utilitário de desinstalação do aplicativo. Um limite para o número de solicitações ajudará a impedir sobrecarga da rede.

5. No campo **Número máximo de tentativas de desinstalação**, defina um limite para o número de tentativas de desinstalar o aplicativo. Se a desinstalação do Kaspersky Endpoint Security terminar com um erro, a tarefa reiniciará a remoção automaticamente.

6. Caso seja necessário, desmarque a caixa de seleção **Verificar o tipo do sistema operacional antes de baixar**. Isso permite que você impeça o download do utilitário de desinstalação se o sistema operacional do computador não atender aos requisitos de software. Se tiver certeza de que o sistema operacional do computador atende aos requisitos de software, você pode ignorar essa verificação.

Etapa 4. Seleção da conta para executar a tarefa

Selecione a conta para instalar o Agente de rede usando as ferramentas do sistema operacional. Neste caso, os direitos de administrador são necessários para acessar o computador. Você pode adicionar várias contas. Se uma conta não tiver direitos suficientes, o Assistente de Instalação usará a próxima conta. Se você desinstalar o Kaspersky Endpoint Security usando as ferramentas do Agente de Rede, não precisará selecionar uma conta.

Etapa 5. Concluir a criação da tarefa

Finalize o assistente, clicando no botão **Concluir**. Uma nova tarefa será exibida na lista de tarefas.

Para executar uma tarefa, marque a caixa de seleção ao lado da tarefa e clique no botão **Iniciar**. A aplicação será desinstalada no modo silencioso. Após a conclusão da desinstalação, o Kaspersky Endpoint Security solicita que o computador seja reiniciado.

Se a operação de desinstalação do aplicativo estiver protegida por senha, digite a senha da conta KLAdmin nas propriedades da tarefa *Desinstalar aplicativo remotamente*. Sem a senha, a tarefa não será executada.

Para usar a senha da conta KLAdmin na tarefa Desinstalar aplicativo remotamente:

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Tarefas**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Desinstalar aplicativo remotamente** do Kaspersky Security Center.

   A janela de propriedades da tarefa é exibida.

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

4. Marque a caixa de seleção **Usar senha de desinstalação**.

5. Digite a senha da conta KLAdmin.

6. Salvar alterações.

Reinicie o computador para concluir a desinstalação. Para fazer isso, o Agente de Rede exibe uma janela pop-up.

Removendo o aplicativo remotamente usando o Active Directory

É possível desinstalar remotamente o aplicativo usando uma política de grupo do Microsoft Windows. Para desinstalar o aplicativo, é preciso abrir o Console de Gerenciamento de Política de Grupo (gpmc.msc) e usar o Editor de Política de Grupo para criar uma tarefa de remoção de aplicativo (para obter mais detalhes, visite o site de suporte técnico da Microsoft).

Se a operação de desinstalação do aplicativo estiver protegida por senha, é necessário fazer o seguinte:

1. Crie um arquivo BAT com o seguinte conteúdo:

   ```
   msiexec.exe /x<GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
   ```

   `<GUID>` é o identificador exclusivo do aplicativo. É possível descobrir o GUID do aplicativo na Base de Dados de Conhecimento do Suporte Técnico ou por meio do uso do seguinte comando:

   ```
   wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
   ```

   Exemplo

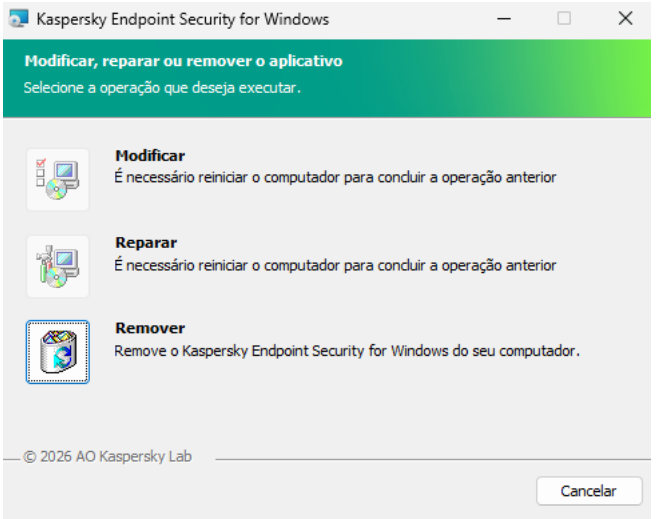
   ```
   msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
   ```

2. Crie uma nova política do Microsoft Windows para os computadores no Console de Gerenciamento do Grupo de Política (gpmc.msc).

3. Use a nova política para executar o arquivo BAT criado nos computadores.

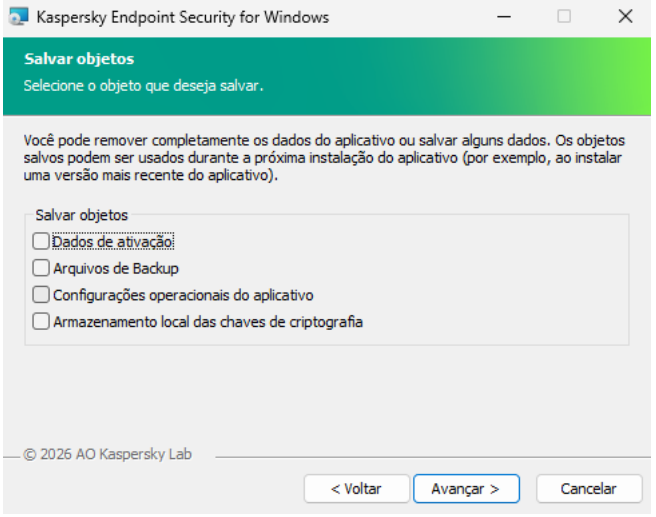
Remover o aplicativo localmente

É possível remover o aplicativo localmente usando o Assistente de instalação. O Kaspersky Endpoint Security é removido usando o método normal para um sistema operativo Windows, que é feito através do Painel de Controle. O assistente de Instalação é iniciado. Siga as instruções na tela.



Seleção da operação de remoção do aplicativo

Você pode especificar quais dados usados pelo aplicativo você deseja salvar para uso futuro, durante a próxima instalação do aplicativo (como quando fizer um upgrade para uma versão mais recente do aplicativo). Se você não especificar nenhum dado, o aplicativo será completamente removido (veja a figura abaixo).



Salvar dados após a remoção

Você pode salvar os seguintes dados:

- **Dados de ativação**, evita a ativação do aplicativo novamente. O Kaspersky Endpoint Security adiciona automaticamente uma chave de licença se o prazo de licença não tiver expirado antes da instalação.
- **Arquivos de Backup** – arquivos que são verificados pelo aplicativo e colocados em uma cópia de segurança.

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

Para usar os objetos de Backup após remoção do aplicativo, será necessário restaurar esses objetos antes de remover o aplicativo. No entanto, os especialistas da Kaspersky não recomendam restaurar objetos do Backup, pois isso poderá danificar o computador.

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

- **Armazenamento local das chaves de criptografia** – dados que fornecem acesso a arquivos e unidades que foram criptografados antes da remoção do aplicativo. Para garantir o acesso a arquivos e unidades criptografadas, certifique-se de selecionar a funcionalidade criptografia de dados ao reinstalar o Kaspersky Endpoint Security. Nenhuma outra ação é necessária para acessar arquivos e unidades criptografados anteriormente.

O Kaspersky Endpoint Security salva os dados na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

Também é possível excluir o aplicativo localmente usando a linha de comando.

Licenciamento do aplicativo

Esta seção fornece informações sobre os conceitos gerais relacionados à licença do Kaspersky Endpoint Security.

Sobre o Contrato de Licença do Usuário Final

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

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

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

- Quando instalar o Kaspersky Endpoint Security no modo interativo.
- Lendo o arquivo license.txt. Este documento está incluído no kit de distribuição de aplicativos e também está localizado na pasta de instalação do aplicativo `%ProgramFiles(x86)%\Kaspersky Lab\KES\Doc\<locale>\KES`.

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

Sobre a licença

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

A licença permite o uso do aplicativo de acordo com os termos do Contrato de Licença de Usuário Final e o recebimento de suporte técnico. A lista de recursos disponíveis e os termos de uso do aplicativo dependem do tipo da licença sob a qual o aplicativo foi ativado.

Os seguintes tipos de licença são disponibilizados:

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

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

  O aplicativo só pode ser ativado uma vez usando uma licença de avaliação. O aplicativo não pode ser ativado para uma licença de avaliação depois de ter sido ativado com uma licença comercial.

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

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

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

Sobre o certificado da licença

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

O certificado de licença contém as seguintes informações de licença:

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

Sobre a assinatura

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

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

Quando uma assinatura limitada expira, você pode receber um período de carência de renovação de assinatura durante o qual o aplicativo continua funcionando. A disponibilidade e a duração de tal período de carência são decididas pelo provedor de serviços.

Para usar o Kaspersky Endpoint Security com assinatura, você deve aplicar o código de ativação recebido do provedor do serviço. Após aplicar o código de ativação, a chave ativa é adicionada. A chave ativa define a licença para uso do aplicativo sob a assinatura. Não é possível ativar o aplicativo com a assinatura usando um arquivo de chave. O provedor de serviços só pode oferecer um código de ativação. Não é possível adicionar uma chave reserva sob uma assinatura.

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

Sobre chave de licença

Uma *chave de licença* é uma sequência de bits que você pode usar para ativar e usar o aplicativo de acordo com os termos do Contrato de Licença do Usuário Final.

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

É possível adicionar uma chave de licença ao aplicativo ao aplicar um arquivo de chave ou inserir um código de ativação.

A chave pode ser bloqueada pela Kaspersky se os termos do Contrato de Licença do Usuário Final forem violados. Se a chave foi bloqueada, você terá de adicionar uma chave diferente para continuar a usar o aplicativo.

Há dois tipos de chaves: ativa e reserva.

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

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

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

Se uma chave for adicionada à lista de chaves proibidas, a funcionalidade do aplicativo definida pela licença usada para ativar o aplicativo permanecerá disponível por oito dias. O aplicativo notifica o usuário de que a chave foi adicionada à lista de chaves proibidas. Após oito dias, a funcionalidade do aplicativo fica limitada ao nível de funcionalidade disponível após o vencimento da licença. Você pode usar componentes de proteção e controle e executar uma verificação usando os bancos de dados do aplicativo que foram instalados antes da expiração da licença. O aplicativo também continua a criptografar arquivos que foram modificados e criptografados antes da expiração da licença, mas não criptografará novos arquivos. O uso do Kaspersky Security Network não está disponível.

Sobre o código de ativação

Um *código de ativação* é uma sequência exclusiva de 20 caracteres alfanuméricos. Você insere um código de ativação para adicionar uma chave de licença que ativa o Kaspersky Endpoint Security. Você recebe um código de ativação no endereço de e-mail especificado após a compra do Kaspersky Endpoint Security.

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

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

Se o código de ativação tiver sido perdido após a ativação do aplicativo, você pode restaurar o código de ativação. Pode ser necessário um código de ativação, por exemplo, para registrar uma Kaspersky CompanyAccount. Caso o código de ativação tenha sido perdido após a ativação do aplicativo, entre em contato com o parceiro da Kaspersky com quem a licença foi comprada.

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 fornecido quando comprou o Kaspersky Endpoint Security ou solicitou a versão de avaliação do Kaspersky Endpoint Security.

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

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

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

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

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

Comparação da funcionalidade do aplicativo dependendo do tipo de licença para estações de trabalho

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

Consulte também a comparação das funcionalidades do aplicativo para servidores

Consulte a comparação das funcionalidades do aplicativo, dependendo do tipo de licença do Kaspersky Next na Ajuda do Kaspersky Next.

Comparação de recursos do Kaspersky Endpoint Security

Recurso	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Proteção Avançada Contra Ameaças								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Detecção de Comportamento	✓	✓	✓	✓	✓	✓	✓	✓
Anticryptor	✓	✓	✓	✓	✓	✓	✓	✓
Prevenção de Exploits	✓	✓	✓	✓	✓	✓	✓	✓
Prevenção de Intrusão do Host	✓	✓	✓	✓	✓	✓	✓	✓
Mecanismo de Remediação	✓	✓	✓	✓	✓	✓	✓	✓
Proteção Essencial Contra Ameaças								
Proteção Contra Ameaças ao Arquivo	✓	✓	✓	✓	✓	✓	✓	✓
Proteção Contra Ameaças da Web	✓	✓	✓	✓	✓	✓	✓	✓
Proteção Contra Ameaças ao Correio	✓	✓	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓	✓	✓
Proteção Contra Ameaças à Rede	✓	✓	✓	✓	✓	✓	✓	✓
Prevenção contra ataque BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
Proteção AMSI	✓	✓	✓	✓	✓	✓	✓	✓
Controles de Segurança								

Recurso	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Inspeção do Log	–	–	–	–	–	–	–	–
Controle de aplicativos	✓	✓	✓	✓	✓	✓	✓	✓
Controle de dispositivos	✓	✓	✓	✓	✓	✓	✓	✓
Controle da Web	✓	✓	✓	✓	✓	✓	✓	✓
Controle Adaptativo de Anomalias	–	✓	✓	✓	✓	✓	–	✓
Monitor de integridade do sistema	–	–	–	–	–	–	–	–
Criptografia de Dados								
Kaspersky Disk Encryption	–	✓	✓	✓	✓	✓	–	✓
Criptografia de Unidade de Disco BitLocker	–	✓	✓	✓	✓	✓	–	✓
Criptografia em Nível de Arquivo	–	✓	✓	✓	✓	✓	–	✓
Criptografia de unidades removíveis	–	✓	✓	✓	✓	✓	–	✓
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(A licença do Kaspersky Sandbox deve ser adquirida separadamente)*	✓	✓	✓	✓	✓	✓	✓	✓
Integração com KUMA *(a licença para a integração KUMA deve ser adquirida separadamente)*	✓	✓	✓	✓	✓	✓	✓	✓
Modo Light Agent *(para ativar o aplicativo, é necessário adicionar uma chave de licença no SVM ao qual o Light Agent está conectado)*	–	–	–	–	–	–	✓	✓

Comparação da funcionalidade do aplicativo dependendo do tipo de licença para servidores

O conjunto de funcionalidades do Kaspersky Endpoint Security disponível nos servidores depende do tipo de licença (consulte a tabela abaixo).

Consulte também a comparação das funcionalidades do aplicativo para estações de trabalho

Consulte a comparação das funcionalidades do aplicativo, dependendo do tipo de licença do Kaspersky Next na Ajuda do Kaspersky Next.

Comparação de recursos do Kaspersky Endpoint Security

Recurso	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Proteção Avançada Contra Ameaças								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Detecção de Comportamento	✓	✓	✓	✓	✓	✓	✓	✓
Anticryptor	✓	✓	✓	✓	✓	✓	✓	✓
Prevenção de Exploits	✓	✓	✓	✓	✓	✓	✓	✓
Prevenção de Intrusão do Host	–	–	–	–	–	–	–	–
Mecanismo de Remediação	✓	✓	✓	✓	✓	✓	✓	✓
Proteção Essencial Contra Ameaças								
Proteção Contra Ameaças ao Arquivo	✓	✓	✓	✓	✓	✓	✓	✓
Proteção Contra Ameaças da Web	–	✓	✓	✓	✓	✓	✓	✓
Proteção Contra Ameaças ao Correio	–	✓	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓	✓	✓
Proteção Contra Ameaças à Rede	✓	✓	✓	✓	✓	✓	✓	✓
Prevenção contra ataque BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
Proteção AMSI	✓	✓	✓	✓	✓	✓	✓	✓
Controles de Segurança								
Inspeção do Log	–	–	–	–	–	–	–	✓

Recurso	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Controle de aplicativos	–	✓	✓	✓	✓	✓	–	✓
Controle de dispositivos	–	✓	✓	✓	✓	✓	✓	✓
Controle da Web	–	✓	✓	✓	✓	✓	✓	✓
Controle Adaptativo de Anomalias	–	–	–	–	–	–	–	–
Monitor de integridade do sistema	–	–	–	–	–	–	–	✓
Criptografia de Dados								
Kaspersky Disk Encryption	–	–	–	–	–	–	–	–
Criptografia de unidade de disco BitLocker	–	✓	✓	✓	✓	✓	–	✓
Criptografia em Nível de Arquivo	–	–	–	–	–	–	–	–
Criptografia de unidades removíveis	–	–	–	–	–	–	–	–
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(A licença do Kaspersky Sandbox deve ser adquirida separadamente)*	✓	✓	✓	✓	✓	✓	✓	✓
Integração com KUMA *(a licença para a integração KUMA deve ser adquirida separadamente)*	✓	✓	✓	✓	✓	✓	✓	✓
Modo Light Agent *(para ativar o aplicativo, é necessário adicionar uma chave de licença no SVM ao qual o Light Agent está conectado)*	–	–	–	–	–	–	✓	✓

Ativar o aplicativo

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

O aplicativo é ativado das seguintes formas:

- Localmente na interface do aplicativo, usando o Assistente de Ativação. Você pode adicionar a chave ativa e a chave reserva dessa forma.
- Usando remotamente o pacote de software Kaspersky Security Center.
  - Utilizando a tarefa *Adicionar chave*.

    Esse método permite adicionar uma chave a um computador específico ou computadores que fazem parte de um grupo de administração. Você pode adicionar a chave ativa e a chave reserva dessa forma.
  - Distribuindo aos computadores uma chave que fica armazenada no Servidor de Administração do Kaspersky Security Center.

    Esse método permite adicionar automaticamente uma chave a computadores que já estão conectados ao Kaspersky Security Center e a novos computadores. Para usar esse método, você deve primeiro adicionar a chave no Servidor de Administração do Kaspersky Security Center. Para obter mais informações sobre como adicionar chaves ao Servidor de Administração do Kaspersky Security Center, consulte a Ajuda do Kaspersky Security Center.

    O código de ativação comprado com assinatura é distribuído em primeiro lugar.
  - Adicionando a chave ao pacote de instalação do Kaspersky Endpoint Security.

    Esse método permite a adição da chave nas propriedades do pacote de instalação durante a implementação do Kaspersky Endpoint Security. O aplicativo é ativado automaticamente após a instalação.
- Uso da linha de comando.

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

Se o Kaspersky Endpoint Security estiver sendo usado no modo Light Agent para proteger ambientes virtuais, não há necessidade de ativar o aplicativo separadamente.

Ativar o aplicativo

Como ativar o aplicativo no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **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

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Adicionar chave**.

Etapa 2. Adicionar uma chave

Digite um código de ativação ou selecione um arquivo de chave.

Para obter mais informações sobre como adicionar chaves ao repositório do Kaspersky Security Center, consulte a Ajuda do Kaspersky Security Center.

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, como por exemplo, *Ativar o Kaspersky Endpoint Security for Windows*.

Etapa 6. Concluir a criação da tarefa

Conclua o 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 resultado, o Kaspersky Endpoint Security será ativado nos computadores dos usuários em modo silencioso.

Como ativar o aplicativo no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

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

3. No campo **Nome da tarefa**, insira uma breve descrição, como *Ativação do Kaspersky Endpoint Security for Windows*.

4. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa. Vá para a próxima etapa.

Etapa 2. 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 3. Selecionar uma licença

Selecione a licença que você quer usar para ativar o aplicativo. Vá para a próxima etapa.

É possível adicionar chaves ao Web Console (**Operações** → **Licenciamento**).

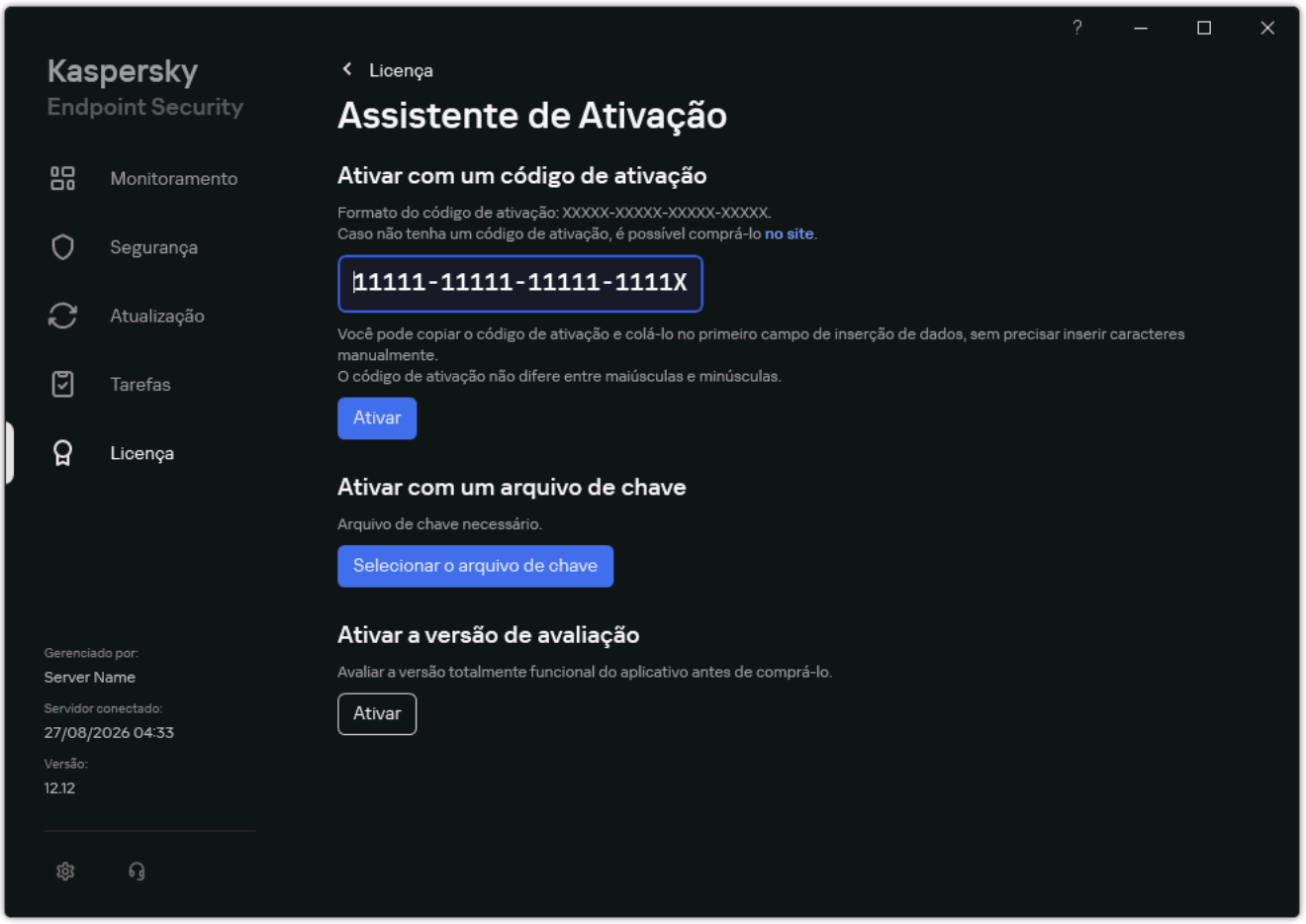
Etapa 4. Concluir a criação da tarefa

Finalize o assistente, clicando no botão **Concluir**. Uma nova tarefa será exibida na lista de tarefas. Para executar uma tarefa, marque a caixa de seleção ao lado da tarefa e clique no botão **Iniciar**. Como resultado, o Kaspersky Endpoint Security será ativado nos computadores dos usuários em modo silencioso.

Como ativar o aplicativo na interface do aplicativo

1. Na janela principal do aplicativo, acesse a seção **Licença**.
2. Clique **Ativar o aplicativo usando uma nova licença**.

O Assistente de Ativação do aplicativo é iniciado. Siga as instruções do Assistente de Ativação.



Ativar o aplicativo

Nas propriedades da tarefa *Adicionar chave*, você pode adicionar uma chave reserva no computador. Uma *chave reserva* fica ativa quando a chave ativa expira. A disponibilidade de uma chave reserva permite que você evite limitações de funcionalidades do aplicativo quando uma licença expira.

Como adicionar automaticamente uma chave de licença aos computadores por meio do Console de administração (MMC)

1. No Console de Administração, acesse a pasta **Licenças da Kaspersky**.

   Uma lista de chaves de licença é exibida.

2. Abra as propriedades da chave de licença.

3. Na seção **Geral**, marque a caixa de seleção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.

4. Salvar alterações.

   Como resultado, a chave será distribuída automaticamente para os computadores apropriados. Durante a distribuição automática de uma chave como chave ativa ou reserva, o limite de licenciamento do número de computadores (definido nas propriedades da chave) é levado em consideração. Se o limite de licenciamento for atingido, a distribuição dessa chave para computadores será interrompida automaticamente. É possível visualizar o número de computadores aos quais a chave foi adicionada, entre outros dados, nas propriedades da chave na seção **Dispositivos**.

Como adicionar automaticamente uma chave de licença aos computadores por meio do Web Console e do Cloud Console

1. Na janela principal do Web Console, selecione **Operações** → **Licenciamento** → **Licenças**.

   Uma lista de chaves de licença é exibida.

2. Abra as propriedades da chave de licença.

3. Na guia **Geral**, ative a opção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.

4. Salvar alterações.

   Como resultado, a chave será distribuída automaticamente para os computadores apropriados. Durante a distribuição automática de uma chave como chave ativa ou reserva, o limite de licenciamento do número de computadores (definido nas propriedades da chave) é levado em consideração. Se o limite de licenciamento for atingido, a distribuição dessa chave para computadores será interrompida automaticamente. É possível visualizar o número de computadores aos quais a chave foi adicionada e outros dados nas propriedades da chave na guia **Dispositivos**.

Caso esteja ativando o aplicativo com um *código de ativação*, é necessário ter acesso à Internet para se conectar aos servidores de ativação da Kaspersky. Caso esteja ativando o aplicativo com um *arquivo de chave*, o acesso à Internet não será necessário. Caso os computadores estejam em um segmento de rede isolado sem acesso à Internet, para ativar o aplicativo com um código, será necessário permitir o uso do Servidor de Administração do Kaspersky Security Center como um servidor proxy. Ou seja, o aplicativo pode obter acesso aos servidores de ativação através do Servidor de Administração com acesso à Internet.

Como permitir o uso do Servidor de Administração como um servidor proxy para ativar o aplicativo no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Configurações gerais** → **Configurações de aplicativos**.

4. Marque a caixa de seleção **Usar o Kaspersky Security Center como servidor proxy para ativação**.

5. Salvar alterações.

Como permitir o uso do Servidor de Administração como um servidor proxy para ativar o aplicativo no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Integração KSC**.

5. Marque a caixa de seleção **Usar o Kaspersky Security Center como servidor proxy para ativação**.

6. Salvar alterações.

Caso não possa ativar o aplicativo com um *código de ativação*, existe a possibilidade de tentar obter um *arquivo de chave* com o uso da solução da Kaspersky para tentar ativar o aplicativo novamente com o uso de um método diferente.

Monitoramento de uso de licença

Você pode monitorar o uso de licenças das seguintes maneiras:

- Visualize o *Relatório de uso das chaves de licença* para a infraestrutura da organização (**Monitoramento** → **Relatórios**).
- Visualize os status de computadores na guia **Dispositivos gerenciados** → **Dispositivos**. Caso o aplicativo não esteja ativado, o computador terá o status *O aplicativo não está ativado*.
- Visualize as informações da licença nas propriedades do computador.
- Visualize as propriedades da chave (**Operações** → **Licenciamento**).

Detalhes da ativação do aplicativo como parte do Kaspersky Security Center Cloud Console

É fornecida uma versão de avaliação do Kaspersky Security Center Cloud Console. A *versão de avaliação* é uma versão especial do Kaspersky Security Center Cloud Console projetada para familiarizar um usuário com os recursos do aplicativo. Nesta versão, você pode executar ações em um espaço de trabalho por um período de 30 dias. Todos os aplicativos gerenciados são executados automaticamente sob uma licença de avaliação do Kaspersky Security Center Cloud Console, incluindo o Kaspersky Endpoint Security. No entanto, você não pode ativar o Kaspersky Endpoint Security usando sua própria licença de avaliação quando a licença de avaliação do Kaspersky Security Center Cloud Console expirar. Para obter informações detalhadas sobre o licenciamento do Kaspersky Security Center, consulte a Ajuda do Kaspersky Security Center Cloud Console.

> A versão de avaliação do Kaspersky Security Center Cloud Console não permite que você alterne posteriormente para uma versão comercial. Qualquer espaço de trabalho de avaliação será excluído automaticamente com todo o seu conteúdo após o vencimento dos 30 dias.

Remover uma chave de licença

Para remover uma chave de licença, é preciso executar uma tarefa especial em seus computadores. É possível remover uma chave de licença, por exemplo, para reorganizar as unidades de licenciamento. Além disso, quando a licença expira, o Kaspersky Endpoint Security notifica o usuário. Caso tenha adicionado uma chave de licença com um curto prazo para testar o aplicativo (por exemplo, add-on do EDR Optimum), é possível remover essa chave da licença para se livrar de notificações e corrigir o status do computador.

A tarefa *Remover a chave* permite remover qualquer chave de licença do computador. É possível remover chaves de licença ativas, bem como chaves de licença reservas. Além da chave da licença de ativação do Kaspersky Endpoint Security, é possível remover chaves de licença individuais de soluções Kaspersky Detection and Response (por exemplo, add-on do EDR Optimum).

Como remover uma chave de licença no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **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

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Remover a chave**.

Etapa 2. Selecionar uma licença

Selecione a chave de licença que deseja excluir. É possível selecionar uma chave de licença do armazenamento de chaves do Kaspersky Security Center ou selecionar um arquivo de chave.

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

Insira um nome para a tarefa, por exemplo, *Remover a chave para beta*.

Etapa 6. Concluir a criação da tarefa

Conclua o 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 remover uma chave de licença no Web Console

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.
2. Na lista suspensa **Tipo de tarefa**, selecione **Remover a chave**.
3. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Remover a chave para beta*.
4. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa. Vá para a próxima etapa.

Etapa 2. 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 3. Selecionar uma licença

Selecione a chave de licença que deseja excluir. É possível selecionar uma chave de licença do armazenamento de chaves do Kaspersky Security Center ou selecionar um arquivo de chave. Vá para a próxima etapa.

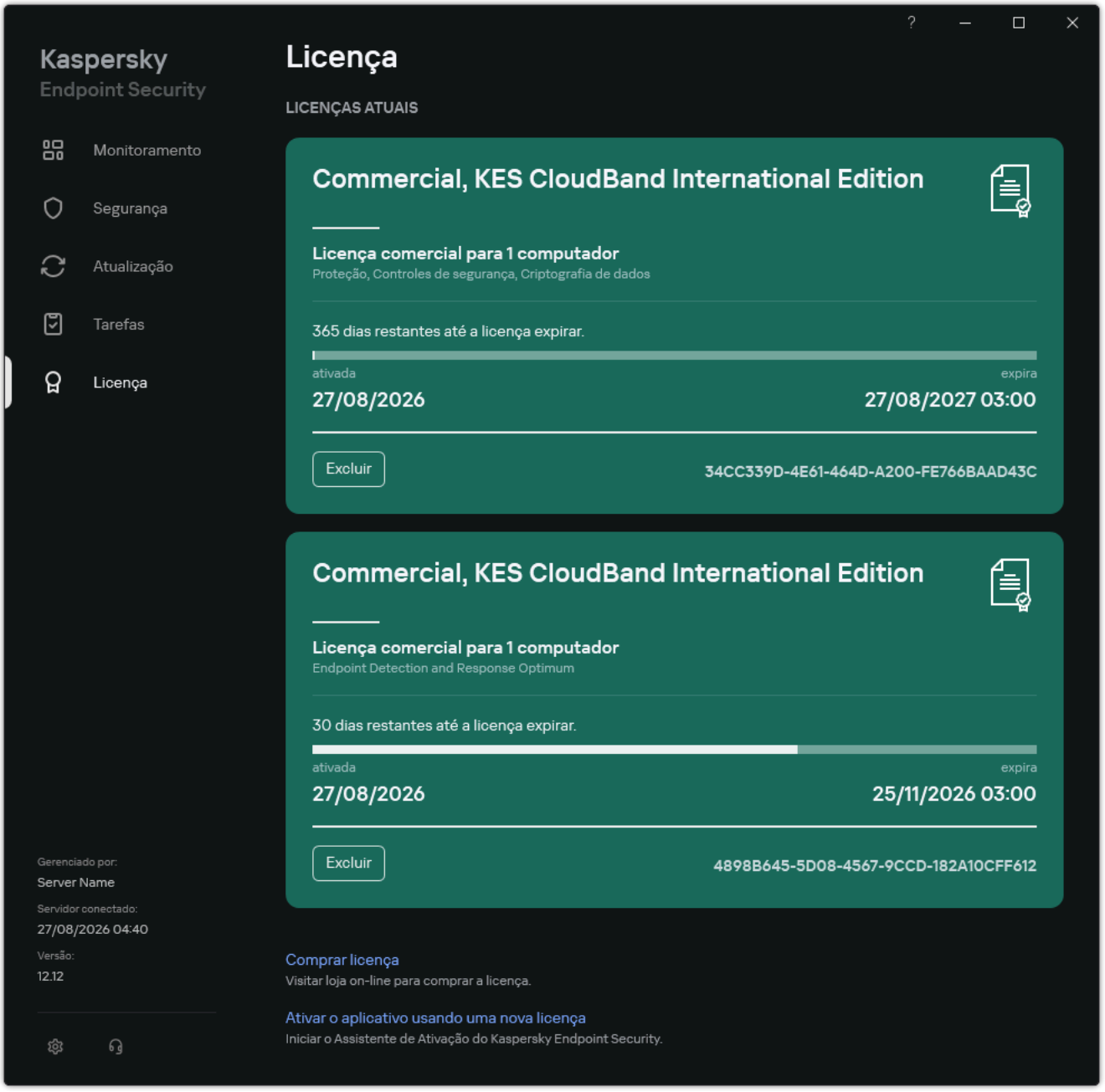
Etapa 4. Concluir a criação da tarefa

Finalize o assistente, clicando no botão **Concluir**. Uma nova tarefa será exibida na lista de tarefas. Para executar uma tarefa, marque a caixa de seleção ao lado da tarefa e clique no botão **Iniciar**.

Como remover uma chave de licença na interface do aplicativo

1. Na janela principal do aplicativo, acesse a seção **Licença**.

2. Selecione a chave que deseja excluir e clique em **Excluir**.



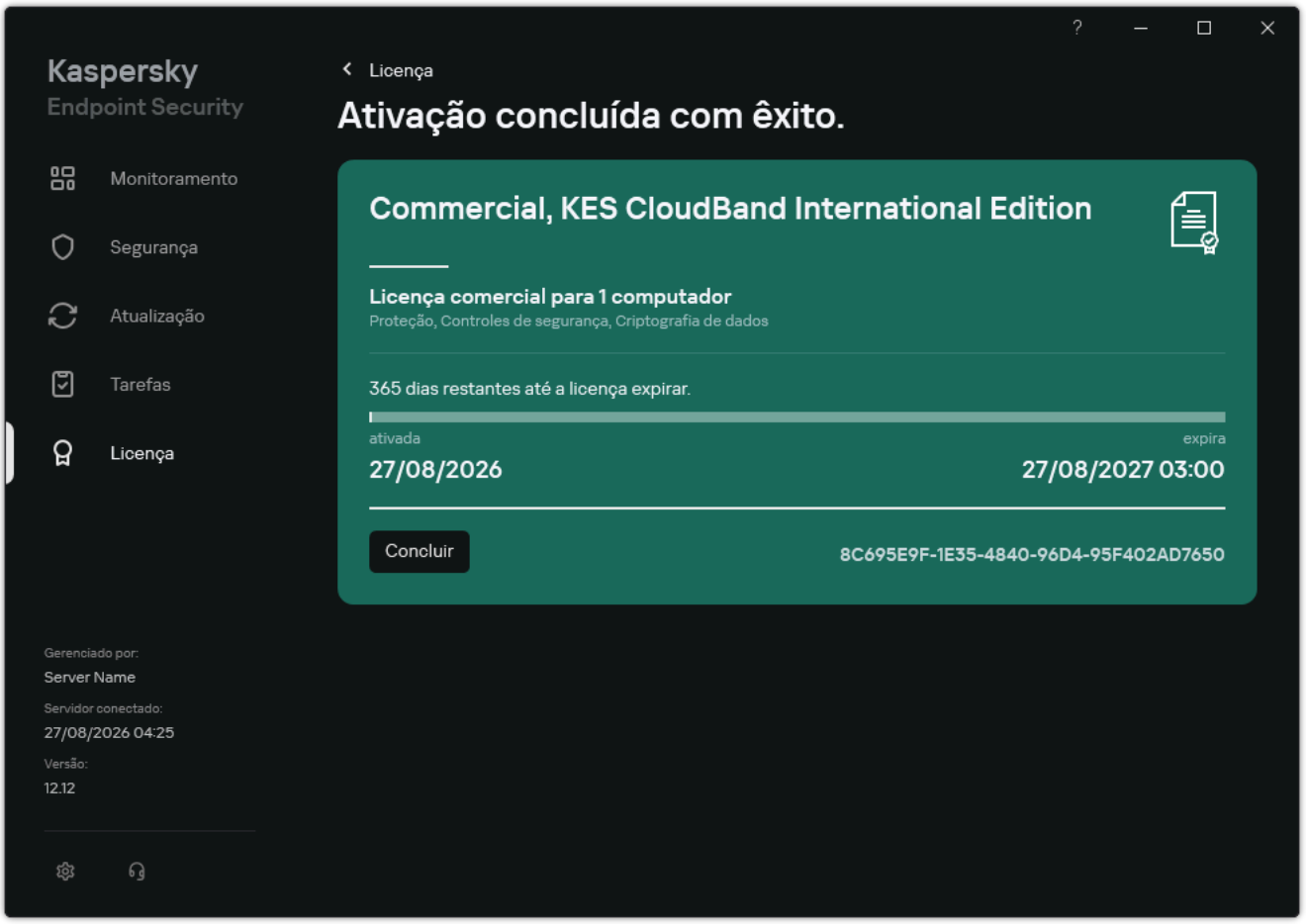
A janela Licença

Também é possível remover uma chave de licença na linha de comando.

Exibir informações da licença

Para exibir informações sobre uma licença:

Na janela principal do aplicativo, acesse a seção **Licença** (veja a figura abaixo).



A janela Licença

A seção exibe os seguintes detalhes:

- *Status da chave*. Várias chaves podem ser armazenadas em um computador. Há dois tipos de chaves: ativa e reserva. O aplicativo não pode ter mais de uma chave ativa. Uma chave reserva pode tornar-se ativa somente após a chave ativa expirar ou após a chave ativa for excluída ao clicar em **Excluir**.

- *Nome do aplicativo*. Nome completo do produto Kaspersky adquirido.

- *Tipo de licença*. Os seguintes tipos de licenças estão disponíveis: avaliação e comercial.

- *Funcionalidade*. Os recursos do aplicativo disponíveis de acordo com a sua licença. Os recursos podem incluir Proteção, Controles de Segurança, Criptografia de dados, entre outros. A lista de recursos disponíveis também é fornecida no Certificado de licença.

- *Informações adicionais sobre a licença*. Data de início e data de término do período da licença (apenas para a chave ativa), duração restante do período da licença.

  O tempo de expiração da licença é exibido de acordo com o fuso horário configurado no sistema operacional.

- *Chave*. Uma chave é uma sequência alfanumérica única, gerada a partir de um código de ativação ou de um arquivo de chave.

Na janela Licenciamento, você também pode executar uma das seguintes operações:

- **Comprar licença** / **Renovar licença**. Abre o site da loja virtual da Kaspersky, onde você pode comprar ou renovar uma licença. Para fazer isso, insira informações da sua empresa e pague o pedido.

- **Ativar o aplicativo usando uma nova licença**. Inicia o Assistente de Ativação do Aplicativo. Neste Assistente, você pode adicionar uma chave usando um código de ativação ou um arquivo de chave. O Assistente de ativação do aplicativo permite que você adicione uma chave ativa e somente uma chave reserva.

Comprar uma licença

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

Para comprar uma licença:

1. Na janela principal do aplicativo, acesse a seção **Licença**.

2. Realize uma das seguintes ações:

   - Caso nenhuma chave seja adicionada ou se uma chave para uma licença de avaliação tenha sido adicionada, clique no botão **Comprar licença**.

   - Se a chave da licença comercial foi adicionada, clique no botão **Renovar licença**.

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

Renovar a assinatura

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

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

Se você estiver usando o aplicativo com uma assinatura limitada, na data de expiração da assinatura (ou na data de expiração do período de carência de renovação de assinatura) o Kaspersky Endpoint Security notifica-o sobre isso e deixa de tentar renovar a assinatura automaticamente. Nesse caso, o Kaspersky Endpoint Security comporta-se da mesma forma como quando uma licença comercial do aplicativo expira: o aplicativo é executado sem atualizações e o Kaspersky Security Network fica indisponível.

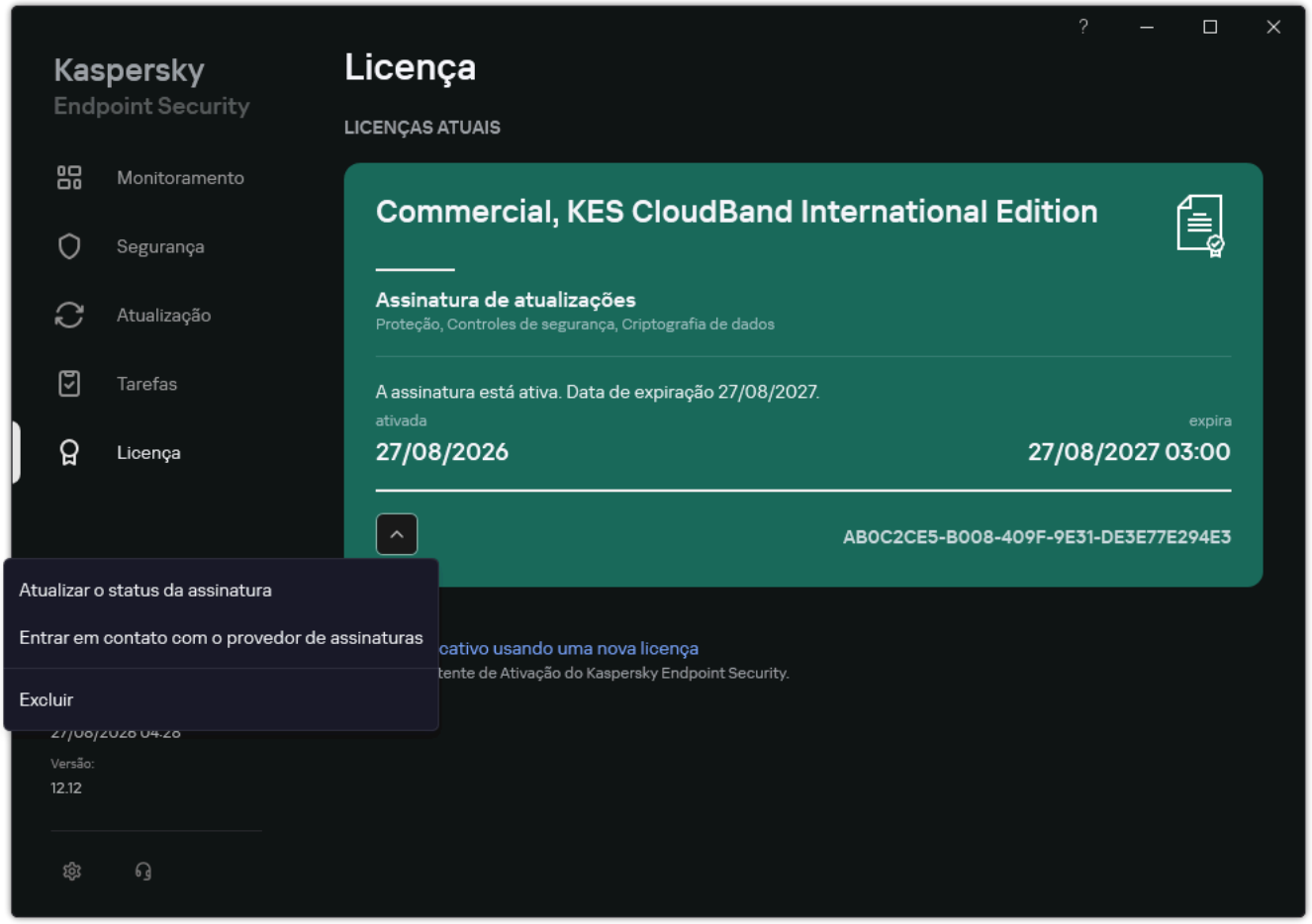
Você pode renovar a assinatura no site do provedor do serviço.

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

1. Na janela principal do aplicativo, acesse a seção **Licença**.

2. Clique **Entrar em contato com o provedor de assinaturas**.

   É possível fazer a atualização de status da assinatura manualmente. Isso poderá ser necessário se a assinatura tiver sido renovada após o período de carência e o aplicativo não tiver atualizado o status da assinatura automaticamente.



Renovar a assinatura

Iniciar

Após a instalação do Kaspersky Endpoint Security, você pode gerenciar o aplicativo usando as seguintes interfaces:

- Interface local do aplicativo.
- Console de Administração do Kaspersky Security Center.
- Kaspersky Security Center Web Console.
- Kaspersky Security Center Cloud Console.

Console de administração do Kaspersky Security Center

O Kaspersky Security Center permite que você instale e desinstale remotamente, inicie e interrompa o Kaspersky Endpoint Security, defina as configurações do aplicativo, altere o conjunto de componentes de aplicativos disponíveis, adicione chaves e inicie e pare as tarefas de atualização e verificação.

O aplicativo pode ser gerenciado através do Kaspersky Security Center utilizando o plug-in de gerenciamento do Kaspersky Endpoint Security.

Para obter mais informações sobre o gerenciamento do aplicativo por meio do Kaspersky Security Center, consulte a Ajuda do Kaspersky Security Center.

Kaspersky Security Center Web Console e Kaspersky Security Center Cloud Console

Kaspersky Security Center Web Console (doravante também denominado *Web Console*). Esta é uma interface da Web para gerenciar um sistema de proteção baseado em aplicativos da Kaspersky. Você pode trabalhar no Kaspersky Security Center Web Console usando um navegador em qualquer dispositivo. Para obter informações detalhadas sobre o Kaspersky Security Center Web Console, consulte a Ajuda do Kaspersky Security Center.

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

O Web Console e o Cloud Console permitem:

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

O gerenciamento do Kaspersky Endpoint Security por meio do Web Console, do Cloud Console e do Console de administração do Kaspersky Security Center fornecem recursos de gerenciamento diferentes. Os componentes e tarefas disponíveis também variam para os diferentes consoles.

Sobre o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows

O plug-in de gerenciamento do Kaspersky Endpoint Security for Windows permite a interação entre o Kaspersky Endpoint Security e o Kaspersky Security Center. O plug-in de gerenciamento permite que você gerencie o Kaspersky Endpoint Security usando políticas, tarefas e configurações locais do aplicativo. A interação com o Kaspersky Security Center Web Console é fornecida pelo plug-in da Web.

A versão do plug-in de gerenciamento pode diferenciar da versão do aplicativo do Kaspersky Endpoint Security instalado no computador cliente. Se a versão instalada do plug-in de gerenciamento tiver menos funcionalidades do que a versão instalada do Kaspersky Endpoint Security, as configurações das funções ausentes não serão reguladas pelo plug-in de gerenciamento. Estas configurações podem ser modificadas pelo usuário na interface local do Kaspersky Endpoint Security.

O plug-in da Web não é instalado por padrão no Kaspersky Security Center Web Console. O plug-in da web deve ser instalado em um computador que tenha o Kaspersky Security Center Web Console instalado. A funcionalidade do plug-in da web está disponível para todos os administradores que têm acesso ao Web Console em um navegador. É possível visualizar a lista de plug-ins da Web instalados na interface do Web Console (**Configurações do console** → **Plug-in da web**).

Se você estiver usando o Kaspersky Endpoint Security como parte da solução Kaspersky Endpoint Detection and Response Optimum, será necessário instalar o plug-in de gerenciamento do Kaspersky Endpoint Detection and Response. O plug-in de gerenciamento é obrigatório para exibição dos detalhes do alerta. *Detalhes de alertas* é uma ferramenta para visualizar todas as informações coletadas sobre uma ameaça detectada. Os detalhes da alertas incluem, por exemplo, o histórico de arquivos aparentes no computador. Portanto, para criar tarefas de resposta a ameaças, o plug-in de gerenciamento do Kaspersky Endpoint Security é necessário e, para visualizar os detalhes do alerta, o plug-in de gerenciamento do EDR é necessário.

Instalar o plug-in da web

Você pode instalar o plug-in da Web da seguinte maneira:

- Instale o plug-in da Web usando o assistente de início rápido do Kaspersky Security Center Web Console.

  O Web Console solicita automaticamente a execução do assistente de início rápido ao conectar o Web Console ao servidor de administração pela primeira vez. Também é possível executar o assistente de início rápido na interface do Web Console (**Descoberta e implementação** → **Implementação e atribuição** → **Assistente de início rápido**). O assistente de início rápido também pode verificar se os plug-ins da Web instalados estão atualizados e fazer o download das atualizações necessárias. Para obter mais detalhes sobre o assistente de inicialização rápida do Kaspersky Security Center Web Console, consulte a Ajuda do Kaspersky Security Center.

- Instale o plug-in da web pela lista de pacotes de distribuição disponíveis no Web Console.

  Para instalar o plug-in da Web, selecione o pacote de distribuição do plug-in da Web do Kaspersky Endpoint Security na interface do Web Console (**Configurações do console** → **Plug-in da web**). A lista de pacotes de distribuição disponíveis é atualizada automaticamente depois que novas versões de aplicativos da Kaspersky são lançadas.

- Faça download do pacote de distribuição para o Web Console a partir de uma fonte externa.

  Para instalar o plug-in da Web, adicione o arquivo ZIP do pacote de distribuição para o plug-in da Web do Kaspersky Endpoint Security na interface do Web Console (**Configurações do console** → **Plug-in da web**). O pacote de distribuição do plug-in da Web pode ser baixado no site da Kaspersky, por exemplo.

A partir do Kaspersky Endpoint Security 12.11 for Windows, o procedimento de instalação do plug-in da Web foi alterado. O pacote de distribuição agora inclui dois plug-ins da Web: *Kaspersky Endpoint Security for Windows 14.2.0* e o *Unified Protection and Management Plug-in*. Isso se deve à transição para um plug-in da Web unificado para gerenciamento dos aplicativos da Kaspersky. O plug-in da Web unificado permite criar uma única política para gerenciar várias aplicativos da Kaspersky (por exemplo, Kaspersky Endpoint Security for Windows, macOS e Linux). A transição para o plug-in da Web unificado pode precisar de várias versões. Após a conclusão da transição, o pacote de distribuição incluirá apenas o *Unified Protection and Management Plug-in*.

Atualização do plug-in de gerenciamento

Para atualizar o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows, faça o download da versão mais recente do plug-in (incluída no kit de distribuição) e execute o assistente de instalação do plug-in.

Se uma nova versão do plug-in de web for disponibilizada, o Web Console exibirá a notificação *Atualizações disponíveis para plug-ins em uso*. Você pode prosseguir com a atualização da versão do plug-in da web a partir dessa notificação do Web Console. Também é possível verificar manualmente se há novas atualizações do plug-in da web na interface do Web Console (**Configurações do console** → **Plugins da web**). A versão anterior do plug-in da web será automaticamente removida durante a atualização.

> Quando o plug-in da web for atualizado, os componentes já existentes (por exemplo, políticas ou tarefas) serão salvos. As novas configurações de itens que implementam novas funções do Kaspersky Endpoint Security aparecerão nos itens existentes e terão os valores padrões.

Você pode atualizar o plug-in da web da seguinte maneira:

- Atualize o plug-in da web na lista de plug-ins no modo on-line.

  Para atualizar o plug-in da web, selecione o pacote de distribuição do plug-in da web do Kaspersky Endpoint Security na interface do Web Console (**Configurações do console** → **Plugins da web**). O Web Console verifica se há atualizações disponíveis nos servidores da Kaspersky e faz o download das atualizações relevantes.

- Atualizar o plug-in da web a partir de um arquivo.

  Para atualizar o plug-in da Web, selecione o arquivo ZIP do pacote de distribuição do plug-in da Web do Kaspersky Endpoint Security na interface do Console da Web (**Configurações do console** → **Plug-ins da Web**). O pacote de distribuição do plug-in da Web pode ser baixado no site da Kaspersky, por exemplo. Você somente pode atualizar o plug-in da web do Kaspersky Endpoint Security para uma versão mais recente. O plug-in da web não pode ser atualizado para uma versão mais antiga.

Se algum item for aberto (como uma política ou tarefa), o plug-in da web verificará as suas informações de compatibilidade. Se a versão do plug-in da web for igual ou posterior à versão especificada nas informações de compatibilidade, você poderá modificar as configurações desse item. Caso contrário, não será possível usar o plug-in da web para alterar as configurações do item selecionado. É recomendável atualizar o plug-in da web.

Considerações especiais ao trabalhar com versões diferentes de plug-ins de gerenciamento

Você pode gerenciar o Kaspersky Endpoint Security por meio do Kaspersky Security Center apenas se tiver um Plug-in de Gerenciamento cuja versão seja igual ou posterior à especificada nas informações sobre a compatibilidade do Kaspersky Endpoint Security com o Plug-in de Gerenciamento. É possível visualizar a versão mínima necessária do Plug-in de Gerenciamento no arquivo installer.ini incluído no kit de distribuição.

Se algum item for aberto (como uma política ou tarefa), o Plug-in de gerenciamento verificará as informações de compatibilidade. Se a versão do plug-in de gerenciamento for igual ou posterior à versão especificada nas informações de compatibilidade, você pode modificar as configurações desse item. Caso contrário, não será possível usar o plug-in de gerenciamento para alterar as configurações do item selecionado. Recomenda-se fazer um upgrade do plug-in de gerenciamento.

Caso o plugin de gerenciamento do Kaspersky Endpoint Security seja instalado no Console de Administração, considere a seguinte possibilidade ao instalar uma nova versão do plug-in de gerenciamento:

- A versão anterior do plug-in de gerenciamento do Kaspersky Endpoint Security será removida.
- A nova versão do plug-in de gerenciamento do Kaspersky Endpoint Security é compatível com o gerenciamento da versão anterior do Kaspersky Endpoint Security for Windows em computadores de usuários.
- Você pode usar a nova versão do plug-in de gerenciamento para alterar as configurações em políticas, tarefas e outros elementos criados pela versão anterior do plug-in de gerenciamento.
- Para novas configurações, a nova versão do Plug-in de gerenciamento atribui os valores padrões quando uma política, perfil de política ou tarefa são salvos pela primeira vez.

  Depois de atualizar o Plug-in de gerenciamento, é recomendável verificar e salvar os valores das novas configurações das políticas e dos perfis de políticas. Se você não fizer isso, os novos grupos de configurações do Kaspersky Endpoint Security no computador do usuário usarão os valores padrões e poderão ser editados (o atributo). É recomendável verificar as configurações que iniciam com políticas e perfis de política no nível superior da hierarquia. Também é recomendável usar a conta de usuário que tenha direitos de acesso a todas as áreas funcionais do Kaspersky Security Center.

  Para saber mais sobre os novos recursos do aplicativo, consulte as Notas de Versão ou a ajuda do aplicativo.

- Se um novo parâmetro tiver sido adicionado a um grupo de configurações na nova versão do Plug-in de gerenciamento, o status definido anteriormente do atributo / desse grupo de configurações não é modificado.

Considerações especiais ao usar protocolos criptografados para interagir com serviços externos

O Kaspersky Endpoint Security e o Kaspersky Security Center usam um canal de comunicação criptografado com TLS (Transport Layer Security) para trabalhar com serviços externos da Kaspersky. O Kaspersky Endpoint Security usa serviços externos para as seguintes funções:

- Atualização dos bancos de dados e módulos do software do aplicativo;
- Ativação do aplicativo com um código de ativação (ativação 2.0);
- uso da Kaspersky Security Network.

O uso de TLS protege o aplicativo, fornecendo os seguintes recursos:

- Criptografia. O conteúdo das mensagens é confidencial e não é divulgado a terceiros.
- Integridade. O destinatário da mensagem tem certeza de que o conteúdo da mensagem não foi modificado desde que a mensagem foi encaminhada pelo remetente.
- Autenticação. O destinatário tem certeza de que a comunicação é estabelecida apenas com um servidor confiável Kaspersky.

O Kaspersky Endpoint Security usa certificados de chave pública para autenticação do servidor. Uma Public Key Infrastructure (PKI) é necessária para trabalhar com certificados. Uma autoridade de certificação é parte de uma PKI. A Kaspersky usa sua própria Autoridade de Certificação porque os serviços da Kaspersky são altamente técnicos e não públicos. Nesse caso, quando os certificados raiz Thawte, VeriSign, GlobalTrust e outros são revogados, a PKI da Kaspersky permanece operacional sem interrupções.

Ambientes que possuem MITM (ferramentas de software e hardware com suporta para a análise do protocolo HTTPS) são considerados inseguros pelo Kaspersky Endpoint Security. Podem ser encontrados erros ao trabalhar com os serviços da Kaspersky. Por exemplo, pode haver erros relacionados ao uso de Self-Signed Certificate. Esses erros podem ocorrer porque uma ferramenta de inspeção HTTPS do seu ambiente não reconhece a PKI da Kaspersky. Para retificar esses problemas, você deve configurar exclusões para interagir com serviços externos.

Interface do aplicativo

Janela principal do aplicativo

Monitoramento	• **Relatórios**. Exibir eventos que ocorreram durante a operação do aplicativo, componentes e tarefas individuais. • **Backup**. Exibir uma lista de cópias salvas de arquivos infectados que o aplicativo excluiu. • **Tecnologias de detecção de ameaças**. Exibir informações sobre tecnologias de detecção de ameaças e o número de ameaças detectadas por essas tecnologias. • **Kaspersky Security Network**. Status da conexão entre o Kaspersky Endpoint Security e a Kaspersky Security Network, e estatísticas globais KSN. *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 Endpoint Security a novas ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos positivos. Caso participe da Kaspersky Security Network, os serviços da KSN fornecem à Kaspersky Endpoint Security informações sobre a reputação dos endereços da Web verificados, além de informações sobre a categoria e a reputação dos arquivos verificados. • **Monitoramento de atividades do aplicativo**. Exibir informações sobre a operação dos aplicativos instalados. O monitoramento de atividades do aplicativo mantém o rastreio do arquivo, do registro e dos eventos do sistema operacional associados ao aplicativo. • **Monitor de Rede**. Exibir informações sobre a atividade de rede do computador em tempo real. • **Monitor de criptografia**. Monitora a criptografia do disco ou o processo de descriptografia em tempo real. O monitor de criptografia estará disponível se o componente Kaspersky Disk Encryption ou o componente Criptografia de unidade de disco BitLocker estiverem instalados.
Segurança	Status operacional dos componentes instalados. Também é possível continuar configurando os componentes ou visualizando os relatórios.
Atualização	Gerenciar as tarefas de atualização do Kaspersky Endpoint Security. Você pode atualizar bancos de dados de antivírus e módulos de aplicativo e reverter a última atualização. Um administrador pode ocultar a seção do usuário ou o gerenciamento de tarefas restritas.
Tarefas	Gerenciar as tarefas de verificação do Kaspersky Endpoint Security. É possível executar uma verificação de malware e uma verificação de integridade do aplicativo. Um administrador pode ocultar tarefas de um usuário ou restringir o gerenciamento de tarefas.

Licença	Licenciamento do aplicativo. É possível comprar uma licença, ativar o aplicativo ou renovar uma assinatura. Também é possível visualizar informações sobre a licença atual.
	Definir as configurações do aplicativo. Um administrador pode proibir alterações nas configurações do Kaspersky Security Center.
	Informações sobre o aplicativo: versão atual do Kaspersky Endpoint Security, data da versão do banco de dados, chave e outras informações. Você também pode acessar os recursos de informação da Kaspersky que fornecem informações úteis, recomendações e respostas às perguntas frequentes sobre como comprar, instalar e usar o aplicativo.
	Mensagens contendo informações sobre atualizações disponíveis e solicitações de acesso a arquivos e dispositivos criptografados.

Ícone do aplicativo na área de notificação da barra de tarefas

Logo após a instalação do Kaspersky Endpoint 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 Endpoint 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 Endpoint Security exibirá um aviso com uma descrição do problema na proteção do computador.

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

- **Kaspersky Endpoint Security for Windows**. Abre a janela principal do aplicativo. Nesta janela, é possível ajustar a operação dos componentes e das tarefas do aplicativo e exibir estatísticas de arquivos processados e ameaças detectadas.
- **Pausar a proteção** / **Reiniciar a proteção**. Pausa a operação de proteção e controle de todos os componentes que não estiverem bloqueados ( ) na política. Antes de executar essa operação, recomenda-se desativar a política do Kaspersky Security Center.

  Antes de pausar a operação de proteção e controle dos componentes, o aplicativo solicita a senha para acessar o Kaspersky Endpoint Security (senha de conta ou temporária). Você pode então selecionar o período de pausa: por um período de tempo específico, até a reinicialização ou mediante solicitação do usuário.

  Este item do menu de contexto está disponível se a Proteção por senha estiver ativada. Para reiniciar a operação de proteção e controle dos componentes, selecione **Reiniciar a proteção** no menu de contexto do aplicativo.

Interromper a operação de proteção e controle dos componentes não afeta o desempenho das tarefas de atualização e verificação de malware. O aplicativo também continua usando a Kaspersky Security Network.

- **Desativar política** / **Ativar política**. Desativação da política do Kaspersky Security Center no computador. Todas as configurações do Kaspersky Endpoint Security estão disponíveis para configuração, incluindo configurações que possuem um cadeado fechado na política (). Se a política estiver desativada, o aplicativo solicita a senha para acessar o Kaspersky Endpoint Security (senha da conta ou senha temporária). Este item do menu de contexto está disponível se a Proteção por senha estiver ativada. Para ativar a política, selecione **Ativar política** no menu de contexto do aplicativo.

- **Configurações**. Abre a janela de configurações do aplicativo.

- **Suporte**. Isso abre a janela contendo as informações necessárias para entrar em contato com o Suporte Técnico da Kaspersky.

- **Sobre**. Este item abre uma janela de informações que contém detalhes do aplicativo.

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

Menu de contexto do ícone do aplicativo

Interface de aplicativo simplificada

Se uma política do Kaspersky Security Center configurada para exibir a interface de aplicativo simplificada for aplicada a um computador cliente no qual o Kaspersky Endpoint Security está instalado, a janela do aplicativo principal não estará disponível nesse computador cliente. Clique com o botão direito para abrir o menu de contexto do ícone do Kaspersky Endpoint Security (consulte a figura abaixo) que contém os seguintes itens:

- **Desativar política** / **Ativar política**. Desativação da política do Kaspersky Security Center no computador. Todas as configurações do Kaspersky Endpoint Security estão disponíveis para configuração, incluindo configurações que possuem um cadeado fechado na política (). Se a política estiver desativada, o aplicativo solicita a senha para acessar o Kaspersky Endpoint Security (senha da conta ou senha temporária). Este item do menu de contexto está disponível se a Proteção por senha estiver ativada. Para ativar a política, selecione **Ativar política** no menu de contexto do aplicativo.

- **Tarefas**. Lista suspensa com os seguintes itens:

  - **Verificação de integridade do aplicativo**.

  - **Reversão de bancos de dados para a versão anterior**.

  - **Verificação completa**.

  - **Verificação personalizada**.

- **Verificação de áreas críticas**.
- **Atualização**.

- **Suporte**. Isso abre a janela contendo as informações necessárias para entrar em contato com o Suporte Técnico da Kaspersky.
- **Sair**. Este item encerra o Kaspersky Endpoint Security. Quando você clica neste menu de contexto o aplicativo é retirado da RAM do computador.

Menu de contexto do ícone de aplicativo ao exibir a interface simplificada

Configurar a exibição da interface do aplicativo

Você pode configurar o modo de exibição da interface do aplicativo para um usuário. O usuário pode interagir com o aplicativo das seguintes maneiras:

- **Simplificado**. Em um computador cliente, a janela principal do aplicativo está inacessível e apenas o ícone na área de notificação do Windows está disponível. No menu de contexto do ícone, o usuário pode executar um número limitado de operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security também exibe apenas as notificações que exigem ação do usuário acima do ícone do aplicativo.
- **Completo**. Em um computador cliente, a janela principal do Kaspersky Endpoint Security e o ícone na área de notificação do Windows estão disponíveis. No menu de contexto do ícone, o usuário pode executar operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security também exibe notificações acima do ícone do aplicativo.
- **Não exibir interface do usuário**. Em um computador cliente, nenhum sinal da operação do Kaspersky Endpoint Security é exibido. O ícone na área de notificação do Windows e as notificações não estão disponíveis.

Como configurar o modo de exibição da interface do aplicativo no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Interface**.

4. No bloco **Interação com o usuário**, configure como a interface do aplicativo será exibida:

   - **Exibir interface do usuário**. Em um computador cliente, a janela principal do Kaspersky Endpoint Security e o ícone na área de notificação do Windows estão disponíveis. No menu de contexto do ícone, o usuário pode executar operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security também exibe notificações acima do ícone do aplicativo. Caso necessário, é possível ativar a funcionalidade **Ocultar a seção Monitoramento de atividades do aplicativo** para ocultar dados sobre a atividade do aplicativo no computador, restringindo assim o acesso do usuário à ferramenta monitoramento de atividades do aplicativo.

   - **Exibir interface simplificada**. Em um computador cliente, a janela principal do aplicativo está inacessível e apenas o ícone na área de notificação do Windows está disponível. No menu de contexto do ícone, o usuário pode executar um número limitado de operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security também exibe apenas as notificações que exigem ação do usuário acima do ícone do aplicativo.

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

5. Salvar alterações.

Como configurar o modo de exibição da interface do aplicativo no Web Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Interação com o usuário**.

5. No bloco **Visibilidade para usuários**, configure como a interface do aplicativo será exibida:

   - **Exibir interface do usuário**. Caso essa funcionalidade esteja desativada, nenhum sinal de operação do Kaspersky Endpoint Security será exibido em um computador cliente. O ícone na área de notificação do Windows e as notificações não estão disponíveis.

   - **Simplificado**. Em um computador cliente, a janela principal do aplicativo está inacessível e apenas o ícone na área de notificação do Windows está disponível. No menu de contexto do ícone, o usuário pode executar um número limitado de operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security também exibe apenas as notificações que exigem ação do usuário acima do ícone do aplicativo.

   - **Completo**. Em um computador cliente, a janela principal do Kaspersky Endpoint Security e o ícone na área de notificação do Windows estão disponíveis. No menu de contexto do ícone, o usuário pode executar operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security também exibe notificações acima do ícone do aplicativo.

   - **Ocultar a seção Monitoramento de atividades do aplicativo**. Caso queira ocultar as informações de atividade do aplicativo no computador de um usuário, é possível restringir o acesso do usuário à ferramenta Monitoramento de atividades do aplicativo.

6. Para aplicar a política aos computadores, feche os ícones de cadeado 🔒 e salve as alterações.

Preparação do aplicativo para uso

Depois de implementar o aplicativo em computadores clientes, para trabalhar com o Kaspersky Endpoint Security a partir do Kaspersky Security Center Web Console, você deve executar as seguintes ações:

- Criar e configurar uma política.

  Estabelecer políticas permite que você aplique configurações de aplicativo universais para todos os computadores clientes em um grupo de administração. O assistente de início rápido do Kaspersky Security Center cria automaticamente uma política para o Kaspersky Endpoint Security.

- Crie as tarefas *Atualização de bancos de dados e módulos do aplicativo* e *Verificação de malware*.

  A tarefa *Atualização de bancos de dados e módulos do aplicativo* é necessária para manter a segurança do computador atualizada. Quando a tarefa é executada, o Kaspersky Endpoint Security atualiza os bancos de dados de antivírus e os módulos do aplicativo. A tarefa *Atualização de bancos de dados e módulos do aplicativo* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização de bancos de dados e módulos do aplicativo*, instale o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows enquanto executa o assistente.

  A tarefa *Verificação de malware* é necessária para a detecção oportuna de vírus e outros malwares. Você precisa criar manualmente a tarefa de *Verificação de malware*.

  Como criar uma tarefa de Verificação de malware no console de administração (MMC)

  1. No Console de Administração do Kaspersky Security Center, selecione **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

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Verificação de malware**.

Etapa 2. Escopo da verificação

Crie uma lista de objetos que o Kaspersky Endpoint Security verifica ao executar uma tarefa de verificação.

Etapa 3. Ação do Kaspersky Endpoint Security

Escolha a ação na detecção de ameaças:

- **Desinfectar e excluir se a desinfecção falhar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Caso a desinfecção falhe, o aplicativo excluirá o arquivo.

- **Desinfectar e informar se a desinfecção falhar**. Caso esta opção seja selecionada, o Kaspersky Endpoint Security tentará desinfectar automaticamente todos os arquivos infectados que são detectados. Caso a desinfeção não seja possível, o Kaspersky Endpoint Security adicionará as informações sobre os arquivos infectados e detectados na lista de ameaças ativas.

- **Informar**. Caso esta opção seja selecionada, o Kaspersky Endpoint Security adiciona as informações sobre arquivos infectados à lista de ameaças ativas na detecção destes arquivos.

- **Executar a Desinfecção Avançada imediatamente**. Se a caixa de seleção estiver selecionada, o Kaspersky Endpoint Security usa a tecnologia Advanced Desinfection para tratar ameaças ativas durante a verificação.

  A *tecnologia de desinfecção avançada* objetiva eliminar do sistema operacional aplicativos maliciosos que já iniciaram seus processos na RAM e que impedem que o Kaspersky Endpoint Security os remova, usando outros métodos. Como resultado, a ameaça é neutralizada. Enquanto a Desinfecção Avançada estiver em andamento, é recomendável abster-se de iniciar novos processos ou editar os registros do sistema operacional. A tecnologia de desinfecção avançada usa uma grande quantidade de recursos do sistema operacional, que talvez torne os outros aplicativos mais lentos. Depois que a desinfecção avançada concluir, o Kaspersky Endpoint Security reiniciará o computador sem solicitar a confirmação do usuário.

- **Executar apenas quando o computador estiver ocioso**. Início adiado da tarefa quando os recursos do computador estão ocupados. O Kaspersky Endpoint Security inicia a tarefa de verificação se o computador estiver bloqueado ou se a proteção de tela estiver ativada. Caso interrompa a execução da tarefa, por exemplo, desbloqueando o computador, o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que foi interrompido. Essa opção de programação permite conservar os recursos do computador quando ele está sendo utilizado.

Etapa 4. 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 5. Seleção da conta para executar a tarefa

Selecione uma conta para executar a tarefa de *Verificação de malware*. Por padrão, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de usuário local. Se o escopo da verificação incluir unidades de rede ou outros objetos com acesso restrito, selecione uma conta de usuário com os direitos de acesso suficientes.

Etapa 6. Configurar um agendamento de início de tarefa

Configure um agendamento para iniciar uma tarefa, por exemplo, manualmente ou após o download dos bancos de dados antivírus no repositório.

Etapa 7. Definir o nome da tarefa

Insira um nome para a tarefa, por exemplo, *Verificação completa diária*.

Etapa 8. Concluir a criação da tarefa

Conclua o 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 resultado, a tarefa de Verificação de malware será executada nos computadores do usuário de acordo com a programação especificada.

Como criar uma tarefa de Verificação de malware no Web Console

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Verificação de malware**.

   c. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Verificação semanal*.

   d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Vá para a próxima etapa.

5. Selecione uma conta para executar a tarefa. Por padrão, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de usuário local.

6. Conclua o assistente.

   Uma nova tarefa será exibida na lista de tarefas.

7. Para configurar a programação da tarefa, acesse as propriedades da tarefa.

   Recomenda-se agendar a tarefa para ser executada pelo menos uma vez por semana.

8. Marque a caixa de seleção ao lado da tarefa.

9. Clique **Iniciar**.

   Você pode monitorar o status da tarefa e o número de dispositivos nos quais a tarefa foi concluída com êxito ou concluída com um erro.

Como resultado, a tarefa de Verificação de malware será executada nos computadores do usuário de acordo com a programação especificada.

- Otimize o desempenho do Kaspersky Endpoint Security.

Gerenciamento de políticas

Uma *política* é um conjunto de configurações do aplicativo definidas para um grupo de administração. Você pode configurar várias políticas com valores diferentes para um aplicativo. Um aplicativo pode ser executado em diferentes configurações para diferentes grupos de administração. Cada grupo de administração pode ter a sua própria política para um aplicativo.

Cada configuração de política tem o atributo (“cadeado”). O status desse atributo determina se a configuração será enviada para os dispositivos gerenciados no grupo de administração:

- Se o "cadeado" estiver aberto (), o valor dessa configuração não será enviado para os dispositivos gerenciados. A configuração estará disponível para modificação na interface local do aplicativo. Essas configurações são chamadas de *desbloqueadas*.

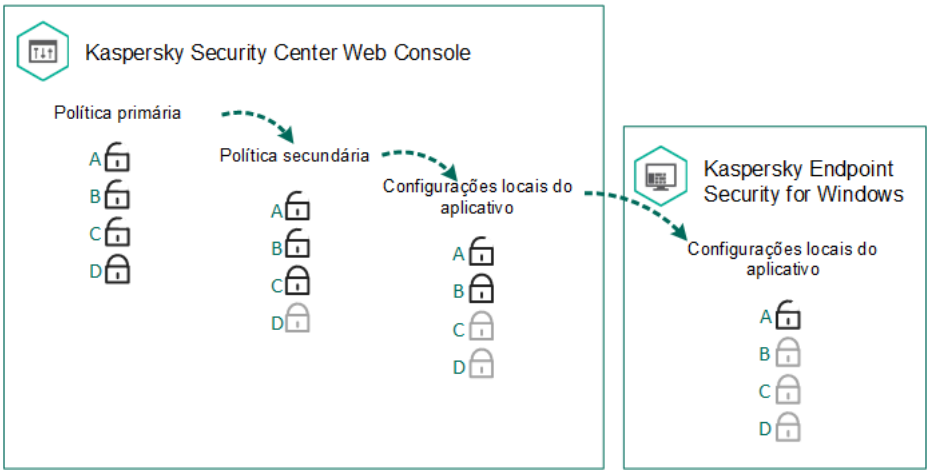
- Se o "cadeado" estiver fechado (), o valor dessa configuração será enviado e aplicado aos dispositivos gerenciados. Essas configurações são chamadas de *bloqueadas*. As configurações bloqueadas não podem ser modificadas na interface local do aplicativo.

As configurações da política são enviadas aos computadores clientes pelo Agente de Rede durante a *sincronização*. Por padrão, o Servidor de Administração executa a sincronização imediatamente após a alteração das configurações da política. A porta UDP 15000 no computador cliente é usada para a sincronização. O Servidor de Administração executa a sincronização a cada 15 minutos, por padrão. Se a sincronização falhar depois que as configurações da política forem alteradas, a próxima tentativa de sincronização será executada segundo a programação configurada.

Herança de configurações

Políticas, como grupos de administração, são organizadas em uma hierarquia. *Política secundária* é uma política de níveis de hierarquia aninhados, que é uma política para grupos de administração aninhados e servidores de administração secundários.

Por padrão, uma política filha herda configurações da política pai. Se a configuração na política principal tiver o atributo 🔒 ("cadeado" fechado), o valor dessa configuração será substituído nas políticas secundárias e nas configurações locais do aplicativo de acordo com a política principal, e a configuração será bloqueada. Se necessário, você pode desativar a herança de configurações da política principal. As políticas de ausência não afetam outras políticas por meio da hierarquia de grupos de administração.



Herança de configurações

Os direitos de acesso às configurações da política (ler, gravar, executar) são especificados para cada usuário com acesso ao Servidor de Administração do Kaspersky Security Center e separadamente para cada escopo funcional do Kaspersky Endpoint Security. Para definir os direitos de acesso para as configurações da política, vá para a seção **Segurança** da janela de propriedades do Servidor de Administração do Kaspersky Security Center (por padrão, essa seção está oculta na interface do console).

Revisões da política

O Kaspersky Security Center rastreia as modificações da política e cria revisões. Uma *revisão* é um conjunto de parâmetros modificados salvos pelo usuário. As revisões permitem comparar e reverter as alterações nos parâmetros da política. Além do conjunto de parâmetros modificados, a revisão inclui informações sobre o usuário que fez as alterações, assim como a hora, endereço IP, comentário do usuário e outros dados pertinentes.

Para exibir o log de revisão, abra as propriedades da política e vá para a seção **Histórico de revisões**. Para obter mais detalhes sobre o funcionamento com revisões, consulte a ajuda do Kaspersky Security Center.

Criar uma política

Ao criar uma política, o assistente sugere as configurações pertinentes para o modo selecionado. Por exemplo, para o modo Light Agent, é necessário adicionar um Servidor de proteção (SVM). Ao usar o aplicativo para proteger um servidor SQL, é necessário adicionar as exclusões de verificação predefinidas para garantir que a operação do servidor não sofra interferências. O assistente sugere as configurações pertinentes da política depois de selecionar um modo. Então, é possível editar essas configurações nas propriedades da política.

Como criar um política no Console de administração (MMC)

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

2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, selecione a pasta com o nome do grupo de administração a que pertence o computador cliente desejado.

3. No espaço de trabalho, selecione a guia **Políticas**.

4. Clique **Nova política**.

   O Assistente de Políticas é iniciado.

5. Siga as instruções do Assistente de Políticas.

Etapa 1. Selecionar o aplicativo para criar a política de grupo

Selecione o aplicativo **Kaspersky Endpoint Security for Windows (14.2)**.

Etapa 2. Nomear a política de grupo

Insira um nome para a política de grupo, por exemplo, *Política para o escritório*.

Também é possível criar políticas com base nas existentes usando o Assistente de Políticas. Para fazer isso, ao especificar o nome da política de grupo, marque a caixa de seleção **Usar as configurações de política para uma versão anterior do aplicativo**. O assistente também permite criar uma política do Kaspersky Endpoint Security (KES) com base na política de uma solução diferente, por exemplo, do Kaspersky Security for Windows Server (KSWS) ou do Kaspersky Security for Virtualization Light Agent for Windows

Etapa 3. Participação na Kaspersky Security Network

Leia e aceite os termos da Declaração da Kaspersky Security Network (KSN).

Etapa 4. Selecionar o modo de uso do aplicativo em computadores

Dependendo do tipo de uso desejado do Kaspersky Endpoint Security, é possível configurar uma política para os seguintes modos de aplicativo:

- Modo Standard para proteger hosts

  Nesse modo, é possível selecionar como deseja configurar a política:

  - **Criar uma política com configurações padrão**. As configurações padrão são consideradas ideais. Elas são recomendadas pelos peritos da Kaspersky. As configurações padrão fornecem o nível de proteção recomendado e o uso ideal de recursos.

  - **Alterar configurações da política no assistente**. Este método permite gerenciar as configurações da política passo a passo com o uso de um assistente. Também é possível gerenciar as configurações de política usando um arquivo de configuração do aplicativo (consulte a próxima etapa).

- Endpoint Detection and Response Agent para garantir a proteção contra ameaças avançadas e ataques direcionados.

  O *Endpoint Detection and Response Agent* é um aplicativo instalado em estações de trabalho e servidores individuais na infraestrutura de TI da organização para oferecer suporte às soluções de Detection and Response da Kaspersky. Na próxima etapa, é necessário selecionar uma solução para a integração do EDR Agent.

- Light Agent para garantir a proteção em ambientes virtuais.

  Para usar o aplicativo no modo Light Agent, é necessário configurar uma conexão com uma máquina virtual SVM. Essas configurações são necessárias para que o aplicativo funcione no modo Light Agent.

O Kaspersky Endpoint Security fornece uma política comum para todos os modos de aplicativo e tipos de SO. Isso significa que a política abrange todo o conjunto de configurações. No entanto, o aplicativo pode ignorar algumas das configurações da política porque o Kaspersky Endpoint Security é implementado em um modo no qual algumas funcionalidades não estão disponíveis. Por exemplo, ao usar o aplicativo no modo Endpoint Detection and Response Agent, somente as configurações relevantes para a integração com as soluções do Kaspersky Detection and Response e para a integração com o KUMA estão disponíveis.

Recomendamos usar políticas diferentes para diferentes modos e tipos de sistema operacional.

Etapa 5. Importando configurações

Esta etapa estará disponível caso a configuração manual da política na etapa 4 seja selecionada.

É possível criar uma política de acordo com as configurações do Kaspersky Endpoint Security por meio de um arquivo de configuração CFG. O Assistente de nova política não oferece suporte a arquivos de configuração criptografados. Ao exportar o arquivo de configuração, ignore a etapa de criptografia do arquivo.

Ao importar um arquivo de configuração CFG do aplicativo, nem todas as configurações de política ficam disponíveis para o assistente. Por exemplo, os perfis de política estão ausentes nas configurações do aplicativo. Caso queira transferir todas as configurações e perfis para a política, é possível importar outra política de um arquivo KLP.

Ao importar um arquivo de configuração, o Kaspersky Endpoint Security não transfere as senha do contêiner de criptografia. Caso use a autenticação bidirecional ao se conectar aos servidores, será necessário especificar as senhas do contêiner de criptografia do zero.

Etapa 6 - 10. Definição das configurações da política

Esta etapa estará disponível caso a configuração manual da política na etapa 4 seja selecionada.

Siga as etapas para gerenciar as configurações de política.

Etapa 11. Configuração da zona confiável

Configure a zona confiável. É possível adicionar exclusões de verificação e aplicativos confiáveis predefinidos. As exclusões predefinidas de verificação e aplicativos confiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, Microsoft Exchange e System Center Configuration Manager. Isso significa que não será necessário configurar manualmente uma zona confiável para o aplicativo nos servidores. Exclusões de verificação e aplicativos confiáveis predefinidos também podem ajudar a configurar rapidamente o Kaspersky Endpoint Security no modo Light Agent em ambientes virtuais Citrix e VMware.

Etapa 12. Selecionar o status da política

- **Ativo**. Depois da sincronização seguinte, a política será usada como a política ativa no computador.

  As configurações de uma política ativa são salvas nos computadores clientes durante a sincronização. Você não pode aplicar simultaneamente várias políticas a um computador, portanto, apenas uma política pode estar ativa em cada grupo.

- **Inativo**. Política de reserva. Se necessário, uma política inativa pode ser trocada para o status ativo.

  Você pode criar um número ilimitado de políticas inativas. Uma política inativa não afeta as configurações do aplicativo em computadores na rede. As políticas inativas funcionam como preparativos para situações de emergência, como um ataque de vírus. Se ocorrer um ataque por meio de pen drives, você poderá ativar uma política que bloqueie o acesso aos pen drives. Nesse caso, a política ativa torna-se automaticamente inativa.

- **Fora do escritório**. A política é ativada quando um computador sai do perímetro da rede da organização.

Conclua o assistente.

Como criar uma política no Web Console e no Cloud Console

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

2. Clique **Adicionar**.

   O Assistente de Políticas é iniciado.

3. Selecione o Kaspersky Endpoint Security e clique em **Avançar**.

4. Leia e aceite os termos da Declaração da Kaspersky Security Network (KSN) e clique em **Avançar**.

5. Selecione o modo do aplicativo:

   - Modo Standard para proteger estações de trabalho e servidores

   - Endpoint Detection and Response Agent para garantir a proteção contra ameaças avançadas e ataques direcionados.

     Ao selecionar esse modo, é possível criar uma política para integrar o computador com as soluções do Kaspersky Detection and Response. O assistente solicita a configuração da integração para o Kaspersky Managed Detection and Response e, em seguida, para o Kaspersky Anti Targeted Attack Platform (EDR).

   - Light Agent para garantir a proteção em ambientes virtuais.

     Ao selecionar esse modo, na próxima etapa, é necessário configurar a conexão com o Servidor de proteção (SVM). Essas configurações são necessárias para que o aplicativo funcione no modo Light Agent.

O Kaspersky Endpoint Security fornece uma política comum para todos os modos de aplicativo e tipos de SO. Isso significa que a política abrange todo o conjunto de configurações. No entanto, o aplicativo pode ignorar algumas das configurações da política porque o Kaspersky Endpoint Security é implementado em um modo no qual algumas funcionalidades não estão disponíveis. Por exemplo, ao usar o aplicativo no modo Endpoint Detection and Response Agent, somente as configurações relevantes para a integração com as soluções do Kaspersky Detection and Response e para a integração com o KUMA estão disponíveis.

Recomendamos usar políticas diferentes para diferentes modos e tipos de sistema operacional.

6. Configure a zona confiável. É possível adicionar exclusões de verificação e aplicativos confiáveis predefinidos. As exclusões predefinidas de verificação e aplicativos confiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, Microsoft Exchange e System Center Configuration Manager. Isso significa que não será necessário configurar manualmente uma zona confiável para o aplicativo nos servidores. Exclusões de verificação e aplicativos confiáveis predefinidos também podem ajudar a configurar rapidamente o Kaspersky Endpoint Security no modo Light Agent em ambientes virtuais Citrix e VMware.

7. Na guia **Geral**, você pode executar as seguintes ações:

   - Alterar o nome da política.

   - Selecionar o status da política:

     - **Ativo**. Depois da sincronização seguinte, a política será usada como a política ativa no computador.

       As configurações de uma política ativa são salvas nos computadores clientes durante a sincronização. Você não pode aplicar simultaneamente várias políticas a um computador, portanto, apenas uma política pode estar ativa em cada grupo.

     - **Inativo**. Política de reserva. Se necessário, uma política inativa pode ser trocada para o status ativo.

       Você pode criar um número ilimitado de políticas inativas. Uma política inativa não afeta as configurações do aplicativo em computadores na rede. As políticas inativas funcionam como preparativos para situações de emergência, como um ataque de vírus. Se ocorrer um ataque por meio de pen drives, você poderá ativar uma política que bloqueie o acesso aos pen drives. Nesse caso, a política ativa torna-se automaticamente inativa.

     - **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 propriedades da política filha, o botão de alternância **Herdar configurações da política principal** será automaticamente ativado e não poderá ser desativado. 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**, você pode definir as configurações da política do Kaspersky Endpoint Security.

9. Conclua o assistente.

Como resultado, as configurações do Kaspersky Endpoint Security serão configuradas nos computadores clientes durante a próxima sincronização. É possível visualizar as informações sobre a política que está sendo aplicada ao computador na interface do Kaspersky Endpoint Security clicando no botão na tela principal (por exemplo, o nome da política). Para fazer isso, nas configurações da política do Agente de rede, você precisa habilitar o recebimento de dados de política estendidos. Para obter mais informações sobre uma política do Agente de rede, consulte a Ajuda do Kaspersky Security Center.

Exportação e importação de uma política

O Kaspersky Endpoint Security permite exportar uma política com suas configurações e perfis para um arquivo KLP. Então, é possível usar a funcionalidade de exportação/importação de políticas para fazer backup, migrá-las para outro servidor ou, por exemplo, migrá-las do Kaspersky Security Center Windows para o Kaspersky Security Center Linux. Para obter detalhes sobre o gerenciamento de políticas, consulte a ajuda do Kaspersky Security Center.

Como exportar e importar uma política no Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertencem os respectivos computadores clientes.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Para exportar uma política:
   a. Clique na política que deseja exportar.
   b. Clique no link **Exportar a política para arquivo** na parte direita da janela.
   c. Na janela exibida, especifique o nome do arquivo KLP para o qual deseja exportar a política e selecione a pasta na qual deseja salvar o arquivo.
   d. Salvar o arquivo.
5. Para importar uma política:
   a. Clique **Importar política de arquivo**.
   b. Na janela exibida, selecione o arquivo de política KLP que deseja importar.
   c. Abra o arquivo.

   O procedimento adiciona uma nova política com o status *Política inativa*.

Como exportar e importar a política no Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Para exportar uma política:
   a. Marque a caixa de seleção ao lado da política que deseja exportar.
   b. Clique no botão **Exportar**.

c. Na janela exibida, especifique o nome do arquivo KLP para o qual deseja exportar a política e selecione a pasta na qual deseja salvar o arquivo.

d. Salvar o arquivo.

3. Para importar uma política:

a. Clique **Importar**.

b. Selecione o arquivo de política KLP que deseja importar.

c. Depois que a política for processada com êxito, selecione o grupo de administração ao qual deseja aplicar a política.

d. Clique no botão **Concluída** para concluir a importação da política.

O procedimento adiciona uma nova política com o status *Inativo*.

Indicador do nível de segurança

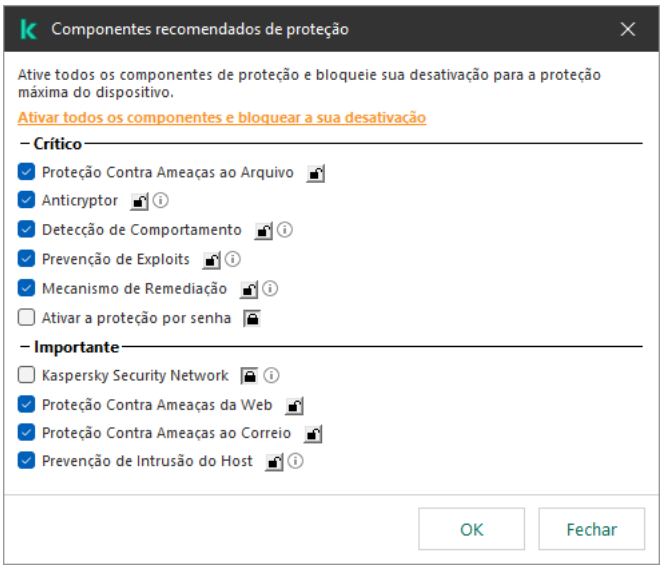
O indicador de nível de segurança é exibido na parte superior da janela de propriedades da política. O indicador pode assumir um dos seguintes valores:

- **Nível de proteção alto**. O indicador assume esse valor e ficará verde se todos os componentes das seguintes categorias forem ativados:
  - **Crítico**. Essa categoria inclui os seguintes componentes:
    - Proteção Contra Ameaças ao Arquivo.
    - Detecção de Comportamento.
    - Prevenção de Exploits.
    - Mecanismo de Remediação.
    - Proteção de serviços do aplicativo contra gerenciamento externo.
  - **Importante**. Essa categoria inclui os seguintes componentes:
    - Kaspersky Security Network.
    - Proteção Contra Ameaças da Web.
    - Proteção Contra Ameaças ao Correio.
    - Prevenção de Intrusão do Host.
    - Proteção por senha.
- **Nível de proteção médio**. O indicador assume esse valor e fica amarelo se um dos componentes importantes for desativado.

- **Nível de proteção baixo**. O indicador assume esse valor e fica vermelho em uma dos seguintes casos:
  - Um ou vários componentes críticos estão desativados.
  - Dois ou mais componentes importantes estão desativados.

Se o valor do indicador estiver no **Nível de proteção médio** ou **Nível de proteção baixo**, um link que abre a janela **Componentes recomendados de proteção** é exibido à direita do indicador. Nessa janela, você pode ativar qualquer um dos componentes de proteção recomendados.

Após atualizar o aplicativo, o indicador de nível de proteção pode indicar um nível de proteção inferior ao anterior ao da atualização. Isso ocorre porque a versão mais recente do aplicativo introduz novos componentes ou recursos importantes para a segurança do computador. Após atualizar o aplicativo, é necessário gerenciar as novas configurações para garantir que o nível de proteção permaneça alto.



Indicador de nível de segurança da política

Gerenciamento de tarefas

Você pode criar os seguintes tipos de tarefas na administração do Kaspersky Endpoint Security por meio do Kaspersky Security Center:

- Tarefas locais configuradas para um computador cliente individual.
- Tarefas de grupo configuradas para computadores clientes que pertencem aos grupos de administração.
- Tarefas para uma seleção de computadores.

Você pode criar qualquer número de tarefas de grupo, tarefas para uma seleção de computadores ou tarefas locais. Para obter mais informações sobre como trabalhar com grupos de administração e seleções de computadores, consulte a ajuda do Kaspersky Security Center.

O Kaspersky Endpoint Security dá suporte às seguintes tarefas:

- **Verificação de malware**. O Kaspersky Endpoint Security verifica as áreas do computador especificadas nas configurações da tarefa para detectar vírus e outras ameaças. A tarefa *Verificação de malware* é necessária para a operação do Kaspersky Endpoint Security e é criada durante o assistente de início rápido. Recomenda-se agendar a tarefa para ser executada pelo menos uma vez por semana.

- **Adicionar chave**. O Kaspersky Endpoint Security adiciona uma chave para ativar aplicativos, incluindo uma chave adicional. Antes de executar a tarefa, certifique-se de que o número de computadores nos quais a tarefa será executada não exceda o número de computadores permitidos pela licença.

- **Alterar componentes do aplicativo**. O Kaspersky Endpoint Security instala ou remove componentes em computadores de cliente segundo a lista de componentes especificados nas configurações da tarefa. O componente Proteção Contra Ameaças ao Arquivo não pode ser removido. O conjunto ideal de componentes do Kaspersky Endpoint Security ajuda a conservar recursos do computador.

- **Inventário**. O Kaspersky Endpoint Security recebe informações sobre todos os arquivos executáveis do aplicativo que estão armazenados nos computadores. A tarefa *Inventário* é executada pelo componente Controle de Aplicativos. Se o componente Controle de Aplicativos não for instalado, a tarefa terminará com um erro.

- **Atualização de bancos de dados e módulos do aplicativo**. O Kaspersky Endpoint Security atualiza bancos de dados e módulos do aplicativo. A tarefa *Atualização de bancos de dados e módulos do aplicativo* é necessária para a operação do Kaspersky Endpoint Security e é criada durante o assistente de início rápido. É recomendado configurar uma programação que execute a tarefa pelo menos uma vez por dia.

- **Limpar dados**. O Kaspersky Endpoint Security exclui arquivos e pastas dos computadores dos usuários imediatamente ou se não houver conexão com o Kaspersky Security Center por um longo período de tempo.

- **Reversão de atualização**. O Kaspersky Endpoint Security reverte a última atualização de bancos de dados e módulos do aplicativo. Isso pode ser necessário se, por exemplo, os novos bancos de dados contiverem dados incorretos que podem fazer com que o Kaspersky Endpoint Security bloqueie um aplicativo seguro.

- **Verificação de integridade do aplicativo**. O Kaspersky Endpoint Security analisa os arquivos de aplicativos, verifica se há corrupção ou modificações nos arquivos e verifica as assinaturas digitais dos arquivos de aplicativos.

- **Gerenciar contas do Agente de Autenticação**. O Kaspersky Endpoint Security define as configurações da conta do Agente de Autenticação. Um Agente de Autenticação é necessário para trabalhar com unidades criptografadas. Antes que o sistema operacional seja carregado, o usuário precisa concluir a autenticação com o Agente.

Caso o aplicativo esteja funcionando como parte da solução Endpoint Detection and Response da Kaspersky, será possível executar tarefas adicionais como ações de resposta de detecção (responses). Por exemplo, é possível encerrar os processos remotamente com o uso da tarefa *Encerrar processo*.

As tarefas são executadas em um computador apenas se o Kaspersky Endpoint Security estiver em execução.

Criação de uma tarefa

Como criar uma tarefa no console de administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Selecione a pasta **Tarefas** na árvore do Console de Administração.
3. Clique **Nova tarefa**.
   O Assistente de Tarefas é iniciado.
4. Siga as instruções do Assistente de Tarefas.

Como criar uma tarefa no Web Console

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.
   b. Na lista suspensa **Tipo de tarefa**, selecione a tarefa que deseja executar nos computadores dos usuários.
   c. No campo **Nome da tarefa**, insira uma breve descrição.
   d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.
4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Vá para a próxima etapa.
5. Selecione uma conta para executar a tarefa. Por padrão, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de usuário local.
6. Conclua o assistente.

Uma nova tarefa será exibida na lista de tarefas. A tarefa terá as configurações padrão. Para configurar as configurações da tarefa, vá para as propriedades da tarefa. Para executar uma tarefa, é necessário marcar a caixa de seleção ao lado da tarefa e clicar no botão **Iniciar**. Após o início da tarefa, você pode pausar e retomar a tarefa mais tarde.

Na lista de tarefas, você pode monitorar os resultados da tarefa, que incluem o status da tarefa e as estatísticas do desempenho da tarefa nos computadores. Também é possível criar uma seleção de eventos para monitorar a conclusão das tarefas (**Monitoramento** → **Seleções de eventos**). Para obter mais detalhes sobre a seleção de eventos, consulte a ajuda do Kaspersky Security Center. Os resultados da execução da tarefa também são salvos localmente no log de eventos do Windows e nos relatórios do Kaspersky Endpoint Security.

Gerenciamento de acesso da tarefa

Os direitos de acesso às tarefas do Kaspersky Endpoint Security (ler, gravar, executar) são definidos para cada usuário com acesso ao Servidor de Administração do Kaspersky Security Center através das configurações do acesso a áreas funcionais do Kaspersky Endpoint Security. Para configurar o acesso a áreas funcionais do Kaspersky Endpoint Security, acesse a seção **Segurança** da janela de propriedades do Servidor de Administração do Kaspersky Security Center. Para obter mais detalhes sobre o gerenciamento de tarefas por meio do Kaspersky Security Center, consulte a Ajuda do Kaspersky Security Center.

É possível configurar os direitos dos usuários para acessar tarefas com o uso de uma política (*modo de gerenciamento de tarefas*). Por exemplo, você pode ocultar tarefas de grupo na interface do Kaspersky Endpoint Security.

Como configurar o modo de gerenciamento de tarefas na interface do Kaspersky Endpoint Security através do Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Tarefas locais** → **Gerenciamento de tarefas**.
4. Configure o modo de gerenciamento de tarefas (consulte a tabela abaixo).
5. Salvar alterações.

Como configurar o modo de gerenciamento de tarefas na interface do Kaspersky Endpoint Security por meio do Web Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Interação com o usuário**.
5. Em **Ações permitidas**, configure o modo de gerenciamento de tarefas (consulte a tabela abaixo).
6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Configurações do gerenciamento de tarefas

Parâmetro	Descrição
Acessar tarefas locais	Se a caixa de seleção for marcada, as tarefas locais serão exibidas na interface local do Kaspersky Endpoint 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 essa caixa de seleção estiver desmarcada, as tarefas locais ficarão ocultas na interface do aplicativo. 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 Endpoint Security, ou ao trabalhar com a linha de comando. Um usuário ainda pode iniciar uma verificação de um Arquivo ou pasta selecionando a opção **Verificar Vírus** no menu de contexto do arquivo ou da pasta. A tarefa de verificação é iniciada com os valores padrões de configurações da tarefa de verificação personalizada.

Parâmetro	Descrição
Visualizar tarefas de grupo	Se a caixa de seleção for marcada, as tarefas de grupo serão exibidas na interface local do Kaspersky Endpoint Security. O usuário pode visualizar a lista de todas as tarefas na interface do aplicativo. Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security exibe uma lista de tarefas vazia.
Gerenciar tarefas de grupo	Se a caixa de seleção estiver marcada, os usuários podem iniciar e interromper as tarefas de grupo especificadas no console do Kaspersky Security Center. Os usuários podem iniciar e parar tarefas na interface do aplicativo ou na interface simplificada do aplicativo. Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security inicia tarefas agendadas automaticamente ou o administrador inicia tarefas manualmente no console do Kaspersky Security Center.

Definir as configurações locais do aplicativo

No Kaspersky Security Center, você pode definir as configurações do Kaspersky Endpoint Security em um determinado computador. Elas constituem as *configurações locais do aplicativo*. Algumas configurações podem não estar acessíveis para edição. Essas configurações estão bloqueadas pelo atributo 🔒 nas propriedades da política.

Como definir as configurações locais do aplicativo no Console de administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertencem os respectivos computadores clientes.
3. No espaço de trabalho, selecione a guia **Dispositivos**.
4. Clique duas vezes para abrir a janela de propriedades do computador.
5. Na janela de propriedades do computador, selecione a seção **Aplicativos**.
6. Na lista de aplicativos da Kaspersky instalados no computador, selecione **Kaspersky Endpoint Security for Windows (14.2)** e clique duas vezes para abrir as propriedades do aplicativo.
7. Na seção **Configurações gerais**, configure o Kaspersky Endpoint Security, bem como relatórios e armazenamento.

   As demais seções na janela de propriedades do aplicativo são padrão para o Kaspersky Security Center. Uma descrição dessas seções é fornecida na Ajuda do Kaspersky Security Center.

   > Se um aplicativo estiver sujeito a uma política que proíbe modificações de configurações específicas, não será possível editá-las ao definir a configuração do aplicativo na seção **Configurações gerais**.

8. Salvar alterações.

Como definir as configurações locais do aplicativo no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Ativos (dispositivos)**.
2. Selecione o computador para o qual você deseja definir as configurações locais do aplicativo.

   Isso abre as propriedades do computador.
3. Selecione a guia **Aplicativos**.

4. Clique **Kaspersky Endpoint Security for Windows 14.2**.

   Isso abre as configurações locais do aplicativo.

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

6. Defina as configurações locais do aplicativo.

7. Salvar alterações.

As configurações locais do aplicativo são iguais às configurações da política, exceto pelas configurações de criptografia.

Iniciar e interromper o Kaspersky Endpoint Security

Depois de instalar o Kaspersky Endpoint Security no computador de um usuário, o aplicativo é iniciado automaticamente. Por padrão, o Kaspersky Endpoint 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 Endpoint Security após o início do sistema operacional pode levar até dois minutos, dependendo dos recursos do computador. Durante este tempo, o nível da proteção do computador é reduzido. O download de bancos de dados de antivírus quando Kaspersky Endpoint Security é iniciado em um sistema operacional já iniciado não causa uma redução do nível de proteção do computador.

Como configurar a inicialização do Kaspersky Endpoint Security no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Configurações gerais** → **Configurações de aplicativos**.

4. Usar a caixa de seleção **Iniciar o aplicativo na inicialização do computador (recomendado)** para configurar a inicialização do aplicativo.

5. Salvar alterações.

Como configurar a inicialização do Kaspersky Endpoint Security no Web Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Interação com o usuário**.

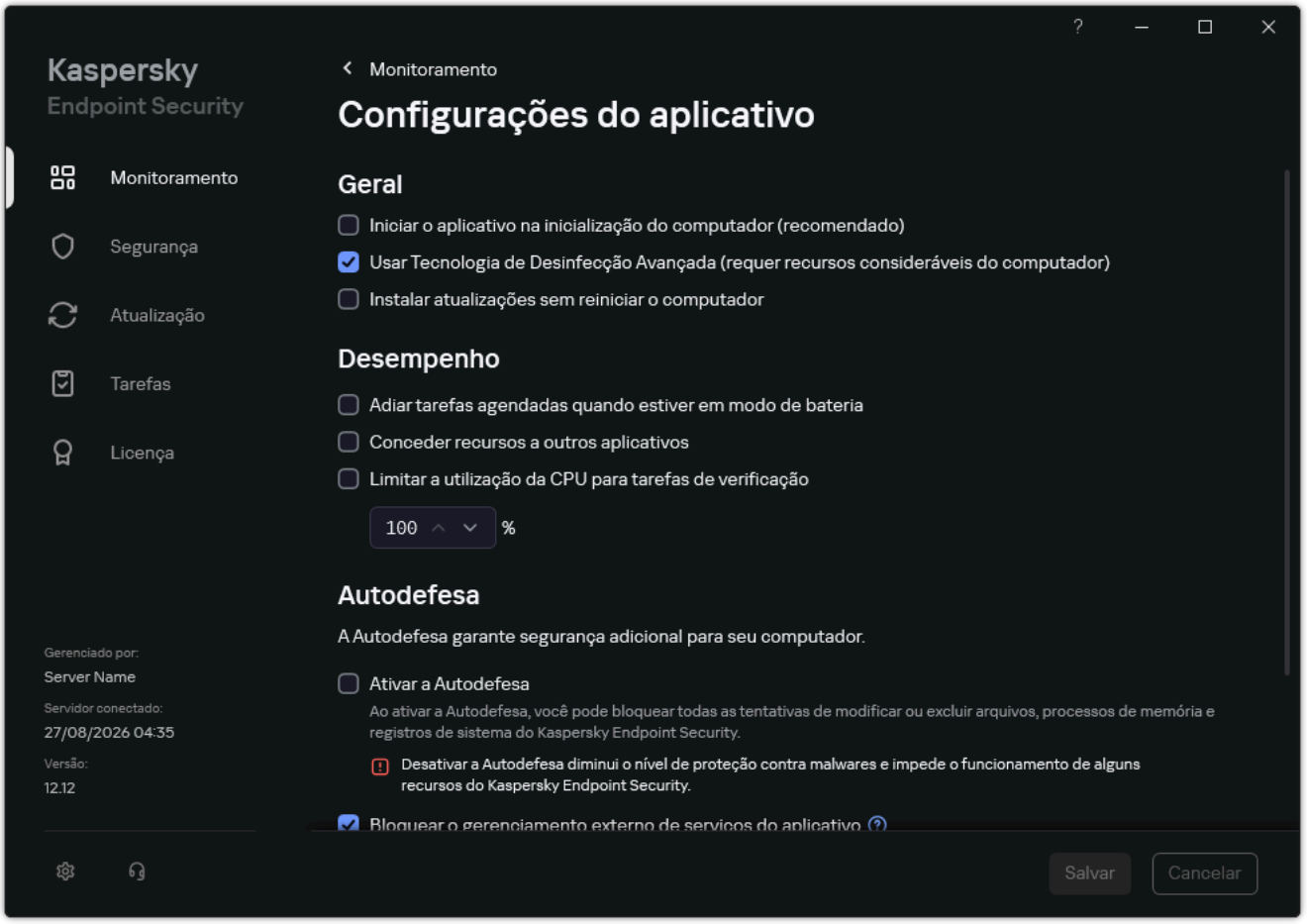
5. Usar a caixa de seleção **Iniciar o Kaspersky Endpoint Security durante a inicialização do computador (recomendado)** para configurar a inicialização do aplicativo.

6. Salvar alterações.

Como configurar a inicialização do Kaspersky Endpoint Security na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações do aplicativo**.



Configurações do Kaspersky Endpoint Security for Windows

3. Usar a caixa de seleção **Iniciar o aplicativo na inicialização do computador (recomendado)** para configurar a inicialização do aplicativo.

4. Salvar alterações.

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

É possível monitorar o status do aplicativo usando o widget **Status da proteção**.

Como iniciar ou parar o Kaspersky Endpoint Security no Console de administração (MMC)

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

2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertencem os respectivos computadores clientes.

3. No espaço de trabalho, selecione a guia **Dispositivos**.

4. Clique duas vezes para abrir a janela de propriedades do computador.

5. Na janela de propriedades do computador, selecione a seção **Aplicativos**.

6. Na lista de aplicativos da Kaspersky instalados no computador, selecione **Kaspersky Endpoint Security for Windows (14.2)** e clique duas vezes para abrir as propriedades do aplicativo.

7. Realize 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 parar o Kaspersky Endpoint Security no Web Console

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

2. Clique no nome do computador no qual você quer iniciar ou interromper o Kaspersky Endpoint Security.

   A janela de propriedades do computador é exibida.

3. Selecione a guia **Aplicativos**.

4. Marque a caixa de seleção ao lado de **Kaspersky Endpoint Security for Windows**.

5. Clique nos botões **Iniciar** ou **Parar**.

Como iniciar ou parar o Kaspersky Endpoint Security na linha de comando

1. Execute o interpretador da linha de comando (cmd.exe) como um administrador.

2. Vá para a pasta onde se encontra o arquivo executável klpsm.exe.

3. Para iniciar o aplicativo a partir da linha de comando, insira `klpsm.exe start_avp_service`.

4. Para parar o aplicativo na linha de comando, insira `klpsm.exe stop_avp_service`.

> Para interromper o aplicativo por meio da linha de comando, ative o gerenciamento externo dos serviços do sistema.

Iniciar e encerrar o aplicativo a partir da linha de comando

Pausar e reiniciar a Proteção e Controle do computador

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

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

- O ícone indica que a proteção e o controle do computador foram pausados.
- O ícone indica que a proteção e o controle do computador estão 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. Clique com o botão direito do mouse para abrir o ícone do menu de contexto do aplicativo que está na área de notificação da barra de tarefas.
2. No menu de contexto, selecione **Pausar a proteção** (veja a figura abaixo).

   Este item do menu de contexto está disponível se a Proteção por senha estiver ativada.
3. Selecione uma das seguintes opções:
   - **Pausar por <intervalo de tempo>** – a proteção e o controle do computador serão reiniciados após decorrer o tempo especificado na lista suspensa abaixo.
   - **Pausar até a reinicialização do aplicativo**– 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.
4. Clique **Pausar a proteção**.

   O Kaspersky Endpoint Security pausará a operação de proteção e controle de todos os componentes que não estiverem bloqueados ( ) na política. Antes de executar essa operação, recomenda-se desativar a política do Kaspersky Security Center.

Menu de contexto do ícone do aplicativo

Para reiniciar a proteção e controle do computador:

1. Clique com o botão direito do mouse para abrir o ícone do menu de contexto do aplicativo que está na área de notificação da barra de tarefas.

2. No menu de contexto, selecione **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.

Criar e usar um arquivo de configuração

Um arquivo de configuração com configurações do Kaspersky Endpoint Security permite que você realize as seguintes tarefas:

- Executar a instalação local do Kaspersky Endpoint Security via linha de comando com configurações predefinidas.

- Executar a instalação remota do Kaspersky Endpoint Security via Kaspersky Security Center com configurações predefinidas.

- Transferir configurações do aplicativo para uma política.

- Migrar as configurações do Kaspersky Endpoint Security de um computador para outro (consulte as instruções abaixo).

Exportação de um arquivo de configuração

A partir da versão 14.2 do Kaspersky Endpoint Security, o arquivo de configuração exportado pode ser criptografado. Como o arquivo de configuração pode conter credenciais, recomendamos criptografá-lo. Não é possível editar um arquivo criptografado. Qualquer tentativa de modificação de um arquivo de configuração o tornará corrompido.

A criptografia do arquivo de configuração possui os seguintes recursos especiais:

- O Kaspersky Endpoint Security permite importar arquivos criptografados somente na interface do usuário do aplicativo ou na linha de comando. Não é possível usar esse arquivo em um console do Kaspersky Security Center para configurar uma política ou instalar o aplicativo remotamente. Se você pretende adicionar o arquivo a uma política ou a um pacote de instalação, ignore a etapa de criptografia do arquivo.

- Não é possível recuperar a senha de um arquivo criptografado.

- As versões do Kaspersky Endpoint Security anteriores à 14.1 não são compatíveis com a importação de arquivos de configuração criptografados. Se você pretende importar o arquivo para uma versão anterior do aplicativo, ignore a etapa de criptografia do arquivo.

Para criar o arquivo de configuração:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Gerenciar configurações**.
3. Clique **Exportar**.
4. Para salvar o arquivo de configuração, a Proteção por senha deve estar ativada. O usuário deve ter a permissão **Exportar configurações**.
5. Na janela exibida, especifique o caminho no qual você quer salvar o arquivo de configuração e digite o seu nome.

   Para usar o arquivo de configuração para a instalação local ou remota do Kaspersky Endpoint Security, é necessário nomeá-lo para install.cfg.

6. Se necessário, ative o botão de alternância **Criptografar o arquivo exportado** e insira a senha de criptografia do arquivo de configuração.

   Salve a senha em um armazenamento seguro. Não é possível recuperar essa senha.

7. Salvar o arquivo.

Assim, o aplicativo criará um arquivo de configuração.

Importação de um arquivo de configuração

Ao importar um arquivo de configuração, o Kaspersky Endpoint Security não transfere as senha do contêiner de criptografia. Caso use a autenticação bidirecional ao se conectar aos servidores, será necessário especificar as senhas do contêiner de criptografia do zero.

Para importar configurações do Kaspersky Endpoint Security de um arquivo de configuração:

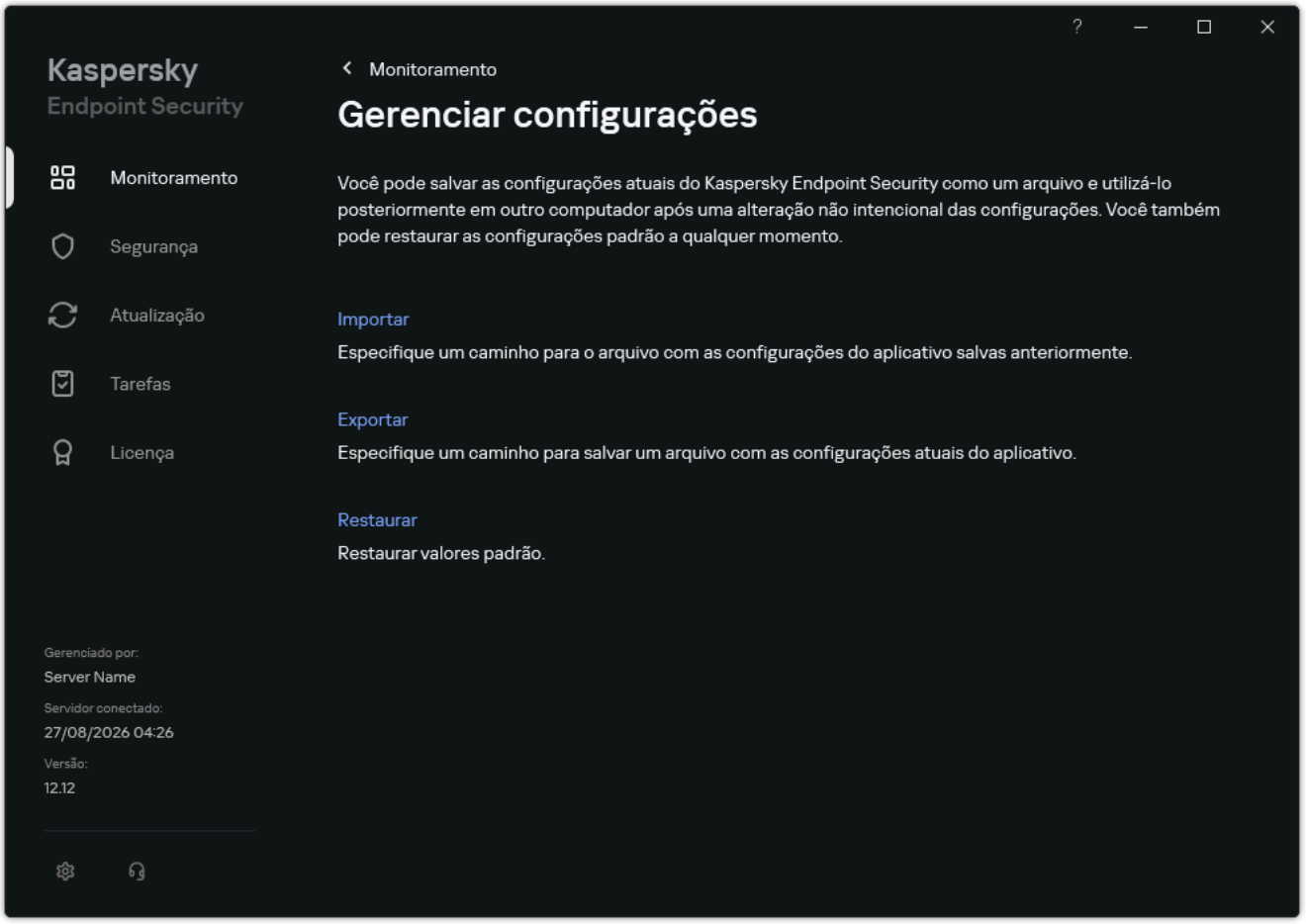
1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Gerenciar configurações**.
3. Clique **Importar**.
4. Na janela exibida, insira o caminho para o arquivo de configuração.

5. Se o arquivo de configuração estiver criptografado, insira a senha especificada durante a exportação.

> Se você esquecer a senha de criptografia do arquivo de configuração, não será possível recuperá-la. Nesse caso, será necessário repetir as etapas de exportação do arquivo de configuração.

6. Abra o arquivo.

Todos os valores das configurações do Kaspersky Endpoint Security serão definidos de acordo com o arquivo de configuração selecionado.



Gerenciamento das configurações do aplicativo

Restaurar as configurações padrão do aplicativo

É possível restaurar as configurações do aplicativo recomendadas pela Kaspersky a qualquer momento. Quando as configurações são restauradas, o nível de segurança **Recomendado** é definido para todos os componentes de proteção.

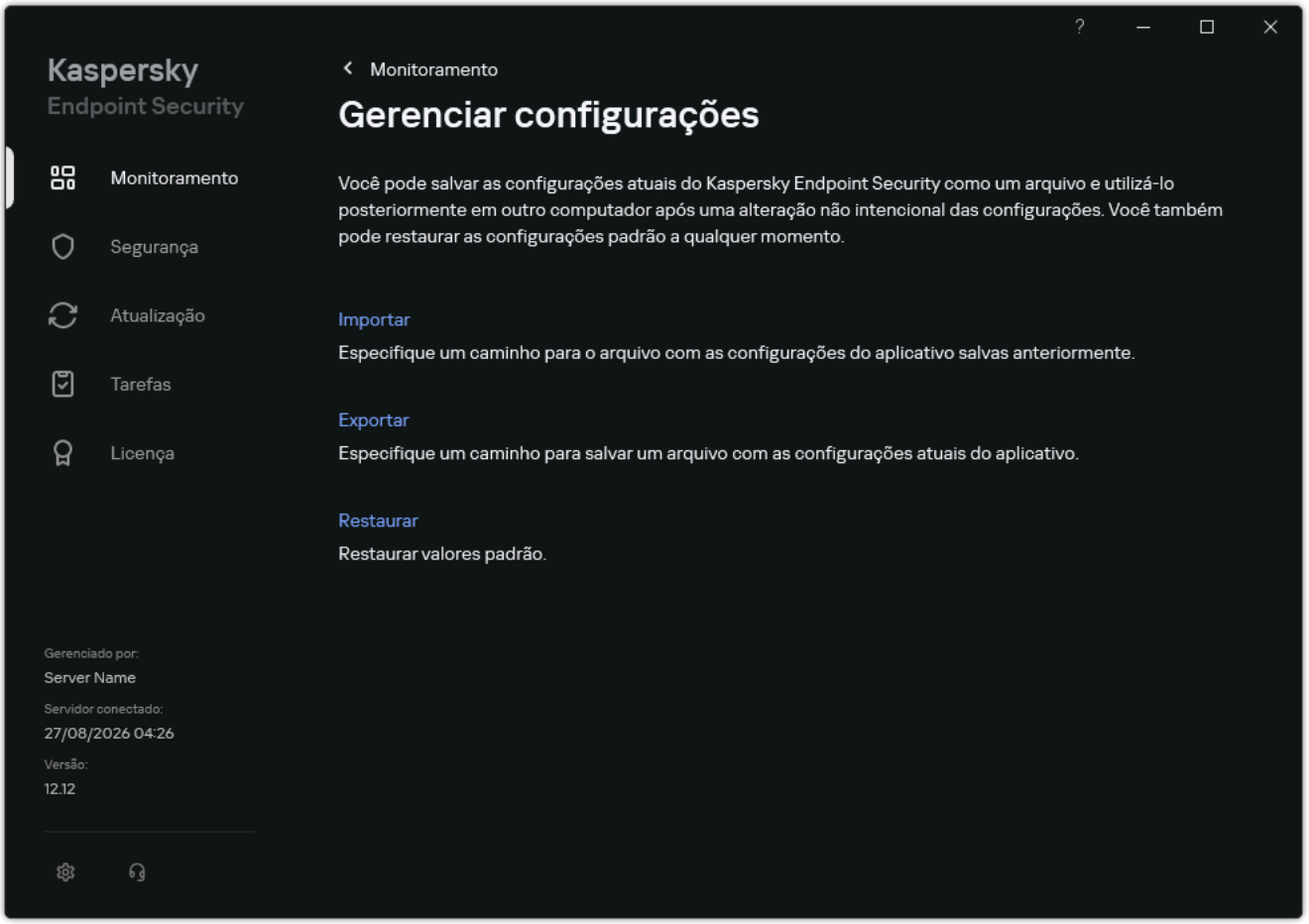
Para restaurar as configurações padrão do aplicativo:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Gerenciar configurações**.

3. Clique **Restaurar**.

4. Salvar alterações.



Gerenciamento das configurações do aplicativo

Desempenho e compatibilidade do Kaspersky Endpoint Security com outros aplicativos

O desempenho do Kaspersky Endpoint Security refere-se ao número de tipos de objeto que podem danificar o computador que são detectáveis, bem como o consumo de energia e de recursos do computador.

Selecionar tipos de objetos detectáveis

O Kaspersky Endpoint Security permite ajustar detalhadamente a proteção de seu computador e selecionar os tipos de objetos que o aplicativo detecta durante a operação. O Kaspersky Endpoint Security sempre verifica o sistema operacional para detectar vírus, worms e Cavalos de troia. Não é possível desativar a verificação de objetos desse tipo. Estes malware conseguem causar grandes danos ao computador. O aumento da segurança do computador é obtido com a expansão da gama de tipos de objetos, que podem ser detectados por meio do controle de softwares legais que podem ser usados por criminosos para danificar o computador ou os dados pessoais.

Usar o modo de economia de energia

No que diz respeito a laptops, o consumo de energia devido ao uso de aplicativos precisa ser levado em consideração. As tarefas agendadas do Kaspersky Endpoint Security geralmente utilizam uma grande quantidade de recursos. Quando o computador está ligado usando a bateria, você pode usar o modo de economia de energia para poupar esta.

No modo de economia de energia, as seguintes tarefas agendadas são adiadas automaticamente:

- Tarefa de verificação completa;
- Tarefa de verificação de áreas críticas;
- Tarefa de verificação personalizada;
- Tarefa de verificação de integridade.

Quer o modo de economia de energia esteja ou não ativo, o Kaspersky Endpoint Security pausa as tarefas de criptografia quando um computador portátil alterna para a energia da bateria. O aplicativo continua as tarefas de criptografia quando o computador portátil alterna da energia da bateria para energia elétrica.

Conceder recursos a outros aplicativos

O consumo de recursos do computador durante sua verificação pode aumentar a carga na CPU e nos subsistemas do disco rígido. Para resolver o problema da operação simultânea durante um maior carregamento da CPU e de subsistemas do disco rígido, o Kaspersky Endpoint Security pode conceder mais recursos a outros aplicativos.

Usar a tecnologia de desinfecção avançada

Os aplicativos maliciosos atuais conseguem invadir os níveis mais baixos de um sistema operacional, o que torna praticamente impossível excluí-los. Depois de detectar atividade maliciosa no sistema operacional, o Kaspersky Endpoint Security executa um procedimento de desinfeção extenso que usa uma tecnologia de desinfecção avançada especial. A *tecnologia de desinfecção avançada* objetiva eliminar do sistema operacional aplicativos maliciosos que já iniciaram seus processos na RAM e que impedem que o Kaspersky Endpoint Security os remova, usando outros métodos. Como resultado, a ameaça é neutralizada. Enquanto a Desinfecção Avançada estiver em andamento, é recomendável abster-se de iniciar novos processos ou editar os registros do sistema operacional. A tecnologia de desinfecção avançada usa uma grande quantidade de recursos do sistema operacional, que talvez torne os outros aplicativos mais lentos.

Depois que o processo de Desinfecção avançada estiver concluído em um computador executando o Microsoft Windows para estações de trabalho, o Kaspersky Endpoint Security solicitará a permissão do usuário para reiniciar o computador. Após a reinicialização do sistema, o Kaspersky Endpoint Security exclui os arquivos de malware files e inicia uma verificação completa "leve" do computador.

Uma solicitação de reinicialização é impossível em computadores que executem o Microsoft Windows para servidores devido às especificações do Kaspersky Endpoint Security para servidores de arquivos. Uma reinicialização não planejada de um servidor de arquivos pode gerar problemas envolvendo a indisponibilidade temporária dos dados do servidor ou perda de dados não salvos. É recomendável reiniciar um servidor de arquivos estritamente de acordo com o agendamento. É por isso que a Tecnologia de Desinfecção Avançada é desativada por padrão para servidores de arquivos.

Se uma infecção ativa for detectada em um servidor de arquivos, ela é retransmitida ao Kaspersky Security Center com a informação de que é necessária a Desinfecção avançada. Para desinfetar uma infecção ativa em um servidor, ative a Tecnologia de Desinfecção Avançada para servidores e inicie uma tarefa de grupo de *Verificação de malware* em um horário conveniente para os usuários do servidor.

Ativar ou desativar o modo de economia de energia

Modo de economia de energia é uma funcionalidade que reduz a carga sobre os recursos do laptop e prolonga a vida útil da bateria sem comprometer significativamente o nível de segurança. No modo de economia de energia, o aplicativo limita a execução de tarefas agendadas. Dessa forma, o modo de economia de energia garante um equilíbrio entre o nível de segurança e a duração da bateria do laptop.

Quando o modo de economia de energia está ativado e um computador está funcionando com a bateria, as seguintes tarefas não são executadas, mesmo que estejam programadas:

- *Verificação completa*.
- *Verificação de áreas críticas*.
- *Verificação personalizada*.
- *Verificação de integridade do aplicativo*.
- *Verificação de IOC*.
- *Atualização de bancos de dados e módulos do aplicativo* (somente patches)

O aplicativo ignora as atualizações agendadas dos bancos de dados somente quando o laptop está sendo alimentado pela bateria e o nível de carga está abaixo de 30% (valor padrão). Você pode alterar, por meio da edição do registro, o nível mínimo de carga da bateria a partir do qual o aplicativo começa a ignorar as atualizações agendadas do banco de dados de antivírus (consulte as instruções abaixo). Em todos os outros casos, o Kaspersky Endpoint Security atualiza os bancos de dados de acordo com o agendamento, independentemente do laptop estar conectado ou funcionando com energia da bateria ou se o aplicativo estiver no modo de economia de energia.

Como ativar ou desativar o modo de economia de energia no Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Configurações gerais** → **Configurações de aplicativos**.

5. No bloco **Desempenho**, use a caixa de seleção **Adiar tarefas agendadas quando estiver em modo de bateria** para ativar ou desativar o modo de economia de energia.

6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar ou desativar o modo de economia de energia no Web Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Desempenho**.

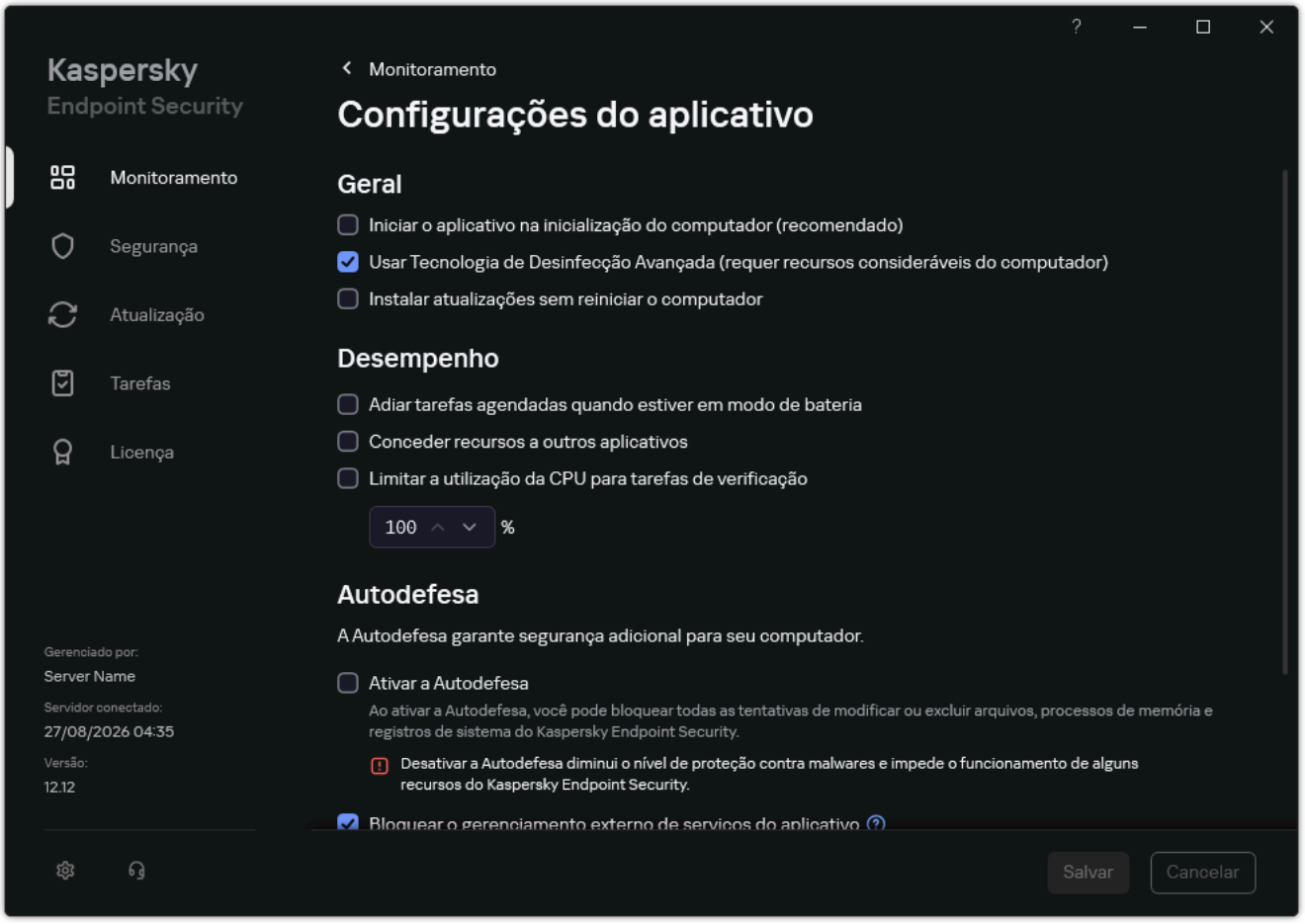
5. No bloco **Adiar ou ignorar tarefas agendadas quando estiver em modo de bateria**, use a caixa de seleção **Adiar ou ignorar tarefas agendadas quando estiver em modo de bateria (depende do SO)** para ativar ou desativar o modo de economia de energia.

6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar ou desativar o modo de economia de energia na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações do aplicativo**.



Configurações do Kaspersky Endpoint Security for Windows

3. No bloco **Desempenho**, use a caixa de seleção **Adiar tarefas agendadas quando estiver em modo de bateria** para ativar ou desativar o modo de economia de energia.

4. Salvar alterações.

Como alterar o nível mínimo de carga a partir do qual o aplicativo começa a ignorar as atualizações agendadas do banco de dados de antivírus

1. Abra o editor de registro no computador.

2. No editor de registro, vá para a seguinte seção:

   - Para sistemas operacionais de 64 bits:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES.14.2\environment`

   - Para sistemas operacionais de 32 bits:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\environment]`

3. Abra `UpdaterAccumulatorThreshold` para edição.

4. Especifique o nível mínimo de carga a partir do qual o aplicativo começa a ignorar as atualizações agendadas do banco de dados de antivírus.

Ativar ou desativar a concessão de recursos a outros aplicativos

O consumo de recursos do computador pelo Kaspersky Endpoint 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 Endpoint 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 Endpoint 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 Endpoint Security leva mais tempo. Por padrão, o aplicativo está configurado para ceder recursos a outros aplicativos.

Como ativar ou desativar a concessão de recursos a outros aplicativos no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Configurações gerais** → **Configurações de aplicativos**.

4. No bloco **Desempenho**, use a caixa de seleção **Conceder recursos a outros aplicativos** para ativar ou desativar a concessão de recursos a outros aplicativos.

5. Salvar alterações.

Como ativar ou desativar a concessão recursos a outros aplicativos no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Desempenho**.

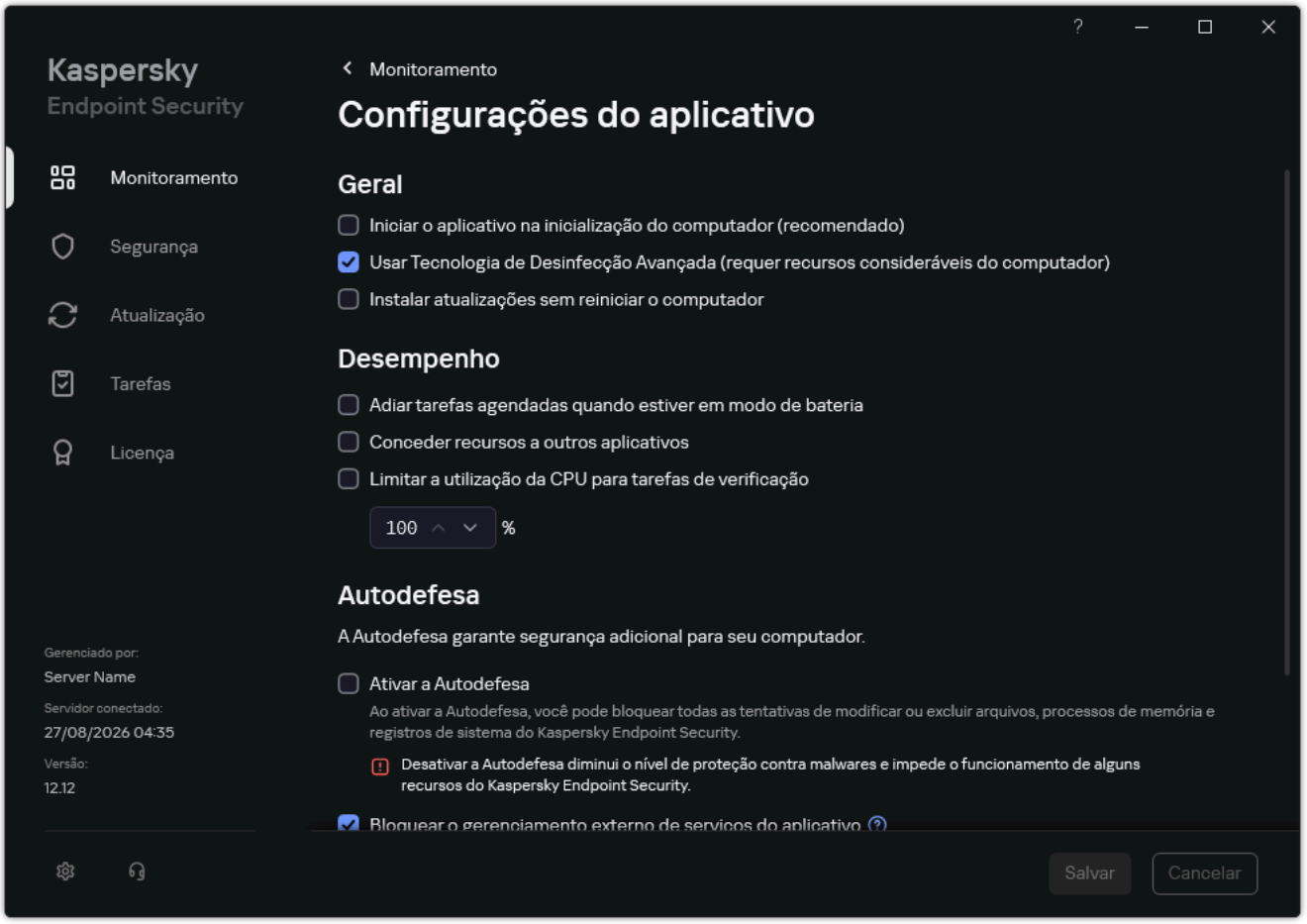
5. No bloco **Conceder recursos a outros aplicativos**, ative o botão de alternância **Conceder recursos a outros aplicativos** para ativar ou desativar a concessão de recursos a outros aplicativos.

6. Salvar alterações.

Como ativar ou desativar a concessão de recursos a outros aplicativos na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações do aplicativo**.



Configurações do Kaspersky Endpoint Security for Windows

3. No bloco **Desempenho**, use a caixa de seleção **Conceder recursos a outros aplicativos** para ativar ou desativar a concessão de recursos a outros aplicativos.

4. Salvar alterações.

Práticas recomendadas para otimizar o desempenho do Kaspersky Endpoint Security

Ao implantar o Kaspersky Endpoint Security for Windows, é possível utilizar as seguintes recomendações para configurar a proteção do computador e otimizar o desempenho. Para obter mais informações sobre como lidar com problemas de desempenho do computador, consulte a Base de Dados de Conhecimento do Suporte Técnico.

Geral

Defina as configurações gerais do aplicativo de acordo com as seguintes recomendações:

1. Atualize o Kaspersky Endpoint Security para a versão mais recente.

   As versões mais recentes do aplicativo corrigem erros, têm testabilidade aprimorada e desempenho otimizado.

2. Ative os componentes de proteção com as configurações padrão.

   As configurações padrão são consideradas ideais. Elas são recomendadas pelos peritos da Kaspersky. As configurações padrão fornecem o nível de proteção recomendado e o uso ideal de recursos. Se necessário, é possível restaurar as configurações padrão do aplicativo.

3. Ative os recursos de otimização de desempenho do aplicativo.

   O aplicativo possui recursos de otimização de desempenho: modo de conservação de energia e concessão de recursos para outros aplicativos. Certifique-se de que essas opções estejam ativadas.

Verificação de malware em estações de trabalho

A ativação da Verificação em segundo plano é recomendada para a Verificação de malware em estações de trabalho. *Verificação em segundo plano* é um modo de verificação do Kaspersky Endpoint Security que não exibe notificações ao usuário. A verificação em segundo plano utiliza menos recursos do computador do que outros tipos de verificações (como uma verificação completa). Neste modo, o Kaspersky Endpoint Security verifica os objetos de inicialização, o setor de inicialização, a memória do sistema e a partição do sistema. As configurações de verificação em segundo plano são consideradas ideais. Elas são recomendadas pelos peritos da Kaspersky. Assim, para realizar uma Verificação de malware no computador, é possível utilizar apenas o modo de verificação em segundo plano, sem utilizar outras tarefas de verificação.

Caso a verificação em segundo plano não atenda suas necessidades, configure a tarefa de *Verificação de malware* de acordo com as seguintes recomendações:

1. Defina um limite para o consumo de recursos da CPU durante a verificação do computador.

   É possível limitar o uso da CPU ao executar a tarefa *Verificação de malware*. Para fazer isso, nas configurações do aplicativo, especifique a porcentagem máxima de carga da CPU para todos os núcleos que podem ser usados durante a verificação do computador. Isso pode aumentar o tempo necessário para verificar seu computador.

2. Configure a programação ideal de verificação do computador.

   É possível configurar a tarefa para ser executada quando o computador estiver operando com carga mínima. Por exemplo, é possível configurar a tarefa para ser executada à noite ou nos finais de semana.

   Caso os usuários desliguem o computador fora do horário comercial, será possível ativar a função Wake-on-LAN. O recurso Wake-on-LAN permite ligar o computador remotamente, por meio do envio de um sinal especial pela rede local. Para utilizar esse recurso, é necessário ativar o Wake-on-LAN nas configurações do BIOS. Também é possível desligar o computador automaticamente após o término da verificação.

   Caso não consiga configurar um cronograma de verificação ideal, defina as tarefas para serem executadas apenas quando o computador estiver ocioso. O Kaspersky Endpoint Security inicia a tarefa de verificação se o computador estiver bloqueado ou se a proteção de tela estiver ativada. Caso interrompa a execução da tarefa, por exemplo, desbloqueando o computador, o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que foi interrompido.

3. Defina um escopo da verificação.

   Selecione os seguintes objetos para verificação (conjunto mínimo de escopos de verificação):

   - Memória Kernel
   - Executando processos e Objetos de inicialização
   - Setores de inicialização
   - %systemroot% (sem incluir subpastas)
   - %systemroot%\System (sem incluir subpastas)
   - %systemroot%\System32 (sem incluir subpastas)
   - %systemroot%\System32\drivers (sem incluir subpastas)
   - %systemroot%\SysWOW64 (sem incluir subpastas)
   - %systemroot%\SysWOW64\drivers (sem incluir subpastas)

4. Ativar as tecnologias iSwift e iChecker.

   - Tecnologia iSwift.

     Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iSwift é um avanço da tecnologia iChecker do sistema de arquivos NTFS.

   - Tecnologia iChecker.

     Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iChecker tem algumas limitações: ela não funciona com arquivos grandes e se aplica somente a objetos com uma estrutura reconhecida pelo aplicativo (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

   Só é possível ativar as tecnologias iSwift e iChecker no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security. Não é possível ativar essas tecnologias no Kaspersky Security Center Web Console.

5. Desative a verificação de arquivos protegidos por senha.

   Caso a verificação de arquivos protegidos por senha estiver ativada, um prompt de senha será exibido antes que o arquivo seja verificado. Como é recomendado que a tarefa seja agendada durante o horário ausente, o usuário não poderá inserir a senha. É possível verificar os arquivos protegidos por senha manualmente.

6. Desativar a inicialização simultânea de várias tarefas de verificação.

   O Kaspersky Endpoint Security enfileirará novas tarefas de verificação se a verificação atual continuar. Isso ajuda a otimizar a carga no computador.

Verificação de malware nos servidores

Configure a tarefa de *Verificação de malware* de acordo com as seguintes recomendações:

1. Defina um limite para o consumo de recursos da CPU durante a verificação do computador.

   É possível limitar o uso da CPU ao executar a tarefa *Verificação de malware*. Para fazer isso, nas configurações do aplicativo, especifique a porcentagem máxima de carga da CPU para todos os núcleos que podem ser usados durante a verificação do computador. Isso pode aumentar o tempo necessário para verificar seu computador.

2. Configure a programação ideal de verificação do computador.

   É possível configurar a tarefa para ser executada quando o computador estiver operando com carga mínima. Por exemplo, é possível configurar a tarefa para ser executada à noite ou nos finais de semana.

3. Ativar as tecnologias iSwift e iChecker.

   - Tecnologia iSwift.

     Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iSwift é um avanço da tecnologia iChecker do sistema de arquivos NTFS.

   - Tecnologia iChecker.

     Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iChecker tem algumas limitações: ela não funciona com arquivos grandes e se aplica somente a objetos com uma estrutura reconhecida pelo aplicativo (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

   Só é possível ativar as tecnologias iSwift e iChecker no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security. Não é possível ativar essas tecnologias no Kaspersky Security Center Web Console.

4. Desative a verificação de arquivos protegidos por senha.

   Caso a verificação de arquivos protegidos por senha estiver ativada, um prompt de senha será exibido antes que o arquivo seja verificado. Como é recomendado que a tarefa seja agendada durante o horário ausente, o usuário não poderá inserir a senha. É possível verificar os arquivos protegidos por senha manualmente.

5. Desativar a inicialização simultânea de várias tarefas de verificação.

   O Kaspersky Endpoint Security enfileirará novas tarefas de verificação se a verificação atual continuar. Isso ajuda a otimizar a carga no computador.

Kaspersky Security Network

Para melhorar a proteção do computador, o Kaspersky Endpoint Security usa dados recebidos de usuários em todo o mundo. O Kaspersky Security Network foi criado para obter esses dados.

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 Endpoint Security a novas ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos positivos. Caso participe da Kaspersky Security Network, os serviços da KSN fornecem à Kaspersky Endpoint Security informações sobre a reputação dos endereços da Web verificados, além de informações sobre a categoria e a reputação dos arquivos verificados.

Edite as configurações do Kaspersky Security Network de acordo com as seguintes recomendações:

1. Desative o modo KSN estendido.

   O *modo KSN estendido* é um modo no qual o Kaspersky Endpoint Security envia dados adicionais para a Kaspersky.

2. Configurar a Kaspersky Private Security Network.

   A *Kaspersky Private Security Network (KPSN)* é uma solução que permite aos usuários de computadores que hospedam o Kaspersky Endpoint 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.

3. Ativar modo na nuvem.

   O *Modo nuvem* refere-se ao modo operacional do aplicativo no qual o Kaspersky Endpoint Security usa uma versão simplificada dos bancos de dados de antivírus. A Kaspersky Security Network oferece suporte ao funcionamento do aplicativo quando bancos de dados de antivírus leves estão em uso. A versão leve dos bancos de dados de antivírus permite usar aproximadamente metade da RAM do computador que, de outra forma, seria usada nos bancos de dados comuns. Se você não participa da Kaspersky Security Network ou se o modo de nuvem está desativado, o Kaspersky Endpoint Security faz o download da versão completa dos bancos de dados antivírus dos servidores da Kaspersky.

Verificação de malware

Uma verificação de malware é vital para a segurança do computador. Execute verificações de malware regularmente para eliminar a possibilidade de disseminar malwares não detectados pelos componentes de proteção devido a uma configuração de nível de segurança baixo ou por outros motivos.

O Kaspersky Endpoint Security não verifica arquivos cujo conteúdo está localizado no armazenamento na nuvem do OneDrive e cria entradas de log informando que esses arquivos não foram verificados.

Verificação completa

Uma verificação detalhada de todo o computador. Kaspersky Endpoint Security verifica os seguintes objetos:

- Memória Kernel
- Os objetos que são carregados quando o sistema operacional é iniciado
- Setores de inicialização
- Backup do sistema operacional
- Todos os discos rígidos e unidades removíveis

Os especialistas da Kaspersky recomendam não alterar o escopo da tarefa *Verificação completa*.

Para conservar os recursos do computador, é recomendável executar uma tarefa de verificação em segundo plano, em vez de uma tarefa de verificação completa. Isso não afetará o nível de segurança do computador.

Verificação de áreas críticas

Por padrão, o Kaspersky Endpoint Security verifica a memória kernel, os processos de execução e os setores de inicialização de disco.

Os especialistas da Kaspersky recomendam não alterar o escopo da tarefa *Verificação de áreas críticas*.

Verificação personalizada

O Kaspersky Endpoint Security verifica os objetos que foram selecionados pelo usuário. Você pode verificar qualquer objeto da seguinte lista:

- Memória do sistema
- Os objetos que são carregados quando o sistema operacional é iniciado
- Backup do sistema operacional
- Discos rígidos, unidades removíveis e de rede
- Qualquer arquivo selecionado

Verificação em segundo plano

Verificação em segundo plano é um modo de verificação do Kaspersky Endpoint Security que não exibe notificações ao usuário. A verificação em segundo plano utiliza menos recursos do computador do que outros tipos de verificações (como uma verificação completa). Neste modo, o Kaspersky Endpoint Security verifica os objetos de inicialização, o setor de inicialização, a memória do sistema e a partição do sistema.

Verificação de integridade do aplicativo

O Kaspersky Endpoint Security verifica os módulos do aplicativo para detectar corrupção ou modificações.

Verificar o computador

Uma verificação é uma parte essencial da segurança do computador. Execute verificações de malware regularmente para eliminar a possibilidade de disseminar malwares não detectados pelos componentes de proteção devido a uma configuração de nível de segurança baixo ou por outros motivos. O componente fornece proteção ao computador com a ajuda de bancos de dados de antivírus, o serviço na nuvem Kaspersky Security Network e análise heurística.

O Kaspersky Endpoint Security tem as seguintes tarefas padrão predefinidas: *Verificação completa*, *Verificação de áreas críticas*, *Verificação personalizada*. Caso a sua organização possua o sistema de administração do Kaspersky Security Center implantado, é possível criar uma tarefa de *Verificação de malware* e configurar a verificação.

Como executar a tarefa de verificação no Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Tarefas**.

3. Selecione a tarefa de verificação e clique duas vezes para abrir as propriedades da tarefa.

   Caso seja necessário, crie a tarefa *Verificação de malware*.

4. Na janela de propriedades da tarefa, selecione a seção **Configurações**.

5. Configure a tarefa de verificação (consulte a tabela abaixo).

   Caso seja necessário, configure o agendamento da tarefa de verificação.

6. Salvar alterações.

7. Executar a tarefa de verificação.

O Kaspersky Endpoint Security começará a verificar o computador. Caso o usuário interrompa a execução da tarefa (por exemplo, desligando o computador), o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que a verificação foi interrompida.

Como executar uma tarefa de verificação no Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Tarefas**.

   A lista de tarefas é aberta.

2. Clique na tarefa de verificação.

   A janela de propriedades da tarefa é exibida.

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

4. Configure a tarefa de verificação (consulte a tabela abaixo).

   Caso seja necessário, configure o agendamento da tarefa de verificação.

5. Salvar alterações.

6. Executar a tarefa de verificação.

O Kaspersky Endpoint Security começará a verificar o computador. Caso o usuário interrompa a execução da tarefa (por exemplo, desligando o computador), o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que a verificação foi interrompida.

Como executar uma tarefa de verificação na interface do aplicativo

1. Na janela principal do aplicativo, acesse a seção **Tarefas**.

2. Na janela aberta, selecione a tarefa de verificação e clique em ⚙.

> Caso a tarefa de verificação não seja exibida, significa que o administrador proibiu o uso de tarefas locais na política.

> Na interface do aplicativo, você pode configurar somente tarefas de verificação locais: *Verificação completa*, *Verificação de áreas críticas*, *Verificação personalizada*. Não é possível configurar, na interface do aplicativo, tarefas de grupo adicionadas por meio do Console do Kaspersky Security Center. O botão ⚙ não é exibido para tarefas de grupo.

3. Configure a tarefa de verificação (consulte a tabela abaixo).

   Caso seja necessário, configure o agendamento da tarefa de verificação.

4. Salvar alterações.

5. Executar a tarefa de verificação.

   O Kaspersky Endpoint Security começará a verificar o computador. O aplicativo mostrará o progresso da verificação, o número de arquivos verificados e o tempo restante da verificação. É possível interromper a tarefa a qualquer momento clicando no botão **Interromper**.

Para otimizar o desempenho do Kaspersky Endpoint Security durante a verificação do computador, é possível gerenciar as configurações avançadas da tarefa *Verificação completa* e limitar o uso de recursos da CPU.

No Kaspersky Security Center, também é possível usar a tarefa *Verificação em segundo plano* em vez da tarefa *Verificação completa* para otimizar o desempenho do aplicativo. Isso não afetará o nível de segurança do computador. A verificação em segundo plano não pode ser configurada.

Assim, o Kaspersky Endpoint Security verifica o computador e, caso uma ameaça seja detectada, a ação definida é executada nas configurações do aplicativo. Normalmente, o aplicativo tenta desinfectar os arquivos infectados. Assim, os arquivos infectados podem receber os seguintes status:

- **Adiado**. O arquivo infectado não pôde ser desinfectado. O aplicativo exclui o arquivo infectado após a reinicialização do computador.
- **Registrado**. O arquivo infectado não pôde ser desinfectado. O aplicativo adiciona as informações sobre os arquivos infectados detectados na lista de ameaças ativas.
- **Gravação não compatível** ou **Erro de gravação**. O arquivo infectado não pôde ser desinfectado. O aplicativo não tem acesso de gravação.
- **Já processado**. O aplicativo detectou um arquivo infectado anteriormente. O aplicativo desinfecta ou exclui o arquivo infectado após a reinicialização do computador.

Configurações da Verificação

Parâmetro	Descrição
Nível de segurança	O Kaspersky Endpoint Security pode usar diferentes grupos de configurações para executar uma verificação. Estes grupos de configurações armazenados no aplicativo são denominados *níveis de segurança*: • **Alto**. O Kaspersky Endpoint Security verifica todos os tipos de arquivos. Ao verificar arquivos compostos, o aplicativo verifica arquivos compactados, pacotes de distribuição, arquivos nos formatos do Office, mas não verifica arquivos compactados protegidos por senha. Quando esse nível de segurança for definido, o aplicativo utilizará a análise heurística com o nível de detalhe da **Verificação profunda**. • **Recomendado**. O Kaspersky Endpoint Security verifica todos os tipos de arquivos. Ao verificar arquivos compostos, o aplicativo verifica arquivos compactados, pacotes de distribuição, arquivos nos formatos do Office, mas não verifica arquivos compactados protegidos por senha. Quando esse nível de segurança for definido, o aplicativo utilizará a análise heurística com o nível de detalhe da **Verificação média**. • **Baixo**. O Kaspersky Endpoint Security verifica somente os formatos de arquivo especificados. Ao verificar arquivos compostos, o aplicativo verifica arquivos compactados, pacotes de distribuição, arquivos nos formatos do Office, mas não verifica arquivos compactados protegidos por senha. Quando esse nível de segurança for definido, o aplicativo utilizará a análise heurística com o nível de detalhe da **Verificação superficial**. Você pode selecionar um dos níveis de segurança pré-configurados ou definir manualmente configurações de nível de segurança. A alteração das configurações do nível de segurança não impede a reversão para as configurações de nível recomendado.

Parâmetro	Descrição
Ação ao detectar ameaça	**Desinfectar e excluir se a desinfecção falhar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Caso a desinfecção falhe, o aplicativo excluirá o arquivo. **Desinfectar e informar se a desinfecção falhar**. Caso esta opção seja selecionada, o Kaspersky Endpoint Security tentará desinfectar automaticamente todos os arquivos infectados que são detectados. Caso a desinfeção não seja possível, o Kaspersky Endpoint Security adicionará as informações sobre os arquivos infectados e detectados na lista de ameaças ativas. **Informar**. Caso esta opção seja selecionada, o Kaspersky Endpoint Security adiciona as informações sobre arquivos infectados à lista de ameaças ativas na detecção destes arquivos. Antes de tentar desinfectar ou excluir um arquivo infectado, o aplicativo cria uma cópia de backup do arquivo no caso de você precisar restaurá-lo ou se ele puder ser desinfetado no futuro. Ao detectar arquivos infectados que fazem parte do aplicativo Windows Store, o Kaspersky Endpoint Security tenta excluir o arquivo.
Executar a Desinfecção Avançada imediatamente *(disponível apenas no console do Kaspersky Security Center)*	A Desinfecção Avançada durante uma tarefa de verificação de vírus em um computador será executada somente se o recurso de Desinfecção Avançada estiver ativado nas propriedades da política aplicada a este computador. Caso a caixa de seleção esteja marcada, o Kaspersky Endpoint Security desinfeta a infecção ativa imediatamente após a detecção durante a execução da tarefa de verificação de vírus. Depois que a infecção ativa é desinfectada, o Kaspersky Endpoint Security reinicia o computador sem avisar o usuário. Caso a caixa de seleção esteja desmarcada, o Kaspersky Endpoint Security não desinfecta a infecção ativa imediatamente após ser detectada durante a execução da tarefa de verificação de vírus. O Kaspersky Endpoint Security gera eventos de infecção ativa em relatórios de aplicativos locais e no lado do Kaspersky Security Center. A infecção ativa pode ser desinfectada quando a tarefa de verificação de vírus é executada novamente com o recurso desinfecção avançada ativado. Dessa forma, o administrador do sistema pode escolher o momento apropriado para fazer a desinfecção avançada e, posteriormente, reiniciar os computadores automaticamente.
Escopo da verificação	Lista de objetos que o Kaspersky Endpoint Security verifica ao executar uma tarefa de verificação. Os objetos dentro do escopo da verificação podem incluir a memória central, processos em execução, setores de inicialização, armazenamento de backup do sistema, discos rígidos, unidades removíveis ou unidades de rede, uma pasta ou um arquivo. No Kaspersky Endpoint Security for Windows 12.12, o e-mail está excluído do escopo da verificação de aplicativos. A verificação de mensagens de e-mail recebidas e enviadas é realizada pelo componente Proteção Contra Ameaças ao Correio. Caso esteja usando uma versão anterior do plug-in de gerenciamento, o aplicativo excluirá o e-mail do escopo da verificação, mesmo que a política o inclua.
Agendamento de verificações	**Manualmente**. Modo de execução no qual você pode iniciar a verificação manualmente quando conveniente. **Por agendamento**. Neste modo de execução de tarefa de verificação, o aplicativo inicia a tarefa de verificação de acordo com o agendamento criado. Se esse modo de execução da tarefa de verificação for selecionado, você também poderá iniciar a tarefa de verificação manualmente.
Adiar a execução após a inicialização do aplicativo em N minutos	Início adiado da tarefa de verificação após a inicialização do aplicativo. Na inicialização do sistema operacional, muitos processos estão em execução, portanto, é vantajoso adiar a execução da tarefa de verificação em vez de executá-la imediatamente após a inicialização do Kaspersky Endpoint Security.
Executar as tarefas ignoradas	Caso a caixa de seleção esteja marcada, o Kaspersky Endpoint Security iniciará a tarefa de verificação ignorada assim que possível. A tarefa pode ser ignorada, por exemplo, se o computador estiver desligado na hora de início agendada para a tarefa de verificação. Quando o aplicativo tem a oportunidade de executar tarefas perdidas, ele executa as tarefas aleatoriamente dentro de um determinado intervalo de tempo para distribuir a carga no computador. Caso a caixa de seleção seja desmarcada, o Kaspersky Endpoint Security não executará as tarefas ignoradas. Em vez disso, ele executará a próxima tarefa de acordo com o agendamento atual.

Parâmetro	Descrição
Executar apenas quando o computador estiver ocioso	Início adiado da tarefa quando os recursos do computador estão ocupados. O Kaspersky Endpoint Security inicia a tarefa de verificação se o computador estiver bloqueado ou se a proteção de tela estiver ativada. Caso interrompa a execução da tarefa, por exemplo, desbloqueando o computador, o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que foi interrompido. Essa opção de programação permite conservar os recursos do computador quando ele está sendo utilizado.
Executar verificação como	Por padrão, a tarefa de verificação é executada no nome do usuário com cujos direitos você está registrado no sistema operacional. O escopo da proteção pode incluir unidades de rede ou outros objetos que exijam direitos de acesso especiais. É possível especificar um usuário que tenha os direitos necessários nas configurações do aplicativo e executar a tarefa de verificação por meio desta conta de usuário.
Tipos de arquivos	O Kaspersky Endpoint Security considera arquivos sem uma extensão como executáveis. O aplicativo sempre verifica arquivos executáveis independentemente dos tipos de arquivos que você seleciona para a verificação. **Todos os arquivos**. Se esta configuração for ativada, o Kaspersky Endpoint Security verificará todos os arquivos sem exceção (todos os formatos e extensões). **Arquivos verificados por formato**. Se esta configuração for ativada, o aplicativo verificará apenas arquivos infetáveis. Antes de verificar um arquivo quanto a código malicioso, o cabeçalho interno do arquivo é analisado para determinar o formato do arquivo (por exemplo, .txt, .doc ou .exe). A verificação também procura arquivos com extensões específicas. **Arquivos verificados por extensão**. Se esta configuração for ativada, o aplicativo verificará apenas arquivos infetáveis. O formato do arquivo é determinado com base na extensão do arquivo. Por padrão, o Kaspersky Endpoint Security realiza a verificação de arquivos de acordo com o seu formato. Verificar arquivos por extensão é menos seguro porque um arquivo malicioso pode ter uma extensão que não está na lista de potencialmente infectáveis (por exemplo, `.123`).
Verificar somente arquivos novos e alterados	Verifica apenas os arquivos novos e aqueles que foram modificados desde a última vez em que foram verificados. Isso ajuda a reduzir a duração de uma verificação. Esse modo se aplica a arquivos simples e compostos.
Ignorar arquivo verificado por mais de N segundos	Limitação do tempo de execução da tarefa. Depois do tempo especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está marcada como concluída. Na próxima vez que o Kaspersky Endpoint Security executar a tarefa, ela será executada desde o início e dentro do cronograma.
Não executar várias tarefas de verificação ao mesmo tempo	Adie as tarefas de verificação agendadas se uma verificação agendada iniciada anteriormente ainda estiver em execução. O Kaspersky Endpoint Security enfileirará as tarefas de verificação agendadas se a verificação atual continuar. Isso ajuda a otimizar a carga no computador. Por exemplo, você programou tarefas de verificação para serem executadas às 18h e às 20h. O Kaspersky Endpoint Security adiará a tarefa de verificação das 20h se a tarefa de verificação programada para as 18h ainda estiver em execução. O aplicativo executará uma verificação após a conclusão da tarefa iniciada às 18h. No entanto, o Kaspersky Endpoint Security inicia imediatamente uma tarefa de verificação, mesmo que uma das seguintes tarefas de verificação esteja em execução: • Verificação de unidades removíveis na conexão. • Verificação pelo menu de contexto. • A verificação de áreas críticas foi iniciada detecção de um indicador de comprometimento (IoC). Caso a caixa de seleção esteja desmarcada, o Kaspersky Endpoint Security permite executar várias tarefas de verificação ao mesmo tempo. A execução de várias tarefas de verificação requer mais recursos do computador.
Verificar arquivos compactados	Verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros arquivos compactados. O aplicativo verifica os arquivos por extensão e formato. Ao verificar os arquivos, o aplicativo executa uma descompactação recursiva. Isso permite detectar ameaças em arquivos multinível (arquivo dentro de arquivo).
Verificar pacotes de distribuição	Verificação de pacotes de distribuição de aplicativos 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 aplicativo verifica arquivos em formato do Office com menos de 1 MB, independentemente de a caixa de seleção estar marcada ou não.

Parâmetro	Descrição
Verificar arquivos de formato de e-mail	Verificar arquivos de formato de e-mail e banco de dados de e-mail. O aplicativo verifica arquivos PST e OST usados por clientes de e-mail MS Outlook e Windows Mail, bem como arquivos EML. O Kaspersky Endpoint Security não oferece suporte à versão de 64 bits do cliente de mail Microsoft Outlook. Isso significa que o Kaspersky Endpoint Security não verifica os arquivos do Microsoft Outlook (arquivos PST e OST) se uma versão de 64 bits do Microsoft Outlook estiver instalada no computador, mesmo se o correio estiver incluído no escopo da verificação. Se a caixa de seleção for marcada, o Kaspersky Endpoint Security dividirá o arquivo de formato de e-mail em seus componentes (cabeçalho, corpo, anexos) e os verificará quanto a ameaças. Se esta caixa de seleção for desmarcada, o Kaspersky Endpoint Security verificará o arquivo de formato de e-mail como um arquivo único. Quando um objeto malicioso for descoberto em arquivos PST ou OST, o Kaspersky Endpoint Security o tornará inofensivo de acordo com a ação selecionada (por exemplo, desinfecção ou exclusão do arquivo). Se forem detectados objetos maliciosos em arquivos de outros clientes de e-mail (por exemplo, Mozilla Thunderbird), o Kaspersky Endpoint Security não desinfectará nem excluirá esses arquivos para evitar a exclusão indesejada de suas mensagens de e-mail. O Kaspersky Endpoint Security adiciona somente as informações sobre os arquivos infectados detectados na lista de ameaças ativas. Você precisa excluir as mensagens de e-mail com arquivos maliciosos anexados na interface do usuário do seu cliente de e-mail. Se, por qualquer motivo, não for possível excluir mensagens com objetos maliciosos no momento, você poderá processar essas ameaças na interface do usuário do Kaspersky Endpoint Security adicionando os objetos detectados à lista de exclusões da verificação.
Verificar arquivos compactados protegidos por senha	Se a caixa de seleção for marcada, o aplicativo verificará arquivos compactados protegidos por senha. Antes que os arquivos em um arquivo compactado possam ser verificados, você deve inserir a senha. Se a caixa de seleção for desmarcada, o aplicativo ignorará a verificação de arquivos compactados protegidos por senha.
Não descompactar arquivos compostos de grandes dimensões	Se esta caixa de seleção for marcada, o aplicativo não verificará arquivos compostos se o tamanho deles exceder o valor especificado. Se esta caixa de seleção estiver desmarcada, o aplicativo verificará os arquivos compostos de todos os tamanhos. O aplicativo verifica arquivos grandes extraídos de arquivos compactados independentemente de a caixa de seleção estar selecionada ou não.
Aprendizado de máquina e análise de assinatura	O machine learning e análise de assinatura usa o banco de dados do Kaspersky Endpoint Security que contém descrições de ameaças conhecidas e modos de neutralizá-las. A Proteção que usa este método fornece o nível de segurança aceitável mínimo. Com base nas recomendações dos especialistas da Kaspersky, o aprendizado de máquina e análise de assinatura sempre estarão ativados.
Análise Heurística	A tecnologia foi desenvolvida para detectar ameaças que não podem ser detectadas usando a versão atual dos bancos de dados do aplicativo Kaspersky. Detecta arquivos que podem estar infectados por um vírus desconhecido ou por uma nova variedade de um vírus conhecido. Ao verificar arquivos em busca de códigos maliciosos, o analisador heurístico executa instruções nos arquivos executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível de análise heurística assegura um equilíbrio entre a eficácia da verificação quanto a novas ameaças, a carga nos recursos do sistema operacional e a duração da análise heurística.
Tecnologia iSwift *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iSwift é um avanço da tecnologia iChecker do sistema de arquivos NTFS.
Tecnologia iChecker *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iChecker tem algumas limitações: ela não funciona com arquivos grandes e se aplica somente a objetos com uma estrutura reconhecida pelo aplicativo (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

Verificar unidades removíveis quando conectadas ao computador

O Kaspersky Endpoint Security verifica todos os arquivos executados ou copiados, mesmo se o arquivo estiver localizado em uma unidade removível (componente de Proteção contra ameaças ao arquivo). Para evitar a propagação de vírus e outros malwares, é possível configurar as verificações automáticas de unidades removíveis quando elas estiverem conectadas ao computador. O Kaspersky Endpoint Security tentará desinfectar automaticamente todos os arquivos infectados que são detectados. Se a desinfeção falhar, o Kaspersky Endpoint Security excluirá os arquivos. O componente mantém o computador seguro ao executar as verificações que implementam aprendizado de máquina, análise heurística (alto nível) e análise de assinatura. O Kaspersky Endpoint Security também utiliza as tecnologias de otimização da verificação do iSwift e iChecker. As tecnologias estão sempre ativas e não podem ser desativadas.

Como configurar a execução de verificação de unidades removíveis no console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Tarefas locais** → **Verificação de unidades removíveis**.
4. Na lista suspensa **Ação sobre a conexão de uma unidade removível**, selecione **Verificação detalhada** ou **Verificação rápida**.
5. Configure as opções avançadas para a verificação de unidades removíveis (consulte a tabela abaixo).
6. Salvar alterações.

Como configurar a execução de verificação de unidades removíveis no Web Console e Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Proteção Contra Ameaças ao Host** → **Verificação de unidades removíveis**.
5. Use o botão de alternância do **Verificação de Unidades Removíveis ATIVADA** para ativar ou desativar o componente.
6. No bloco **Tipo de verificação**, selecione **Verificação detalhada** ou **Verificação rápida**.
7. Configure as opções avançadas para a verificação de unidades removíveis (consulte a tabela abaixo).
8. Salvar alterações.

Como configurar a execução de verificação de unidades removíveis na interface do aplicativo

1. Na janela principal do aplicativo, acesse a seção **Tarefas**.
2. Na janela aberta, selecione a tarefa de verificação e clique em ⚙.
3. Use o botão de alternância **Verificação de unidades removíveis** para ativar ou desativar verificações de unidades removíveis durante a conexão com o computador.
4. Configure as opções avançadas para a verificação de unidades removíveis (consulte a tabela abaixo).
5. Salvar alterações.

Como resultado, o Kaspersky Endpoint Security executa uma verificação de unidades removíveis para unidades removíveis que não são maiores que o tamanho máximo especificado. Caso a tarefa *Verificação de unidades removíveis* não seja exibida, significa que o administrador proibiu o uso de tarefas locais na política.

Configurações da tarefa da verificação de unidades removíveis

Parâmetro	Descrição
Tipo de verificação	**Verificação detalhada**. Caso esta opção seja selecionada, Kaspersky Endpoint Security verificará todos os arquivos quando uma unidade removível for conectada, inclusive os arquivos aninhados em objetos compostos, os arquivos compactados, os pacotes de distribuição e os arquivos em formatos office. O Kaspersky Endpoint Security não verifica os arquivos em formatos de e-mail ou arquivos protegidos por senha. **Verificação rápida**. Caso esta opção seja selecionada, depois que uma unidade removível for conectada, o Kaspersky Endpoint Security verificará apenas os arquivos de formato específicos mais vulneráveis à infecção, e não descompactará os objetos compostos.
Tamanho máximo da unidade (MB)	Caso esta caixa de seleção seja marcada, o Kaspersky Endpoint Security executará a ação selecionada em unidades removíveis com um tamanho não superior ao tamanho máximo especificado da unidade. Se o tamanho da unidade removível exceder o valor configurado, o Kaspersky Endpoint Security ignorará a verificação. Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security executará a ação selecionada em unidades removíveis de qualquer tamanho.
Ocultar a barra de progresso da verificação	Caso a caixa de seleção seja marcada, o Kaspersky Endpoint Security exibirá o andamento da verificação de unidades removíveis em uma janela separada e na seção **Tarefas**. Se a caixa de seleção for desmarcada, o Kaspersky Endpoint Security executará a verificação de unidades removíveis em segundo plano.
Impedir que os usuários interrompam a verificação	Caso esta caixa de seleção seja marcada, então, para a tarefa de verificação das unidades removíveis na interface local do Kaspersky Endpoint Security, o botão **Interromper** na seção **Tarefas** e o botão **Interromper** na janela de verificação das unidades removíveis não estão disponíveis.

Verificação em segundo plano

Verificação em segundo plano é um modo de verificação do Kaspersky Endpoint Security que não exibe notificações ao usuário. A verificação em segundo plano utiliza menos recursos do computador do que outros tipos de verificações (como uma verificação completa). Neste modo, o Kaspersky Endpoint Security verifica os objetos de inicialização, o setor de inicialização, a memória do sistema e a partição do sistema.

Para conservar os recursos do computador, é recomendável executar uma tarefa de verificação em segundo plano, em vez de uma tarefa de verificação completa. Isso não afetará o nível de segurança do computador. Essas tarefas têm o mesmo escopo de verificação. Para otimizar a carga no computador, o aplicativo não executa uma tarefa de verificação completa e uma tarefa de verificação em segundo plano ao mesmo tempo. Caso tenha executado uma tarefa de verificação completa, o Kaspersky Endpoint Security não iniciará uma tarefa de verificação em segundo plano por sete dias após a conclusão da tarefa de verificação completa.

Uma verificação em segundo plano é iniciada nos seguintes casos:

- Após a atualização do banco de dados antivírus.
- 30 minutos após o Kaspersky Endpoint Security ter iniciado.
- A cada seis horas.
- Quando o computador está ocioso por cinco minutos ou mais (o computador está bloqueado ou a proteção de tela está ligada).

A verificação em segundo plano quando o computador está inativo é interrompida quando qualquer uma das seguintes condições for verdadeira:

- O computador entrou no modo ativo.

  Se a verificação em segundo plano não tiver sido executada por mais de dez dias, a verificação não será interrompida.

- O computador (laptop) mudou para o modo de bateria.

Ao executar uma verificação sem segundo plano, o Kaspersky Endpoint Security não verifica arquivos cujo conteúdo está localizado no armazenamento em nuvem do OneDrive.

Como ativar a verificação em segundo plano no console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Tarefas locais** → **Verificação em segundo plano**.
4. Usar a caixa de seleção **Ativar a verificação em segundo plano** para ativar ou desativar a verificação em segundo plano.
5. Salvar alterações.

Como ativar a verificação em segundo plano no Web Console e Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Acesse **Proteção Contra Ameaças ao Host** → **Proteção Contra Ameaças ao Arquivo**.
5. Em **Verificação em segundo plano**, use o botão de alternância de **Verificação em segundo plano ATIVADA** para ativar ou desativar a verificação em segundo plano.
6. Salvar alterações.

Como ativar a verificação em segundo plano na interface do aplicativo

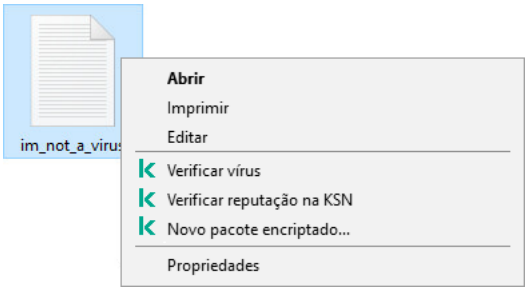
1. Na janela principal do aplicativo, acesse a seção **Tarefas**.
2. Na janela aberta, selecione a tarefa de verificação e clique em ⚙.
3. Use o botão de alternância **Verificação em segundo plano** para ativar ou desativar verificações em segundo plano.
4. Salvar alterações.

Se *Verificação em segundo plano* não for exibido, significa que o administrador restringiu o uso de tarefas locais na política.

Verificar pelo menu de contexto

O Kaspersky Endpoint Security permite que você faça a verificação de arquivos individuais em busca de vírus e outros malwares a partir do menu de contexto (veja a figura abaixo).

Ao executar uma verificação a partir do menu de contexto, o Kaspersky Endpoint Security não verifica arquivos cujo conteúdo está localizado no armazenamento em nuvem do OneDrive.



Verificar pelo menu de contexto

Como configurar a Verificação pelo menu de contexto no console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Tarefas locais** → **Verificação pelo menu de contexto**.
4. Configure a verificação pelo menu de contexto (consulte a tabela abaixo).
5. Salvar alterações.

Como configurar a verificação pelo menu de contexto no Web Console e Cloud Console

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

   A janela de propriedades da política é exibida.

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

4. Acesse **Proteção Contra Ameaças ao Host** → **Proteção Contra Ameaças ao Arquivo**.

5. Em **Verificação pelo menu de contexto**, configure a Verificação pelo menu de contexto (consulte a tabela abaixo).

6. Salvar alterações.

Como configurar a verificação pelo menu de contexto na interface do aplicativo

1. Na janela principal do aplicativo, acesse a seção **Tarefas**.

2. Na janela aberta, selecione a tarefa de verificação e clique em ⚙.

3. Configure a verificação pelo menu de contexto (consulte a tabela abaixo).

4. Salvar alterações.

Caso a tarefa *Verificação pelo menu de contexto* não seja exibida, significa que o administrador proibiu o uso de tarefas locais na política.

Configurações da tarefa Verificar a partir do menu de contexto

Parâmetro	Descrição
Nível de segurança	O Kaspersky Endpoint Security pode usar diferentes grupos de configurações para executar uma verificação. Estes grupos de configurações armazenados no aplicativo são denominados *níveis de segurança*: • **Alto**. O Kaspersky Endpoint Security verifica todos os tipos de arquivos. Ao verificar arquivos compostos, o aplicativo verifica arquivos compactados, pacotes de distribuição, arquivos nos formatos do Office, mas não verifica arquivos compactados protegidos por senha. Quando esse nível de segurança for definido, o aplicativo utilizará a análise heurística com o nível de detalhe da **Verificação profunda**. • **Recomendado**. O Kaspersky Endpoint Security verifica todos os tipos de arquivos. Ao verificar arquivos compostos, o aplicativo verifica arquivos compactados, pacotes de distribuição, arquivos nos formatos do Office, mas não verifica arquivos compactados protegidos por senha. Quando esse nível de segurança for definido, o aplicativo utilizará a análise heurística com o nível de detalhe da **Verificação média**. • **Baixo**. O Kaspersky Endpoint Security verifica somente os formatos de arquivo especificados. Ao verificar arquivos compostos, o aplicativo verifica arquivos compactados, pacotes de distribuição, arquivos nos formatos do Office, mas não verifica arquivos compactados protegidos por senha. Quando esse nível de segurança for definido, o aplicativo utilizará a análise heurística com o nível de detalhe da **Verificação superficial**.
Ação ao detectar ameaça	**Desinfectar e excluir se a desinfecção falhar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Caso a desinfecção falhe, o aplicativo excluirá o arquivo. **Desinfectar e informar se a desinfecção falhar**. Caso esta opção seja selecionada, o Kaspersky Endpoint Security tentará desinfectar automaticamente todos os arquivos infectados que são detectados. Caso a desinfeção não seja possível, o Kaspersky Endpoint Security adicionará as informações sobre os arquivos infectados e detectados na lista de ameaças ativas. **Informar**. Caso esta opção seja selecionada, o Kaspersky Endpoint Security adiciona as informações sobre arquivos infectados à lista de ameaças ativas na detecção destes arquivos.
Tipos de arquivos	O Kaspersky Endpoint Security considera arquivos sem uma extensão como executáveis. O aplicativo sempre verifica arquivos executáveis independentemente dos tipos de arquivos que você seleciona para a verificação. **Todos os arquivos**. Se esta configuração for ativada, o Kaspersky Endpoint Security verificará todos os arquivos sem exceção (todos os formatos e extensões). **Arquivos verificados por formato**. Se esta configuração for ativada, o aplicativo verificará apenas arquivos infetáveis. Antes de verificar um arquivo quanto a código malicioso, o cabeçalho interno do arquivo é analisado para determinar o formato do arquivo (por exemplo, .txt, .doc ou .exe). A verificação também procura arquivos com extensões específicas. **Arquivos verificados por extensão**. Se esta configuração for ativada, o aplicativo verificará apenas arquivos infetáveis. O formato do arquivo é determinado com base na extensão do arquivo. Por padrão, o Kaspersky Endpoint Security realiza a verificação de arquivos de acordo com o seu formato. Verificar arquivos por extensão é menos seguro porque um arquivo malicioso pode ter uma extensão que não está na lista de potencialmente infectáveis (por exemplo, `.123`).

Parâmetro	Descrição
Verificar somente arquivos novos e alterados	Verifica apenas os arquivos novos e aqueles que foram modificados desde a última vez em que foram verificados. Isso ajuda a reduzir a duração de uma verificação. Esse modo se aplica a arquivos simples e compostos.
Ignorar arquivo verificado por mais de N segundos	Limitação do tempo de execução da tarefa. Depois do tempo especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está marcada como concluída. Na próxima vez que o Kaspersky Endpoint Security executar a tarefa, ela será executada desde o início e dentro do cronograma.
Verificar arquivos compactados	Verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros arquivos compactados. O aplicativo verifica os arquivos por extensão e formato. Ao verificar os arquivos, o aplicativo executa uma descompactação recursiva. Isso permite detectar ameaças em arquivos multinível (arquivo dentro de arquivo).
Verificar pacotes de distribuição	A caixa de seleção ativa/desativa a verificação de pacotes de instalação.
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 aplicativo 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	Verificar arquivos de formato de e-mail e banco de dados de e-mail. O aplicativo verifica arquivos PST e OST usados por clientes de e-mail MS Outlook e Windows Mail, bem como arquivos EML. O Kaspersky Endpoint Security não oferece suporte à versão de 64 bits do cliente de mail Microsoft Outlook. Isso significa que o Kaspersky Endpoint Security não verifica os arquivos do Microsoft Outlook (arquivos PST e OST) se uma versão de 64 bits do Microsoft Outlook estiver instalada no computador, mesmo se o correio estiver incluído no escopo da verificação. Se a caixa de seleção for marcada, o Kaspersky Endpoint Security dividirá o arquivo de formato de e-mail em seus componentes (cabeçalho, corpo, anexos) e os verificará quanto a ameaças. Se esta caixa de seleção for desmarcada, o Kaspersky Endpoint Security verificará o arquivo de formato de e-mail como um arquivo único. Quando um objeto malicioso for descoberto em arquivos PST ou OST, o Kaspersky Endpoint Security o tornará inofensivo de acordo com a ação selecionada (por exemplo, desinfecção ou exclusão do arquivo). Se forem detectados objetos maliciosos em arquivos de outros clientes de e-mail (por exemplo, Mozilla Thunderbird), o Kaspersky Endpoint Security não desinfectará nem excluirá esses arquivos para evitar a exclusão indesejada de suas mensagens de e-mail. O Kaspersky Endpoint Security adiciona somente as informações sobre os arquivos infectados detectados na lista de ameaças ativas. Você precisa excluir as mensagens de e-mail com arquivos maliciosos anexados na interface do usuário do seu cliente de e-mail. Se, por qualquer motivo, não for possível excluir mensagens com objetos maliciosos no momento, você poderá processar essas ameaças na interface do usuário do Kaspersky Endpoint Security adicionando os objetos detectados à lista de exclusões da verificação.
Verificar arquivos compactados protegidos por senha	Se a caixa de seleção for marcada, o aplicativo verificará arquivos compactados protegidos por senha. Antes que os arquivos em um arquivo compactado possam ser verificados, você deve inserir a senha. Se a caixa de seleção for desmarcada, o aplicativo ignorará a verificação de arquivos compactados protegidos por senha.
Não descompactar arquivos compostos de grandes dimensões	Se esta caixa de seleção for marcada, o aplicativo não verificará arquivos compostos se o tamanho deles exceder o valor especificado. Se esta caixa de seleção estiver desmarcada, o aplicativo verificará os arquivos compostos de todos os tamanhos. O aplicativo verifica arquivos grandes extraídos de arquivos compactados independentemente de a caixa de seleção estar selecionada ou não.
Aprendizado de máquina e análise de assinatura	O machine learning e análise de assinatura usa o banco de dados do Kaspersky Endpoint Security que contém descrições de ameaças conhecidas e modos de neutralizá-las. A Proteção que usa este método fornece o nível de segurança aceitável mínimo. Com base nas recomendações dos especialistas da Kaspersky, o aprendizado de máquina e análise de assinatura sempre estarão ativados.
Análise Heurística	A tecnologia foi desenvolvida para detectar ameaças que não podem ser detectadas usando a versão atual dos bancos de dados do aplicativo Kaspersky. Detecta arquivos que podem estar infectados por um vírus desconhecido ou por uma nova variedade de um vírus conhecido. Ao verificar arquivos em busca de códigos maliciosos, o analisador heurístico executa instruções nos arquivos executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível de análise heurística assegura um equilíbrio entre a eficácia da verificação quanto a novas ameaças, a carga nos recursos do sistema operacional e a duração da análise heurística.

Parâmetro	Descrição
Tecnologia iSwift	Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iSwift é um avanço da tecnologia iChecker do sistema de arquivos NTFS.
Tecnologia iChecker	Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iChecker tem algumas limitações: ela não funciona com arquivos grandes e se aplica somente a objetos com uma estrutura reconhecida pelo aplicativo (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

Verificação de integridade de aplicativos

O Kaspersky Endpoint Security verifica os módulos do aplicativo para detectar corrupção ou modificações. Por exemplo, se uma biblioteca do aplicativo tiver uma assinatura digital incorreta, a biblioteca é considerada corrompida. A tarefa *Verificação de integridade do aplicativo* destina-se à verificação de arquivos de aplicativos. Execute a tarefa de *Verificação de integridade do aplicativo* se o Kaspersky Endpoint Security detectou um objeto malicioso, mas não o neutralizou.

É possível criar a tarefa *Verificação de integridade do aplicativo* no Kaspersky Security Center Web Console e no Console de Administração. Não é possível criar uma tarefa no Kaspersky Security Center Cloud Console.

Violações da integridade do aplicativo podem ocorrer nos seguintes casos:

- Um objeto malicioso modificou os arquivos do Kaspersky Endpoint Security. Nesse caso, execute o procedimento de restauração do Kaspersky Endpoint Security usando as ferramentas do sistema operacional. Após a restauração, execute uma verificação completa do computador e repita a verificação de integridade.
- A assinatura digital expirou. Nesse caso, atualize o Kaspersky Endpoint Security.

Como executar uma verificação de integridade do aplicativo por meio do Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **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

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Verificação de integridade do aplicativo**.

Etapa 2. 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 3. Configurar um agendamento de início de tarefa

Configure um agendamento para iniciar uma tarefa, por exemplo, manualmente ou quando um surto de vírus for detectado.

Etapa 4. Definir o nome da tarefa

Digite um nome para a tarefa, por exemplo, *Verificação de integridade após o computador ter sido infectado*.

Etapa 5. Concluir a criação da tarefa

Conclua o 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 resultado, o Kaspersky Endpoint Security verificará a integridade do aplicativo. Também é possível configurar um agendamento de verificação de integridade do aplicativo nas propriedades da tarefa (veja a tabela abaixo).

Como executar uma verificação de integridade do aplicativo por meio do Web Console

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Verificação de integridade do aplicativo**.

c. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Verificar a integridade do aplicativo após uma infecção no computador*.

d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Vá para a próxima etapa.

5. Selecione uma conta para executar a tarefa. Por padrão, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de usuário local.

6. Conclua o assistente.

   Uma nova tarefa será exibida na lista de tarefas.

7. Marque a caixa de seleção ao lado da tarefa.

Como resultado, o Kaspersky Endpoint Security verificará a integridade do aplicativo. Também é possível configurar um agendamento de verificação de integridade do aplicativo nas propriedades da tarefa (veja a tabela abaixo).

Como executar uma verificação de integridade na interface do aplicativo

1. Na janela principal do aplicativo, acesse a seção **Tarefas**.

2. A lista de tarefas é aberta; selecione a tarefa *Verificação de integridade do aplicativo* e clique em **Executar**.

Como resultado, o Kaspersky Endpoint Security verificará a integridade do aplicativo. Também é possível configurar um agendamento de verificação de integridade do aplicativo nas propriedades da tarefa (veja a tabela abaixo). Caso a tarefa *Verificação de integridade do aplicativo* não seja exibida, significa que o administrador proibiu o uso de tarefas locais na política.

Configurações da tarefa de verificação de integridade

Parâmetro	Descrição
Agendamento de verificações	**Manualmente**. Modo de execução no qual você pode iniciar a verificação manualmente quando conveniente. **Por agendamento**. Neste modo de execução de tarefa de verificação, o aplicativo inicia a tarefa de verificação de acordo com o agendamento criado. Se esse modo de execução da tarefa de verificação for selecionado, você também poderá iniciar a tarefa de verificação manualmente.
Executar as tarefas ignoradas	Caso a caixa de seleção esteja marcada, o Kaspersky Endpoint Security iniciará a tarefa de verificação ignorada assim que possível. A tarefa pode ser ignorada, por exemplo, se o computador estiver desligado na hora de início agendada para a tarefa de verificação. Quando o aplicativo tem a oportunidade de executar tarefas perdidas, ele executa as tarefas aleatoriamente dentro de um determinado intervalo de tempo para distribuir a carga no computador. Caso a caixa de seleção seja desmarcada, o Kaspersky Endpoint Security não executará as tarefas ignoradas. Em vez disso, ele executará a próxima tarefa de acordo com o agendamento atual.
Executar apenas quando o computador estiver ocioso	Início adiado da tarefa quando os recursos do computador estão ocupados. O Kaspersky Endpoint Security inicia a tarefa de verificação se o computador estiver bloqueado ou se a proteção de tela estiver ativada. Caso interrompa a execução da tarefa, por exemplo, desbloqueando o computador, o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que foi interrompido. Essa opção de programação permite conservar os recursos do computador quando ele está sendo utilizado.

Editar o escopo da verificação

O *Escopo da verificação* é uma lista de caminhos para pastas e caminhos que o Kaspersky Endpoint Security verifica ao executar a tarefa. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.

Para editar o escopo da verificação, recomendamos o uso da tarefa *Verificação personalizada*. Os especialistas da Kaspersky recomendam não alterar o escopo das tarefas de *Verificação completa* e *Verificação de áreas críticas*.

O Kaspersky Endpoint Security tem os seguintes objetos predefinidos como parte do escopo da verificação:

- **Memória do sistema**.
- **Processos em execução e objetos de inicialização**.

  Memória ocupada por processos e arquivos executáveis de aplicativos executados na inicialização do sistema.
- **Setores de inicialização do disco**.

  Setores de iniciação de disco rígido e disco removível.
- **Backup do sistema**.

  Conteúdo da pasta informações do volume do sistema.
- **Todos os dispositivos externos**.
- **Todos os discos rígidos**.
- **Todas as unidades de rede**.

  No Kaspersky Endpoint Security for Windows 12.12, o e-mail está excluído do escopo da verificação de aplicativos. A verificação de mensagens de e-mail recebidas e enviadas é realizada pelo componente Proteção Contra Ameaças ao Correio. Caso esteja usando uma versão anterior do plug-in de gerenciamento, o aplicativo excluirá o e-mail do escopo da verificação, mesmo que a política o inclua.

  Recomendamos criar uma tarefa de verificação separada para verificar unidades de rede ou pastas compartilhadas. Nas configurações da tarefa *Verificação de malware*, especifique um usuário que tenha acesso de gravação para esta unidade; isso é necessário para mitigar as ameaças detectadas. Caso o servidor no qual a unidade de rede está localizada tenha suas próprias ferramentas de segurança, não executar a tarefa de verificação dessa unidade. Dessa forma, é possível evitar a verificação do objeto duas vezes e melhorar o desempenho do servidor.

Para excluir as pastas ou os arquivos do escopo da verificação, adicione a pasta ou o arquivo à zona confiável.

Como editar o escopo da verificação no console de administração (MMC)

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

2. Na árvore do console, selecione **Tarefas**.

3. Selecione a tarefa de verificação e clique duas vezes para abrir as propriedades da tarefa.

   Caso seja necessário, crie a tarefa *Verificação de malware*.

4. Na janela de propriedades da tarefa, selecione a seção **Configurações**.

5. Na seção **Escopo da verificação**, clique no botão **Configurações**.

6. Na janela que é aberta, selecione os objetos que deseja adicionar ao escopo da verificação ou excluir dele.

7. Se desejar adicionar um novo objeto ao escopo da verificação:

   a. Clique **Adicionar**.

   b. No campo **Objeto**, 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.

      - `?` (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 em qualquer lugar em um caminho de arquivo ou pasta. Por exemplo, se quiser que o escopo da verificação inclua a pasta Downloads para todas as contas de usuário no computador, insira a máscara `C:\Users\*\Downloads\`.

      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**.

   Você pode excluir um objeto das verificações sem excluí-lo da lista de objetos no escopo da verificação. Para fazer isso, desmarque a caixa de seleção ao lado do objeto.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como editar o escopo da verificação no Web Console e Cloud Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Tarefas**.

   A lista de tarefas é aberta.

2. Clique na tarefa de verificação.

   A janela de propriedades da tarefa é exibida. Caso seja necessário, crie a tarefa *Verificação de malware*.

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

4. Na seção **Escopo da verificação**, selecione os objetos que deseja adicionar ao escopo da verificação ou excluir.

5. Se desejar adicionar um novo objeto ao escopo da verificação:

   a. Clique **Adicionar**.

   b. 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.

      - `?` (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 em qualquer lugar em um caminho de arquivo ou pasta. Por exemplo, se quiser que o escopo da verificação inclua a pasta Downloads para todas as contas de usuário no computador, insira a máscara `C:\Users\*\Downloads\`.

   Você pode excluir um objeto das verificações sem excluí-lo da lista de objetos no escopo da verificação. Para fazer isso, coloque a chave de alternância ao lado na posição desativada.

6. Salvar alterações.

Como editar um escopo da verificação na interface do aplicativo

1. Na janela principal do aplicativo, acesse a seção **Tarefas**.

2. A lista de tarefas é aberta; selecione a tarefa *Verificação personalizada* e clique em **Selecionar**.

   Também é possível editar o escopo da verificação para outras tarefas. Os especialistas da Kaspersky recomendam não alterar o escopo das tarefas de *Verificação completa* e *Verificação de áreas críticas*.

3. Na janela que é aberta, selecione os objetos que deseja adicionar ao escopo da verificação.

4. Salvar alterações.

Caso a tarefa de verificação não seja exibida, significa que o administrador proibiu o uso de tarefas locais na política.

Execução de uma verificação programada

A verificação de malware usando a tarefa *Verificação de malware* pode levar tempo, além de aumentar o uso de recursos computacionais do Kaspersky Endpoint Security. Portanto, é recomendável selecionar um momento ideal para executar a tarefa, assim, o impacto no desempenho de outros aplicativos será minimizado.

Por exemplo, se os profissionais de sua organização trabalharem em um horário fixo, é possível configurar a execução de uma verificação no computador para o período noturno ou nos fins de semana. Se não for possível executar a tarefa por qualquer motivo (por exemplo, o computador não está ligado no momento), você poderá configurar a tarefa ignorada para iniciar automaticamente assim que for possível. Essa função deve ser usada com cuidado, pois ela pode deixar os aplicativos mais lentos no computador do usuário quando o computador for ligado pela manhã.

Se não for possível determinar um agendamento de verificações ideal e que atenda às suas necessidades, é possível configurar a execução da verificação quando uma das seguintes condições especiais for atendida:

- Após uma atualização do banco de dados.

  O Kaspersky Endpoint Security executa a verificação do computador com os bancos de dados de assinatura atualizados.

- Após iniciar o aplicativo.

  O Kaspersky Endpoint Security executa uma verificação do computador em determinado período após a inicialização do aplicativo. Na inicialização do sistema operacional, muitos processos estão em execução, portanto, é vantajoso adiar a execução da tarefa de verificação em vez de executá-la imediatamente após a inicialização do Kaspersky Endpoint Security.

- Recurso Wake-on-LAN.

  O Kaspersky Endpoint Security executa uma verificação do computador na programação, mesmo se o computador estiver desligado. Para fazer isso, o aplicativo utiliza o recurso Wake-on-LAN do sistema operacional. O recurso Wake-on-LAN permite ligar o computador remotamente, por meio do envio de um sinal especial pela rede local. Para utilizar esse recurso, é necessário ativar o Wake-on-LAN nas configurações do BIOS.

  É possível configurar a execução da verificação utilizando o Wake-on-LAN apenas para a tarefa de *Verificação de malware* no Kaspersky Security Center. Não é possível ativar o Wake-on-LAN para verificar o computador na interface do aplicativo.

- Quando o computador estiver ocioso.

  O Kaspersky Endpoint Security executa uma verificação do computador na programação quando o protetor de tela está ativo ou a tela está bloqueada. Caso o usuário desbloqueie o computador, o Kaspersky Endpoint Security pausa a verificação. Nesse caso, a verificação completa poderá levar vários dias para ser concluída.

- Quando a tarefa foi ignorada.

  O Kaspersky Endpoint Security executa a tarefa ignorada assim que possível. A tarefa pode ser ignorada, por exemplo, se o computador estiver desligado na hora de início agendada para a tarefa de verificação. Quando o aplicativo tem a oportunidade de executar tarefas perdidas, ele executa as tarefas aleatoriamente dentro de um determinado intervalo de tempo para distribuir a carga no computador.

Como configurar o agendamento de verificação no Web Console e Cloud Console

1. Na janela principal do Web Console, selecione **Tarefas**.

   A lista de tarefas é aberta.

2. Clique na tarefa de verificação.

   A janela de propriedades da tarefa é exibida.

3. Na janela de propriedades da tarefa, selecione a guia **Agendamento**.

4. Configure o agendamento da tarefa de verificação.

5. Dependendo da frequência selecionada, defina as configurações avançadas que especificam o agendamento da execução da tarefa (veja a tabela abaixo).

6. Salvar alterações.

Como configurar o agendamento de verificação na interface do aplicativo

É possível configurar o agendamento de verificação apenas se uma política não for aplicada ao computador. Para computadores sob uma política, é possível configurar o agendamento de *Verificação de malware* no Kaspersky Security Center.

1. Na janela principal do aplicativo, acesse a seção **Tarefas**.

2. Na janela aberta, selecione a tarefa de verificação e clique em ⚙.

   É possível configurar uma programação para executar uma verificação completa, uma verificação de áreas críticas ou uma verificação de integridade. Só é possível executar uma verificação personalizada manualmente.

3. Clique **Agendamento de verificações**.

4. Na janela que é aberta, configure o agendamento de execução da tarefa de verificação.

5. Dependendo da frequência selecionada, defina as configurações avançadas que especificam o agendamento da execução da tarefa (veja a tabela abaixo).

6. Salvar alterações.

Configurações do Agendamento de verificações

Parâmetro	Descrição
Agendamento de verificações	**Manualmente**. Modo de execução no qual você pode iniciar a verificação manualmente quando conveniente. **Por agendamento**. Neste modo de execução de tarefa de verificação, o aplicativo inicia a tarefa de verificação de acordo com o agendamento criado. Se esse modo de execução da tarefa de verificação for selecionado, você também poderá iniciar a tarefa de verificação manualmente.
Adiar a execução após a inicialização do aplicativo em N minutos	Início adiado da tarefa de verificação após a inicialização do aplicativo. Na inicialização do sistema operacional, muitos processos estão em execução, portanto, é vantajoso adiar a execução da tarefa de verificação em vez de executá-la imediatamente após a inicialização do Kaspersky Endpoint Security.
Executar as tarefas ignoradas	Caso a caixa de seleção esteja marcada, o Kaspersky Endpoint Security iniciará a tarefa de verificação ignorada assim que possível. A tarefa pode ser ignorada, por exemplo, se o computador estiver desligado na hora de início agendada para a tarefa de verificação. Quando o aplicativo tem a oportunidade de executar tarefas perdidas, ele executa as tarefas aleatoriamente dentro de um determinado intervalo de tempo para distribuir a carga no computador. Caso a caixa de seleção seja desmarcada, o Kaspersky Endpoint Security não executará as tarefas ignoradas. Em vez disso, ele executará a próxima tarefa de acordo com o agendamento atual.
Executar apenas quando o computador estiver ocioso	Início adiado da tarefa quando os recursos do computador estão ocupados. O Kaspersky Endpoint Security inicia a tarefa de verificação se o computador estiver bloqueado ou se a proteção de tela estiver ativada. Caso interrompa a execução da tarefa, por exemplo, desbloqueando o computador, o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que foi interrompido. Essa opção de programação permite conservar os recursos do computador quando ele está sendo utilizado.

Parâmetro	Descrição
Usar atraso aleatório automaticamente para início da tarefa *(disponível apenas no console do Kaspersky Security Center)*	Caso a caixa de seleção 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. Horários de início aleatórios ajudam a evitar que um grande número de computadores acessem simultaneamente o servidor de administração quando a tarefa é executada na programação. O intervalo de horários de início aleatórios é calculado automaticamente quando a tarefa é criada, dependendo do número de computadores que têm a tarefa atribuída. Posteriormente, a tarefa é sempre executada em na hora de início calculada. No entanto, sempre que as configurações da tarefa são modificadas ou a tarefa é executada manualmente, a hora de início calculada muda. Caso a caixa de seleção esteja desmarcada, a tarefa será executada exatamente no horário programado.
Usar retardo aleatório para inícios de tarefa em um intervalo de (min)	Se essa caixa de seleção estiver marcada, a tarefa será executada nos computadores em um horário aleatório dentro de um determinado período. Horários de início aleatórios ajudam a evitar que um grande número de computadores acessem simultaneamente o servidor de administração quando a tarefa é executada na programação. Caso a caixa de seleção esteja desmarcada, a tarefa será executada exatamente no horário programado.
Parar a tarefa se ela for executada por mais que (min) *(disponível apenas no console do Kaspersky Security Center)*	Limitação do tempo de execução da tarefa. Depois do tempo especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está marcada como concluída. Na próxima vez que o Kaspersky Endpoint Security executar a tarefa, ela será executada desde o início e dentro do cronograma. Para reduzir o tempo de execução da tarefa, é possível, por exemplo, configurar o escopo da verificação ou otimizar a verificação.
Ligar dispositivos usando a função Wake-On-LAN antes de iniciar a tarefa (min) *(disponível apenas no console do Kaspersky Security Center)*	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. Marque a caixa de seleção caso queira executar a tarefa em todos os computadores, incluindo computadores desligados.
Desligar os dispositivos após concluir a tarefa *(disponível apenas no console do Kaspersky Security Center)*	Se esta caixa de seleção estiver marcada, o computador será desligado após a conclusão da tarefa. Por exemplo, é possível ativar essa funcionalidade para verificar o computador às sextas-feiras após o horário comercial. Quando a tarefa é concluída, o aplicativo desliga o computador durante o fim de semana.
Pausar tarefa	É possível especificar um intervalo de tempo durante o qual a execução de uma tarefa agendada anteriormente será pausada. Após o término do período de tempo especificado, a tarefa será retomada. Isso pode ser necessário, por exemplo, para minimizar o impacto do Kaspersky Endpoint Security no desempenho do computador durante os períodos de pico de uso.
Desativar agendamento de	Se a caixa de seleção estiver marcada, o Kaspersky Endpoint Security interromperá a execução da tarefa agendada a partir da data especificada. A tarefa será definida para o modo **Manualmente**.

Execução de uma verificação como um usuário diferente

Por padrão, a tarefa de verificação é executada no nome do usuário com cujos direitos você está registrado no sistema operacional. O escopo da proteção pode incluir unidades de rede ou outros objetos que exijam direitos de acesso especiais. É possível especificar um usuário que tenha os direitos necessários nas configurações do aplicativo e executar a tarefa de verificação por meio desta conta de usuário.

É possível executar as seguintes verificações como um usuário diferente:

- Verificação de Áreas Críticas.
- Verificação Completa.
- Verificação Personalizada.
- Verificação pelo menu de contexto.

Não é possível configurar os direitos do usuário para executar uma Verificação de unidades removíveis, uma Verificação em segundo plano ou uma Verificação de integridade.

Como executar verificação uma verificação no console de administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertencem os respectivos computadores clientes.
3. No espaço de trabalho, selecione a guia **Tarefas**.
4. Selecione a tarefa de verificação e clique duas vezes para abrir as propriedades da tarefa.
5. Na janela de propriedades da tarefa, selecione a seção **Conta**.
6. Insira as credenciais da conta do usuário cujos direitos deseja usar para executar uma tarefa de verificação.
7. Salvar alterações.

Como executar uma verificação como um usuário diferente no web console ou no cloud console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Tarefas**.

   A lista de tarefas é aberta.
2. Clique na tarefa de verificação.

   A janela de propriedades da tarefa é exibida.
3. Selecione a guia **Configurações**.
4. No bloco **Conta**, clique no botão **Configurações**.
5. Insira as credenciais da conta do usuário cujos direitos deseja usar para executar uma tarefa de verificação.
6. Salvar alterações.

Como executar uma verificação como um usuário diferente na interface do aplicativo

1. Na janela principal do aplicativo, acesse a seção **Tarefas**.
2. Na janela aberta, selecione a tarefa de verificação e clique em ⚙.
3. Nas propriedades da tarefa, selecionar **Configurações avançadas** → **Executar verificação como**.
4. Na janela que é aberta, insira as credenciais da conta do usuário cujos direitos deseja usar para executar uma tarefa de verificação.
5. Salvar alterações.

Caso a tarefa de verificação não seja exibida, significa que o administrador proibiu o uso de tarefas locais na política.

Otimização da verificação

Limitação do uso da CPU durante a verificação do computador

É possível limitar o uso da CPU ao executar a tarefa *Verificação de malware*. Isso pode aumentar o tempo necessário para verificar seu computador.

Como limitar o uso da CPU ao verificar o computador no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Configurações de aplicativos**.
4. Em **Desempenho**, marque a caixa de seleção **Limitar a utilização da CPU para tarefas de verificação** e insira o valor médio de consumo de recursos da CPU em porcentagem.
5. Salvar alterações.

Como limitar o uso da CPU ao verificar o computador na Web Console

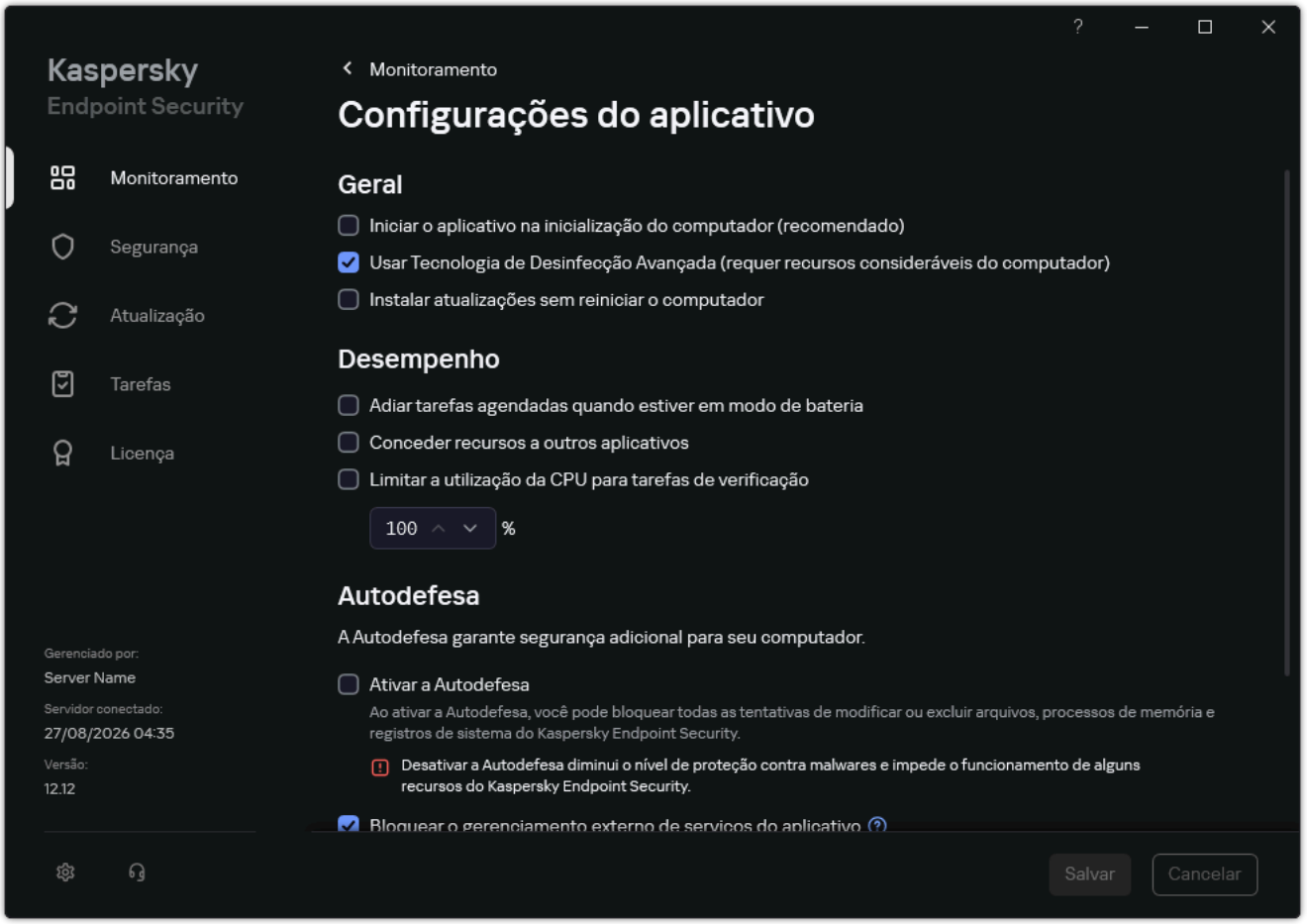
1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Desempenho**.
5. Em **Limitar a utilização da CPU para tarefas de verificação**, defina o botão de alternância para **Limitar a utilização da CPU para tarefas de verificação** e insira o valor médio de consumo de recursos da CPU em porcentagem.
6. Salvar alterações.

Como limitar o uso da CPU ao verificar o computador na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações do aplicativo**.



Configurações do Kaspersky Endpoint Security for Windows

3. Em **Desempenho**, marque a caixa de seleção **Limitar a utilização da CPU para tarefas de verificação** e insira o valor médio de consumo de recursos da CPU em porcentagem.

4. Salvar alterações.

Definição das configurações de tarefa avançada para Verificação de malware.

Pode otimizar a verificação dos arquivos: reduza o tempo da verificação e aumente a velocidade de processamento do Kaspersky Endpoint Security. Isso é possível quando são verificados apenas os arquivos novos e aqueles que foram alterados após a verificação anterior. Esse modo se aplica a arquivos simples e compostos. Você também pode limitar o tempo de verificação de um arquivo simples. Decorrido o intervalo de tempo especificado, o Kaspersky Endpoint Security exclui o arquivo da verificação atual (exceto arquivos compactados e objetos que incluem vários arquivos).

Um método comum para ocultar vírus e outro tipo de malware é incorporá-los em arquivos compostos, como arquivos compactados e bancos de dados. Para detectar vírus e outro tipo de malware que estão ocultos dessa forma, é necessário descompactar os arquivos compostos, o que pode reduzir a velocidade da verificação. É possível restringir os tipos dos arquivos compostos a verificar, o que aumentará a velocidade da verificação.

Também é possível ativar o uso das tecnologias iChecker e iSwift. As tecnologias iChecker e iSwift aumentam a velocidade dos arquivos de verificações, por meio da exclusão de arquivos que permaneceram inalterados desde a verificação mais recente.

Como otimizar a verificando no console de administração (MMC)

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

2. Na árvore do console, selecione **Tarefas**.

3. Selecione a tarefa de verificação e clique duas vezes para abrir as propriedades da tarefa.

   Caso seja necessário, crie a tarefa *Verificação de malware*.

4. Na janela de propriedades da tarefa, selecione a seção **Configurações**.

5. No bloco **Nível de segurança**, clique no botão **Configurações**.

   Isso abre a janela de configurações da tarefa de verificação.

6. No bloco **Otimização**, defina as configurações de verificação:

   - **Verificar somente arquivos novos e alterados**. Verifica apenas os arquivos novos e aqueles que foram modificados desde a última vez em que foram verificados. Isso ajuda a reduzir a duração de uma verificação. Esse modo se aplica a arquivos simples e compostos.

     Também é possível configurar a verificação de novos arquivos por tipo. Por exemplo, é possível verificar todos os pacotes de distribuição e verificar apenas novos arquivos e arquivos de formato office.

   - **Ignorar arquivos verificados por mais de N seg**. Limitação do tempo de execução da tarefa. Depois do tempo especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está marcada como concluída. Na próxima vez que o Kaspersky Endpoint Security executar a tarefa, ela será executada desde o início e dentro do cronograma.

   - **Não executar várias tarefas de verificação ao mesmo tempo**. Adie as tarefas de verificação agendadas se uma verificação agendada iniciada anteriormente ainda estiver em execução. O Kaspersky Endpoint Security enfileirará as tarefas de verificação agendadas se a verificação atual continuar. Isso ajuda a otimizar a carga no computador. Por exemplo, você programou tarefas de verificação para serem executadas às 18h e às 20h. O Kaspersky Endpoint Security adiará a tarefa de verificação das 20h se a tarefa de verificação programada para as 18h ainda estiver em execução. O aplicativo executará uma verificação após a conclusão da tarefa iniciada às 18h.

7. Clique **Adicional**.

   Isso abre a janela de configurações de verificação de arquivos compostos.

8. No bloco **Limite de tamanho**, marque a caixa de seleção **Não descompactar arquivos compostos grandes**. Limitação do tempo de execução da tarefa. Depois do tempo especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está marcada como concluída. Na próxima vez que o Kaspersky Endpoint Security executar a tarefa, ela será executada desde o início e dentro do cronograma.

   O Kaspersky Endpoint Security verifica os arquivos grandes que foram extraídos dos arquivos compactados, independentemente de a caixa de seleção **Não descompactar arquivos compostos grandes** estar marcada.

9. Clique **OK**.

10. Vá para a guia **Adicional**.

11. Na seção **Tecnologias de verificação**, marque as caixas de seleção junto aos nomes das tecnologias que deseja usar na verificação:

    - **Tecnologia iSwift**. Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iSwift é um avanço da tecnologia iChecker do sistema de arquivos NTFS.

    - **Tecnologia iChecker**. Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iChecker tem algumas limitações: ela não funciona com arquivos grandes e se aplica somente a objetos com uma estrutura reconhecida pelo aplicativo (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

12. Salvar alterações.

Como otimizar a verificação na Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Tarefas**.

   A lista de tarefas é aberta.

2. Clique na tarefa de verificação.

   A janela de propriedades da tarefa é exibida. Caso seja necessário, crie a tarefa *Verificação de malware*.

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

4. No bloco **Ação ao detectar ameaça**, marque a caixa de seleção **Verificar apenas arquivos novos e modificados**. Verifica apenas os arquivos novos e aqueles que foram modificados desde a última vez em que foram verificados. Isso ajuda a reduzir a duração de uma verificação. Esse modo se aplica a arquivos simples e compostos.

   Também é possível configurar a verificação de novos arquivos por tipo. Por exemplo, é possível verificar todos os pacotes de distribuição e verificar apenas novos arquivos e arquivos de formato office.

5. No bloco **Otimização da verificação**, marque a caixa de seleção **Não descompactar arquivos compostos grandes**. Limitação do tempo de execução da tarefa. Depois do tempo especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está marcada como concluída. Na próxima vez que o Kaspersky Endpoint Security executar a tarefa, ela será executada desde o início e dentro do cronograma.

   O Kaspersky Endpoint Security verifica os arquivos grandes que foram extraídos dos arquivos compactados, independentemente de a caixa de seleção **Não descompactar arquivos compostos grandes** estar marcada.

6. Marque a caixa de seleção **Não executar várias tarefas de verificação ao mesmo tempo**. Adie as tarefas de verificação agendadas se uma verificação agendada iniciada anteriormente ainda estiver em execução. O Kaspersky Endpoint Security enfileirará as tarefas de verificação agendadas se a verificação atual continuar. Isso ajuda a otimizar a carga no computador. Por exemplo, você programou tarefas de verificação para serem executadas às 18h e às 20h. O Kaspersky Endpoint Security adiará a tarefa de verificação das 20h se a tarefa de verificação programada para as 18h ainda estiver em execução. O aplicativo executará uma verificação após a conclusão da tarefa iniciada às 18h.

7. No bloco **Configurações avançadas**, marque a caixa de seleção **Ignorar arquivo verificado por mais de (seg)**. Limitação do tempo de execução da tarefa. Depois do tempo especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está marcada como concluída. Na próxima vez que o Kaspersky Endpoint Security executar a tarefa, ela será executada desde o início e dentro do cronograma.

8. Salvar alterações.

Como otimizar a verificação na interface do aplicativo

1. Na janela principal do aplicativo, acesse a seção **Tarefas**.

2. Na janela aberta, selecione a tarefa de verificação e clique em ⚙.

3. Clique **Configurações avançadas**.

4. No bloco **Otimização**, defina as configurações de verificação:

   - **Verificar somente arquivos novos e alterados**. Verifica apenas os arquivos novos e aqueles que foram modificados desde a última vez em que foram verificados. Isso ajuda a reduzir a duração de uma verificação. Esse modo se aplica a arquivos simples e compostos.

     Também é possível configurar a verificação de novos arquivos por tipo. Por exemplo, é possível verificar todos os pacotes de distribuição e verificar apenas novos arquivos e arquivos de formato office.

   - **Ignorar arquivo verificado por mais de N segundos**. Limitação do tempo de execução da tarefa. Depois do tempo especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está marcada como concluída. Na próxima vez que o Kaspersky Endpoint Security executar a tarefa, ela será executada desde o início e dentro do cronograma.

   - **Não inicie várias tarefas de verificação ao mesmo tempo**. Adie as tarefas de verificação agendadas se uma verificação agendada iniciada anteriormente ainda estiver em execução. O Kaspersky Endpoint Security enfileirará as tarefas de verificação agendadas se a verificação atual continuar. Isso ajuda a otimizar a carga no computador. Por exemplo, você programou tarefas de verificação para serem executadas às 18h e às 20h. O Kaspersky Endpoint Security adiará a tarefa de verificação das 20h se a tarefa de verificação programada para as 18h ainda estiver em execução. O aplicativo executará uma verificação após a conclusão da tarefa iniciada às 18h.

5. No bloco **Limite de tamanho**, marque a caixa de seleção **Não descompactar arquivos compostos de grandes dimensões**. Limitação do tempo de execução da tarefa. Depois do tempo especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está marcada como concluída. Na próxima vez que o Kaspersky Endpoint Security executar a tarefa, ela será executada desde o início e dentro do cronograma.

   O Kaspersky Endpoint Security verifica os arquivos grandes que foram extraídos dos arquivos compactados, independentemente de a caixa de seleção **Não descompactar arquivos compostos de grandes dimensões** estar marcada.

6. Na seção **Tecnologias de verificação**, marque as caixas de seleção junto aos nomes das tecnologias que deseja usar na verificação:

   - **Tecnologia iSwift**. Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iSwift é um avanço da tecnologia iChecker do sistema de arquivos NTFS.

   - **Tecnologia iChecker**. Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iChecker tem algumas limitações: ela não funciona com arquivos grandes e se aplica somente a objetos com uma estrutura reconhecida pelo aplicativo (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

7. Salvar alterações.

Caso a tarefa de verificação não seja exibida, significa que o administrador proibiu o uso de tarefas locais na política.

Atualizar bancos de dados e módulos do software aplicativo

A atualização dos bancos de dados e dos módulos do aplicativo do Kaspersky Endpoint Security assegura ao computador a versão de proteção mais recente. No mundo todo, novos tipos de vírus e malware surgem diariamente. Os bancos de dados do Kaspersky Endpoint Security contêm informações sobre ameaças e formas de neutralizá-las. Para detectar ameaças rapidamente, é necessário atualizar regularmente os bancos de dados e os módulos do aplicativo.

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.

Atualizações frequentes exigem uma licença em vigor. Se não houver uma licença atual, será possível executar a atualização apenas uma vez.

O computador precisa estar conectado à Internet para que o pacote de atualização possa ser baixado dos servidores de atualização da Kaspersky. Por padrão, as configurações de conexão com a Internet são definidas automaticamente. Se você usar um servidor proxy, é necessário ajustar as configurações do servidor proxy.

As atualizações são baixadas por meio do protocolo HTTPS. Elas também podem ser baixadas por meio do protocolo HTTP quando é impossível baixar atualizações pelo protocolo HTTPS.

Ao executar a atualização, os seguintes objetos são baixados e instalados no computador:

- Bancos de dados do Kaspersky Endpoint Security. A proteção do computador é fornecida utilizando bancos de dados com assinatura de vírus e outras ameaças e informações sobre a forma de neutralizá-las. Os componentes de proteção usam estas informações quando procuram e neutralizam arquivos infectados no computador. Os bancos de dados são constantemente atualizados com registros de novas ameaças e métodos para neutralizá-las. Portanto, é recomendável fazer a atualização dos bancos de dados regularmente.

  Além dos bancos de dados do Kaspersky Endpoint Security, também são atualizadas as unidades de rede que ativam os componentes do aplicativo de interceptação de tráfego de rede.

- Módulos do aplicativo. Além dos bancos de dados do Kaspersky Endpoint Security, faça também a atualização dos módulos do programa. A atualização dos módulos do aplicativo soluciona os problemas relativos a vulnerabilidades neste; adiciona novas funções ou aprimora as existentes.

Durante a atualização, os bancos de dados e os módulos do aplicativo no computador são comparados com a versão mais recente na fonte de atualização. Se forem encontradas diferenças nos bancos de dados e nos módulos do aplicativo, em relação às respectivas versões mais recentes, são instaladas as atualizações que faltam no computador.

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 Endpoint 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 resultados da atualização e sobre todos os eventos que ocorrem durante o desempenho da tarefa de atualização são registradas no relatório do Kaspersky Endpoint Security.

Se o aplicativo estiver funcionando em modo Light Agent, considerações especiais estarão envolvidas na atualização de módulos e bancos de dados do aplicativo.

Cenários de atualização do banco de dados e do módulo de aplicativo

A atualização dos bancos de dados e dos módulos do aplicativo do Kaspersky Endpoint Security assegura ao computador a versão de proteção mais recente. No mundo todo, novos tipos de vírus e malware surgem diariamente. Os bancos de dados do Kaspersky Endpoint Security contêm informações sobre ameaças e formas de neutralizá-las. Para detectar ameaças rapidamente, é necessário atualizar regularmente os bancos de dados e os módulos do aplicativo.

Os seguintes objetos são atualizados nos computadores dos usuários:

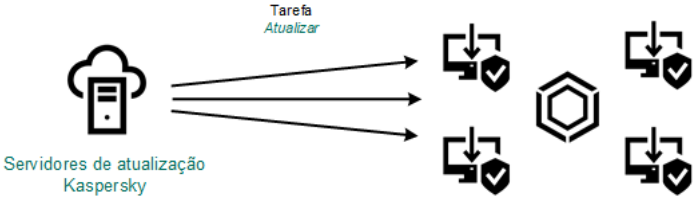
- Bancos de dados de antivírus. Os bancos de dados de antivírus incluem bancos de dados de assinaturas de malware, descrição de ataques de rede, bancos de dados de endereços web de phishing e maliciosos, bancos de dados de banners, bancos de dados de spam e outros dados.

- Módulos do aplicativo. As atualizações do módulo são destinadas a eliminar vulnerabilidades no aplicativo e aprimorar os métodos de proteção do computador. As atualizações do módulo podem alterar o comportamento dos componentes do aplicativo e adicionar novos recursos.

O Kaspersky Endpoint Security dá suporte aos seguintes cenários para atualizar bancos de dados e módulos de aplicativos:

- Atualizar a partir dos servidores da Kaspersky.

  Os servidores de atualização da Kaspersky estão localizados em vários países em todo o mundo. Isso garante atualizações de alta confiabilidade. Se uma atualização não puder ser realizada a partir de um servidor, o Kaspersky Endpoint Security passará para o próximo servidor.



Atualizar a partir dos servidores da Kaspersky

- Atualização centralizada.

  A atualização centralizada reduz o tráfego externo de Internet e oferece monitoramento conveniente da atualização.

  A atualização centralizada consiste nas seguintes etapas:

  1. Faça download do pacote de atualização para um repositório dentro da rede da organização.

     A tarefa do servidor de administração, nomeada *Baixar atualizações no repositório do Servidor de Administração*, faz o download do pacote de atualizações para o repositório.

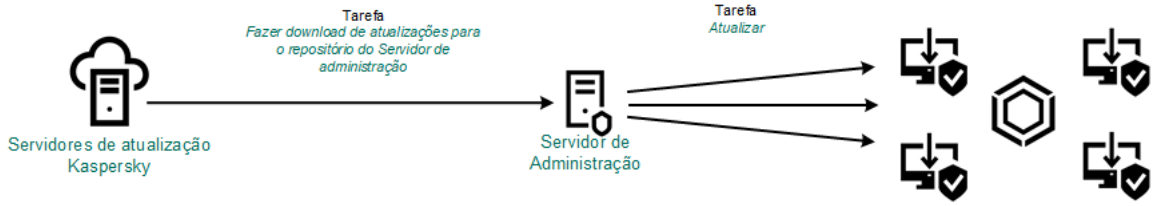
2. Faça o download do pacote de atualização para uma pasta compartilhada (opcional).

   Você pode fazer download do pacote de atualização para uma pasta compartilhada usando os seguintes métodos:

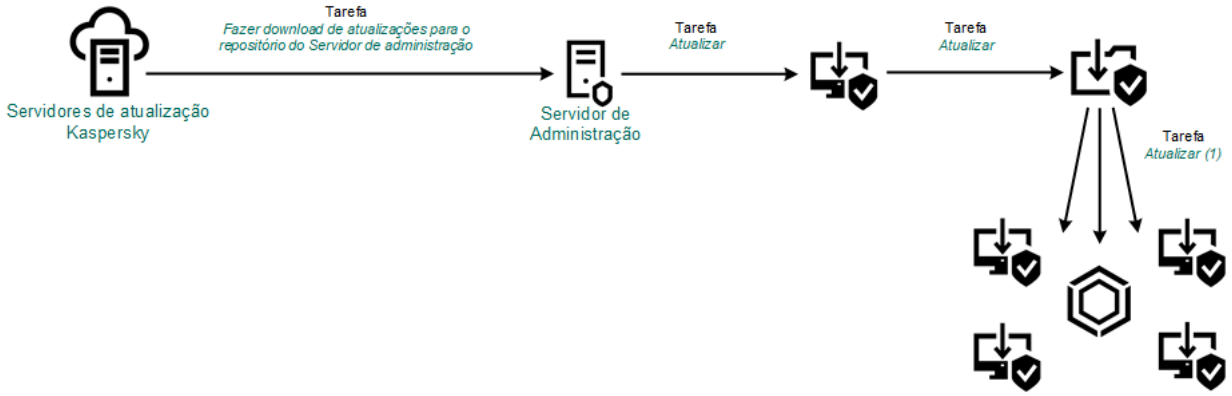
   - Usando a tarefa *Atualização de bancos de dados e módulos do aplicativo* do Kaspersky Endpoint Security. A tarefa destina-se a um dos computadores na rede local da empresa.
   - Utilizando o Kaspersky Update Utility. Para obter informações detalhadas sobre o uso do Kaspersky Update Utility, consulte a Base de Conhecimento Kaspersky.

3. Distribua o pacote de atualização a computadores clientes.

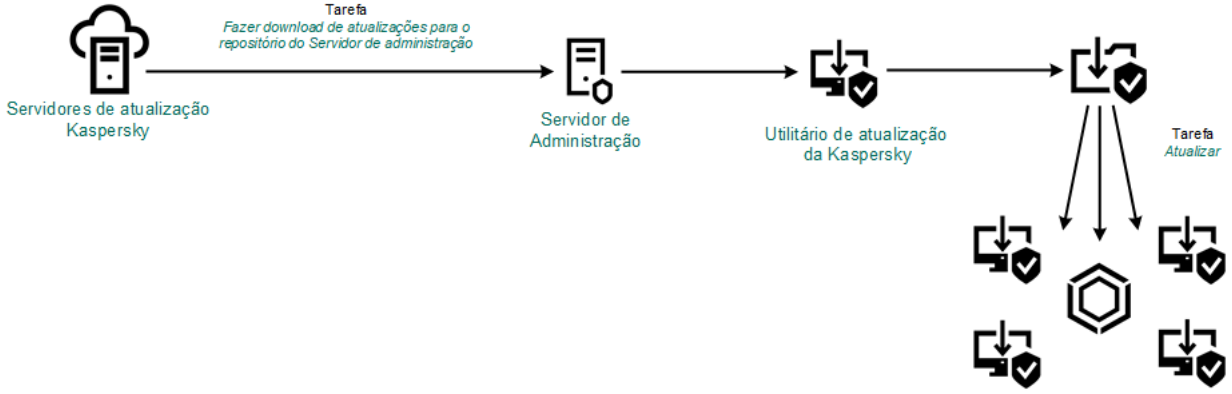
   O pacote de atualização é distribuído a computadores clientes pela tarefa *Atualização de bancos de dados e módulos do aplicativo* do Kaspersky Endpoint Security. Você pode criar um número ilimitado de tarefas de atualização para cada grupo de administração.



Atualizar a partir de um repositório de servidor



Atualizar a partir de uma pasta compartilhada



Atualizar utilizando o Kaspersky Update Utility

Para o Kaspersky Security Center, a lista padrão de fontes de atualizações inclui o Servidor de Administração do Kaspersky Security Center e os servidores de atualização da Kaspersky. Para o Kaspersky Security Center Cloud Console, a lista padrão de fontes de atualização contém pontos de distribuição e servidores de atualização da Kaspersky. Para obter mais informações sobre os pontos de distribuição, consulte a ajuda do Kaspersky Security Center Cloud Console. É possível adicionar outras fontes de atualização à lista. Você pode especificar servidores FTP ou HTTP e pastas compartilhadas como fontes de atualização. Se uma atualização não puder ser realizada a partir de uma fonte de atualização, o Kaspersky Endpoint Security passará para a próxima.

As atualizações são baixadas dos servidores de atualização da Kaspersky ou de outros servidores FTP ou HTTP por meio de protocolos de rede padrão. Se a conexão com um servidor proxy for necessária para acessar a fonte de atualizações, especifique as configurações do servidor proxy nas configurações da política do Kaspersky Endpoint Security.

Atualizar a partir de um repositório de servidor

Para conservar o tráfego de Internet, você pode configurar atualizações de bancos de dados e módulos do aplicativo em computadores da rede local da organização a partir do repositório de um servidor. Para isso, o Kaspersky Security Center deve fazer download de um pacote de atualização para o repositório (servidor FTP ou HTTP, rede ou pasta local) a partir dos servidores de atualização da Kaspersky. Outros computadores na rede local da organização poderão receber o pacote de atualização do repositório do servidor.

A configuração de atualizações do banco de dados e do módulo do aplicativo a partir do repositório de um servidor consiste nas seguintes etapas:

1. Configurar o download de um pacote de atualização para o repositório do Servidor de Administração (a tarefa *Baixar atualizações no repositório do Servidor de Administração*).

   A tarefa *Baixar atualizações no repositório do Servidor de Administração* é criada automaticamente pelo assistente de início rápido do Servidor de Administração, e essa tarefa pode ter apenas uma única instância. Por padrão, o Kaspersky Security Center copia o pacote de atualização para a pasta `\\<server name>\KLSHARE\Updates`. Para obter mais informações sobre como baixar atualizações no repositório do Servidor de Administração, consulte a Ajuda do Kaspersky Security Center.

2. Configurar atualizações do banco de dados e do módulo do aplicativo a partir do repositório do servidor especificado para os computadores restantes na rede local da organização (tarefa *Atualização de bancos de dados e módulos do aplicativo*).

   Como configurar a atualização do Kaspersky Endpoint Security a partir do armazenamento do servidor especificado no Console de Administração (MMC)

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

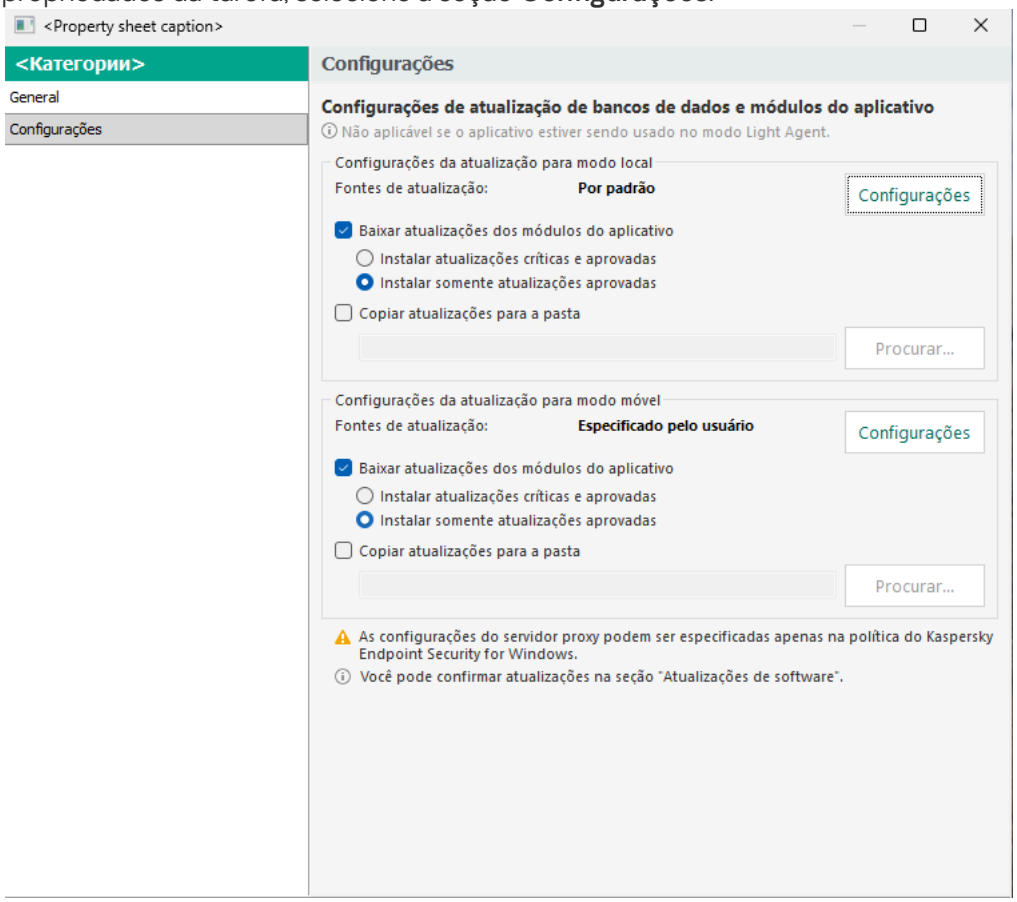
      Na árvore do console, selecione **Tarefas**.

   2. Clique na tarefa **Atualização de bancos de dados e módulos do aplicativo** do Kaspersky Endpoint Security.

      A janela de propriedades da tarefa é exibida.

      A tarefa *Atualização de bancos de dados e módulos do aplicativo* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização de bancos de dados e módulos do aplicativo*, instale o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows enquanto executa o assistente.

3. Na janela de propriedades da tarefa, selecione a seção **Configurações**.



Configurações da tarefa Atualização de bancos de dados e módulos do aplicativo

4. No bloco **Configurações da atualização para modo local**, clique no botão **Configurações**.

5. Na lista de fontes de atualização, certifique-se de que a atualização a partir da fonte **Kaspersky Security Center** está ativada. Além disso, a fonte **Kaspersky Security Center** deve ter a prioridade mais alta.

6. Caso seja necessário, adicione as fontes de atualização:

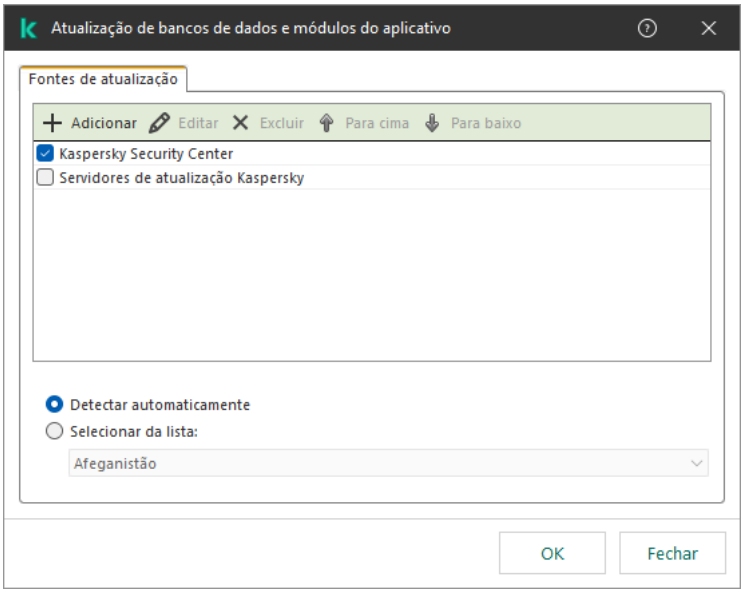
   a. Na lista de fontes de atualizações, clique no botão **Adicionar**.

   b. No campo **Fontes de atualização**, especifique o endereço do servidor FTP ou HTTP, a pasta de rede ou a pasta local onde o Kaspersky Security Center copiará o pacote de atualização recebido dos servidores da Kaspersky.

   > O endereço da fonte de atualização deve corresponder ao endereço especificado no campo **Pasta para armazenar atualizações** quando o download de atualizações foi configurado para o armazenamento do servidor (a tarefa *Baixar atualizações no repositório do Servidor de Administração*).

   c. Clique em **OK**.

É possível excluir a fonte de atualização sem removê-la da lista de fontes de atualização. Para fazer isso, desmarque a caixa de seleção ao lado do objeto.



Fontes de atualizações

7. Configure as prioridades das fontes de atualizações utilizando os botões **Para cima** e **Para baixo**.

   Se uma atualização não puder ser realizada a partir da primeira fonte de atualização, o Kaspersky Endpoint Security passará automaticamente para a próxima fonte.

8. Na janela de propriedades da tarefa, selecione a seção **Agendamento** e configure o modo de execução da tarefa.

9. Por padrão, o Kaspersky Endpoint Security executa a tarefa no modo manual.

10. Salvar alterações.

Como configurar a atualização do Kaspersky Endpoint Security a partir do armazenamento do servidor especificado no Web Console

1. Na janela principal do Web Console, selecione **Tarefas**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Atualização** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

   A tarefa *Atualização* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização*, instale o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows enquanto executa o assistente.

3. Selecione a guia **Configurações do aplicativo** → **Modo local**.

4. Na lista de fontes de atualização, certifique-se de que a atualização a partir da fonte **Kaspersky Security Center** está ativada. Além disso, a fonte **Kaspersky Security Center** deve ter a prioridade mais alta.

5. Caso seja necessário, adicione as fontes de atualização:

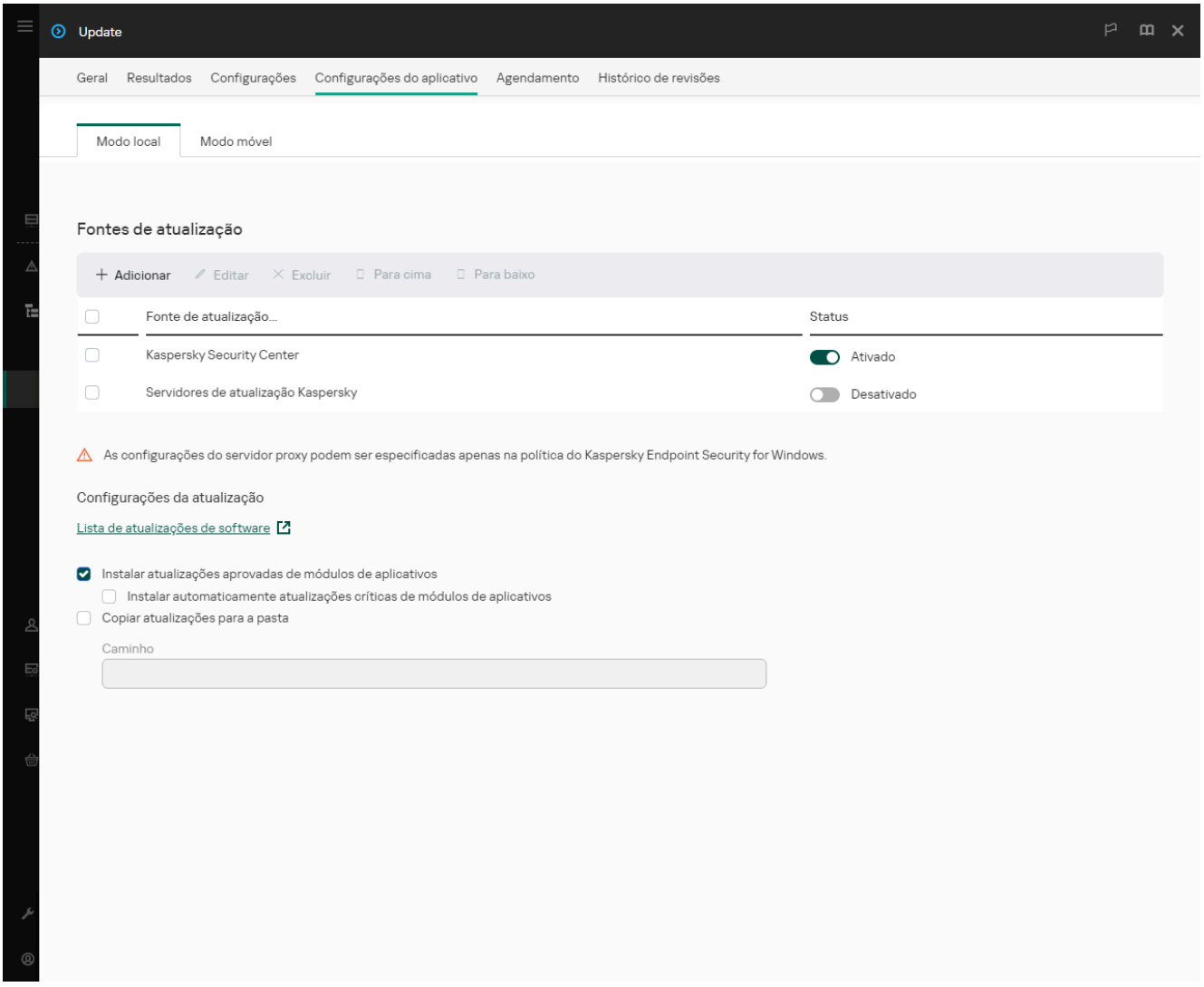
   a. Na lista de fontes de atualizações, clique no botão **Adicionar**.

   b. No campo **Fontes de atualização**, especifique o endereço do servidor FTP ou HTTP, a pasta de rede ou a pasta local onde o Kaspersky Security Center copiará o pacote de atualização recebido dos servidores da Kaspersky.

   > O endereço da fonte de atualização deve corresponder ao endereço especificado no campo **Pasta para armazenar atualizações** quando o download de atualizações foi configurado para o armazenamento do servidor (a tarefa *Baixar atualizações no repositório do Servidor de Administração*).

   c. Clique **Salvar**.

É possível excluir a fonte de atualização sem removê-la da lista de fontes de atualização. Para fazer isso, coloque a chave de alternância ao lado na posição desativada.



Fontes de atualizações

6. Configure as prioridades das fontes de atualizações utilizando os botões **Mover para cima** e **Mover para baixo**.

   Se uma atualização não puder ser realizada a partir da primeira fonte de atualização, o Kaspersky Endpoint Security passará automaticamente para a próxima fonte.

7. Na janela de propriedades da tarefa, selecione a seção **Agendamento** e configure o modo de execução da tarefa.

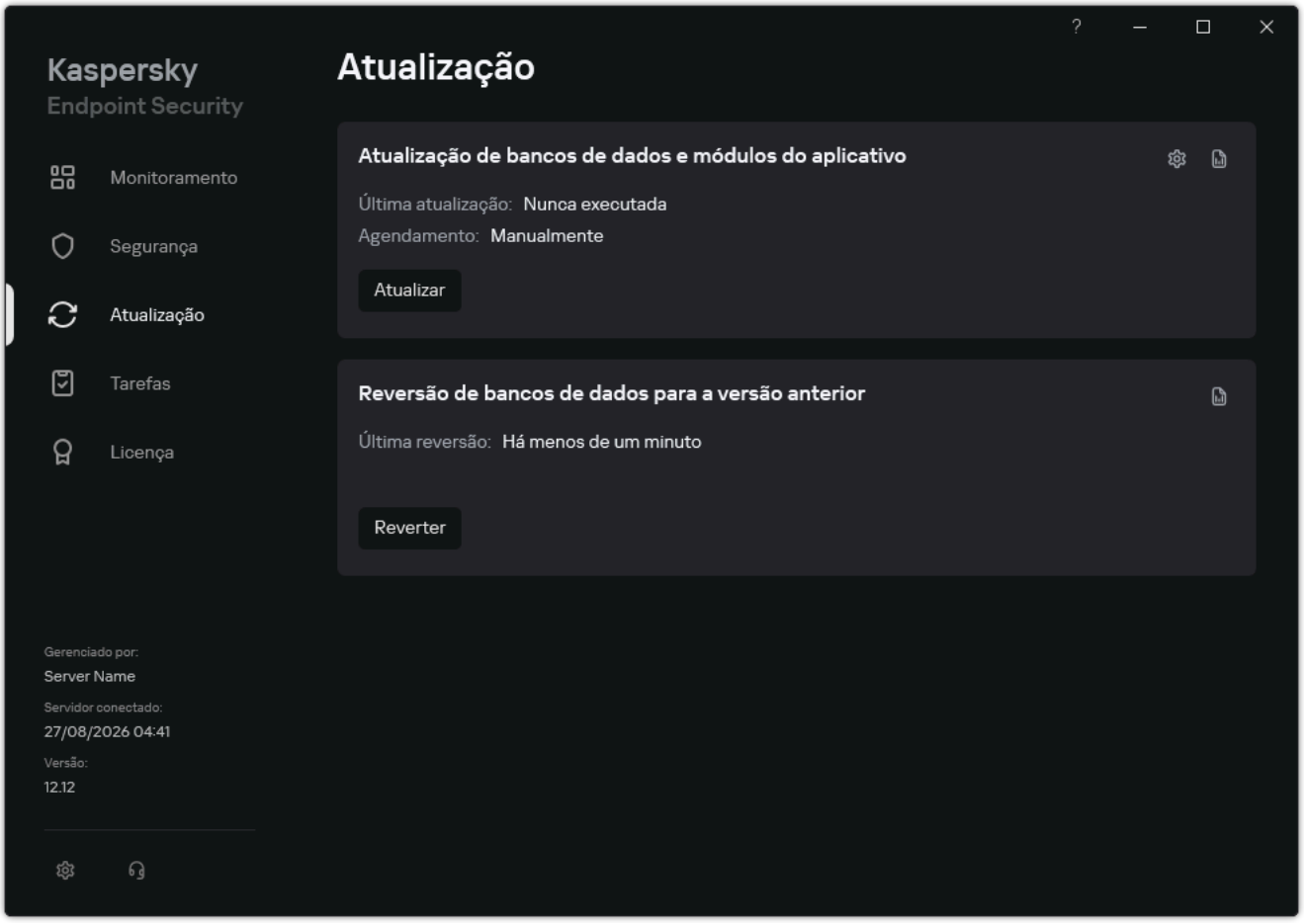
8. Por padrão, o Kaspersky Endpoint Security executa a tarefa no modo manual.

9. Salvar alterações.

Como configurar a atualização do Kaspersky Endpoint Security a partir do armazenamento do servidor especificado na interface do aplicativo

Não é possível configurar a tarefa de grupo *Atualização de bancos de dados e módulos do aplicativo* na interface do aplicativo. Apenas uma tarefa de atualização local, *Atualização de bancos de dados e módulos do aplicativo*, está disponível para o usuário. Caso a tarefa *Atualização de bancos de dados e módulos do aplicativo* não seja exibida, significa que o administrador proibiu o uso de tarefas locais na política.

1. Na janela principal do aplicativo, acesse a seção **Atualização**.



Tarefas de atualização local

2. A lista de tarefas é aberta; selecione a tarefa *Atualização de bancos de dados e módulos do aplicativo* e clique em ⚙.

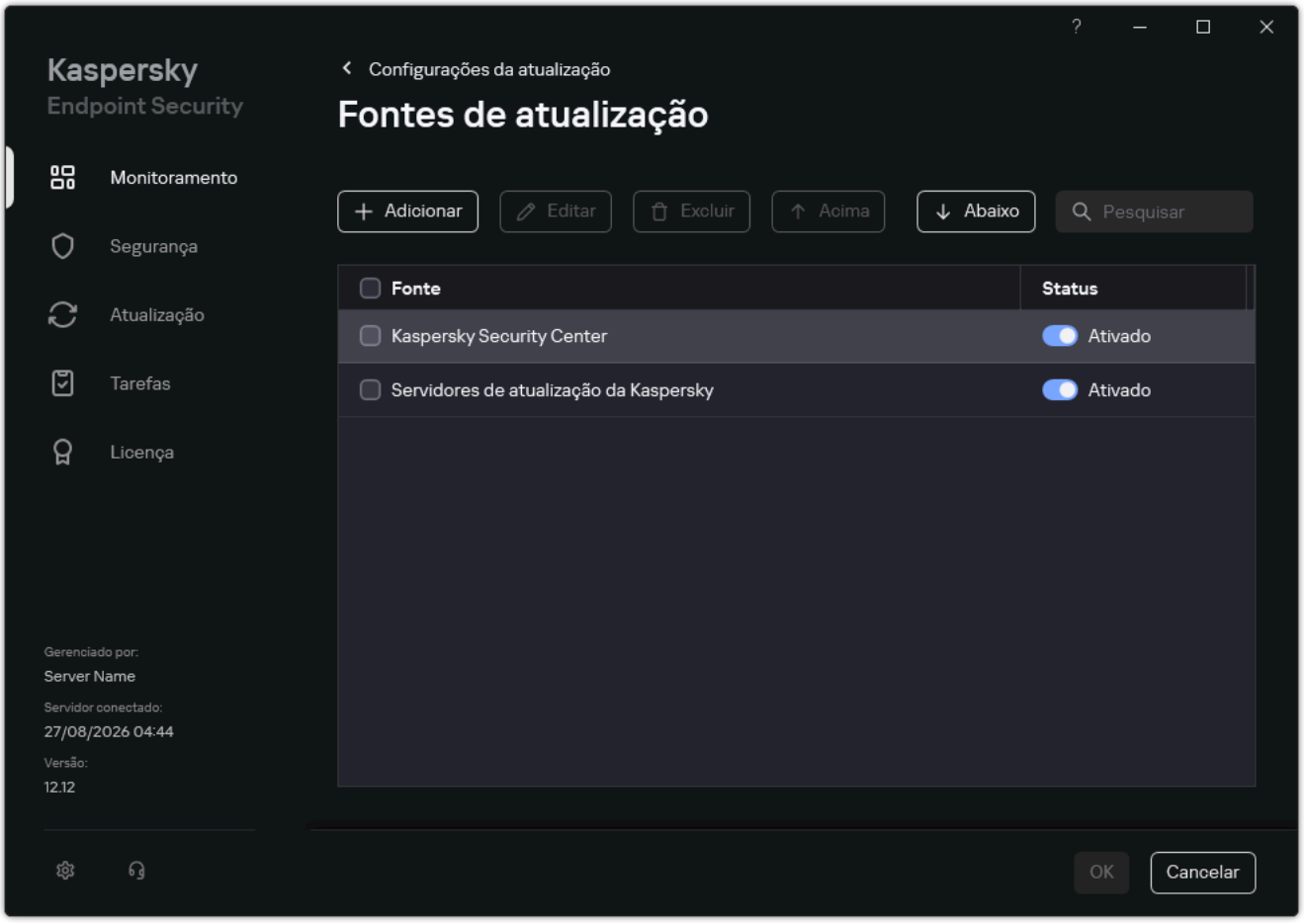
   A janela de propriedades da tarefa é exibida.

3. Na janela de propriedades da tarefa. Clique em **Selecionar fontes de atualização**.

4. Na lista de fontes de atualização, certifique-se de que a atualização a partir da fonte **Kaspersky Security Center** está ativada. Além disso, a fonte **Kaspersky Security Center** deve ter a prioridade mais alta.

5. Caso seja necessário, adicione as fontes de atualização:

   a. Na lista de fontes de atualizações, clique no botão **Adicionar**.



Fontes de atualizações

   a. Especifique o endereço do servidor FTP ou HTTP, a pasta de rede ou a pasta local onde o Kaspersky Security Center copiará o pacote de atualização recebido dos servidores de atualização da Kaspersky.

   > O endereço da fonte de atualização deve corresponder ao endereço especificado no campo **Pasta para armazenar atualizações** quando o download de atualizações foi configurado para o armazenamento do servidor (a tarefa *Baixar atualizações no repositório do Servidor de Administração*).

   b. Clique **Selecionar**.

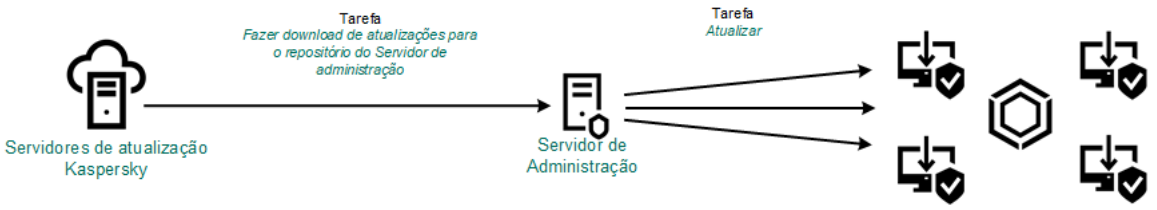
   É possível excluir a fonte de atualização sem removê-la da lista de fontes de atualização. Para fazer isso, coloque a chave de alternância ao lado na posição desativada.

6. Configure as prioridades das fontes de atualizações utilizando os botões **Acima** e **Abaixo**.

   Se uma atualização não puder ser realizada a partir da primeira fonte de atualização, o Kaspersky Endpoint Security passará automaticamente para a próxima fonte.

Caso um computador seja gerenciado pelo Kaspersky Security Center, não será possível configurar o modo de execução para a tarefa *Atualização de bancos de dados e módulos do aplicativo*. Só é possível executar a tarefa manualmente.

7. Salvar alterações.



Atualizar a partir de um repositório de servidor

Atualizar a partir de uma pasta compartilhada

Para conservar o tráfego de Internet, você pode configurar atualizações de bancos de dados e módulos do aplicativo em computadores da rede local da organização a partir de uma pasta compartilhada. Para isso, um dos computadores na rede local da organização deve receber pacotes de atualização do Servidor de Administração do Kaspersky Security Center ou dos servidores de atualização da Kaspersky e, em seguida, copiar o pacote de atualização recebido para a pasta compartilhada. Outros computadores na rede local da organização poderão receber o pacote de atualização desta pasta compartilhada.

A versão e localização do aplicativo Kaspersky Endpoint Security que copia o pacote de atualização para uma pasta compartilhada deve corresponder à versão e localização do aplicativo que atualiza os bancos de dados a partir da pasta compartilhada. Se as versões ou localizações dos aplicativos não forem correspondentes, a atualização do banco de dados pode terminar com um erro.

A configuração de atualizações do banco de dados e do módulo do aplicativo a partir de uma pasta compartilhada consiste nas seguintes etapas:

1. Configuração das atualizações do módulo do aplicativo e banco de dados a partir de um repositório de servidor.

2. Ativação da ação de cópia do pacote de atualização para uma pasta compartilhada em um dos computadores na rede local.

   Como ativar a cópia do pacote de atualização para a pasta compartilhada no Console de administração (MMC)

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

   2. Na árvore do console, selecione **Tarefas**.

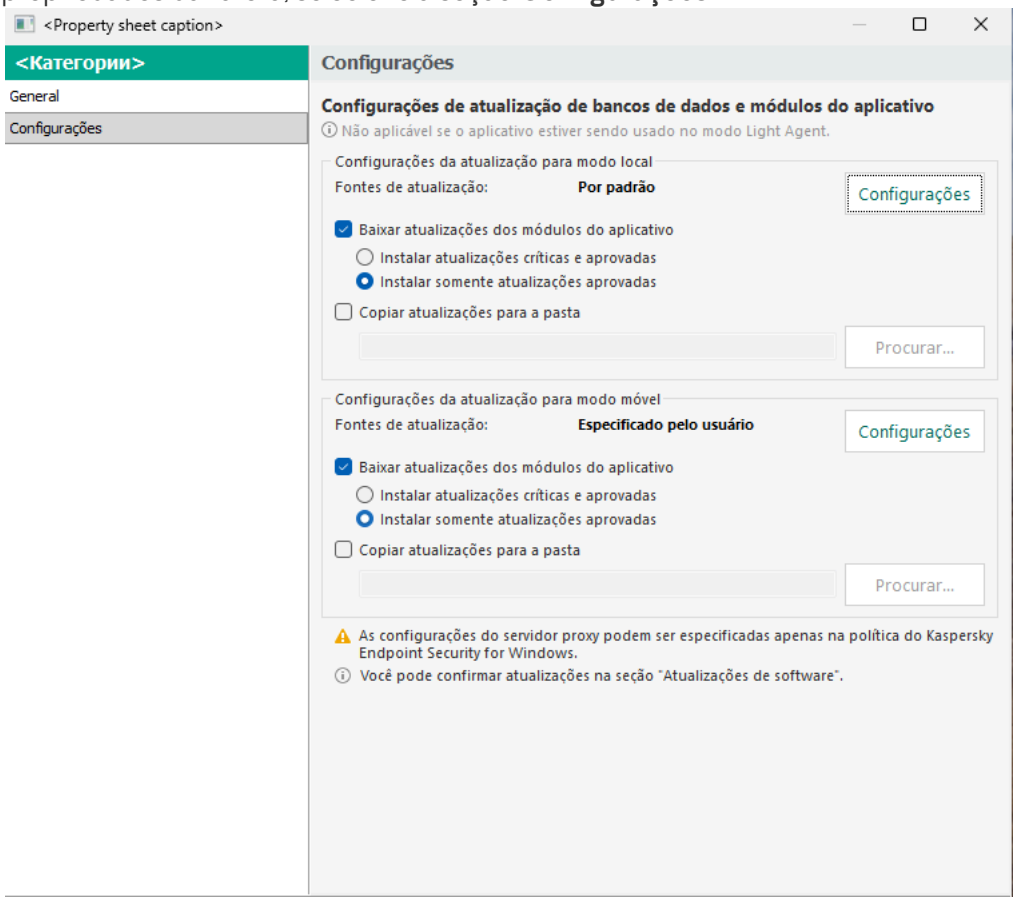
   A tarefa *Atualização de bancos de dados e módulos do aplicativo* deve ser atribuída a um computador que servirá como fonte de atualizações.

   3. Clique na tarefa **Atualização de bancos de dados e módulos do aplicativo** do Kaspersky Endpoint Security.

      A janela de propriedades da tarefa é exibida.

A tarefa *Atualização de bancos de dados e módulos do aplicativo* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização de bancos de dados e módulos do aplicativo*, instale o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows enquanto executa o assistente.

4. Na janela de propriedades da tarefa, selecione a seção **Configurações**.



Configurações da tarefa Atualização de bancos de dados e módulos do aplicativo

5. No bloco **Configurações da atualização para modo local**, clique no botão **Configurações**.

6. Configure as fontes de atualizações.

   As fontes de atualizações podem ser servidores de atualização da Kaspersky, o Servidor de Administração do Kaspersky Security Center, outros servidores FTP ou HTTP, pastas locais ou pastas de rede.

7. Marque a caixa de seleção **Copiar atualizações para a pasta**.

8. No campo **Caminho da pasta** digite o caminho UNC para a pasta compartilhada (por exemplo, `\\<server name>\KLSHARE\Updates`).

   Se o campo for deixado em branco, o Kaspersky Endpoint Security copiará o pacote de atualização para a pasta `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

9. Salvar alterações.

Como ativar a cópia do pacote de atualização para a pasta compartilhada no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **Tarefas**.

   A lista de tarefas é aberta.

A tarefa *Atualização* deve ser atribuída a um computador que servirá como fonte de atualizações.

2. Clique na tarefa **Atualização** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

   A tarefa *Atualização* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização*, instale o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows enquanto executa o assistente.

3. Selecione a guia **Configurações do aplicativo** → **Modo local**.

4. Configure as fontes de atualizações.

   As fontes de atualizações podem ser servidores de atualização da Kaspersky, o Servidor de Administração do Kaspersky Security Center, outros servidores FTP ou HTTP, pastas locais ou pastas de rede.

5. Marque a caixa de seleção **Copiar atualizações para a pasta**.

6. No campo **Caminho** digite o caminho UNC para a pasta compartilhada (por exemplo, `\\<server name>\KLSHARE\Updates`).

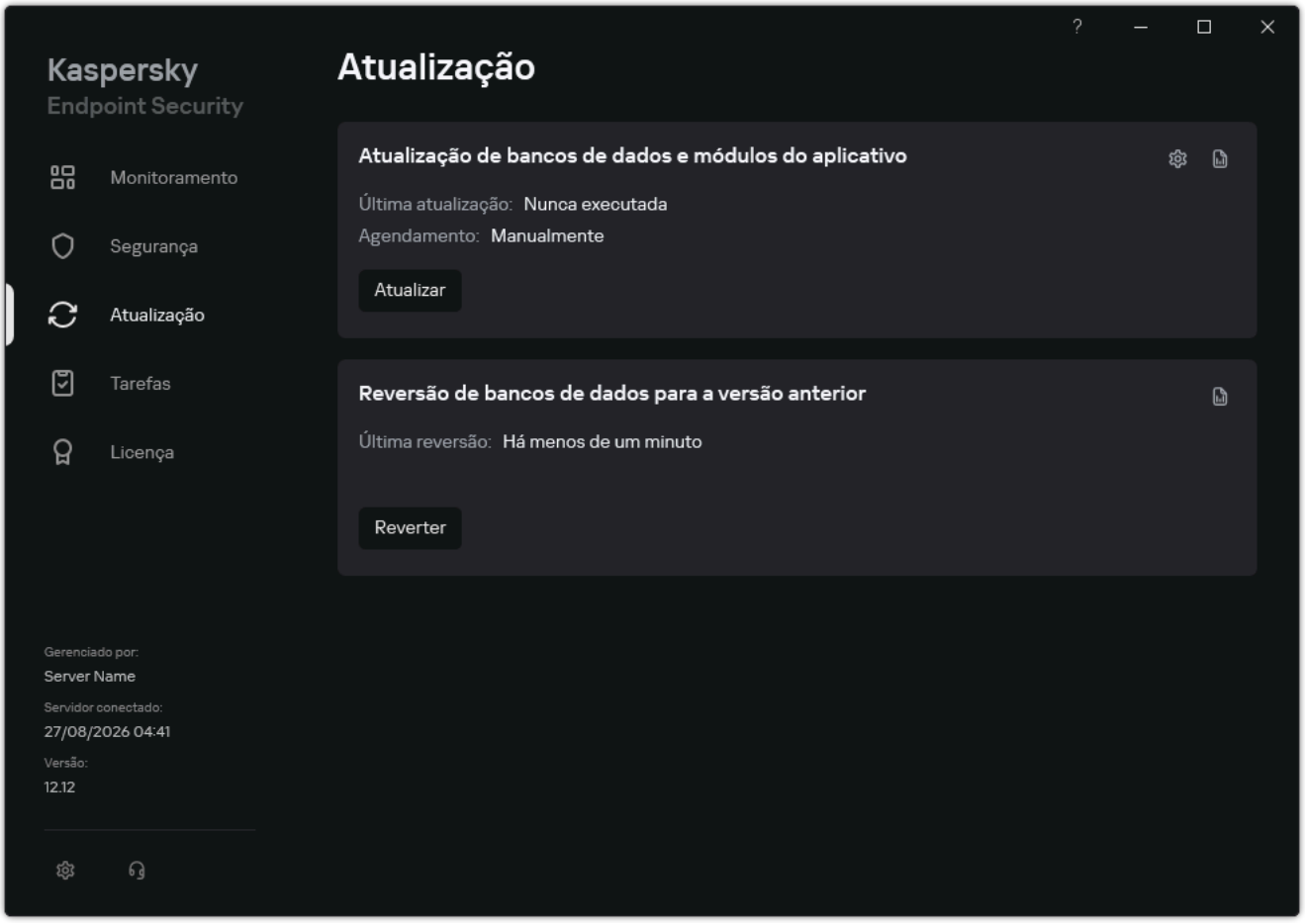
   Se o campo for deixado em branco, o Kaspersky Endpoint Security copiará o pacote de atualização para a pasta `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

7. Salvar alterações.

Como ativar a cópia do pacote de atualização para a pasta compartilhada na interface do aplicativo

> Não é possível configurar a tarefa de grupo *Atualização de bancos de dados e módulos do aplicativo* na interface do aplicativo. Apenas uma tarefa de atualização local, *Atualização de bancos de dados e módulos do aplicativo*, está disponível para o usuário. Caso a tarefa *Atualização de bancos de dados e módulos do aplicativo* não seja exibida, significa que o administrador proibiu o uso de tarefas locais na política.

1. Na janela principal do aplicativo, acesse a seção **Atualização**.



Tarefas de atualização local

2. A lista de tarefas é aberta; selecione a tarefa *Atualização de bancos de dados e módulos do aplicativo* e clique em ⚙.

   A janela de propriedades da tarefa é exibida.

3. No bloco **Distribuição de atualizações**, marque a caixa de seleção **Copiar atualizações para a pasta**.

4. Digite o caminho UNC para a pasta compartilhada (por exemplo, `\\<server name>\KLSHARE\Updates`).

5. Salvar alterações.

3. Configure atualizações do banco de dados e do módulo do aplicativo a partir da pasta compartilhada especificada para os computadores restantes na rede local da organização.

   Como configurar atualizações por meio da pasta compartilhada no Console de Administração (MMC)

   1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Atualização de bancos de dados e módulos do aplicativo**.

4. No Console de Administração do Kaspersky Security Center, selecione **Tarefas**.

   A lista de tarefas é aberta.

5. Clique **Nova tarefa**.

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

Etapa 1. Selecionar o tipo de tarefa

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Atualização de bancos de dados e módulos do aplicativo**.

Etapa 2. Como selecionar fontes de atualização

Adicione uma nova fonte de atualização: uma pasta compartilhada. O endereço de origem deve corresponder ao endereço especificado anteriormente no campo **Caminho da pasta** quando você configurou a cópia do pacote de atualização para a pasta compartilhada. Configure as prioridades das fontes de atualizações utilizando os botões **Para cima** e **Para baixo**.

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.

A tarefa *Atualização de bancos de dados e módulos do aplicativo* deve ser atribuída aos computadores da rede local da organização, exceto o computador que serve como fonte de atualização.

Etapa 4. Seleção da conta para executar a tarefa

Selecione uma conta para executar a tarefa de *Atualização de bancos de dados e módulos do aplicativo*. Por padrão, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de usuário local.

Etapa 5. Configurar um agendamento de início de tarefa

Configure um agendamento para iniciar uma tarefa, por exemplo, manualmente ou após o download dos bancos de dados antivírus no repositório.

Etapa 6. Definir o nome da tarefa

Digite o nome da tarefa, por exemplo, *atualização por meio de uma pasta compartilhada*.

Etapa 7. Concluir a criação da tarefa

Conclua o 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 resultado, a tarefa de atualização será executada nos computadores dos usuários de acordo com a programação especificada.

Como configurar atualizações pela pasta compartilhada no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Atualização**.

   c. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Atualização a partir de uma pasta compartilhada*.

   d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

   > A tarefa *Atualização* deve ser atribuída aos computadores da rede local da organização, exceto o computador que serve como fonte de atualização.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada e clique para avançar para a próxima etapa.

5. Conclua o assistente.

   Uma nova tarefa será exibida na tabela de tarefas.

6. Clique na tarefa *Atualização* recém-criada.

   A janela de propriedades da tarefa é exibida.

7. Selecione a guia **Configurações do aplicativo** → **Modo local**.

8. No bloco **Fontes de atualização**, clique no botão **Adicionar**.

9. Na janela exibida, insira o caminho para a pasta compartilhada.

   O endereço de origem deve corresponder ao endereço especificado anteriormente no campo **Caminho** quando você configurou a cópia do pacote de atualização para a pasta compartilhada (consulte as instruções acima).

10. Clique **OK**.

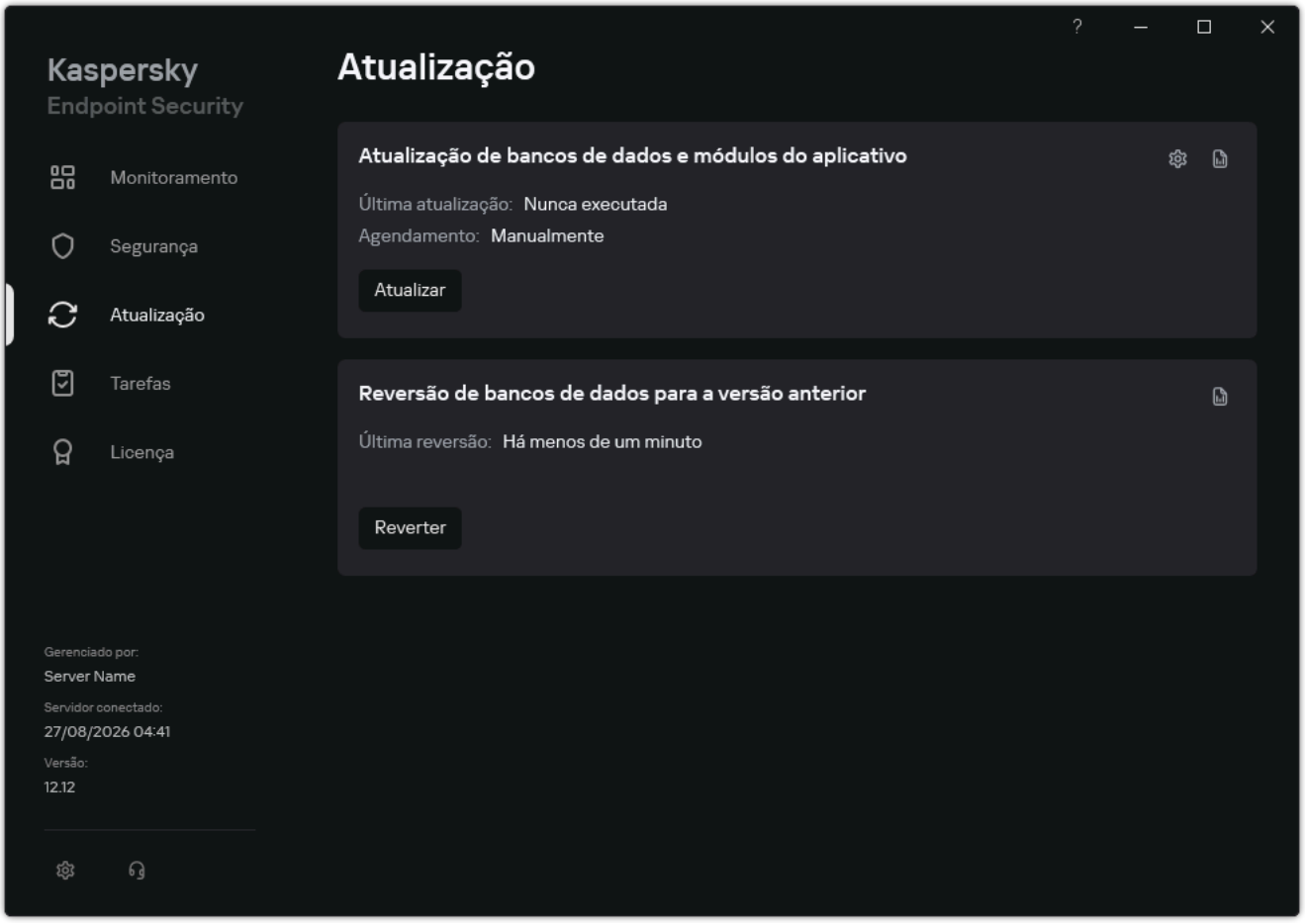
11. Configure as prioridades das fontes de atualizações utilizando os botões **Mover para cima** e **Mover para baixo**.

12. Salvar alterações.

Como configurar atualizações por meio da pasta compartilhada na interface do aplicativo

Não é possível configurar a tarefa de grupo *Atualização de bancos de dados e módulos do aplicativo* na interface do aplicativo. Apenas uma tarefa de atualização local, *Atualização de bancos de dados e módulos do aplicativo*, está disponível para o usuário. Caso a tarefa *Atualização de bancos de dados e módulos do aplicativo* não seja exibida, significa que o administrador proibiu o uso de tarefas locais na política.

1. Na janela principal do aplicativo, acesse a seção **Atualização**.



Tarefas de atualização local

2. A lista de tarefas é aberta; selecione a tarefa *Atualização de bancos de dados e módulos do aplicativo* e clique em ⚙.

   A janela de propriedades da tarefa é exibida.

3. Clique **Selecionar fontes de atualização**.

4. Na janela que é aberta, clique no botão **Adicionar**.

5. Na janela exibida, insira o caminho para a pasta compartilhada.

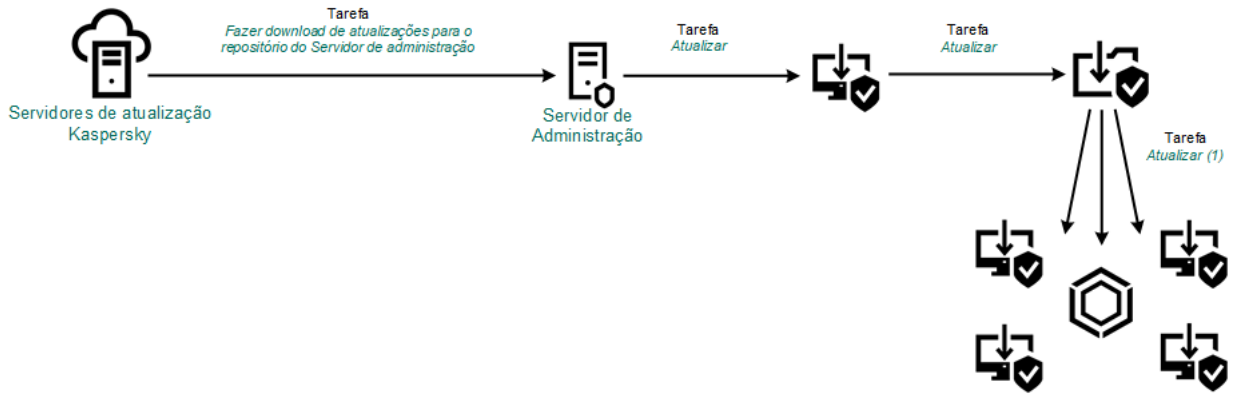
   O endereço de origem deve corresponder ao endereço especificado anteriormente, quando você configurou a cópia do pacote de atualização para a pasta compartilhada (consulte as instruções acima).

6. Clique **Selecionar**.

7. Configure as prioridades das fontes de atualizações utilizando os botões **Acima** e **Abaixo**.

   Se uma atualização não puder ser realizada a partir da primeira fonte de atualização, o Kaspersky Endpoint Security passará automaticamente para a próxima fonte.

8. Salvar alterações.



Atualizar a partir de uma pasta compartilhada

Atualizar utilizando o Kaspersky Update Utility

Para conservar o tráfego de Internet, você pode configurar atualizações de bancos de dados e módulos do aplicativo em computadores da rede local da organização a partir de uma pasta compartilhada usando o utilizando o Kaspersky Update Utility. Para isso, um dos computadores na rede local da organização deve receber pacotes de atualização do Servidor de Administração do Kaspersky Security Center ou dos servidores de atualização da Kaspersky e, em seguida, copiar os pacotes de atualização recebidos para a pasta compartilhada usando o utilitário. Outros computadores na rede local da organização poderão receber o pacote de atualização desta pasta compartilhada.

A versão e localização do aplicativo Kaspersky Endpoint Security que copia o pacote de atualização para uma pasta compartilhada deve corresponder à versão e localização do aplicativo que atualiza os bancos de dados a partir da pasta compartilhada. Se as versões ou localizações dos aplicativos não forem correspondentes, a atualização do banco de dados pode terminar com um erro.

A configuração de atualizações do banco de dados e do módulo do aplicativo a partir de uma pasta compartilhada consiste nas seguintes etapas:

1. Configuração das atualizações do módulo do aplicativo e banco de dados a partir de um repositório de servidor.

2. Instale o Kaspersky Update Utility em um dos computadores da rede local da organização.

3. Configure a cópia do pacote de atualização na pasta compartilhada nas configurações do Kaspersky Update Utility.

   Você fazer o download do pacote de distribuição do Kaspersky Update Utility a partir do Site de suporte técnico da Kaspersky. Após instalar o utilitário, selecione a fonte de atualização (por exemplo, o repositório do Servidor de Administração) e a pasta compartilhada para a qual o Kaspersky Update Utility copiará os pacotes de atualização. Para obter informações detalhadas sobre o uso do Kaspersky Update Utility, consulte a Base de Conhecimento Kaspersky.

4. Configure atualizações do banco de dados e do módulo do aplicativo a partir da pasta compartilhada especificada para os computadores restantes na rede local da organização.

Como configurar atualizações por meio da pasta compartilhada no Console de Administração (MMC)

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

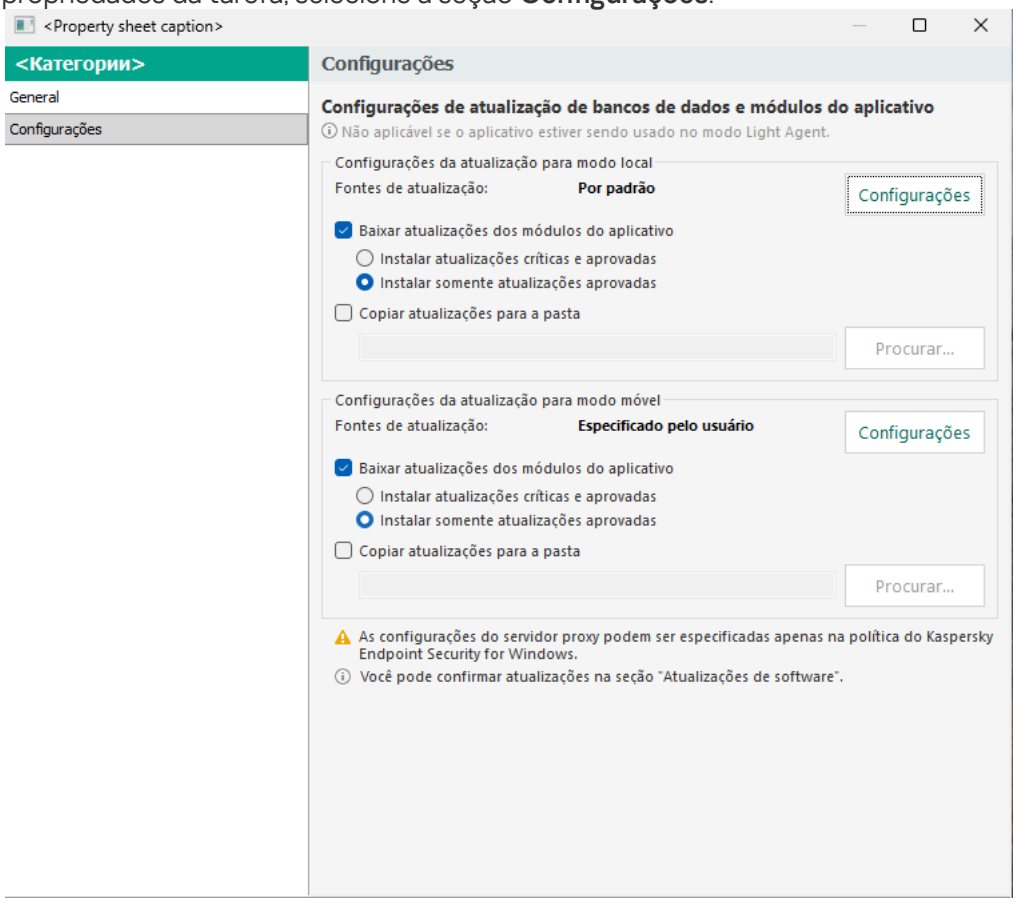
2. Na árvore do console, selecione **Tarefas**.

3. Clique na tarefa **Atualização de bancos de dados e módulos do aplicativo** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

   A tarefa *Atualização de bancos de dados e módulos do aplicativo* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização de bancos de dados e módulos do aplicativo*, instale o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows enquanto executa o assistente.

4. Na janela de propriedades da tarefa, selecione a seção **Configurações**.



Configurações da tarefa Atualização de bancos de dados e módulos do aplicativo

5. No bloco **Configurações da atualização para modo local**, clique no botão **Configurações**.

6. Na lista de fontes de atualizações, clique no botão **Adicionar**.

7. Na janela aberta, digite o caminho UNC para a pasta compartilhada (por exemplo, `\\<server name>\KLSHARE\Updates`).

   O endereço de origem deve corresponder ao endereço indicado nas configurações do Kaspersky Update Utility.

8. Clique **OK**.

9. Configure as prioridades das fontes de atualizações utilizando os botões **Para cima** e **Para baixo**.

   Se uma atualização não puder ser realizada a partir da primeira fonte de atualização, o Kaspersky Endpoint Security passará automaticamente para a próxima fonte.

10. Salvar alterações.

Como configurar atualizações pela pasta compartilhada no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **Tarefas**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Atualização** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

   A tarefa *Atualização* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização*, instale o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows enquanto executa o assistente.

3. Selecione a guia **Configurações do aplicativo** → **Modo local**.

4. Na lista de fontes de atualizações, clique no botão **Adicionar**.

5. Na janela aberta, digite o caminho UNC para a pasta compartilhada (por exemplo, `\\<server name>\KLSHARE\Updates`).

   O endereço de origem deve corresponder ao endereço indicado nas configurações do Kaspersky Update Utility.

6. Clique **OK**.

7. Configure as prioridades das fontes de atualizações utilizando os botões **Para cima** e **Para baixo**.

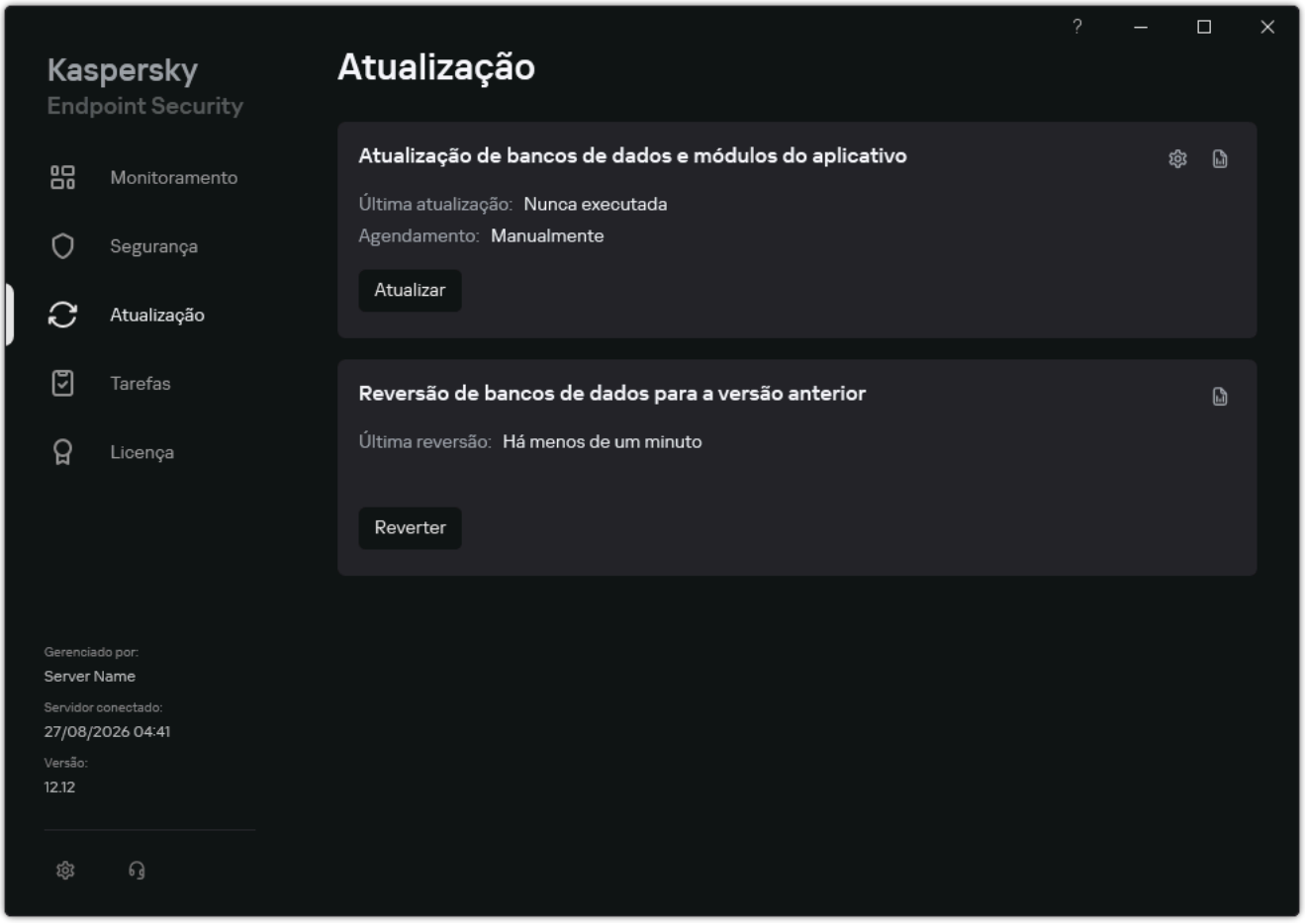
   Se uma atualização não puder ser realizada a partir da primeira fonte de atualização, o Kaspersky Endpoint Security passará automaticamente para a próxima fonte.

8. Salvar alterações.

Como configurar atualizações por meio da pasta compartilhada na interface do aplicativo

Não é possível configurar a tarefa de grupo *Atualização de bancos de dados e módulos do aplicativo* na interface do aplicativo. Apenas uma tarefa de atualização local, *Atualização de bancos de dados e módulos do aplicativo*, está disponível para o usuário. Caso a tarefa *Atualização de bancos de dados e módulos do aplicativo* não seja exibida, significa que o administrador proibiu o uso de tarefas locais na política.

1. Na janela principal do aplicativo, acesse a seção **Atualização**.



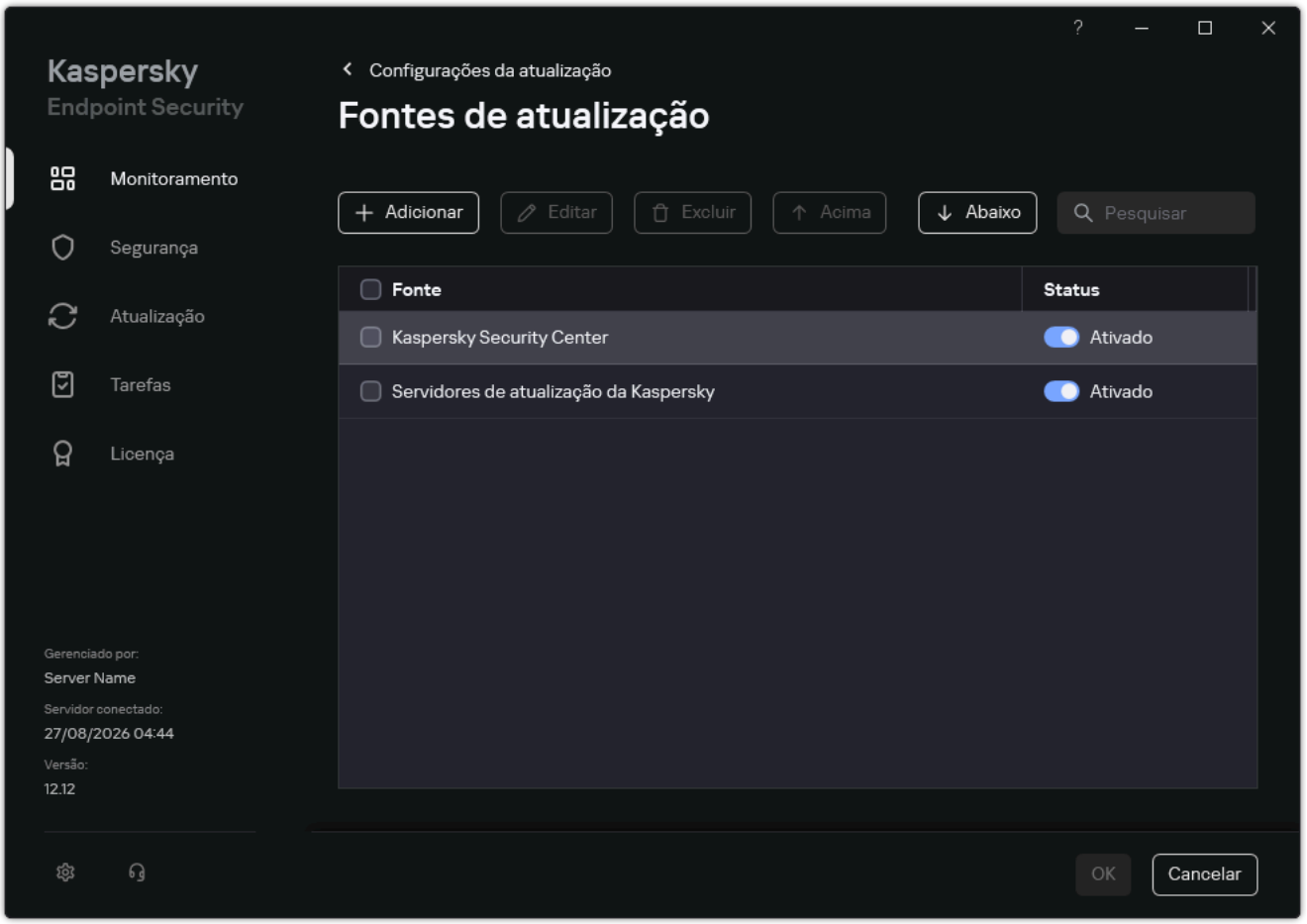
Tarefas de atualização local

2. A lista de tarefas é aberta; selecione a tarefa *Atualização de bancos de dados e módulos do aplicativo* e clique em ⚙.

   A janela de propriedades da tarefa é exibida.

3. Na janela de propriedades da tarefa. Clique em **Selecionar fontes de atualização**.

4. Na lista de fontes de atualizações, clique no botão **Adicionar**.



Fontes de atualizações

5. Digite o caminho UNC para a pasta compartilhada (por exemplo, `\\<server name>\KLSHARE\Updates`).

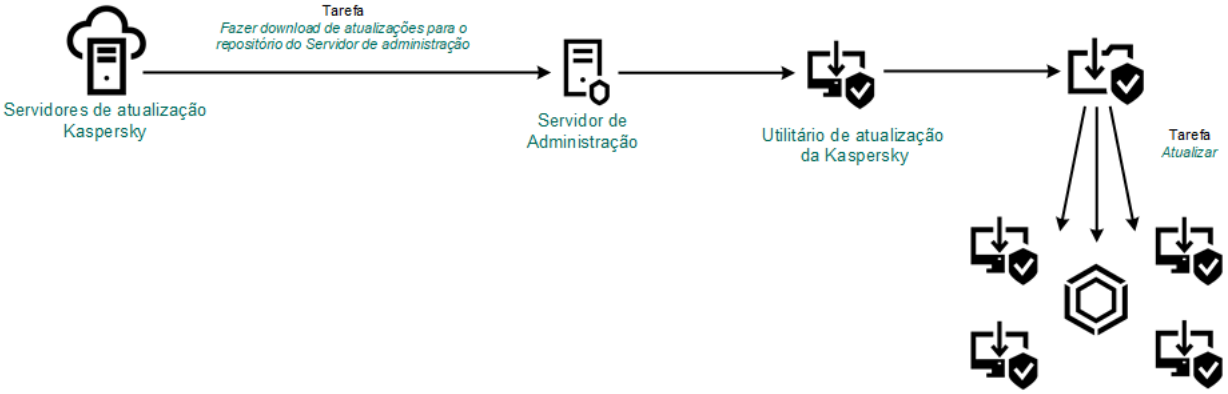
> O endereço de origem deve corresponder ao endereço indicado nas configurações do Kaspersky Update Utility.

6. Clique **Selecionar**.

7. Configure as prioridades das fontes de atualizações utilizando os botões **Acima** e **Abaixo**.

   Se uma atualização não puder ser realizada a partir da primeira fonte de atualização, o Kaspersky Endpoint Security passará automaticamente para a próxima fonte.

8. Salvar alterações.



Atualizar utilizando o Kaspersky Update Utility

Atualizar no modo móvel

O *modo móvel* é o modo de operação do Kaspersky Endpoint Security, quando um computador sai do perímetro da rede da organização (*computador off-line*). Para obter mais detalhes sobre como trabalhar com computadores offline e usuários ausentes, consulte a Ajuda do Kaspersky Security Center.

Um computador off-line fora da rede da organização não pode se conectar ao Servidor de Administração para atualizar bancos de dados e módulos do aplicativo. Por padrão, somente os servidores de atualização da Kaspersky são usadoscomo fonte de atualizações para atualizar bancos de dados e módulos do aplicativo no modo móvel. O uso de um servidor proxy para se conectar à Internet é determinado por uma política de ausência especial. A política de ausência deve ser criada separadamente. Quando o Kaspersky Endpoint Security é colocado no modo móvel, a tarefa de atualização é iniciada a cada duas horas.

Como definir as configurações de atualização para o modo móvel no Console de administração (MMC)

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

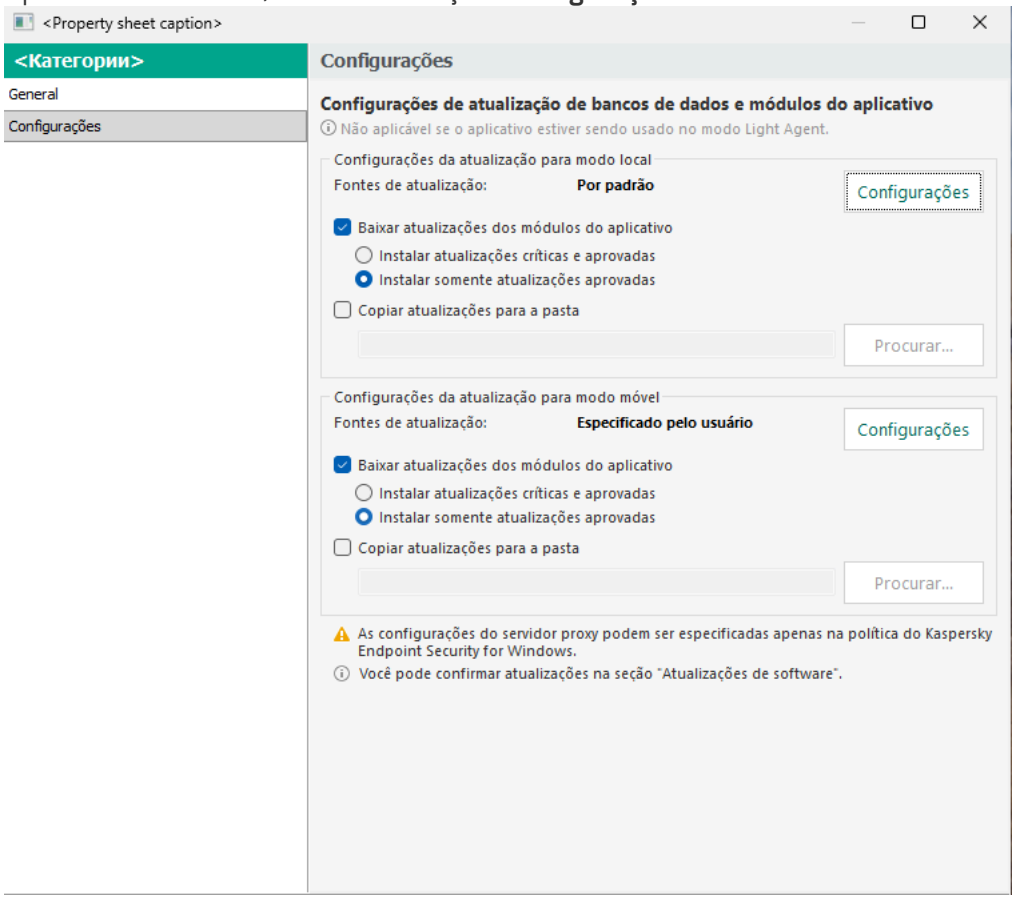
2. Na árvore do console, selecione **Tarefas**.

3. Clique na tarefa **Atualização de bancos de dados e módulos do aplicativo** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

   A tarefa *Atualização de bancos de dados e módulos do aplicativo* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização de bancos de dados e módulos do aplicativo*, instale o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows enquanto executa o assistente.

4. Na janela de propriedades da tarefa, selecione a seção **Configurações**.



Configurações da tarefa Atualização de bancos de dados e módulos do aplicativo

5. No bloco **Configurações da atualização para modo móvel**, clique no botão **Configurações**.

6. Configure as fontes de atualizações. As fontes de atualizações podem ser servidores de atualização da Kaspersky, outros servidores FTP e HTTP, pastas locais ou pastas de rede.

7. Salvar alterações.

Como definir as configurações de atualização para o modo móvel no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **Tarefas**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Atualização** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

   A tarefa *Atualização* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização*, instale o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows enquanto executa o assistente.

3. Selecione a guia **Configurações do aplicativo** → **Modo móvel**.

4. Configure as fontes de atualizações. As fontes de atualizações podem ser servidores de atualização da Kaspersky, outros servidores FTP e HTTP, pastas locais ou pastas de rede.

5. Salvar alterações.

Como resultado, os bancos de dados e os módulos do aplicativo serão atualizados nos computadores dos usuários quando eles alternarem para o modo móvel.

Iniciar e interromper a tarefa de atualização

Seja qual for o modo de execução da tarefa de atualização, você pode iniciar ou interromper a tarefa de atualização do Kaspersky Endpoint Security a qualquer momento.

Para iniciar ou interromper a tarefa de atualização:

1. Na janela principal do aplicativo, acesse a seção **Atualização**.

2. No bloco **Atualização de bancos de dados e módulos do aplicativo**, clique no botão **Atualizar** se quiser iniciar a tarefa de atualização.

O Kaspersky Endpoint Security começará a atualizar os módulos e bancos de dados do aplicativo. O aplicativo exibirá o progresso da tarefa, o tamanho dos arquivos baixados e a fonte de atualização. É possível interromper a tarefa a qualquer momento clicando no botão **Parar a atualização**.

Para iniciar ou interromper a tarefa de atualização quando a interface de aplicativo simplificada é exibida:

1. Clique com o botão direito do mouse para abrir o ícone do menu de contexto do aplicativo que está na área de notificação da barra de tarefas.

2. Na lista suspensa **Tarefas** no menu de contexto, realize um dos seguintes procedimentos:

   - selecione uma tarefa de atualização que não esteja em execução para iniciá-la

   - selecione uma tarefa de atualização em execução para interrompê-la

   - selecione uma tarefa de atualização pausada para retomá-la ou reiniciá-la

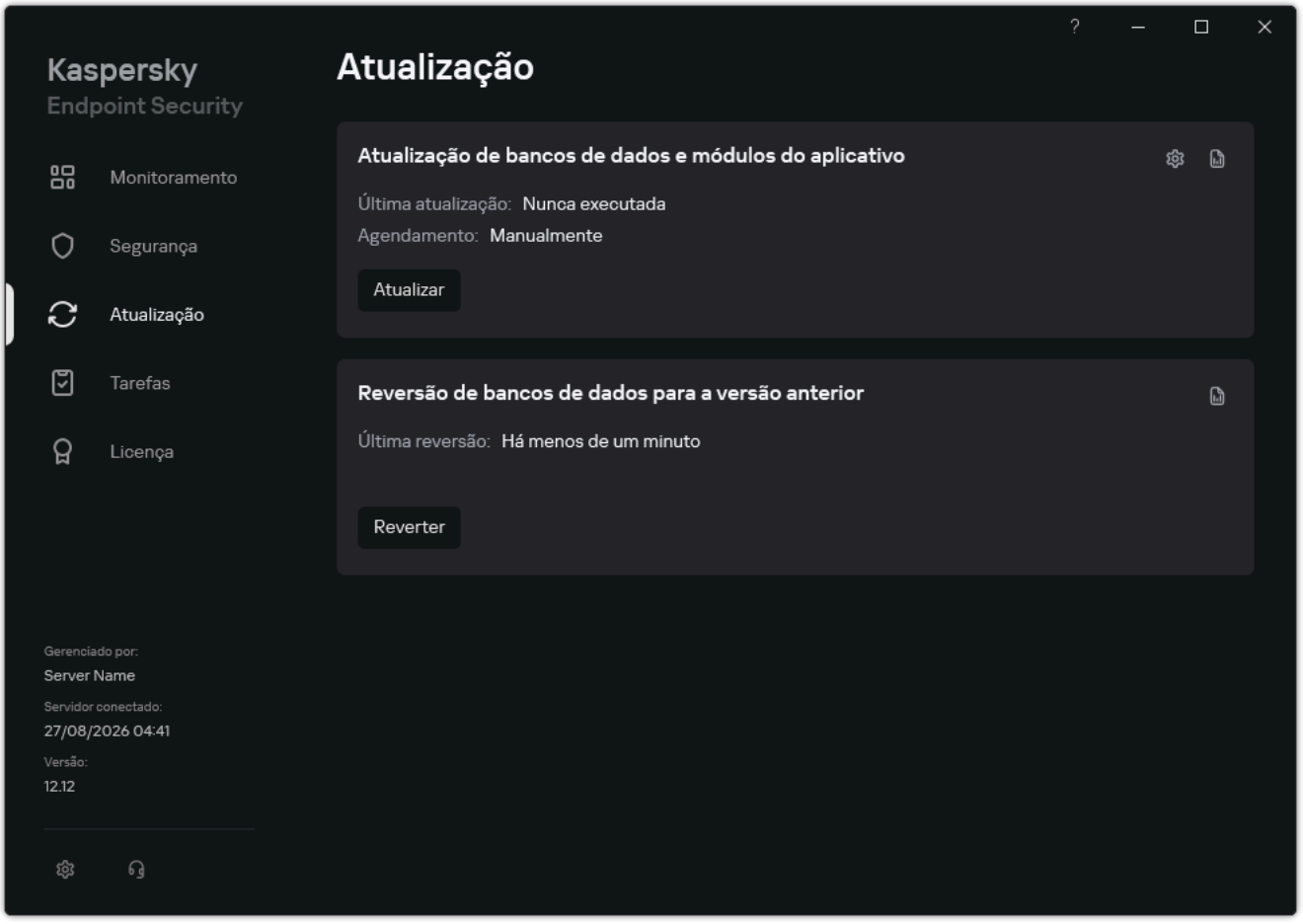
Executar a tarefa de atualização usando os direitos de uma conta de usuário diferente

Por padrão, a tarefa de atualização do Kaspersky Endpoint Security é executada em nome da conta de usuário usada para fazer login no sistema operacional. No entanto, o Kaspersky Endpoint Security pode ser atualizado a partir de uma fonte de atualização que o usuário não pode acessar devido à falta de direitos necessários (por exemplo, de uma pasta compartilhada que contém um pacote de atualização) ou uma fonte de atualização para a qual a autenticação do servidor proxy não está configurada. Nas configurações do aplicativo, especifique o usuário com os direitos necessários e execute a tarefa de atualização do aplicativo usando esta conta de usuário.

Para executar a tarefa de atualização com uma conta de usuário diferente:

Não é possível configurar a tarefa de grupo *Atualização de bancos de dados e módulos do aplicativo* na interface do aplicativo. Apenas uma tarefa de atualização local, *Atualização de bancos de dados e módulos do aplicativo*, está disponível para o usuário. Caso a tarefa *Atualização de bancos de dados e módulos do aplicativo* não seja exibida, significa que o administrador proibiu o uso de tarefas locais na política.

1. Na janela principal do aplicativo, acesse a seção **Atualização**.



Tarefas de atualização local

2. A lista de tarefas é aberta; selecione a tarefa *Atualização de bancos de dados e módulos do aplicativo* e clique em ⚙.

   A janela de propriedades da tarefa é exibida.

3. Clique **Executar atualizações do banco de dados com direitos de usuário**.

4. Na janela aberta, selecione **Outro usuário**.

5. Insira as credenciais da conta de um usuário com as permissões necessárias para acessar a fonte de atualização.

6. Salvar alterações.

Selecionar o modo de execução da tarefa de atualização

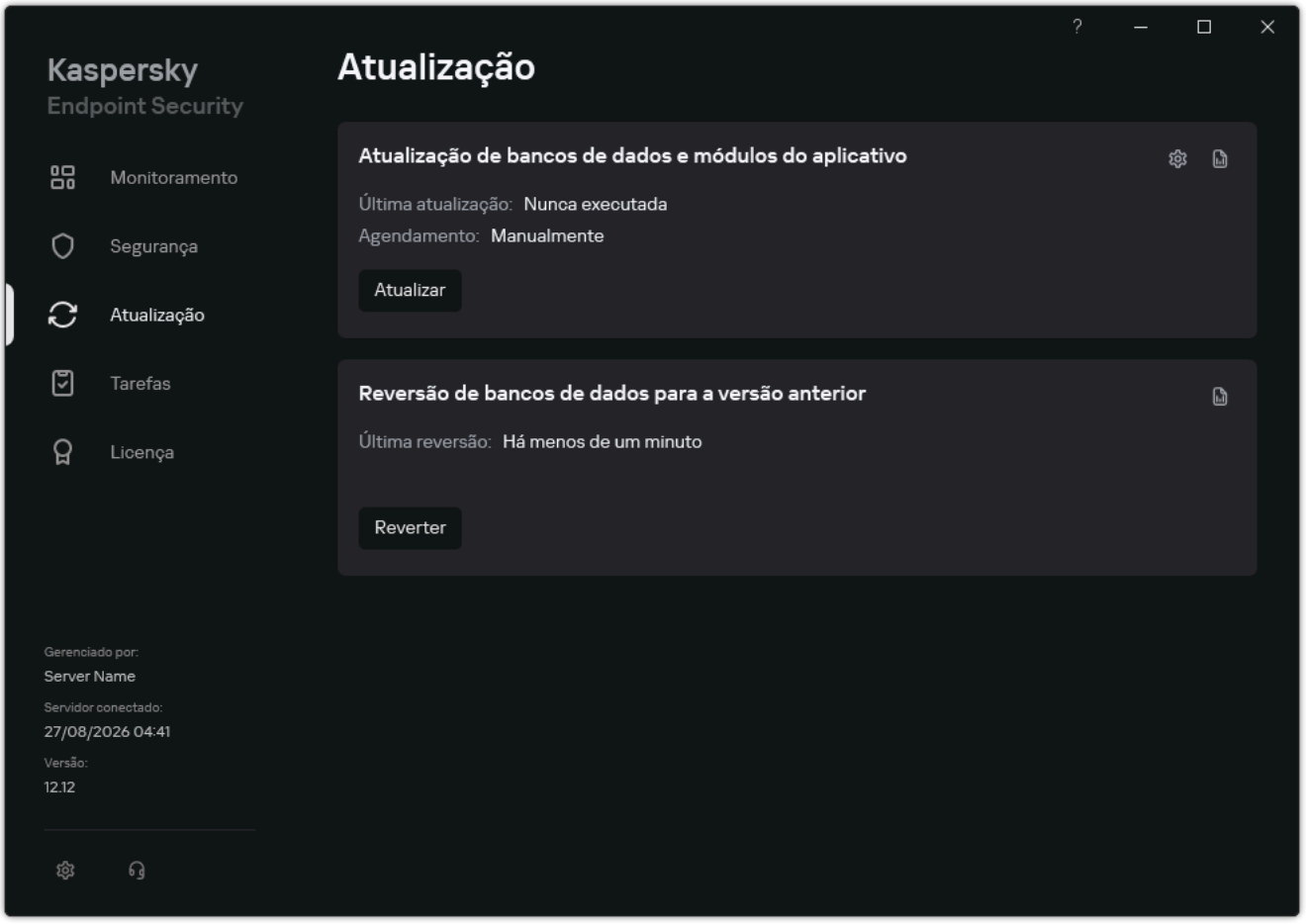
Se não for possível executar a tarefa de atualização por qualquer motivo (por exemplo, o computador não está ligado no momento), você poderá configurar a tarefa ignorada para ser iniciada automaticamente assim que for possível.

Você poderá adiar a execução da tarefa de atualização após o aplicativo iniciar se selecionar o modo de execução da tarefa de atualização **Por agendamento**, e se a hora de início do Kaspersky Endpoint Security corresponder à de início da tarefa de atualização programada. A tarefa de atualização somente pode ser executada após decorrido o intervalo de tempo especificado depois do início do Kaspersky Endpoint Security.

Para selecionar o modo de execução da tarefa de atualização:

Não é possível configurar a tarefa de grupo *Atualização de bancos de dados e módulos do aplicativo* na interface do aplicativo. Apenas uma tarefa de atualização local, *Atualização de bancos de dados e módulos do aplicativo*, está disponível para o usuário. Caso a tarefa *Atualização de bancos de dados e módulos do aplicativo* não seja exibida, significa que o administrador proibiu o uso de tarefas locais na política.

1. Na janela principal do aplicativo, acesse a seção **Atualização**.



Tarefas de atualização local

2. A lista de tarefas é aberta; selecione a tarefa *Atualização de bancos de dados e módulos do aplicativo* e clique em ⚙.

   A janela de propriedades da tarefa é exibida.

3. Clique **Modo de execução**.

4. Na janela que é aberta, selecione o modo de execução da tarefa de atualização:

   - Para o Kaspersky Endpoint Security executar a tarefa de atualização de acordo com a disponibilidade do pacote de atualização na fonte de atualização, selecione **Automaticamente**. A frequência das verificações de pacotes de atualização pelo Kaspersky Endpoint Security aumenta quando há surtos de vírus e diminui quando estes não existem.

   - Se desejar executar a tarefa de atualização manualmente, selecione **Manualmente**.

   - Caso queira configurar um horário para iniciar a tarefa de atualização, selecione outras opções. Defina as configurações avançadas para iniciar a tarefa de atualização:

     - No campo **Adiar a execução após a inicialização do aplicativo em N minutos**, insira o intervalo de tempo pelo qual deseja adiar o início da tarefa de atualização após a inicialização do Kaspersky Endpoint Security.

     - Selecione **Executar a verificação agendada no dia seguinte se o computador estiver desligado** caso queira que o Kaspersky Endpoint Security execute as tarefas de atualização perdidas na primeira oportunidade. Quando o aplicativo tem a oportunidade de executar tarefas perdidas, ele executa as tarefas aleatoriamente dentro de um determinado intervalo de tempo para distribuir a carga no computador.

5. Salvar alterações.

Adicionar uma fonte de atualização

A *fonte de atualização* é um recurso que contém as atualizações dos bancos de dados e dos módulos do aplicativo do Kaspersky Internet Security.

As fontes de atualização incluem o servidor do Kaspersky Security Center, servidores de atualização da Kaspersky e pastas de rede ou locais.

> Caso os servidores de atualização da Kaspersky não estejam disponíveis, o Kaspersky Endpoint Security poderá usar domínios alternativos para atualizar os bancos de dados e módulos do software do aplicativo. Para obter informações detalhadas, consulte a Base de Conhecimento do Suporte Técnico.

A lista padrão de fontes de atualização inclui os servidores de atualização do Kaspersky Security Center e da Kaspersky. É possível adicionar outras fontes de atualização à lista. Você pode especificar servidores FTP ou HTTP e pastas compartilhadas como fontes de atualização.

> O Kaspersky Endpoint Security não oferece suporte as atualizações de servidores HTTPS, a menos que sejam servidores de atualização da Kaspersky.

Se vários recursos forem selecionados como fontes de atualização, o Kaspersky Endpoint Security tentará se conectar a cada um deles, começando pelo primeiro na lista, e executará a tarefa de atualização fazendo a recuperação do pacote de atualização da primeira fonte disponível.

Por padrão, o Kaspersky Endpoint Security usa o servidor do Kaspersky Security Center como a primeira fonte de atualização. Isso ajuda a conservar o tráfego durante a atualização. Se uma política não for aplicada ao computador, os servidores da Kaspersky serão selecionados como a primeira fonte de atualização nas configurações da tarefa de *Atualização de bancos de dados e módulos do aplicativo* local, pois o aplicativo pode não ter acesso ao servidor do Kaspersky Security Center.

Se o aplicativo estiver em execução no modo Light Agent, uma pasta no SVM será selecionada como a fonte de atualização.

Como adicionar uma fonte de atualização no Console de administração (MMC)

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

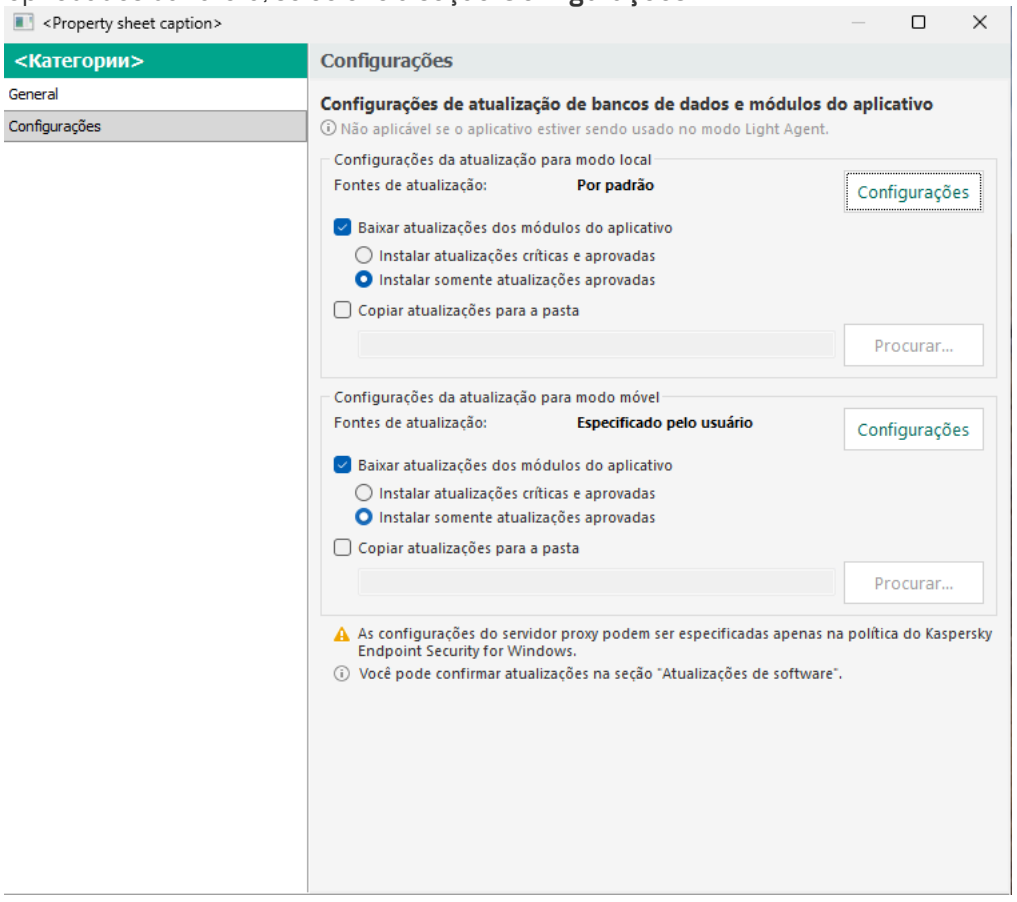
   Na árvore do console, selecione **Tarefas**.

2. Clique na tarefa **Atualização de bancos de dados e módulos do aplicativo** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

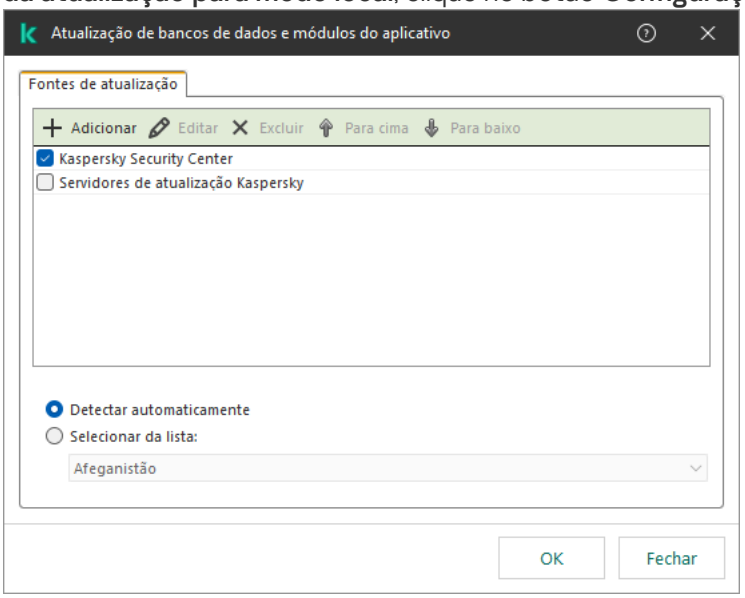
   A tarefa *Atualização de bancos de dados e módulos do aplicativo* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização de bancos de dados e módulos do aplicativo*, instale o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows enquanto executa o assistente.

3. Na janela de propriedades da tarefa, selecione a seção **Configurações**.



Configurações da tarefa Atualização de bancos de dados e módulos do aplicativo

4. No bloco **Configurações da atualização para modo local**, clique no botão **Configurações**.



Fontes de atualizações

5. Na lista de fontes de atualizações, clique no botão **Adicionar**.

6. No campo **Fontes de atualização**, especifique o endereço do servidor FTP ou HTTP, a pasta de rede ou pasta local que contém o pacote de atualização.

   O seguinte formato de caminho é usado para a fonte de atualização:

   - Para um servidor FTP ou HTTP, insira o endereço web ou endereço IP.

     Por exemplo, `http://dnl-01.geo.kaspersky.com/` ou `93.191.13.103`.

     Para um servidor FTP, você pode especificar as configurações de autenticação no endereço no seguinte formato: `ftp://<user name>:<password>@<node>:<port>`.

   - Para uma pasta de rede, digite o caminho UNC.

     Por exemplo, `\\Server\Share\Update distribution`.

   - Para uma pasta local, insira o caminho completo para a pasta.

     Por exemplo, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

   É possível excluir a fonte de atualização sem removê-la da lista de fontes de atualização. Para fazer isso, desmarque a caixa de seleção ao lado do objeto.

7. Clique **OK**.

8. Configure as prioridades das fontes de atualizações utilizando os botões **Para cima** e **Para baixo**.

   Se uma atualização não puder ser realizada a partir da primeira fonte de atualização, o Kaspersky Endpoint Security passará automaticamente para a próxima fonte.

9. Se necessário, adicione uma fonte de atualização para o modo móvel. O *modo móvel* é o modo de operação do Kaspersky Endpoint Security, quando um computador sai do perímetro da rede da organização (*computador off-line*).

10. Salvar alterações.

Como adicionar uma fonte de atualização na Web Console

1. Na janela principal do Web Console, selecione **Tarefas**.

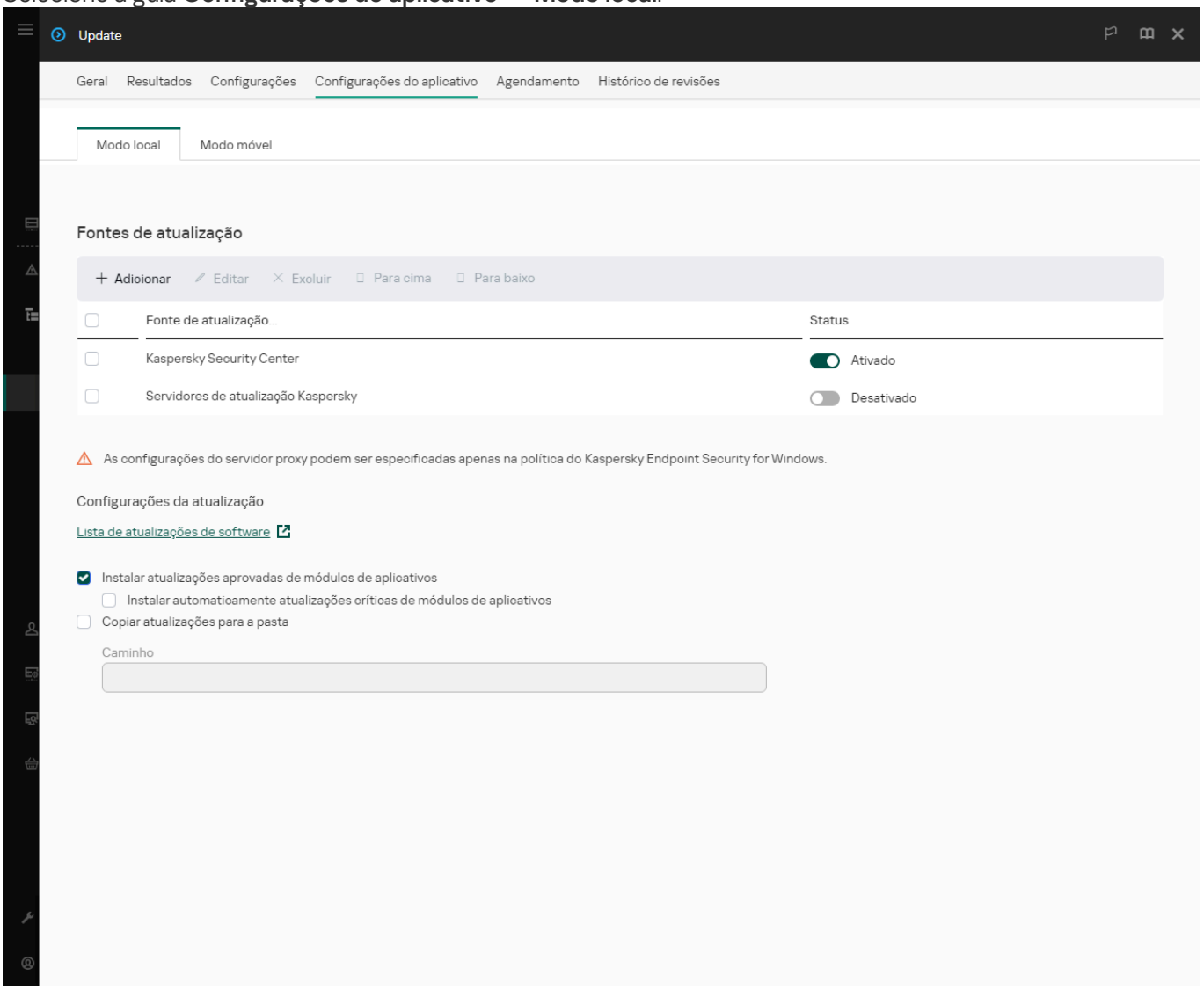
   A lista de tarefas é aberta.

2. Clique na tarefa **Atualização** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

   A tarefa *Atualização* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização*, instale o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows enquanto executa o assistente.

3. Selecione a guia **Configurações do aplicativo** → **Modo local**.



Fontes de atualizações

4. Na lista de fontes de atualizações, clique no botão **Adicionar**.

5. Na janela exibida, especifique o endereço do servidor FTP ou HTTP, a pasta de rede ou pasta local que contém o pacote de atualização.

   O seguinte formato de caminho é usado para a fonte de atualização:

   - Para um servidor FTP ou HTTP, insira o endereço web ou endereço IP.

     Por exemplo, `http://dnl-01.geo.kaspersky.com/` ou `93.191.13.103`.

Para um servidor FTP, você pode especificar as configurações de autenticação no endereço no seguinte formato: `ftp://<user name>:<password>@<node>:<port>`.

- Para uma pasta de rede, digite o caminho UNC.

  Por exemplo, `\\Server\Share\Update distribution`.

- Para uma pasta local, insira o caminho completo para a pasta.

  Por exemplo, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

É possível excluir a fonte de atualização sem removê-la da lista de fontes de atualização. Para fazer isso, coloque a chave de alternância ao lado na posição desativada.

6. Clique **OK**.

7. Configure as prioridades das fontes de atualizações utilizando os botões **Mover para cima** e **Mover para baixo**.

   Se uma atualização não puder ser realizada a partir da primeira fonte de atualização, o Kaspersky Endpoint Security passará automaticamente para a próxima fonte.

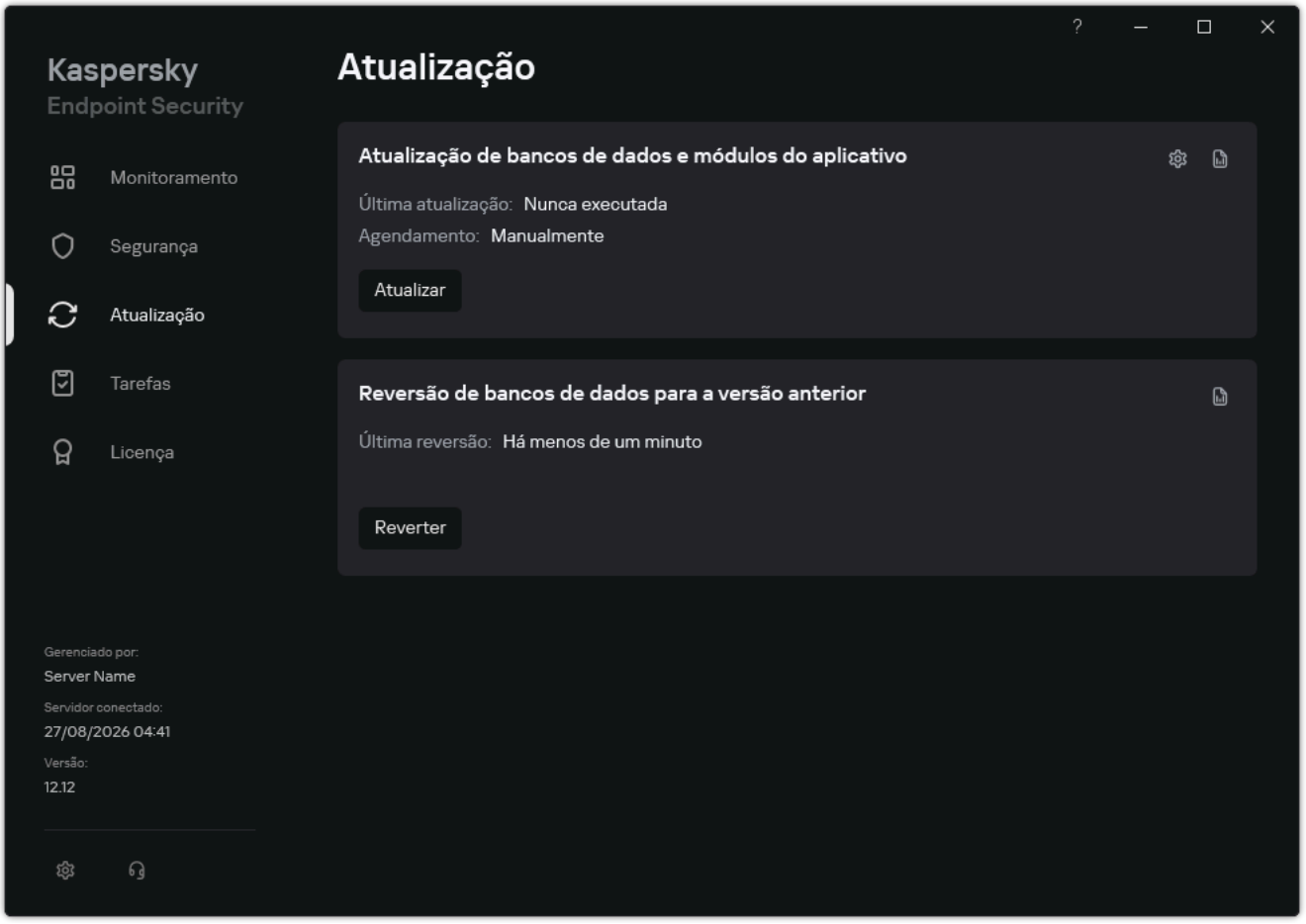
8. Se necessário, adicione uma fonte de atualização para o modo móvel. O *modo móvel* é o modo de operação do Kaspersky Endpoint Security, quando um computador sai do perímetro da rede da organização (*computador off-line*).

9. Salvar alterações.

Como adicionar uma fonte de atualização na interface do aplicativo

Não é possível configurar a tarefa de grupo *Atualização de bancos de dados e módulos do aplicativo* na interface do aplicativo. Apenas uma tarefa de atualização local, *Atualização de bancos de dados e módulos do aplicativo*, está disponível para o usuário. Caso a tarefa *Atualização de bancos de dados e módulos do aplicativo* não seja exibida, significa que o administrador proibiu o uso de tarefas locais na política.

1. Na janela principal do aplicativo, acesse a seção **Atualização**.



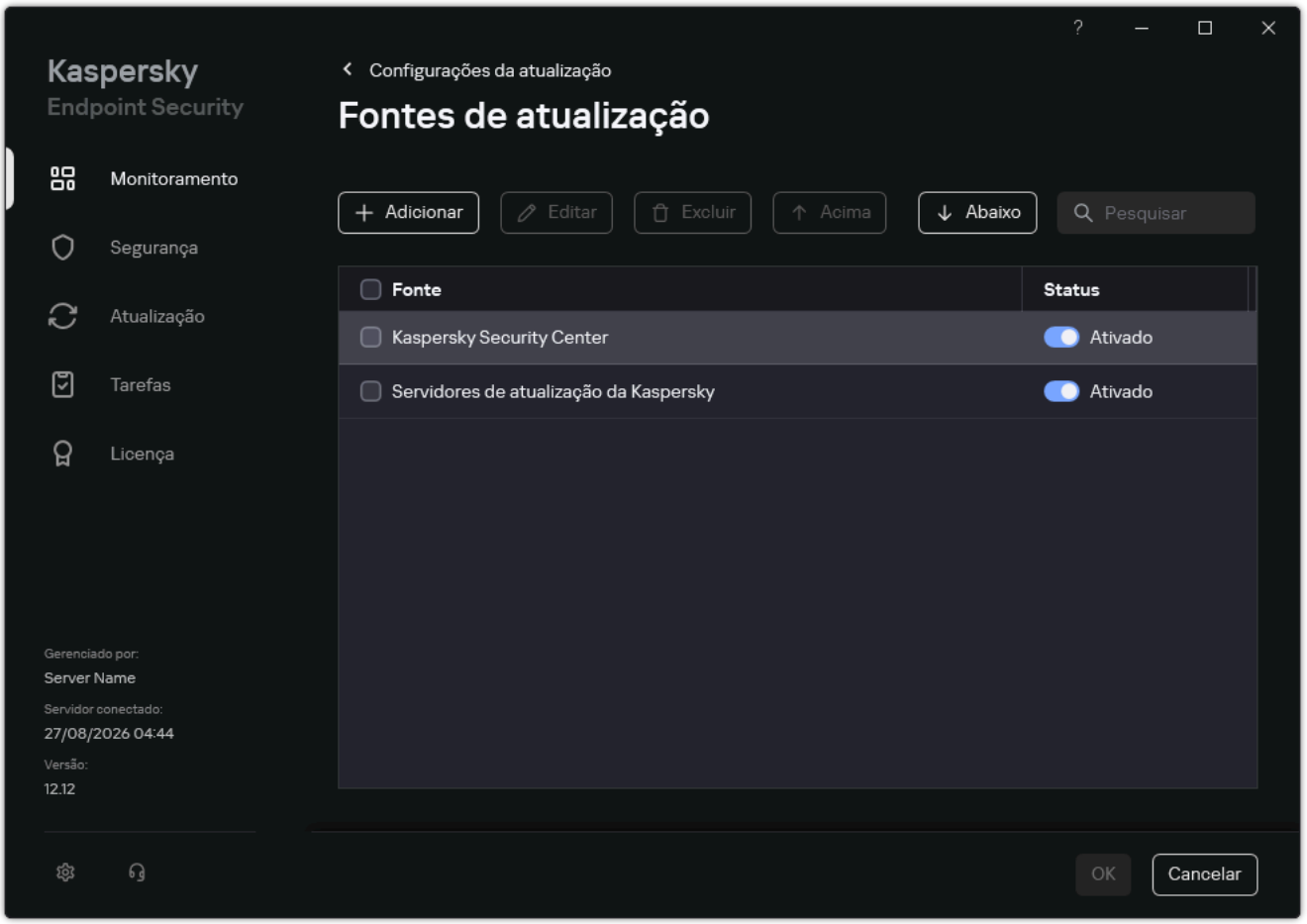
Tarefas de atualização local

2. A lista de tarefas é aberta; selecione a tarefa *Atualização de bancos de dados e módulos do aplicativo* e clique em ⚙.

   A janela de propriedades da tarefa é exibida.

3. Clique **Selecionar fontes de atualização**.

4. Na janela que é aberta, clique no botão **Adicionar**.



Fontes de atualizações

5. Na janela exibida, especifique o endereço do servidor FTP ou HTTP, a pasta de rede ou pasta local que contém o pacote de atualização.

   O seguinte formato de caminho é usado para a fonte de atualização:

   - Para um servidor FTP ou HTTP, insira o endereço web ou endereço IP.

     Por exemplo, `http://dnl-01.geo.kaspersky.com/` ou `93.191.13.103`.

     Para um servidor FTP, você pode especificar as configurações de autenticação no endereço no seguinte formato: `ftp://<user name>:<password>@<node>:<port>`.

   - Para uma pasta de rede, digite o caminho UNC.

     Por exemplo, `\\Server\Share\Update distribution`.

   - Para uma pasta local, insira o caminho completo para a pasta.

     Por exemplo, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

6. Clique **Selecionar**.

7. Configure as prioridades das fontes de atualizações utilizando os botões **Acima** e **Abaixo**.

8. Salvar alterações.

Atualização dos módulos do aplicativo

As atualizações dos módulos do aplicativo corrigem erros, melhoram o desempenho e adicionam novos recursos. Quando uma nova atualização dos módulos do aplicativo estiver disponível, você precisará confirmar a instalação da atualização. Você pode confirmar a instalação de uma atualização do módulo do aplicativo na interface do aplicativo ou no Kaspersky Security Center. Sempre que uma atualização estiver disponível, o aplicativo exibe uma notificação na janela principal do Kaspersky Endpoint Security: . 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.

Depois de instalar uma atualização do aplicativo, pode ser necessário reiniciar o computador.

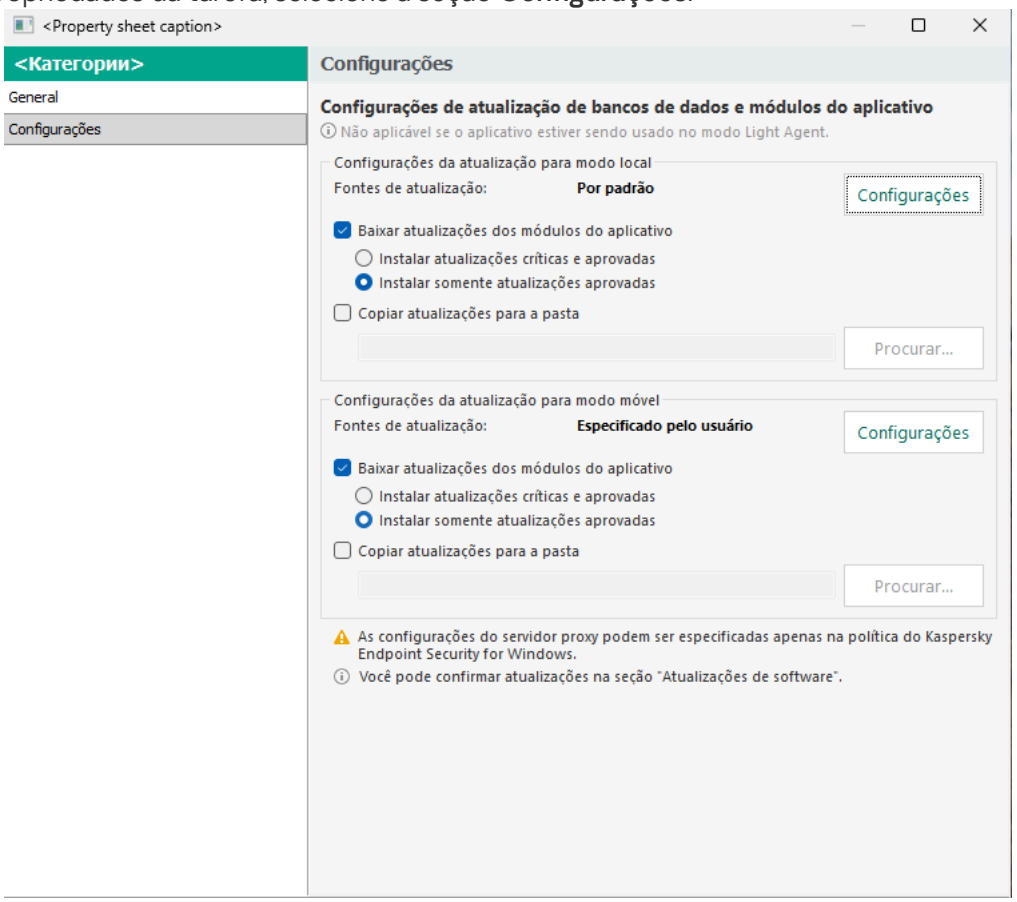
Como configurar as atualizações do módulo do aplicativo no Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Tarefas**.
3. Clique na tarefa **Atualização de bancos de dados e módulos do aplicativo** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

   A tarefa *Atualização de bancos de dados e módulos do aplicativo* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização de bancos de dados e módulos do aplicativo*, instale o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows enquanto executa o assistente.

4. Na janela de propriedades da tarefa, selecione a seção **Configurações**.



Configurações da tarefa Atualização de bancos de dados e módulos do aplicativo

5. No bloco **Configurações da atualização para modo local**, marque a caixa de seleção **Baixar atualizações dos módulos do aplicativo**.

   Se quiser impedir que as atualizações dos módulos do aplicativo sejam baixadas, desmarque a caixa de seleção **Baixar atualizações dos módulos do aplicativo** e proíba o uso de tarefas locais pelo usuário.

6. Selecione as atualizações dos módulos do aplicativo que deseja instalar.

   - **Instalar atualizações críticas e aprovadas**. Se esta opção for selecionada, quando as atualizações do módulo do aplicativo estiverem disponíveis, o Kaspersky Endpoint 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 aprovadas**. Se esta opção for selecionada, quando as atualizações do módulo do aplicativo estiverem disponíveis, o Kaspersky Endpoint 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 está selecionada por padrão.

7. Caso necessário, configure as atualizações do módulo do aplicativo para o modo móvel. O *modo móvel* é o modo de operação do Kaspersky Endpoint Security, quando um computador sai do perímetro da rede da organização (*computador off-line*).

8. Salvar alterações.

Como configurar as atualizações do módulo do aplicativo no Web Console e Cloud Console

1. Na janela principal do Web Console, selecione **Tarefas**.

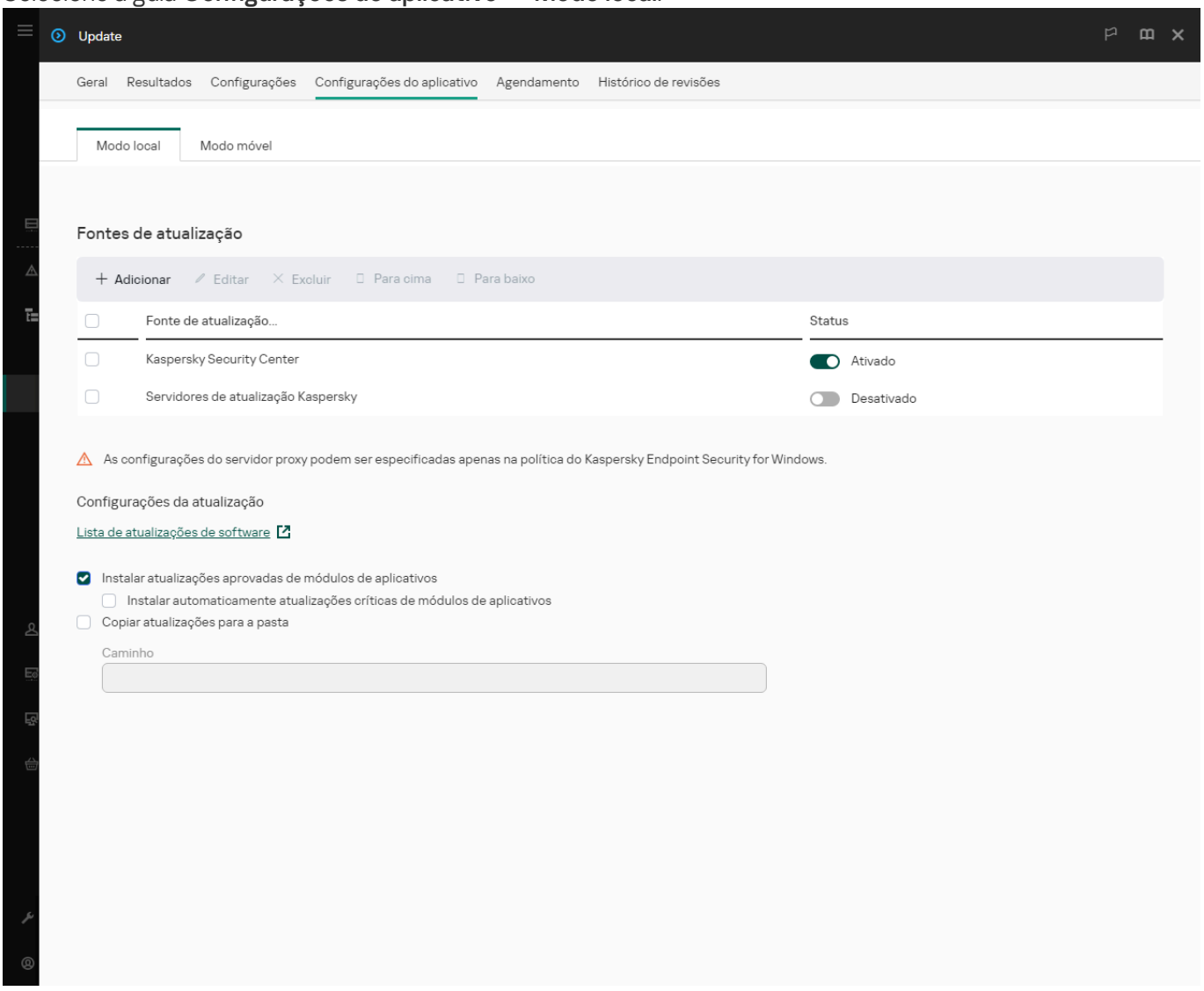
   A lista de tarefas é aberta.

2. Clique na tarefa **Atualização de bancos de dados e módulos do aplicativo** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

   A tarefa *Atualização de bancos de dados e módulos do aplicativo* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização de bancos de dados e módulos do aplicativo*, instale o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows enquanto executa o assistente.

3. Selecione a guia **Configurações do aplicativo** → **Modo local**.



Configurações da tarefa Atualização

4. Em **Configurações da atualização**, selecione as atualizações do módulo do aplicativo que deseja instalar:

   - **Instalar atualizações aprovadas de módulos de aplicativos**. Se esta opção for selecionada, quando as atualizações do módulo do aplicativo estiverem disponíveis, o Kaspersky Endpoint 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 está selecionada por padrão.

   - **Instalar automaticamente atualizações críticas de módulos de aplicativos**. Se esta opção for selecionada, quando as atualizações do módulo do aplicativo estiverem disponíveis, o Kaspersky Endpoint 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.

Se quiser impedir que as atualizações do módulo do aplicativo sejam baixadas, desmarque as caixas de seleção **Instalar atualizações aprovadas de módulos de aplicativos** e **Instalar automaticamente atualizações críticas de módulos de aplicativos** e proíba o uso de tarefas locais pelo usuário.

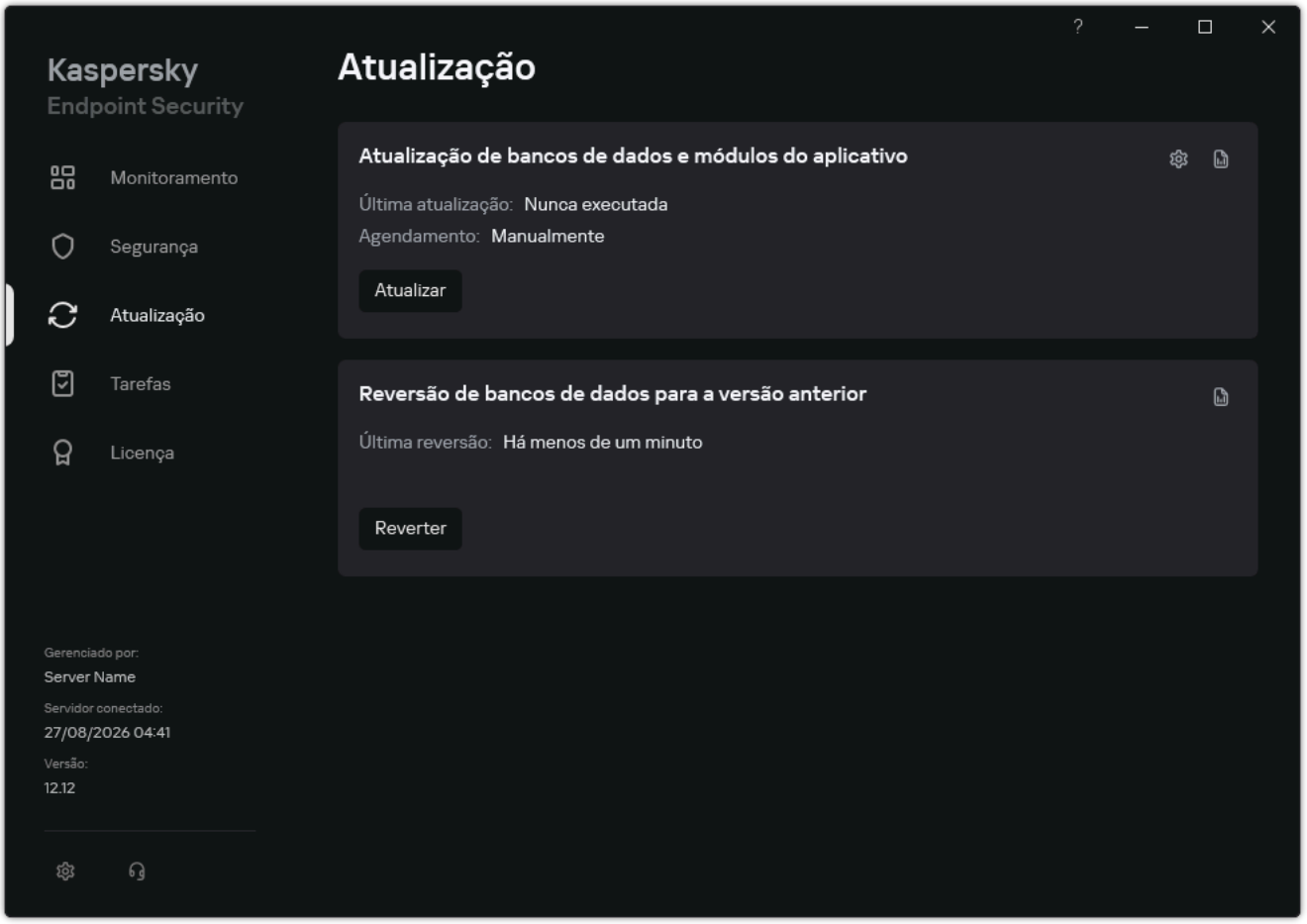
5. Caso necessário, configure as atualizações do módulo do aplicativo para o modo móvel. O *modo móvel* é o modo de operação do Kaspersky Endpoint Security, quando um computador sai do perímetro da rede da organização (*computador off-line*).

6. Salvar alterações.

Como configurar as atualizações do módulo do aplicativo na interface do aplicativo

Não é possível configurar a tarefa de grupo *Atualização de bancos de dados e módulos do aplicativo* na interface do aplicativo. Apenas uma tarefa de atualização local, *Atualização de bancos de dados e módulos do aplicativo*, está disponível para o usuário. Caso a tarefa *Atualização de bancos de dados e módulos do aplicativo* não seja exibida, significa que o administrador proibiu o uso de tarefas locais na política.

1. Na janela principal do aplicativo, acesse a seção **Atualização**.



Tarefas de atualização local

2. A lista de tarefas é aberta; selecione a tarefa *Atualização de bancos de dados e módulos do aplicativo* e clique em ⚙.

   A janela de propriedades da tarefa é exibida.

3. No bloco **Baixar e instalar atualizações dos módulos do aplicativo**, marque a caixa de seleção **Baixar atualizações dos módulos do aplicativo**.

4. 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 Endpoint 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 Endpoint 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 está selecionada por padrão.

5. Salvar alterações.

Usar um servidor proxy para atualizações

Pode ser necessário especificar configurações do servidor proxy para fazer download de atualizações do banco de dados e do módulo do aplicativo a partir da fonte de atualizações. Se houver várias fontes de atualizações, as configurações do servidor proxy serão aplicadas a todas as fontes. Se um servidor proxy não for necessário para algumas fontes de atualizações, você poderá desativar o uso de um servidor proxy nas propriedades da política. O Kaspersky Endpoint Security também usará um servidor proxy para acessar a Kaspersky Security Network e os servidores de ativação.

Para configurar uma conexão para fontes de atualizações por meio de um servidor proxy:

1. Na janela principal do Web Console, clique em ⚙.

   A janela de propriedades do Servidor de Administração é exibida.

2. Ir para a seção **Configurando acesso à internet**.

3. Marque a caixa de seleção **Usar o servidor proxy**.

4. Defina as configurações de conexão do servidor proxy: endereço do servidor proxy, porta e configurações de autenticação (nome de usuário e senha).

5. Salvar alterações.

Para desativar o uso de um servidor proxy para um grupo de administração específico:

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Configurações de rede**.

5. No bloco **Servidor proxy**, clique no botão **Configurações**.

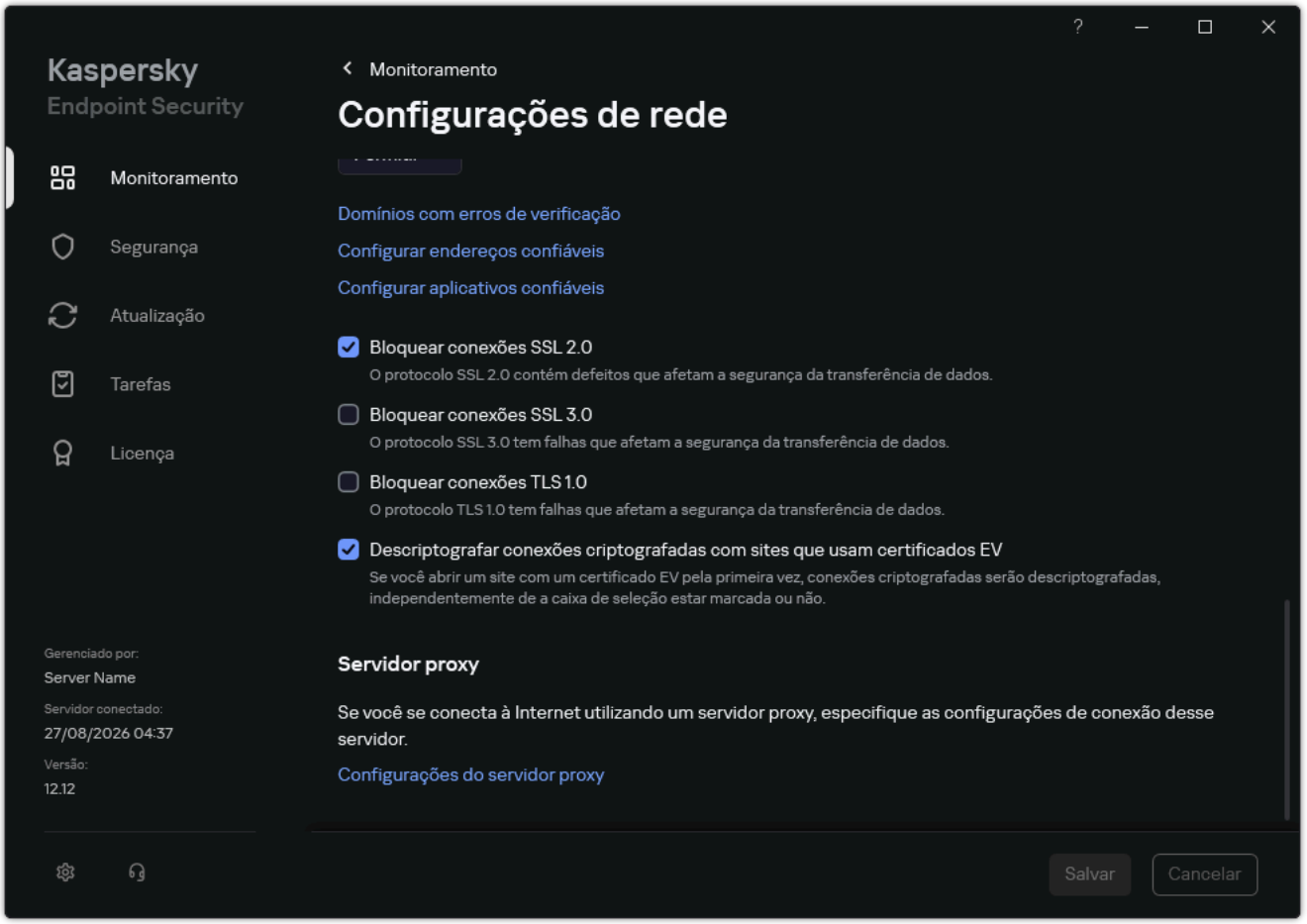
6. Na janela que é aberta, marque a caixa de seleção **Ignorar servidor proxy para endereços locais**.

7. Salvar alterações.

Para definir as configurações do servidor proxy na interface do aplicativo:

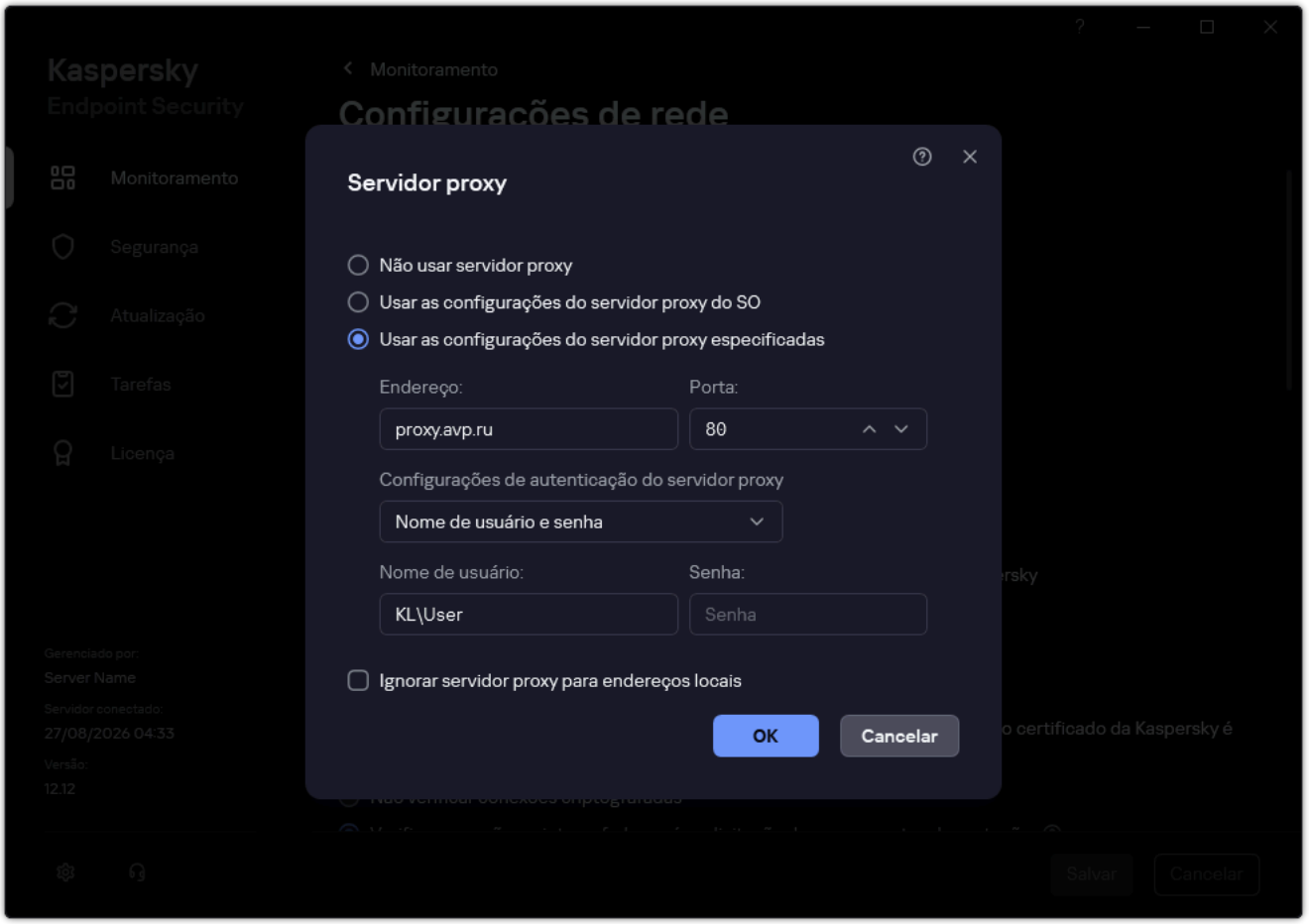
1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações de rede**.



Configurações de aplicativo rede

3. No bloco **Servidor proxy**, clique no link **Configurações do servidor proxy**.



Configurações de conexão do servidor proxy

4. Na janela que é aberta, selecione uma das seguintes opções para determinar o endereço do servidor proxy:

   - **Usar as configurações do servidor proxy do SO**.

     Esta opção está selecionada por padrão. O Kaspersky Endpoint Security usa as configurações do servidor proxy que são definidas nas configurações do sistema operacional.

   - **Usar as configurações do servidor proxy especificadas**.

     Se você selecionou esta opção, defina as configurações para se conectar ao servidor proxy: endereço e porta do servidor proxy.

5. Selecione como deseja que o aplicativo seja autenticado no servidor proxy. Por padrão, o aplicativo usa a autenticação NTLM de domínio do usuário atual.

6. Se quiser desativar o uso do servidor proxy ao atualizar bancos de dados e módulos de aplicativos a partir de uma pasta compartilhada, marque a caixa de seleção **Ignorar servidor proxy para endereços locais**.

7. Salvar alterações.

Como resultado, o Kaspersky Endpoint Security usará o servidor proxy para baixar o módulo do aplicativo e as atualizações do banco de dados. O Kaspersky Endpoint Security também usará um servidor proxy para acessar os servidores da KSN e os servidores de ativação da Kaspersky. Se a autenticação for necessária no servidor proxy, mas as credenciais da conta do usuário não forem fornecidas ou estiverem incorretas, o Kaspersky Endpoint Security solicitará o nome de usuário e a senha.

Reversão da última atualização

Após a segunda atualização dos bancos de dados e dos módulos do aplicativo, é disponibilizada a função de reversão destes às respectivas versões anteriores.

A cada processo de atualização, o Kaspersky Endpoint Security cria uma cópia de backup dos bancos de dados e módulos do programa atuais. Dessa forma, é possível reverter os bancos de dados e os módulos do aplicativo às respectivas versões anteriores se for necessário. Reverter a última atualização é importante, por exemplo, quando a nova versão do banco de dados causa um falso positivo, que resulta no bloqueio de um aplicativo seguro pelo Kaspersky Endpoint Security.

O Kaspersky Endpoint Security no modo Light Agent não é compatível com a tarefa *Reversão de atualização*.

Como reverter a última atualização no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **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

1. Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Reversão de atualização**.

Etapa 2. 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 3. Configurar um agendamento de início de tarefa

Configure o agendamento da tarefa, por exemplo, manualmente.

Etapa 4. Definir o nome da tarefa

Insira um nome para a tarefa.

Etapa 7. Concluir a criação da tarefa

Conclua o 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 reverter a última atualização no Web Console

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Reversão**.

   c. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Reversão de atualização*.

   d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Vá para a próxima etapa.

5. Selecione uma conta para executar a tarefa. Por padrão, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de usuário local.

6. Conclua o assistente.

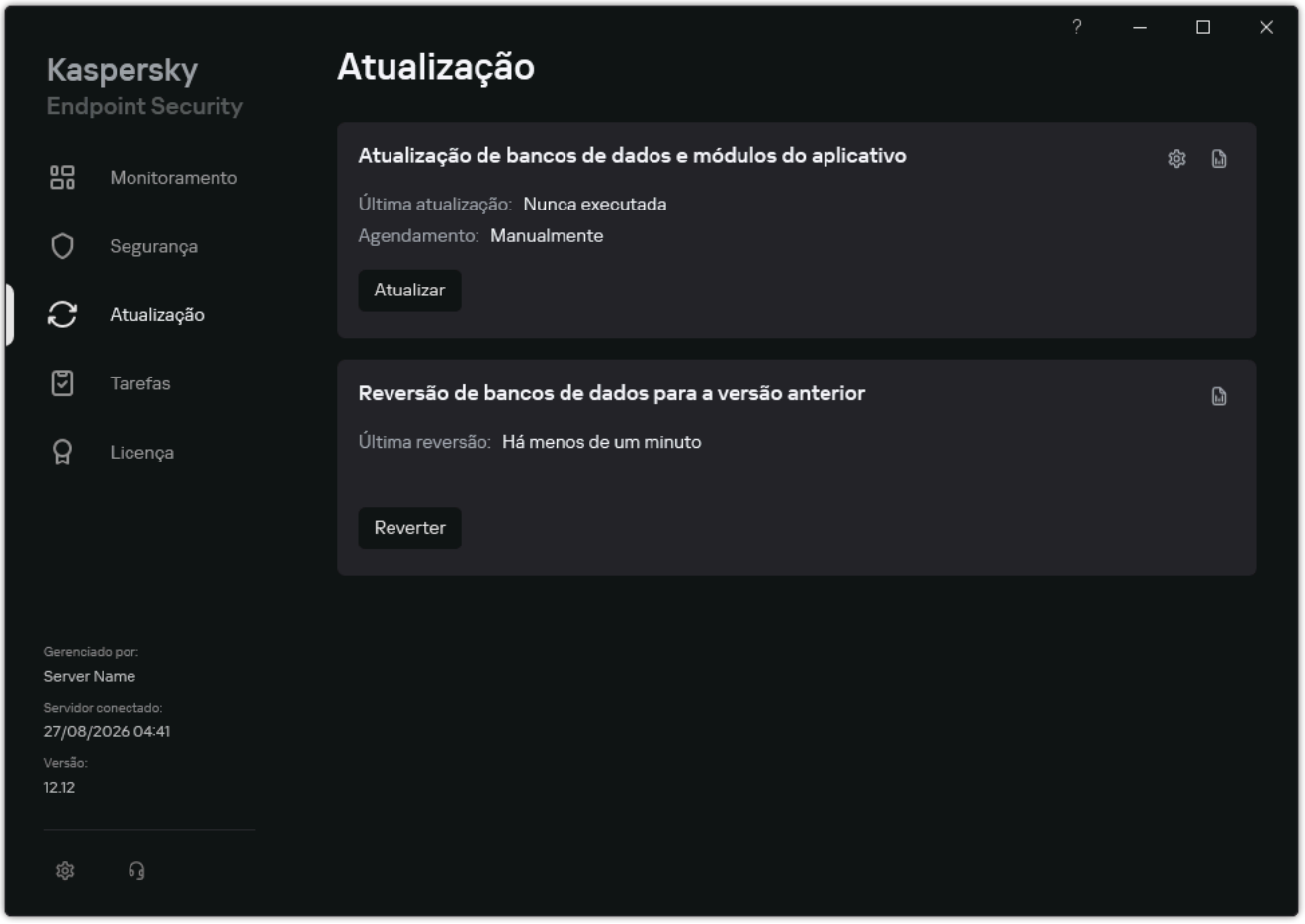
7. Uma nova tarefa será exibida na lista de tarefas.

8. Marque a caixa de seleção ao lado da tarefa.

9. Clique **Iniciar**.

Como reverter a última atualização na interface do aplicativo

1. Na janela principal do aplicativo, acesse a seção **Atualização**.



Tarefas de atualização local

2. No bloco **Reversão de bancos de dados para a versão anterior**, clique no botão **Reverter**.

O Kaspersky Endpoint Security começará a reverter a última atualização do banco de dados. O aplicativo exibirá o progresso da reversão, o tamanho dos arquivos baixados e a fonte de atualização. É possível interromper a tarefa a qualquer momento clicando no botão **Parar a atualização**.

Tecnologia de desinfecção avançada

Para trabalhar com ameaças ativas, o Kaspersky Endpoint Security usa a tecnologia de Desinfecção Avançada. A Desinfecção Avançada funciona de maneira diferente para estações de trabalho e servidores. É possível configurar a desinfecção avançada nas configurações da tarefa de *Verificação de malware* e nas configurações do aplicativo.

Se o Kaspersky Endpoint Security não conseguir interromper a execução de um malware, você poderá usar a tecnologia de Desinfecção Avançada. Para os computadores sob a política, a Desinfecção Avançada está desativada por padrão porque essa tecnologia usa uma quantidade significativa de recursos de computação. Para os computadores que não estão sob a política, a Desinfecção Avançada não está ativada por padrão.

A Desinfecção Avançada funciona de maneira diferente para estações de trabalho e servidores. Para usar a tecnologia em servidores, é necessário ativar a Desinfecção avançada imediata nas propriedades da tarefa de *Verificação de malware*. Esse pré-requisito não é necessário para usar a tecnologia em estações de trabalho.

Como ativar ou desativar a tecnologia de Desinfecção Avançada no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Configurações de aplicativos**.
4. No bloco **Geral**, marque ou desmarque a caixa de seleção **Ativar a Tecnologia de Desinfecção Avançada** para ativar ou desativar a tecnologia de desinfecção avançada.
5. Salvar alterações.

Como ativar ou desativar a tecnologia de Desinfecção Avançada no Web Console e no Cloud Console

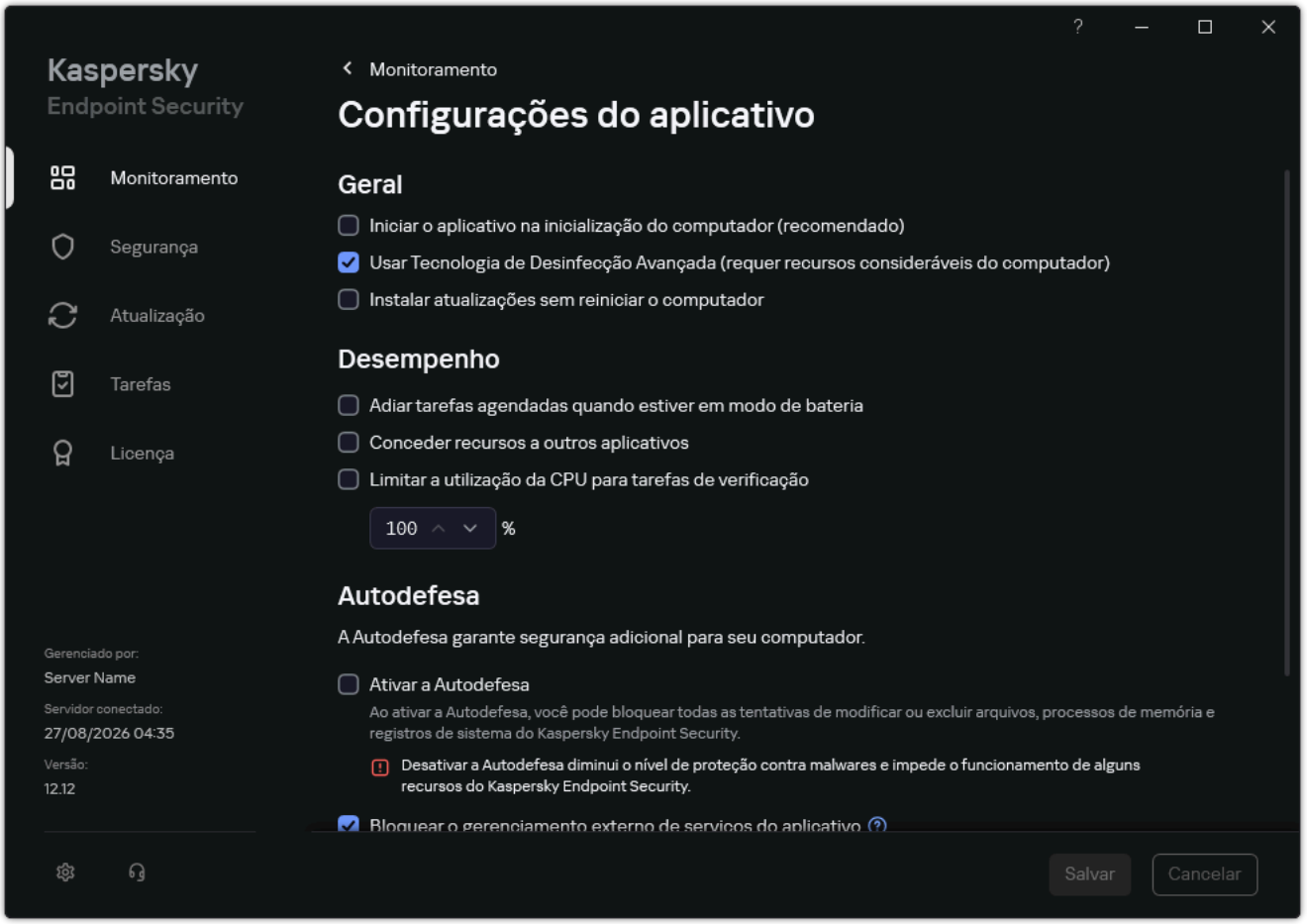
1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Configurações de detecção**.
5. No bloco **Tecnologia de Desinfecção Avançada**, ative ou desative o botão de alternância **Tecnologia de Desinfecção Avançada ATIVADA** para ativar ou desativar a tecnologia de Desinfecção avançada.
6. Salvar alterações.

Como ativar ou desativar a tecnologia de Desinfecção Avançada na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações do aplicativo**.



Configurações do Kaspersky Endpoint Security for Windows

3. No bloco **Geral**, marque ou desmarque a caixa de seleção **Usar Tecnologia de Desinfecção Avançada (requer recursos consideráveis do computador)** para ativar ou desativar a tecnologia de desinfecção avançada.

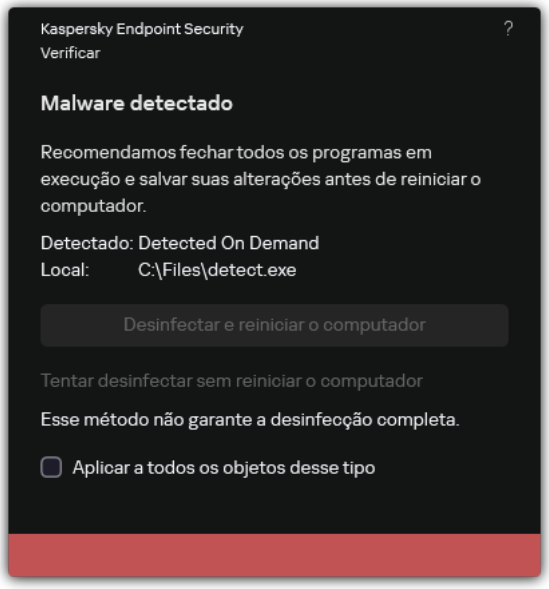
4. Salvar alterações.

Como resultado, o usuário não pode usar a maioria dos recursos do sistema operacional enquanto a Desinfecção avançada estiver em andamento. Quando a desinfecção for concluída, o computador será reiniciado.

Desinfecção de ameaças ativas em estações de trabalho

Para trabalhar com ameaças ativas em estações de trabalho, ative a tecnologia de Desinfecção Avançada nas configurações do aplicativo. Em seguida, configure a experiência do usuário nas propriedades da tarefa de *Verificação de malware*. Há uma caixa de seleção **Executar a Desinfecção Avançada imediatamente** nas propriedades da tarefa. Se o sinalizador for definido, o Kaspersky Endpoint Security executará a desinfecção sem notificar o usuário. Quando a desinfecção for concluída, o computador será reiniciado. Se o sinalizador não estiver definido, o Kaspersky Endpoint Security exibirá uma notificação sobre as ameaças ativas (veja a figura abaixo). Não é possível fechar essa notificação sem processar o arquivo.

A Desinfecção Avançada durante uma tarefa de verificação de vírus em um computador será executada somente se o recurso de Desinfecção Avançada estiver ativado nas propriedades da política aplicada a este computador.



Notificação sobre ameaça ativa

Desinfecção de ameaças ativas em servidores

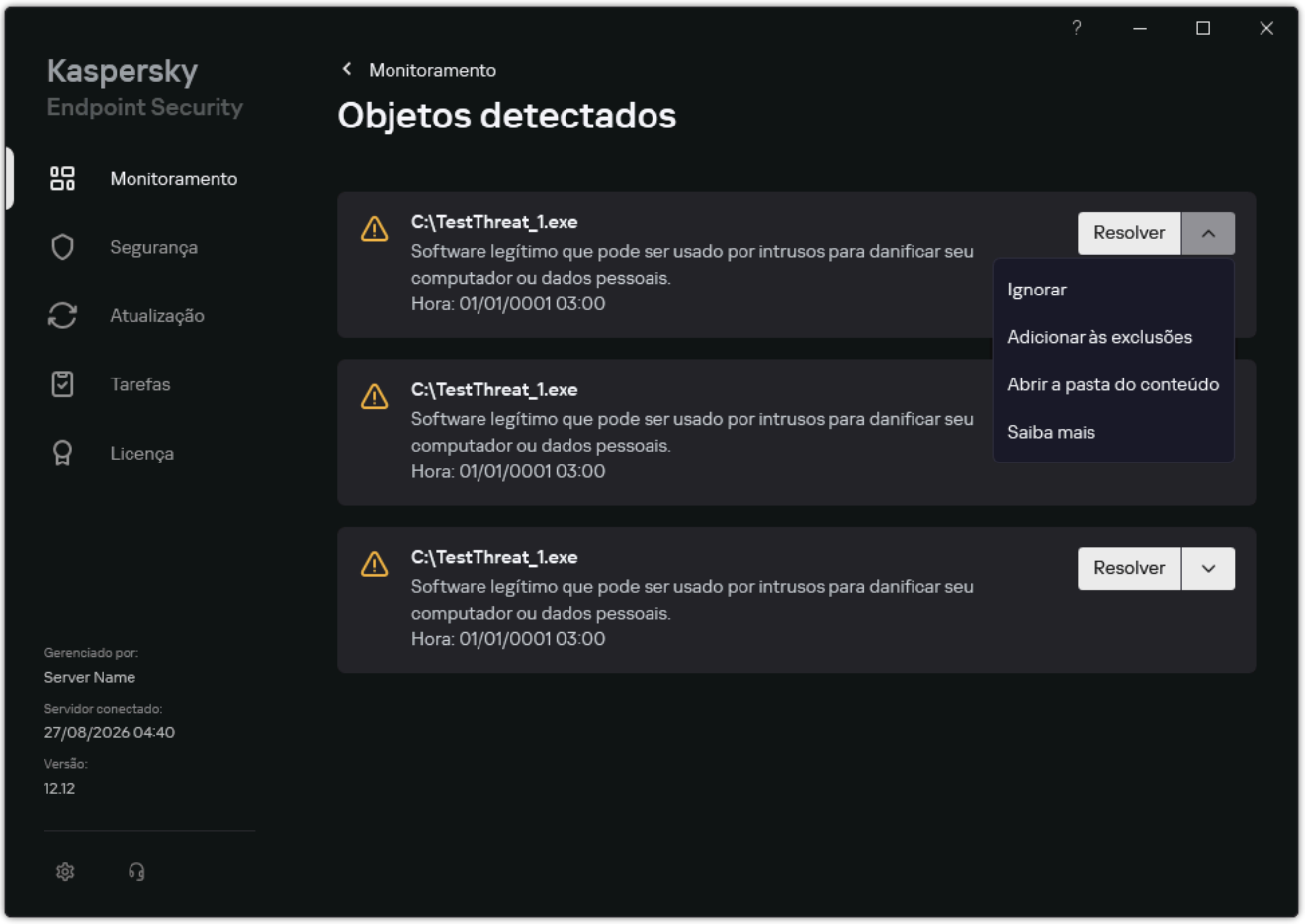
Para trabalhar com ameaças ativas em servidores, é necessário fazer o seguinte:

- ativar a tecnologia de Desinfecção Avançada nas configurações do aplicativo;
- ativar a Desinfecção Avançada imediata nas propriedades da tarefa de *Verificação de malware*.

Se o Kaspersky Endpoint Security estiver instalado em um computador que executa o Windows for Servers, o Kaspersky Endpoint Security não mostrará a notificação. Portanto, o usuário não pode selecionar uma ação para desinfectar uma ameaça ativa. Para desinfetar uma ameaça, é necessário ativar a tecnologia de desinfecção avançada nas configurações do aplicativo e ativar a desinfecção avançada imediatamente nas configurações de tarefa de *Verificação de malware*. Em seguida, será necessário iniciar a tarefa de *Verificação de malware*.

Eliminação de ameaças não processadas

O Kaspersky Endpoint Security registra informações sobre arquivos que não foram processados por algum motivo. Essas informações são registradas como eventos na lista de ameaças ativas (veja a figura abaixo).



Uma lista de ameaças ativas

Um arquivo infectado é considerado *processado* se o Kaspersky Endpoint Security tiver desinfectado o arquivo ou removido a ameaça como parte da verificação de vírus e outros malwares no computador.

O Kaspersky Endpoint Security transferirá o arquivo para a lista de ameaças ativas se, por qualquer motivo, ele não conseguir executar uma ação neste arquivo de acordo com as configurações especificadas do aplicativo durante a verificação do computador quanto a vírus e outras ameaças.

Esta situação ocorre nos seguintes casos:

- O arquivo verificado não está disponível (por exemplo, está localizado em uma unidade de rede ou em uma unidade removível sem privilégios de gravação).
- Nas configurações da tarefa de *Verificação de malware*, a ação ao detectar ameaças é definida como **Informar**. Então, quando a notificação do arquivo infectado foi exibida na tela, o usuário selecionou **Ignorar**.

Se houver alguma ameaça não processada, o Kaspersky Endpoint Security altera o ícone para . Na janela principal do aplicativo, a notificação da ameaça é exibida (veja a figura abaixo). No console do Kaspersky Security Center, o status do computador é alterado para *Crítico* – .

Como processar a ameaça no Console de administração (MMC)

1. No Console de Administração, acesse a pasta **Servidor de Administração** → **Avançado** → **Repositórios** → **Ameaças ativas**.

   A lista de ameaças ativas é aberta.

2. Selecione o objeto que deseja processar.

3. Escolha como deseja lidar com a ameaça:

   - **Desinfectar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Caso a desinfecção falhe, o aplicativo excluirá o arquivo.

   - **Excluir**. Caso esta opção seja selecionada, o aplicativo excluirá todos os arquivos infectados e detectados do repositório de ameaças ativas. Neste caso, o aplicativo mantém o arquivo detectado na memória do computador. Para eliminar a ameaça do computador, selecione **Desinfectar**.

Como processar uma ameaça no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **Operações** → **Repositórios** → **Ameaças ativas**.

   A lista de ameaças ativas é aberta.

2. Selecione o objeto que deseja processar.

3. Escolha como deseja lidar com a ameaça:

   - **Desinfectar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Caso a desinfecção falhe, o aplicativo excluirá o arquivo.

   - **Excluir**. Caso esta opção seja selecionada, o aplicativo excluirá todos os arquivos infectados e detectados do repositório de ameaças ativas. Neste caso, o aplicativo mantém o arquivo detectado na memória do computador. Para eliminar a ameaça do computador, selecione **Desinfectar**.

Como processar uma ameaça na interface do aplicativo

1. Na janela principal do aplicativo, na seção **Monitoramento**, clique no bloco **A proteção está em risco**.

   A lista de ameaças ativas é aberta.

2. Selecione o objeto que deseja processar.

3. Escolha como deseja lidar com a ameaça:

   - **Resolver**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Caso a desinfecção falhe, o aplicativo excluirá o arquivo.

   - **Adicionar às exclusões**. Caso esta ação seja selecionada, o Kaspersky Endpoint Security sugere adicionar o arquivo na lista de exclusões de verificação. As configurações da exclusão são definidas automaticamente. Caso a adição de uma exclusão não esteja disponível, isso significa que o administrador desativou a adição de exclusões nas configurações de política.

   - **Ignorar**. Se essa opção for selecionada, o Kaspersky Endpoint Security excluirá a entrada da lista de ameaças ativas. Se não houver mais nenhuma ameaça ativa na lista, o status do computador será alterado para *OK*. Se o objeto for detectado novamente, o Kaspersky Endpoint Security adicionará uma nova entrada à lista de ameaças ativas.

- **Abrir a pasta do conteúdo**. Se essa opção for selecionada, o Kaspersky Endpoint Security abrirá a pasta que contém o objeto no gerenciador de arquivos. Então, é possível excluir manualmente o objeto ou movê-lo para uma pasta que não esteja dentro do escopo da proteção.

- **Saiba mais**. Caso esta opção seja selecionada, o Kaspersky Endpoint Security abrirá o site do banco de dados de vulnerabilidades e ameaças da Kaspersky.

Para processar ameaças ativas no console do Kaspersky Security Center, você deve ativar a transferência de informações sobre arquivos não processados para o Servidor de Administração. A transferência de dados é ativada por padrão.

Como ativar a transferência de dados de arquivos não processados para o Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Configurações gerais** → **Relatórios e Armazenamento**.

4. No bloco **Transferência de dados para o Servidor de Administração**, clique no botão **Configurações**.

5. Marque a caixa de seleção **Arquivos não processados**.

6. Salvar alterações.

Como ativar a transferência de dados de arquivos não processados para o Web Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Integração KSC**.

5. No bloco **Transferência de dados para o Servidor de Administração**, marque a caixa de seleção **Sobre os arquivos não processados**.

6. Salvar alterações.

Janela principal do aplicativo quando uma ameaça é detectada

Proteção do computador

Status da Proteção em Tempo Real

O Kaspersky Endpoint Security envia a configuração **Status da proteção em tempo real** ao Servidor de Administração do Kaspersky Security Center; o valor dessa configuração depende do estado atual dos componentes de proteção do aplicativo no computador protegido (consulte a tabela abaixo).

O Kaspersky Endpoint Security determina o status da Proteção em Tempo Real com base no status dos seguintes componentes do aplicativo:

- Proteção Contra Ameaças ao Arquivo.
- Proteção Contra Ameaças da Web.
- Proteção Contra Ameaças ao Correio.
- Proteção AMSI.
- Prevenção contra ataque BadUSB.
- Proteção Contra Ameaças à Rede.
- Firewall.
- Prevenção de Exploits.
- Detecção de Comportamento.
- Mecanismo de Remediação.
- Prevenção de Intrusão do Host.

É possível verificar o status da Proteção em Tempo Real do aplicativo em um console do Kaspersky Security Center.

Como descobrir o status da Proteção em Tempo Real no Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Dispositivos gerenciados**.

   O status atual da Proteção em Tempo Real é exibido na lista de dispositivos, na coluna **Status da proteção em tempo real**. Se a coluna **Status da proteção em tempo real** não estiver disponível, gerencie as configurações de colunas clicando no link **Adicionar/Remover colunas**.

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Dispositivos gerenciados**.

O status atual da Proteção em Tempo Real é exibido na lista de dispositivos, na coluna **Status da proteção em tempo real**. Se a coluna **Status da proteção em tempo real** não estiver disponível, gerencie as configurações de colunas clicando no link **Adicionar/Remover colunas**.

Como verificar a Proteção do Computador em Tempo Real no Web Console

Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Ativos (dispositivos)**.

O status atual da Proteção em Tempo Real é exibido na lista de dispositivos, na coluna **Status da proteção em tempo real**. Se a coluna **Status da proteção em tempo real** não estiver disponível, gerencie as configurações de colunas (⚙).

Valores possíveis da configuração Status da proteção em tempo real

Valor	Descrição
Desconhecido	O Servidor de Administração não tem informações sobre o status da Proteção em Tempo Real deste computador.
Não instalado	Nenhum componente está instalado.
Incompatível com a licença	O aplicativo não está ativado ou a licença não permite o funcionamento dos componentes instalados.
Falhou	Um ou mais componentes apresentam falha.
Parado	Um ou mais componentes estão desativados.
Pausado	Um ou mais componentes estão pausados.
Iniciando	Um ou mais componentes estão sendo ativados.
Executando	Os componentes do aplicativo estão ativos e em execução.

Se o valor da configuração **Status da proteção em tempo real** no Kaspersky Security Center for diferente de *Executando*, verifique se os componentes instalados do Kaspersky Endpoint Security presentes na lista estão ativados e se o aplicativo está ativado.

Proteção Contra Ameaças ao Arquivo

O componente Proteção Contra Ameaças ao Arquivo permite evitar infecção do sistema de arquivos do computador. Por padrão, o componente Proteção Contra Ameaças ao Arquivo está localizado de forma permanente na RAM do computador e verifica todos os arquivos abertos, salvos ou executados em tempo real. O componente verifica os arquivos em todas as unidades do computador, inclusive unidades conectadas. O componente fornece proteção ao computador com a ajuda de bancos de dados de antivírus, o serviço na nuvem Kaspersky Security Network e análise heurística.

O componente verifica os arquivos acessados pelo usuário ou aplicativo. Se um arquivo malicioso for detectado, o Kaspersky Endpoint Security bloqueará a operação do arquivo. O aplicativo desinfeta ou exclui o arquivo malicioso, dependendo das configurações do componente Proteção contra ameaças ao arquivo.

Durante a tentativa de acesso a um arquivo cujos conteúdos estão armazenados na nuvem do OneDrive, o Kaspersky Endpoint Security baixa e verifica os conteúdos do arquivo.

Ativar e desativar a Proteção Contra Ameaças ao Arquivo

Por padrão, o componente Proteção Contra Ameaças ao Arquivo é ativado e executado no modo recomendado por especialistas da Kaspersky. Para Proteção contra Ameaças ao Arquivo, o Kaspersky Endpoint Security pode aplicar diferentes grupos de configurações. Estes grupos de configurações armazenados no aplicativo são denominados *níveis de segurança*: **Alto**, **Recomendado**, **Baixo**. As configurações do nível de segurança **Recomendado** são consideradas as configurações ideais recomendadas pelos especialistas da Kaspersky (veja a tabela abaixo). Você pode selecionar um dos níveis de segurança pré-configurados ou definir manualmente configurações de nível de segurança. A alteração das configurações do nível de segurança não impede a reversão para as configurações de nível recomendado.

O componente Proteção Contra Ameaças ao Arquivo usa dados recebidos de outros componentes do aplicativo. A ativação desses componentes é opcional. Os componentes que fornecem dados adicionais incluem:

- Kaspersky Security Network.
- Prevenção de Intrusão do Host.
- Detecção de Comportamento.

Como ativar ou desativar o componente Proteção Contra Ameaças ao Arquivo no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Arquivo**.
4. Use a caixa de seleção **Proteção Contra Ameaças ao Arquivo** para ativar ou desativar o componente.
5. Caso tenha ativado o componente, execute uma das seguintes operações no bloco **Nível de segurança**:
   - Caso queira aplicar um dos níveis de segurança pré-configurados, selecione-o com o controle deslizante:
     - **Alto**. Quando este nível de proteção de arquivo é selecionado, o Antivírus de Arquivos toma o controle mais estrito de todos os arquivos que são abertos, salvos e iniciados. O Componente de proteção de Ameaça de Arquivo verifica todos os tipos de arquivo em todos os discos rígidos, unidades removíveis e unidades de rede do computador. Ele também verifica arquivos compactados, pacotes de instalação e objetos OLE incorporados.
     - **Recomendado**. Esse nível de segurança de arquivo é recomendado pelos especialistas da Kaspersky Lab. O Componente de proteção de Ameaça de Arquivo só verifica os formatos de ficheiro especificados em todos os discos rígidos, unidades removíveis, e unidades de rede do computador e objetos de OLE incorporados. O Componente de proteção de Ameaça de Arquivo não verifica pacotes de instalação ou arquivos.
     - **Baixo**. As configurações desse nível de segurança de arquivo garantem a velocidade máxima de verificação. O componente File Threat Protection verifica somente arquivos com as extensões especificadas em todos os discos rígidos, unidades removíveis e unidades de rede do computador. O Componente de proteção de Ameaça de Arquivo não verifica arquivos compostos.

- Caso queira configurar um nível de segurança personalizado, clique no botão **Configurações** e defina suas próprias configurações do componente (consulte a tabela abaixo).

  É possível restaurar os valores dos níveis de segurança predefinidos clicando no botão **Por padrão**.

6. No bloco **Ação ao detectar ameaça**, selecione a ação que o Kaspersky Endpoint Security deve executar em objetos maliciosos:

   - **Desinfectar e excluir se a desinfecção falhar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Caso a desinfecção falhe, o aplicativo excluirá o arquivo.

   - **Desinfectar e bloquear se a desinfecção falhar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Se a desinfecção falhar, o aplicativo bloqueará o arquivo.

   - **Bloquear**. Se esta opção for selecionada, o aplicativo bloqueará automaticamente o arquivo infectado sem tentar desinfectá-lo ou exclui-lo.

   - **Informar**. Caso esta opção seja selecionada, o Kaspersky Endpoint Security adiciona as informações sobre arquivos infectados à lista de ameaças ativas na detecção destes arquivos.

   Antes de tentar desinfectar ou excluir um arquivo infectado, o aplicativo cria uma cópia de backup do arquivo no caso de você precisar restaurá-lo ou se ele puder ser desinfetado no futuro.

7. Salvar alterações.

Como ativar ou desativar o componente Proteção Contra Ameaças ao Arquivo no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Acesse **Proteção Contra Ameaças ao Host** → **Proteção Contra Ameaças ao Arquivo**.

5. Use o botão de alternância do **Proteção Contra Ameaças ao Arquivo ATIVADA** para ativar ou desativar o componente.

6. Se deseja adicionar um novo objeto ao escopo de proteção:

   a. Em **Configurações avançadas**, selecione a guia **Escopo de proteção**.

   b. Clique **Adicionar**.

   c. Uma janela será aberta; nessa janela, selecione os objetos que deseja adicionar ao escopo de proteção.

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.

- `?` (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 em qualquer lugar em um caminho de arquivo ou pasta. Por exemplo, se quiser que o escopo da verificação inclua a pasta Downloads para todas as contas de usuário no computador, insira a máscara `C:\Users\*\Downloads\`.

É possível excluir um objeto da proteção sem excluí-lo da lista de objetos no escopo de proteção. Para fazer isso, coloque a chave de alternância ao lado na posição desativada.

d. Salvar alterações.

7. No bloco **Ação ao detectar ameaça**, selecione a ação que o Kaspersky Endpoint Security deve executar em objetos maliciosos:

   - **Desinfectar e excluir se a desinfecção falhar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Caso a desinfecção falhe, o aplicativo excluirá o arquivo.

   - **Desinfectar e bloquear se a desinfecção falhar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Se a desinfecção falhar, o aplicativo bloqueará o arquivo.

   - **Bloquear**. Se esta opção for selecionada, o aplicativo bloqueará automaticamente o arquivo infectado sem tentar desinfectá-lo ou exclui-lo.

   Antes de tentar desinfectar ou excluir um arquivo infectado, o aplicativo cria uma cópia de backup do arquivo no caso de você precisar restaurá-lo ou se ele puder ser desinfetado no futuro.

8. Caso seja necessário, edite as configurações avançadas da Proteção Contra Ameaças ao Arquivo.

9. Salvar alterações.

Como ativar ou desativar o componente Proteção Contra Ameaças ao Arquivo na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Arquivo**.

3. Use o botão de alternância do **Proteção Contra Ameaças ao Arquivo** para ativar ou desativar o componente.

4. Caso tenha ativado o componente, execute uma das seguintes operações no bloco **Nível de segurança**:

   - Caso queira aplicar um dos níveis de segurança pré-configurados, selecione-o com o controle deslizante:

     - **Alto**. Quando este nível de proteção de arquivo é selecionado, o Antivírus de Arquivos toma o controle mais estrito de todos os arquivos que são abertos, salvos e iniciados. O Componente de proteção de Ameaça de Arquivo verifica todos os tipos de arquivo em todos os discos rígidos, unidades removíveis e unidades de rede do computador. Ele também verifica arquivos compactados, pacotes de instalação e objetos OLE incorporados.

     - **Recomendado**. Esse nível de segurança de arquivo é recomendado pelos especialistas da Kaspersky Lab. O Componente de proteção de Ameaça de Arquivo só verifica os formatos de ficheiro especificados em todos os discos rígidos, unidades removíveis, e unidades de rede do computador e objetos de OLE incorporados. O Componente de proteção de Ameaça de Arquivo não verifica pacotes de instalação ou arquivos.

     - **Baixo**. As configurações desse nível de segurança de arquivo garantem a velocidade máxima de verificação. O componente File Threat Protection verifica somente arquivos com as extensões especificadas em todos os discos rígidos, unidades removíveis e unidades de rede do computador. O Componente de proteção de Ameaça de Arquivo não verifica arquivos compostos.

   - Caso queira configurar um nível de segurança personalizado, clique no botão **Configurações avançadas** e defina suas próprias configurações do componente (consulte a tabela abaixo).

     É possível restaurar os valores dos níveis de segurança predefinidos clicando no botão **Restaurar nível de segurança recomendado**.

5. No bloco **Ação ao detectar ameaça**, selecione a ação que o Kaspersky Endpoint Security deve executar em objetos maliciosos:

   - **Desinfectar e excluir se a desinfecção falhar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Caso a desinfecção falhe, o aplicativo excluirá o arquivo.

   - **Desinfectar e bloquear se a desinfecção falhar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Se a desinfecção falhar, o aplicativo bloqueará o arquivo.

   - **Bloquear**. Se esta opção for selecionada, o aplicativo bloqueará automaticamente o arquivo infectado sem tentar desinfectá-lo ou exclui-lo.

   - **Informar**. Caso esta opção seja selecionada, o Kaspersky Endpoint Security adiciona as informações sobre arquivos infectados à lista de ameaças ativas na detecção destes arquivos.

   Antes de tentar desinfectar ou excluir um arquivo infectado, o aplicativo cria uma cópia de backup do arquivo no caso de você precisar restaurá-lo ou se ele puder ser desinfetado no futuro.

6. Salvar alterações.

Configurações de Proteção Contra Ameaças ao Arquivo recomendadas pelos especialistas da Kaspersky (nível de segurança recomendado)

Parâmetro	Valor	Descrição
Tipos de arquivos	**Arquivos verificados por formato**	Se esta configuração for ativada, o aplicativo verificará apenas arquivos infetáveis. Antes de verificar um arquivo quanto a código malicioso, o cabeçalho interno do arquivo é analisado para determinar o formato do arquivo (por exemplo, .txt, .doc ou .exe). A verificação também procura arquivos com extensões específicas.
Análise Heurística	**Verificação superficial**	A tecnologia foi desenvolvida para detectar ameaças que não podem ser detectadas usando a versão atual dos bancos de dados do aplicativo Kaspersky. Detecta arquivos que podem estar infectados por um vírus desconhecido ou por uma nova variedade de um vírus conhecido. Ao verificar arquivos em busca de códigos maliciosos, o analisador heurístico executa instruções nos arquivos executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível de análise heurística assegura um equilíbrio entre a eficácia da verificação quanto a novas ameaças, a carga nos recursos do sistema operacional e a duração da análise heurística.
Verificar somente arquivos novos e alterados	**Ativado**	Verifica apenas os arquivos novos e aqueles que foram modificados desde a última vez em que foram verificados. Isso ajuda a reduzir a duração de uma verificação. Esse modo se aplica a arquivos simples e compostos.
Usar tecnologia iSwift	**Ativado**	Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iSwift é um avanço da tecnologia iChecker do sistema de arquivos NTFS.
Usar tecnologia iChecker	**Ativado**	Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iChecker tem algumas limitações: ela não funciona com arquivos grandes e se aplica somente a objetos com uma estrutura reconhecida pelo aplicativo (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).
Verificar arquivos de formatos do Microsoft Office	**Ativado**	Verifica arquivos do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Arquivos de formato do Office também incluem objetos OLE. O aplicativo 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	**Ativado**	Verificar arquivos de formato de e-mail. O aplicativo verifica arquivos MSG e EML. Arquivos de formato de e-mail também incluem objetos OLE e arquivos MHT. O Kaspersky Endpoint Security verifica arquivos em formato de e-mail com menos de 1 MB, independentemente de a caixa de seleção estar marcada ou não.
Modo de verificação	**Modo inteligente**	Nesse modo, a Proteção Contra Ameaças ao Arquivo verifica um objeto com base na análise das ações executadas com o objeto. Por exemplo, ao trabalhar com um documento do Microsoft Office, o Kaspersky Endpoint Security verifica o arquivo quando ele é aberto pela primeira vez e fechado pela última vez. O arquivo não é verificado durante as operações intermediárias de gravação.
Ação ao detectar ameaça	**Desinfectar e excluir se a desinfecção falhar**	Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Caso a desinfecção falhe, o aplicativo excluirá o arquivo.

Pausa automática da Proteção Contra Ameaças ao Arquivo

Você pode configurar a Proteção Contra Ameaças ao Arquivo para pausar automaticamente em um horário especificado ou ao trabalhar com aplicativos específicos.

A Proteção Contra Ameaças ao Arquivo deve ser pausada somente como um último recurso quando entrar em conflito com alguns aplicativos. Se surgir algum conflito durante a execução de um componente, é recomendável entrar em contato com o Suporte Técnico da Kaspersky. Os especialistas de suporte o ajudarão a configurar a execução simultânea do componente Proteção Contra Ameaças ao Arquivo com outros aplicativos em seu computador.

Para configurar a pausa automática da Proteção Contra Ameaças ao Arquivo:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Arquivo**.
3. Clique **Configurações avançadas**.
4. No bloco **Pausar a Proteção Contra Ameaças ao Arquivo**, clique no link **Pausar a Proteção Contra Ameaças ao Arquivo**.
5. Na janela que é aberta, defina as configurações para pausar a Proteção Contra Ameaças ao Arquivo:
   a. Configure uma programação para pausar automaticamente a Proteção Contra Ameaças ao Arquivo.
   b. Crie uma lista de aplicativos cuja operação deve fazer com que a Proteção Contra Ameaças ao Arquivo pause suas atividades.
6. Salvar alterações.

Alterar a ação executada em arquivos infectados pelo componente Proteção Contra Ameaças ao Arquivo

Por padrão, o componente Proteção Contra Ameaças ao Arquivo tentará desinfectar automaticamente todos os arquivos infectados detectados. Se a desinfeção falhar, o Componente de Proteção Contra Ameaças ao Arquivo apaga estes arquivos.

Para alterar a ação executada em arquivos infectados pelo componente Proteção Contra Ameaças ao Arquivo:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Arquivo**.
3. No bloco **Ação ao detectar ameaça**, selecione a opção pertinente:
   - **Desinfectar e excluir se a desinfecção falhar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Caso a desinfecção falhe, o aplicativo excluirá o arquivo.
   - **Desinfectar e bloquear se a desinfecção falhar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Se a desinfecção falhar, o aplicativo bloqueará o arquivo.
   - **Bloquear**. Se esta opção for selecionada, o aplicativo bloqueará automaticamente o arquivo infectado sem tentar desinfectá-lo ou exclui-lo.

Antes de tentar desinfectar ou excluir um arquivo infectado, o aplicativo cria uma cópia de backup do arquivo no caso de você precisar restaurá-lo ou se ele puder ser desinfetado no futuro.

4. Salvar alterações.

Formar o escopo de proteção do componente Proteção Contra Ameaças ao Arquivo

O escopo de proteção refere-se aos objetos que o componente verifica quando está ativado. O escopo de proteção de componentes diferentes tem propriedades diversas. O local e o tipo de arquivos a serem verificados são propriedades do escopo de proteção do componente Proteção Contra Ameaças ao Arquivo. Por padrão, o componente Proteção Contra Ameaças ao Arquivo verifica somente arquivos possivelmente infectáveis que são executados dos discos rígidos, unidades removíveis e unidades de rede.

Ao selecionar o tipo dos arquivos a verificar, considere o seguinte:

1. Há uma baixa probabilidade de introduzir códigos maliciosos em arquivos de determinados formatos e sua subsequente ativação (por exemplo, formato TXT). Ao mesmo tempo, há formatos de arquivos que contêm um código executável (como .exe ou .dll). O código executável também pode ser gravados em formatos de arquivo que não se destinam a essa finalidade (por exemplo, o formato DOC). O risco de infiltração e ativação de código malicioso nesses arquivos é grande.

2. O invasor talvez envie vírus ou outro tipo de aplicativo malicioso para o computador em um arquivo executável renomeado com a extensão .txt. Se você selecionar a verificação de arquivos por extensão, o aplicativo ignora esse arquivo durante a verificação. Se a verificação de arquivos por formato for selecionada, o Kaspersky Endpoint Security analisará o cabeçalho do arquivo independentemente da extensão. Se essa análise revelar que o arquivo tem o formato de um arquivo executável (por exemplo, EXE), o aplicativo o verificará.

Para criar o escopo de proteção:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Arquivo**.

3. Clique **Configurações avançadas**.

4. No bloco **Tipos de arquivos**, especifique o tipo de arquivo que deseja que o componente Proteção Contra Ameaças ao Arquivo verifique:

   - **Todos os arquivos**. Se esta configuração for ativada, o Kaspersky Endpoint Security verificará todos os arquivos sem exceção (todos os formatos e extensões).

   - **Arquivos verificados por formato**. Se esta configuração for ativada, o aplicativo verificará apenas arquivos infetáveis. Antes de verificar um arquivo quanto a código malicioso, o cabeçalho interno do arquivo é analisado para determinar o formato do arquivo (por exemplo, .txt, .doc ou .exe). A verificação também procura arquivos com extensões específicas.

   - **Arquivos verificados por extensão**. Se esta configuração for ativada, o aplicativo verificará apenas arquivos infetáveis. O formato do arquivo é determinado com base na extensão do arquivo.

5. Clique no link **Editar o escopo de proteção**.

6. Na janela que é aberta, selecione os objetos que deseja adicionar ao escopo de proteção ou excluir dele.

> Você não pode remover ou editar objetos que estão incluídos no escopo de proteção padrão.

7. Se deseja adicionar um novo objeto ao escopo de proteção:

   a. Clique **Adicionar**.

      A árvore de pastas é exibida.

   b. No campo **Caminho**, 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.

      - `?` (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 em qualquer lugar em um caminho de arquivo ou pasta. Por exemplo, se quiser que o escopo da verificação inclua a pasta Downloads para todas as contas de usuário no computador, insira a máscara `C:\Users\*\Downloads\`.

      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**.

   Você pode excluir um objeto das verificações sem excluí-lo da lista de objetos no escopo da verificação. Para fazer isso, desmarque a caixa de seleção ao lado do objeto.

8. Salvar alterações.

Usar métodos de verificação

O Kaspersky Endpoint Security usa uma técnica de verificação chamada Machine learning e análise de assinatura. Na análise de assinaturas, o Kaspersky Endpoint Security compara o objeto detectado com os registros do banco de dados. Com base nas recomendações dos especialistas da Kaspersky, o aprendizado de máquina e análise de assinatura sempre estarão ativados.

Para aumentar a eficácia da proteção, você pode usar a análise heurística. Ao verificar arquivos em busca de códigos maliciosos, o analisador heurístico executa instruções nos arquivos executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível de análise heurística assegura um equilíbrio entre a eficácia da verificação quanto a novas ameaças, a carga nos recursos do sistema operacional e a duração da análise heurística.

Para configurar a utilização da análise heurística na operação do componente Proteção Contra Ameaças ao Arquivo:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Arquivo**.
3. Clique **Configurações avançadas**.
4. Caso queira que o aplicativo utilize a análise heurística para proteção contra ameaças a arquivos, marque a caixa de seleção **Análise Heurística** no bloco **Métodos de verificação**. Em seguida, use o controle deslizante para definir o nível de análise heurística: **Verificação superficial**, **Verificação média** ou **Verificação profunda**.
5. Salvar alterações.

Usar tecnologias de verificação na operação do componente Proteção Contra Ameaças ao Arquivo

Para configurar a utilização de tecnologias de verificação na operação do componente Proteção Contra Ameaças ao Arquivo:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Arquivo**.
3. Clique **Configurações avançadas**.
4. Na seção **Tecnologias de verificação**, marque as caixas de seleção junto aos nomes das tecnologias que deseja usar na proteção contra ameaças ao arquivo:
   - **Usar tecnologia iSwift**. Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iSwift é um avanço da tecnologia iChecker do sistema de arquivos NTFS.
   - **Usar tecnologia iChecker**. Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iChecker tem algumas limitações: ela não funciona com arquivos grandes e se aplica somente a objetos com uma estrutura reconhecida pelo aplicativo (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).
5. Salvar alterações.

Otimizar a verificação do arquivo

É possível otimizar a verificação de arquivos, que é executada pelo componente Proteção Contra Ameaças ao Arquivo, reduzindo o tempo da verificação e aumentando a velocidade operacional do Kaspersky Endpoint Security. Isso é possível quando são verificados apenas os arquivos novos e aqueles que foram alterados após a verificação anterior. Esse modo se aplica a arquivos simples e compostos.

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

Para otimizar a verificação de arquivos:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Arquivo**.
3. Clique **Configurações avançadas**.
4. No bloco **Otimização**, marque a caixa de seleção **Verificar somente arquivos novos e alterados**.
5. Salvar alterações.

Verificar arquivos compostos

Um método comum para ocultar vírus e outro tipo de malware é incorporá-los em arquivos compostos, como arquivos compactados e bancos de dados. Para detectar vírus e outro tipo de malware que estão ocultos dessa forma, é necessário descompactar os arquivos compostos, o que pode reduzir a velocidade da verificação. É possível restringir os tipos dos arquivos compostos a verificar, o que aumentará a velocidade da verificação.

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

O componente Proteção Contra Ameaças ao Arquivo desinfecta arquivos compostos nos formatos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR e ICE e exclui arquivos em todos os outros formatos (exceto bancos de dados de e-mail).

Para configurar a verificação de arquivos compostos:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Arquivo**.
3. Clique **Configurações avançadas**.

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 de e-mail ou do Office.

5. Se a verificação apenas de arquivos novos e modificados estiver desativada, defina as configurações para verificar cada tipo de arquivo composto: verificar todos os arquivos deste tipo ou apenas os novos arquivos.

   Se a verificação apenas de arquivos novos e modificados estiver ativada, o Kaspersky Endpoint Security verifica apenas arquivos novos e modificados de todos os tipos de arquivos compostos.

6. Defina as configurações avançadas para verificar arquivos compostos.

   - **Não descompactar arquivos compostos de grandes dimensões**.

     Se esta caixa de seleção for marcada, o Kaspersky Endpoint Security não verificará arquivos compostos se o tamanho deles exceder o valor especificado.

     Se esta caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security verificará os arquivos compostos de todos os tamanhos.

     O Kaspersky Endpoint Security verifica os arquivos grandes que foram extraídos dos arquivos compactados, independentemente de a caixa de seleção **Não descompactar arquivos compostos de grandes dimensões** estar marcada.

   - **Descompactar arquivos compostos em segundo plano**.

     Se a caixa de seleção estiver selecionada, o Kaspersky Endpoint Security fornecerá acesso a arquivos compostos maiores que o valor especificado antes da verificação desses arquivos. Nesse caso, o Kaspersky Endpoint Security descompacta e verifica os arquivos compostos em segundo plano.

     O Kaspersky Endpoint Security fornece acesso a arquivos compostos menores que esse valor somente após descompactar e verificar esses arquivos.

     Se a caixa de seleção não estiver selecionada, o Kaspersky Endpoint Security fornecerá acesso a arquivos compostos somente após descompactar e verificar arquivos de qualquer tamanho.

7. Salvar alterações.

Alterar o modo de verificação

O *Modo de verificação* se refere à condição que aciona a verificação de arquivo pelo componente Proteção Contra Ameaças ao Arquivo. Por padrão, o Kaspersky Endpoint Security realiza a verificação de arquivos no modo de inteligente. Neste modo de verificação, o componente Proteção Contra Ameaças ao Arquivo decide se verificará ou não os arquivos após analisar as operações executadas pelo usuário, por um aplicativo em nome do usuário (usando a conta atualmente ativa ou uma conta de usuário diferente) ou pelo sistema operacional. Por exemplo, ao trabalhar com um documento do Microsoft Office Word, o Kaspersky Endpoint Security verifica o arquivo quando ele é aberto pela primeira vez e fechado pela última vez. O arquivo não é verificado durante as operações intermediárias de gravação.

Para alterar o modo de verificação dos arquivos:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Arquivo**.

3. Clique **Configurações avançadas**.

4. No bloco **Modo de verificação**, selecione o modo desejado:

   - **Modo inteligente**. Nesse modo, a Proteção Contra Ameaças ao Arquivo verifica um objeto com base na análise das ações executadas com o objeto. Por exemplo, ao trabalhar com um documento do Microsoft Office, o Kaspersky Endpoint Security verifica o arquivo quando ele é aberto pela primeira vez e fechado pela última vez. O arquivo não é verificado durante as operações intermediárias de gravação.

   - **Ao acessar e modificar**. Nesse modo, os objetos são verificados pela Proteção Contra Ameaças ao Arquivo sempre que houver uma tentativa de abri-los ou modificá-los.

   - **Ao acessar**. Neste modo, os objetos são verificados pela Proteção Contra Ameaças ao Arquivo ao tentar abri-los.

   - **Ao executar**. Neste modo, os objetos são verificados pela Proteção Contra Ameaças ao Arquivo apenas ao tentar executá-los.

5. Salvar alterações.

Verificação de contêiner

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 Endpoint Security verifica os arquivos não apenas em discos, mas também dentro de contêineres. Ou seja, o Kaspersky Endpoint 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 Endpoint Security dentro do contêiner não é compatível.

Além de fornecer segurança de contêiner, o Kaspersky Endpoint Security permite gerenciar aplicativos dentro de contêineres com o uso do Controle de Aplicativos. O Controle 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.

Ação ao detectar ameaças

Se uma ameaça for detectada dentro de um contêiner, o aplicativo aplica a ação selecionada para o componente Proteção Contra Ameaças ao Arquivo. 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 Endpoint Security pode interromper o contêiner se o objeto detectado não puder ser desinfectado. Por padrão, a funcionalidade de interrupção do contêiner fica desativada.

Como configurar a verificação de contêiners no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Arquivo**.
4. Clique **Configurações**.
5. Uma janela será aberta; nessa janela, selecione a guia **Adicional**.
6. No bloco **Verificar as operações de arquivo 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, é impossível 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 de arquivo 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.
7. Salvar alterações.

Como configurar a verificação de contêiners no Web Console e no Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Acesse **Proteção Contra Ameaças ao Host** → **Proteção Contra Ameaças ao Arquivo**.
5. Em **Configurações avançadas**, selecione a guia **Desempenho**.

6. No bloco **Otimização da verificação**, 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, é impossível 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.

7. Salvar alterações.

Como configurar a verificação de contêiners na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Arquivo**.

3. No bloco **Verificar as operações de arquivo 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, é impossível 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 de arquivo 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.

Prevenção de Intrusão do Host

O componente estará disponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para computadores pessoais. O componente estará indisponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para servidores.

O componente Prevenção de Intrusão do Host impede que os aplicativos executem ações perigosas para o sistema, e garante o controle de acesso aos recursos do sistema operacional e aos dados pessoais. O componente fornece proteção ao computador com a ajuda de bancos de dados antivírus e o serviço na nuvem Kaspersky Security Network.

O componente controla a operação de aplicativos usando *direitos de aplicativo*. Os direitos do aplicativo incluem os seguintes parâmetros de acesso:

- Acesso aos recursos do sistema operacional (por exemplo, opções de inicialização automática, chaves do Registro)
- Acesso a dados pessoais (como arquivos e aplicativos)

A atividade de rede dos aplicativos é controlada pelo componente Firewall por meio das *regras de rede*.

Durante a primeira inicialização do aplicativo, o componente de Prevenção de Intrusão do Host executa as seguintes ações:

1. Verifica a segurança do aplicativo usando bancos de dados de antivírus baixados.
2. Verifica a segurança do aplicativo na Kaspersky Security Network.

   Recomendamos a participação na Kaspersky Security Network para ajudar o componente Prevenção de Intrusão do Host a funcionar de maneira mais eficiente.

3. Coloca o aplicativo em um dos grupos de confiança: *Confiável*, *Baixa restrição*, *Alta restrição*, *Não confiável*.

   Um grupo confiável define os direitos aos quais o Kaspersky Endpoint Security se refere ao controlar a atividade do aplicativo. O Kaspersky Endpoint Security coloca um aplicativo em um grupo de confiança, dependendo do nível de perigo que esse aplicativo pode representar para o computador.

   O Kaspersky Endpoint Security coloca um aplicativo em um grupo de confiança para os componentes Firewall e Prevenção de Intrusão do Host. Você não pode alterar o grupo de confiança apenas para o Firewall ou Prevenção de Intrusão do Host.

   Se você se recusou a participar do KSN ou não há rede, o Kaspersky Endpoint Security coloca o aplicativo em um grupo de confiança, dependendo das configurações do componente Prevenção de Intrusão do Host. Após receber a reputação do aplicativo da KSN, o grupo de confiança pode ser alterado automaticamente.

4. Bloqueia as ações do aplicativo, dependendo do grupo de confiança. Por exemplo, aplicativos do grupo de confiança *Alta restrição* têm acesso negado aos módulos do sistema operacional.

Na próxima vez em que o aplicativo for iniciado, a Prevenção de Intrusão do Host verificará sua integridade. Se o aplicativo não for alterado, o componente usará os direitos atuais do aplicativo para ele. Se o aplicativo foi modificado, o Kaspersky Endpoint Security o analisará como se estivesse sendo iniciado pela primeira vez.

Ativar e desativar a Prevenção de Intrusão do Host

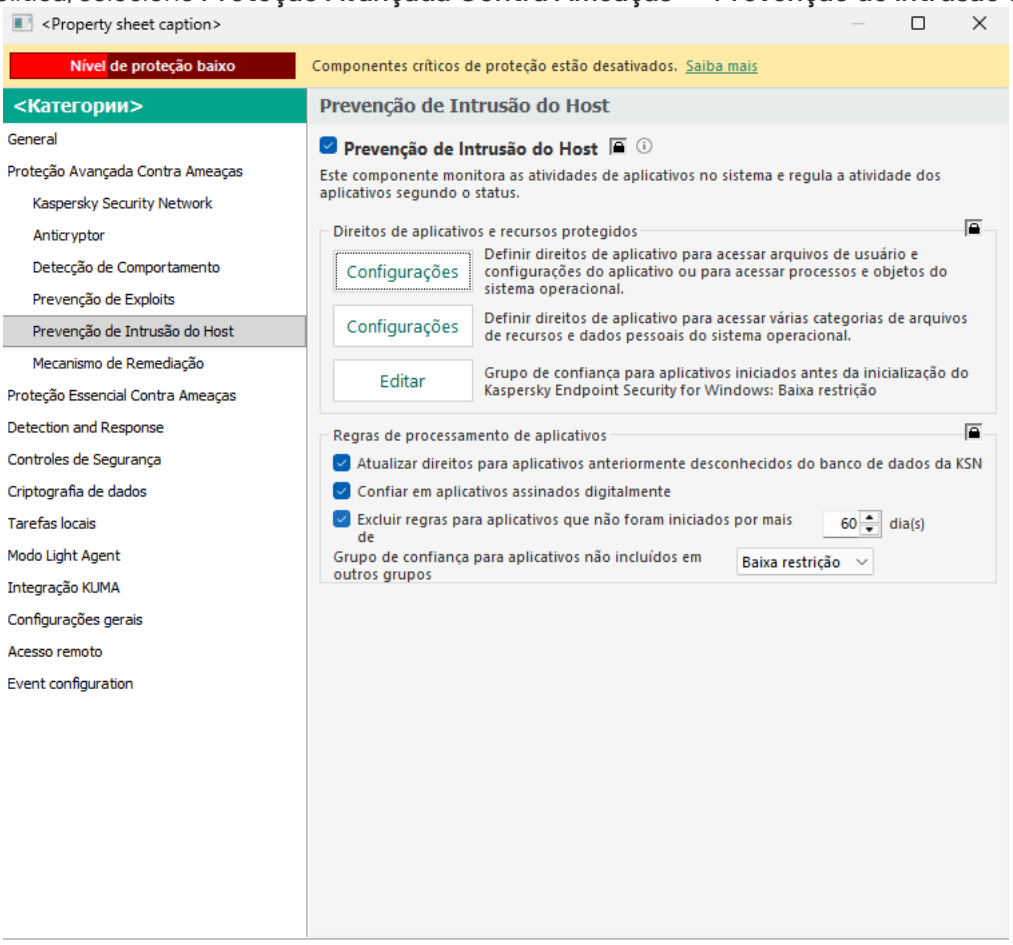
Por padrão, o componente Prevenção de Intrusão do Host é ativado e executado no modo recomendado por especialistas da Kaspersky.

Como ativar ou desativar o componente Prevenção de Intrusão do Host no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.



Configurações da Prevenção de Intrusões

4. Use a caixa de seleção **Prevenção de Intrusão do Host** para ativar ou desativar o componente.

5. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar ou desativar o componente Prevenção de Intrusão do Host no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Proteção Contra Ameaças ao Host** → **Prevenção de Intrusão do Host**.

5. Use o botão de alternância do **Prevenção de Intrusão do Host ATIVADA** para ativar ou desativar o componente.

6. Salvar alterações.

Como ativar ou desativar o componente Prevenção de Intrusão do Host na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.
3. Use o botão de alternância do **Prevenção de Intrusão do Host** para ativar ou desativar o componente.
4. Salvar alterações.

Se o componente de Prevenção de Intrusão do Host estiver ativado, o Kaspersky Endpoint Security colocará um aplicativo em um grupo de confiança dependendo do nível de perigo que esse aplicativo pode representar para o computador. O Kaspersky Endpoint Security bloqueará então as ações do aplicativo dependendo do grupo de confiança.

Gerenciar grupos de confiança de aplicativos

Ao iniciar cada aplicativo pela primeira vez, o componente Prevenção de Intrusão do Host verifica a segurança do aplicativo e o coloca em um dos grupos de confiança.

Na primeira etapa da verificação do aplicativo, o Kaspersky Endpoint Security verifica o banco de dados interno de aplicativos conhecidos para detectar uma entrada correspondente e, ao mesmo tempo, envia uma solicitação ao banco de dados da Kaspersky Security Network (se houver uma conexão com a Internet). De acordo com os resultados da pesquisa no banco de dados interno e o banco de dados do Kaspersky Security Network, o aplicativo é colocado em um grupo de confiança. Cada vez que o aplicativo é iniciado subsequentemente, o Kaspersky Endpoint Security envia uma nova pergunta ao banco de dados da KSN e coloca o aplicativo em um grupo de confiança diferente, se a reputação do aplicativo no banco de dados da KSN tiver sido alterada.

É possível selecionar um grupo de confiança ao qual o Kaspersky Endpoint Security deve colocar automaticamente todos os aplicativos desconhecidos. Os aplicativos que estavam em execução antes do Kaspersky Endpoint Security ser iniciado são colocados automaticamente no grupo de confiança definido nas configurações de Prevenção de Intrusão do Host.

> Para aplicativos iniciados antes do Kaspersky Endpoint Security, só a atividade de rede é controlada. O controle é realizado segundo as regras de rede definidas nas configurações do Firewall.

Alterar o grupo de confiança de um aplicativo

Ao iniciar cada aplicativo pela primeira vez, o componente Prevenção de Intrusão do Host verifica a segurança do aplicativo e o coloca em um dos grupos de confiança.

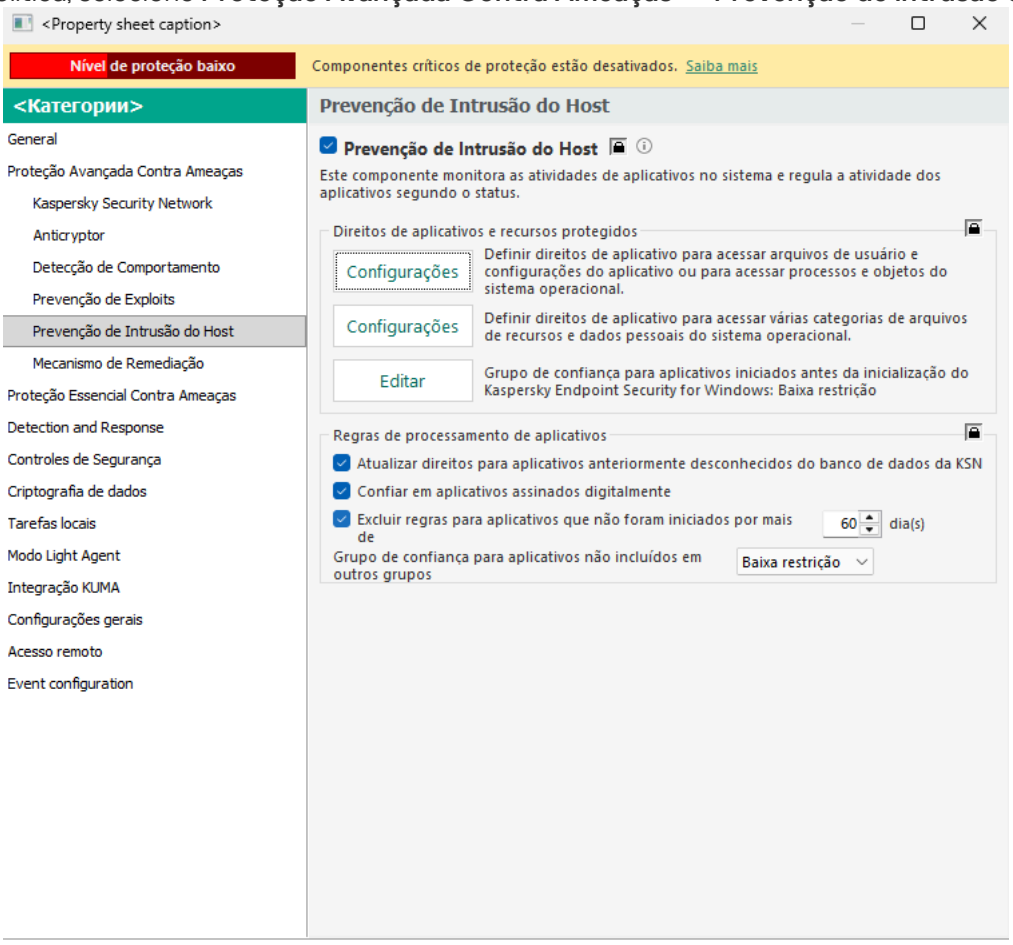
> Os especialistas da Kaspersky não recomendam mover os aplicativos que foram atribuídos automaticamente a um grupo de confiança para outro. Em vez disso, você pode modificar direitos de um aplicativo individual, se necessário.

Como alterar o grupo de confiança de um aplicativo no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.



Configurações da Prevenção de Intrusões

4. No bloco **Direitos de aplicativos e recursos protegidos**, clique no botão **Configurações**.

   Isso abre a janela de configuração de Direitos de aplicativos e a lista de Recursos protegidos.

5. Selecione a guia **Direitos de aplicativos**.

6. Clique **Adicionar**.

7. Na janela que é aberta, insira os critérios para buscar o aplicativo cujo grupo de confiança deseja alterar.

   É possível inserir o nome do aplicativo ou o nome do fornecedor. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.

8. Clique **Atualizar**.

   O Kaspersky Endpoint Security pesquisará o aplicativo na lista consolidada de aplicativos instalados em computadores gerenciados. O Kaspersky Endpoint Security exibirá uma lista de aplicativos que satisfazem os critérios de pesquisa.

9. Selecione o aplicativo desejado.

10. Na lista suspensa **Adicionar o aplicativo selecionado ao grupo de confiança**, selecione o grupo de confiança para o aplicativo.

11. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como alterar o grupo de confiança de um aplicativo na Web Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Proteção Contra Ameaças ao Host** → **Prevenção de Intrusão do Host**.

5. No bloco **Direitos de aplicativos e recursos protegidos**, clique no link **Direitos de aplicativos e recursos protegidos**.

   Isso abre a janela de configuração de Direitos de aplicativos e a lista de Recursos protegidos.

6. Selecione a guia **Direitos de aplicativos**.

   Uma lista de Grupos de confiança será exibida no lado esquerdo da janela e suas propriedades no lado direito.

7. Clique **Adicionar**.

   Então, o assistente para adicionar um aplicativo a um grupo de confiança será iniciado.

8. Selecione um grupo de confiança relevante para o aplicativo.

9. Selecione o tipo de **Aplicativo**. Vá para a próxima etapa.

   Caso queira alterar o grupo de confiança para múltiplos aplicativos, selecione o tipo de **Grupo** e defina um nome para o grupo de aplicativos.

10. Na lista de aplicativos aberta, selecione os aplicativos cujo grupo de confiança deseja alterar.

    Usar um filtro. É possível inserir o nome do aplicativo ou o nome do fornecedor. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.

11. Conclua o assistente.

    O aplicativo será adicionado ao grupo de confiança.

12. Salvar alterações.

Como alterar o grupo de confiança de um aplicativo na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .

2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.

3. Clique **Gerenciar aplicativos**.

   Aparecerá a lista dos aplicativos instalados.

4. Selecione o aplicativo desejado.

5. No menu de contexto do aplicativo, selecione **Restrições** → **<grupo de confiança>**.

6. Salvar alterações.

Como resultado, o aplicativo será colocado no outro grupo de confiança. O Kaspersky Endpoint Security bloqueará então as ações do aplicativo dependendo do grupo de confiança. O status *(definido pelo usuário)* será atribuído ao aplicativo. Se a reputação do aplicativo for alterada na Kaspersky Security Network, o componente Prevenção de Intrusão do Host deixará o grupo de confiança do aplicativo inalterado.

Configurando direitos de grupos de confiança

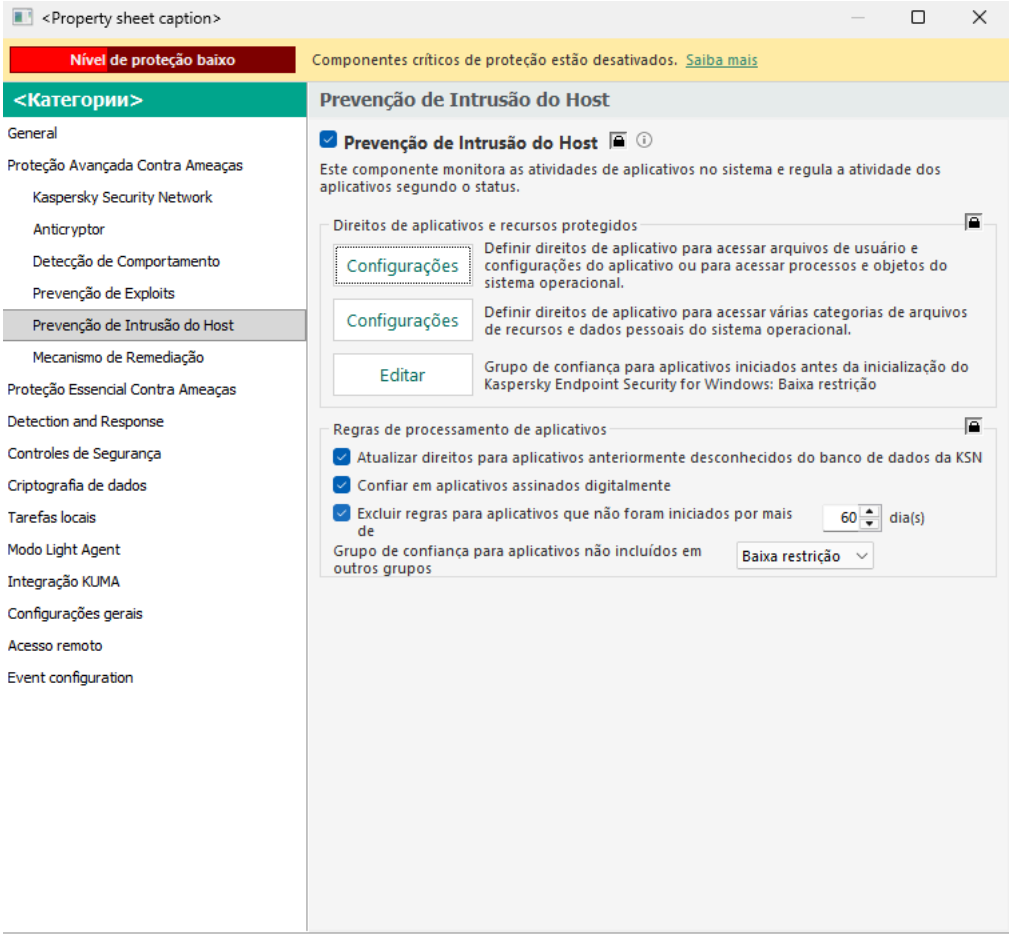
Os direitos de aplicativos ideais são criados por diferentes grupos de confiança por padrão. As configurações de direitos dos grupos do aplicativo que estão em um grupo confiável herdam valores das configurações dos direitos do grupo confiável.

Como mudar os direitos do grupo de confiança no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.



Configurações da Prevenção de Intrusões

4. No bloco **Direitos de aplicativos e recursos protegidos**, clique no botão **Configurações**.

   Isso abre a janela de configuração de Direitos de aplicativos e a lista de Recursos protegidos.

5. Vá para a guia **Direitos de aplicativos**.

6. Selecione o grupo de confiança necessário.

7. No menu de contexto do grupo de confiança, selecione **Direitos de grupo**.

   A janela propriedades do grupo de confiança é aberta.

8. Realize uma das seguintes ações:

   - Caso queira editar os direitos do grupo de confiança que regem as operações com o registro do sistema operacional, arquivos do usuário e configurações do aplicativo, selecione **Registro do sistema e arquivos**.

   - Caso queira editar os direitos do grupo de confiança que regem o acesso aos processos e objetos do sistema operacional, selecione **Direitos**.

   A atividade de rede dos aplicativos é controlada pelo componente Firewall por meio das *regras de rede*.

9. Para o recurso relevante, na coluna da ação correspondente, clique com o botão direito do mouse para abrir o menu de contexto e selecionar a opção necessária: **Herdar**, **Permitir** (✓) ou **Bloquear** (⊘).

10. Caso queira monitorar o uso dos recursos do computador, selecione **Criar log de eventos** (✓ / ⊘).

    O Kaspersky Endpoint Security registrará as informações sobre o funcionamento do componente Prevenção de intrusão do host. Os relatórios contêm informações sobre as operações com recursos de computador realizados pelo aplicativo (permitidas ou proibidas). Os relatórios também contêm informações sobre os aplicativos que utilizam cada recurso.

11. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como alterar os direitos de grupo de confiança no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Proteção Contra Ameaças ao Host** → **Prevenção de Intrusão do Host**.

5. No bloco **Direitos de aplicativos e recursos protegidos**, clique no link **Direitos de aplicativos e recursos protegidos**.

   Isso abre a janela de configuração de Direitos de aplicativos e a lista de Recursos protegidos.

6. Vá para a guia **Direitos de aplicativos**.

   Uma lista de Grupos de confiança será exibida no lado esquerdo da janela e suas propriedades no lado direito.

7. Na parte esquerda da janela, selecione o grupo de confiança relevante.

8. Na parte direita da janela, na lista suspensa, efetue uma das seguintes opções:

   - Caso queira editar os direitos do grupo de confiança que regem as operações com o registro do sistema operacional, arquivos do usuário e configurações do aplicativo, selecione **Registro do sistema e arquivos**.

   - Caso queira editar os direitos do grupo de confiança que regem o acesso aos processos e objetos do sistema operacional, selecione **Direitos**.

A atividade de rede dos aplicativos é controlada pelo componente Firewall por meio das *regras de rede*.

9. Para o recurso relevante, na coluna da ação correspondente, selecione a opção necessária: **Herdar**, **Permitir** ( ), **Bloquear** ( ).

10. Caso queira monitorar o uso dos recursos do computador, selecione **Criar log de eventos** (/).

    O Kaspersky Endpoint Security registrará as informações sobre o funcionamento do componente Prevenção de intrusão do host. Os relatórios contêm informações sobre as operações com recursos de computador realizados pelo aplicativo (permitidas ou proibidas). Os relatórios também contêm informações sobre os aplicativos que utilizam cada recurso.

11. Salvar alterações.

Como alterar os direitos do grupo de confiança na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .

2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.

3. Clique **Gerenciar aplicativos**.

   Aparecerá a lista dos aplicativos instalados.

4. Selecione o grupo de confiança necessário.

5. No menu de contexto do grupo de confiança, selecione **Detalhes e regras**.

   A janela propriedades do grupo de confiança é aberta.

6. Realize uma das seguintes ações:

   - Caso queira editar os direitos do grupo de confiança que regem as operações com o registro do sistema operacional, arquivos do usuário e configurações do aplicativo, selecione **Registro do sistema e arquivos**.

   - Caso queira editar os direitos do grupo de confiança que regem o acesso aos processos e objetos do sistema operacional, selecione **Direitos**.

A atividade de rede dos aplicativos é controlada pelo componente Firewall por meio das *regras de rede*.

7. Para o recurso relevante, na coluna da ação correspondente, clique com o botão direito do mouse para abrir o menu de contexto e selecionar a opção necessária: **Herdar**, **Permitir** ( ) ou **Negar** ( ).

8. Caso queira monitorar o uso dos recursos do computador, selecione **Registrar eventos** ( ).

   O Kaspersky Endpoint Security registrará as informações sobre o funcionamento do componente Prevenção de intrusão do host. Os relatórios contêm informações sobre as operações com recursos de computador realizados pelo aplicativo (permitidas ou proibidas). Os relatórios também contêm informações sobre os aplicativos que utilizam cada recurso.

9. Salvar alterações.

Os direitos do grupo de confiança serão alterados. O Kaspersky Endpoint Security bloqueará então as ações do aplicativo dependendo do grupo de confiança. O status (*Configurações personalizadas*) será atribuído ao grupo de confiança.

Selecionar um grupo confiável de aplicativos iniciados antes do Kaspersky Endpoint Security

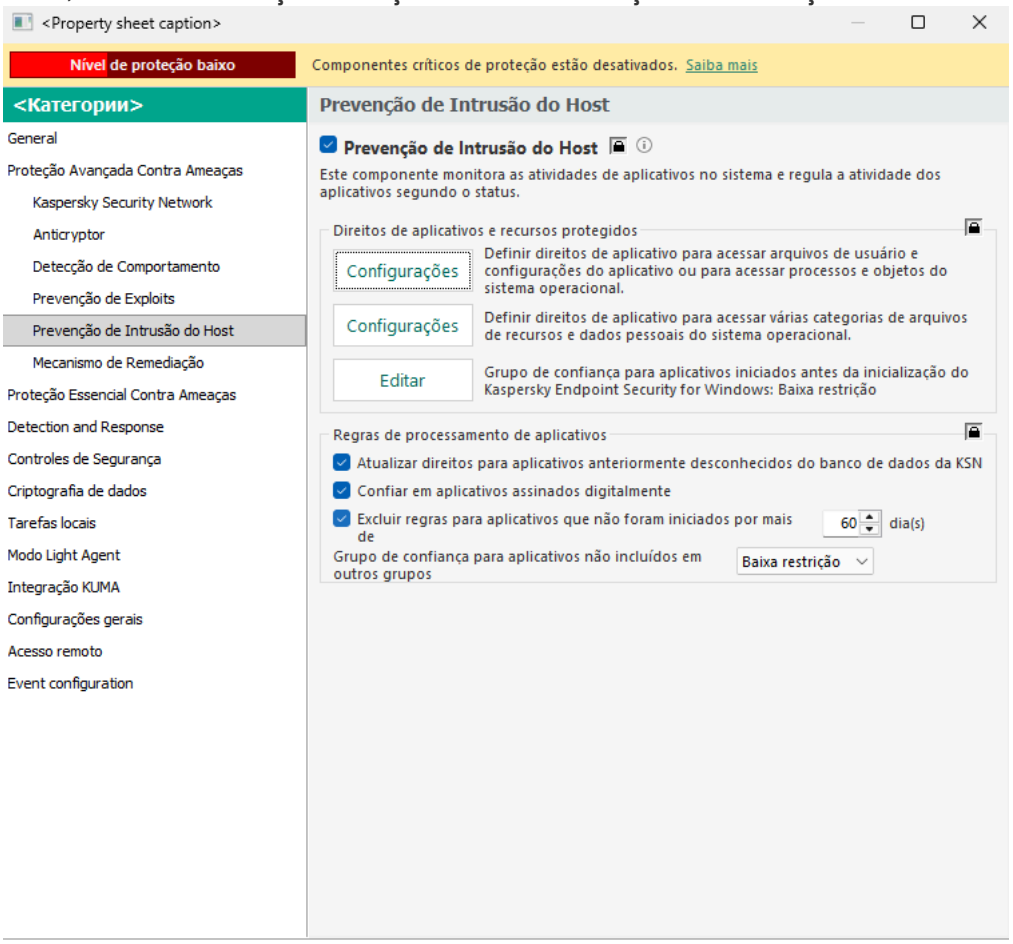
Para aplicativos iniciados antes do Kaspersky Endpoint Security, só a atividade de rede é controlada. O controle é realizado segundo as regras de rede definidas nas configurações do Firewall. Para especificar que regras de rede devem ser aplicadas à monitorização de atividade de rede de tais aplicativos, você deve selecionar um grupo de confiança.

Como selecionar um grupo de confiança de aplicativos iniciados antes do Kaspersky Endpoint Security no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.



Configurações da Prevenção de Intrusões

4. No bloco **Direitos de aplicativos e recursos protegidos**, clique no botão **Editar**.

5. Para que a configuração **Grupo de confiança para aplicativos iniciados antes da inicialização do Kaspersky Endpoint Security**, selecione o grupo de confiança apropriado.

6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como selecionar um grupo de confiança para aplicativos iniciados antes do Kaspersky Endpoint Security no Web Console e no Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Proteção Contra Ameaças ao Host** → **Prevenção de Intrusão do Host**.
5. Para que a configuração **Grupo de confiança para aplicativos iniciados antes da inicialização do Kaspersky Endpoint Security**, selecione o grupo de confiança apropriado.
6. Salvar alterações.

Como selecionar um grupo de confiança para aplicativos iniciados antes do Kaspersky Endpoint Security na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.
3. No bloco **Grupo confiável para aplicativos iniciados antes da inicialização do Kaspersky Endpoint Security**, selecione o grupo de confiança apropriado.
4. Salvar alterações.

Como resultado, um aplicativo iniciado antes do Kaspersky Endpoint Security será colocado no outro grupo de confiança. O Kaspersky Endpoint Security bloqueará então as ações do aplicativo dependendo do grupo de confiança.

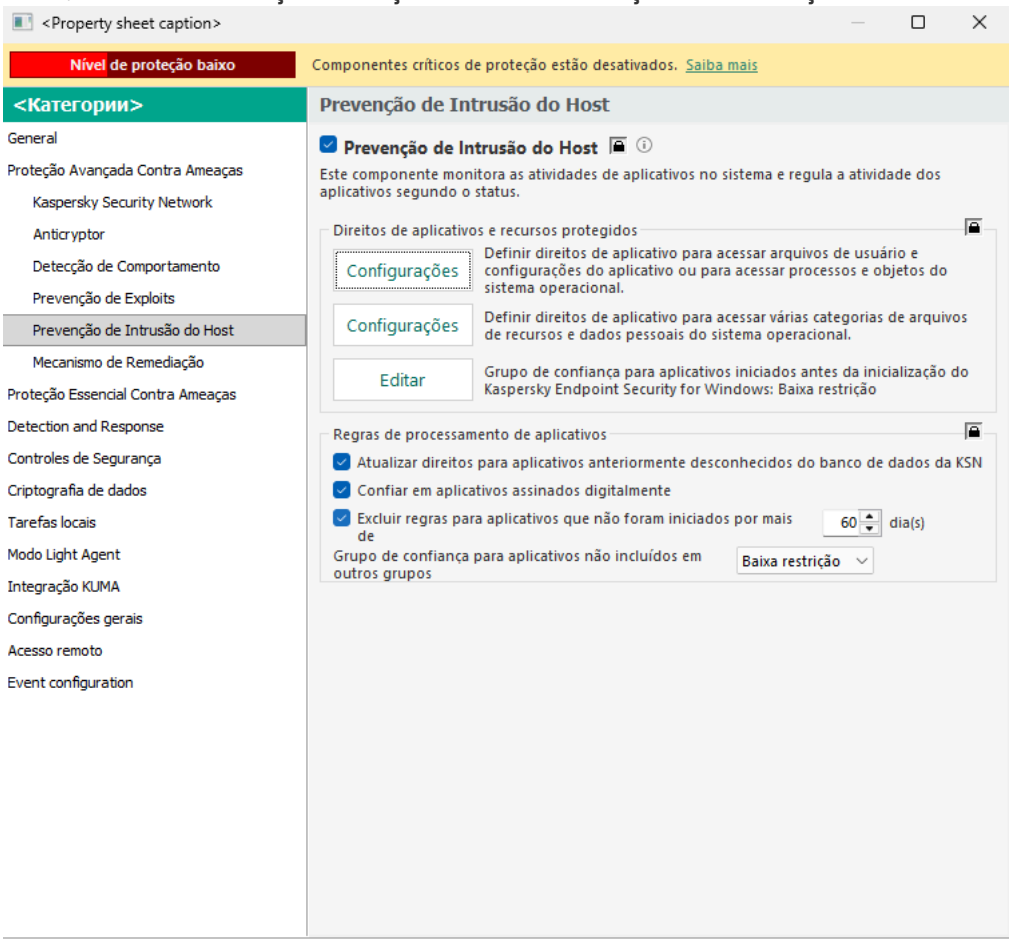
Selecionar um grupo de confiança para aplicativos desconhecidos

Durante a primeira inicialização de um aplicativo, o componente Prevenção de Intrusão do Host determina o grupo de confiança para o aplicativo. Caso não haja acesso à Internet ou se a Kaspersky Security Network não tiver informações sobre o aplicativo, a Kaspersky Endpoint Security colocará o aplicativo no grupo de *Baixa restrição* por padrão. Quando forem detectadas informações sobre um aplicativo previamente desconhecido na KSN, o Kaspersky Endpoint Security atualizará os direitos do aplicativo. É possível editar os direitos de aplicativos manualmente.

Como selecionar um grupo de confiança para aplicativos desconhecidos no console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.



Configurações da Prevenção de Intrusões

4. No bloco **Regras de processamento de aplicativos**, use a lista suspensa **Grupo de confiança para aplicativos não incluídos em outros grupos** para selecionar o grupo de confiança necessário.

   Se a participação na Kaspersky Security Network estiver ativada, o Kaspersky Endpoint Security enviará à KSN uma consulta sobre a reputação de um aplicativo cada vez que ele for iniciado. Com base na resposta recebida, o aplicativo pode ser movido para um grupo confiável diferente daquele especificado nas configurações do componente Prevenção de Intrusão do Host.

5. Use a caixa de seleção **Atualizar direitos para aplicativos anteriormente desconhecidos do banco de dados da KSN** para configurar a atualização automática de direitos para aplicativos desconhecidos.

6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como selecionar um grupo de confiança para aplicativos desconhecidos no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Proteção Contra Ameaças ao Host** → **Prevenção de Intrusão do Host**.

5. No bloco **Regras de processamento de aplicativos**, use a lista suspensa **Grupo de confiança para aplicativos não incluídos em outros grupos** para selecionar o grupo de confiança necessário.

   Se a participação na Kaspersky Security Network estiver ativada, o Kaspersky Endpoint Security enviará à KSN uma consulta sobre a reputação de um aplicativo cada vez que ele for iniciado. Com base na resposta recebida, o aplicativo pode ser movido para um grupo confiável diferente daquele especificado nas configurações do componente Prevenção de Intrusão do Host.

6. Use a caixa de seleção **Atualizar direitos para aplicativos anteriormente desconhecidos do banco de dados da KSN** para configurar a atualização automática de direitos para aplicativos desconhecidos.

7. Salvar alterações.

Como selecionar um grupo de confiança para aplicativos desconhecidos na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.

3. No bloco **Regras de processamento de aplicativos**, selecione o grupo de confiança adequado.

   Se a participação na Kaspersky Security Network estiver ativada, o Kaspersky Endpoint Security enviará à KSN uma consulta sobre a reputação de um aplicativo cada vez que ele for iniciado. Com base na resposta recebida, o aplicativo pode ser movido para um grupo confiável diferente daquele especificado nas configurações do componente Prevenção de Intrusão do Host.

4. Use a caixa de seleção **Atualizar regras para aplicativos anteriormente desconhecidos da KSN** para configurar a atualização automática de direitos para aplicativos desconhecidos.

5. Salvar alterações.

Selecionar um grupo de confiança para aplicativos assinados digitalmente

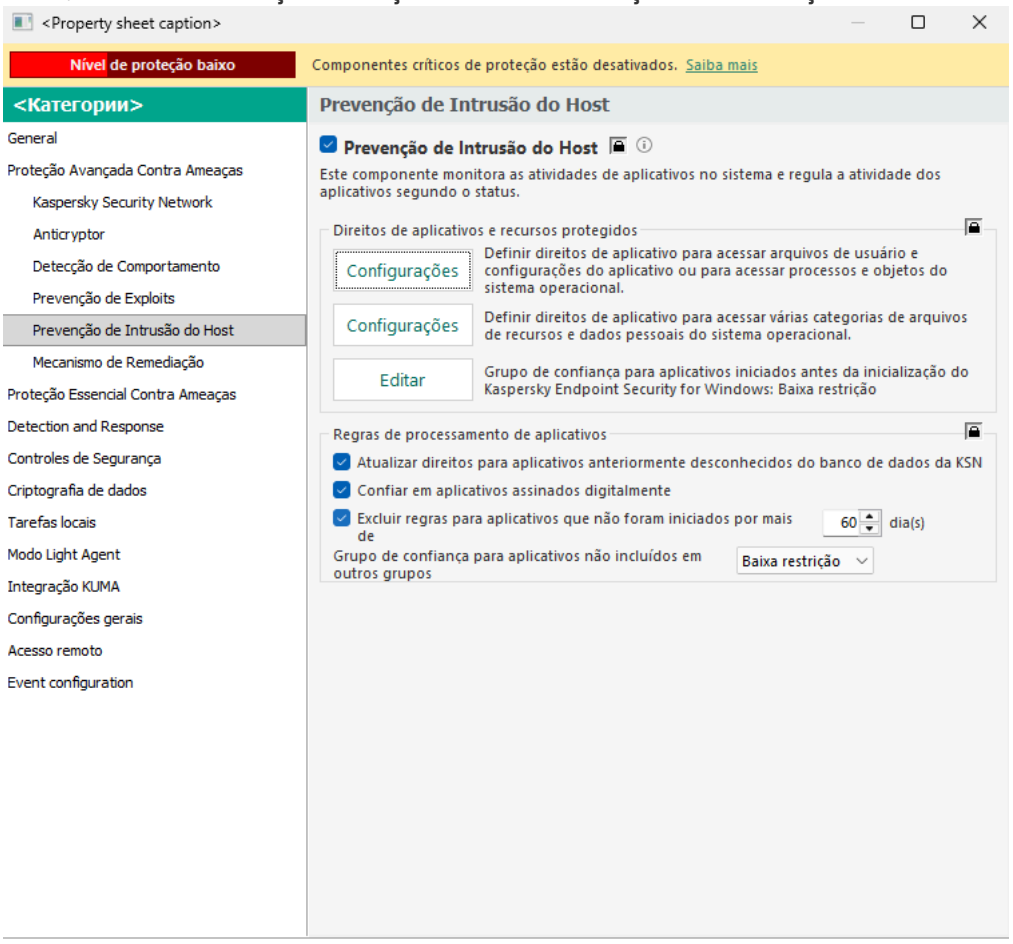
O Kaspersky Endpoint Security sempre coloca aplicativos assinados por certificados da Microsoft ou Certificados da Kaspersky no grupo *Confiável*.

Como selecionar um grupo de confiança para aplicativos assinados digitalmente no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.



Configurações da Prevenção de Intrusões

4. No bloco **Regras de processamento de aplicativos**, use a caixa de seleção **Confiar em aplicativos assinados digitalmente** para ativar ou desativar a atribuição automática ao grupo de confiança Confiáveis para aplicativos contendo a assinatura digital de fornecedores confiáveis.

   Fornecedores confiáveis são aqueles fornecedores incluídos no grupo de confiança pela Kaspersky. Também é possível adicionar certificados de fornecedores manualmente ao armazenamento de certificados do sistema confiável.

   Se esta caixa de seleção estiver desmarcada, o componente Prevenção de Intrusão do Host não considerará aplicativos com assinatura digital como confiáveis e usará outros parâmetros para determinar o grupo de confiança deles.

5. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como selecionar um grupo de confiança para aplicativos assinados digitalmente no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Proteção Contra Ameaças ao Host** → **Prevenção de Intrusão do Host**.

5. No bloco **Regras de processamento de aplicativos**, use a caixa de seleção **Confiar em aplicativos assinados digitalmente** para ativar ou desativar a atribuição automática ao grupo de confiança Confiáveis para aplicativos contendo a assinatura digital de fornecedores confiáveis.

Fornecedores confiáveis são aqueles fornecedores incluídos no grupo de confiança pela Kaspersky. Também é possível adicionar certificados de fornecedores manualmente ao armazenamento de certificados do sistema confiável.

Se esta caixa de seleção estiver desmarcada, o componente Prevenção de Intrusão do Host não considerará aplicativos com assinatura digital como confiáveis e usará outros parâmetros para determinar o grupo de confiança deles.

6. Salvar alterações.

Como selecionar um grupo de confiança para aplicativos assinados digitalmente na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.

3. No bloco **Regras de processamento de aplicativos**, use a caixa de seleção **Confiar em aplicativos assinados digitalmente** para ativar ou desativar a atribuição automática ao grupo de confiança Confiáveis para aplicativos contendo a assinatura digital de fornecedores confiáveis.

   Fornecedores confiáveis são aqueles fornecedores incluídos no grupo de confiança pela Kaspersky. Também é possível adicionar certificados de fornecedores manualmente ao armazenamento de certificados do sistema confiável.

   Se esta caixa de seleção estiver desmarcada, o componente Prevenção de Intrusão do Host não considerará aplicativos com assinatura digital como confiáveis e usará outros parâmetros para determinar o grupo de confiança deles.

4. Salvar alterações.

Gerenciar direitos do aplicativo

Por padrão, a atividade de aplicativos é controlada com base nos direitos do aplicativo que são definidos para o grupo de confiança específico que o Kaspersky Endpoint Security designou para o aplicativo quando ele foi iniciado pela primeira vez. Se necessário, é possível editar os direitos de aplicativos para todo o grupo de confiança, para um aplicativo individual ou para um grupo de aplicativos em um grupo de confiança.

Os direitos de aplicativos definidos manualmente possuem uma prioridade maior do que os direitos de aplicativos definidos para um grupo de confiança. Em outras palavras, se os direitos de aplicativos definidos manualmente diferem dos direitos de aplicativos definidos para um grupo de confiança, o componente de Prevenção de Intrusão do Host controla a atividade de aplicativos de acordo com os direitos de aplicativos definidos manualmente.

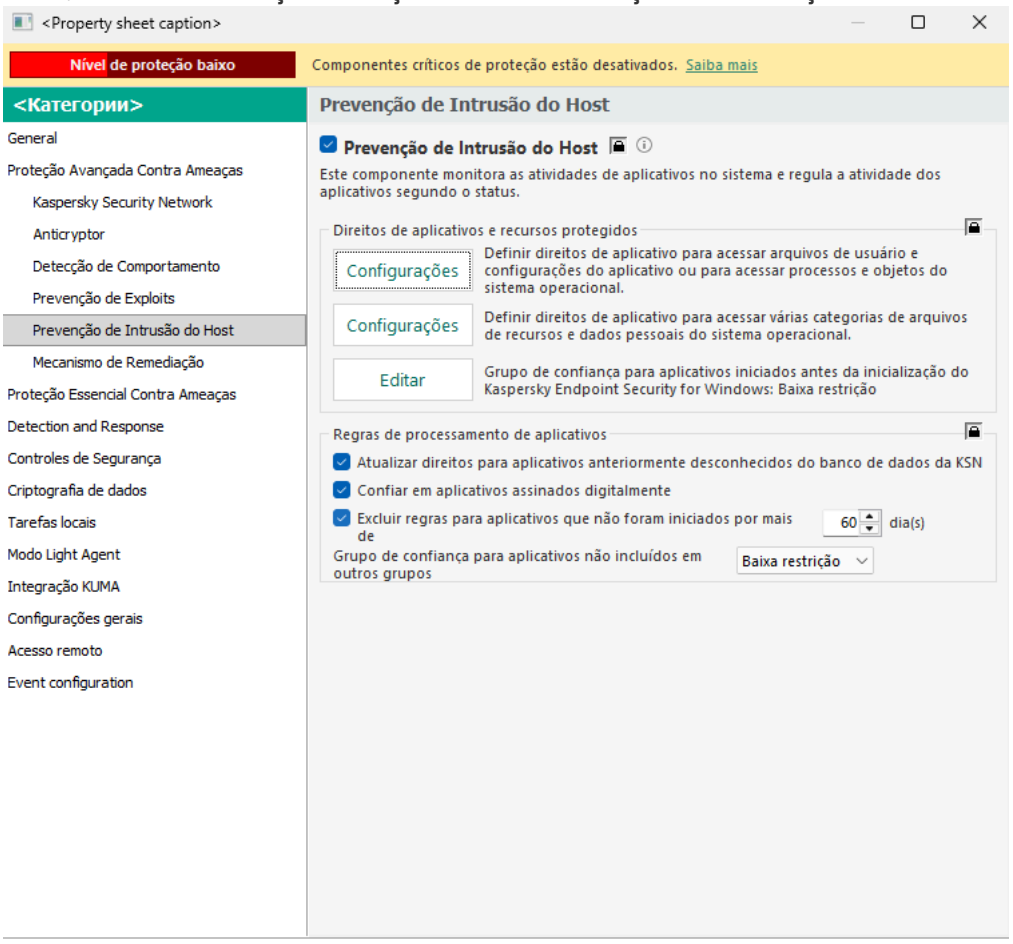
As regras criadas para aplicativos são herdadas pelos aplicativos secundários. Por exemplo, se todas as atividades de rede para o cmd.exe forem negadas, todas as atividade também serão negadas para o notepad.exe quando ele for iniciado usando o cmd.exe. Quando um aplicativo não é secundário ao aplicativo a partir do qual é executado, as regras não são herdadas.

Como alterar ou remover direitos de aplicativos no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.



Configurações da Prevenção de Intrusões

4. No bloco **Direitos de aplicativos e recursos protegidos**, clique no botão **Configurações**.

   Isso abre a janela de configuração de Direitos de aplicativos e a lista de Recursos protegidos.

5. Vá para a guia **Direitos de aplicativos**.

6. Clique **Adicionar**.

7. Na janela que é aberta, insira os critérios para buscar o aplicativo cujos direitos deseja alterar.

   É possível inserir o nome do aplicativo ou o nome do fornecedor. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.

8. Clique **Atualizar**.

   O Kaspersky Endpoint Security pesquisará o aplicativo na lista consolidada de aplicativos instalados em computadores gerenciados. O Kaspersky Endpoint Security exibirá uma lista de aplicativos que satisfazem os critérios de pesquisa.

9. Selecione o aplicativo desejado.

10. Na lista suspensa **Adicionar o aplicativo selecionado ao grupo de confiança**, selecione **Grupos padrão** e clique em **OK**.

    O aplicativo será adicionado ao grupos padrão.

11. Selecione o aplicativo relevante e, então, selecione os **Direitos de aplicativos** a partir do menu de contexto do aplicativo.

    Isso abre as propriedades do aplicativo.

12. Realize uma das seguintes ações:

    - Caso queira editar os direitos do grupo de confiança que regem as operações com o registro do sistema operacional, arquivos do usuário e configurações do aplicativo, selecione **Registro do sistema e arquivos**.

    - Caso queira editar os direitos do grupo de confiança que regem o acesso aos processos e objetos do sistema operacional, selecione **Direitos**.

    A atividade de rede dos aplicativos é controlada pelo componente Firewall por meio das *regras de rede*.

13. Para o recurso relevante, na coluna da ação correspondente, clique com o botão direito do mouse para abrir o menu de contexto e selecionar a opção necessária: **Herdar**, **Permitir** (✓) ou **Bloquear** (⊘).

14. Caso queira monitorar o uso dos recursos do computador, selecione **Criar log de eventos** (✓ / ⊘).

    O Kaspersky Endpoint Security registrará as informações sobre o funcionamento do componente Prevenção de intrusão do host. Os relatórios contêm informações sobre as operações com recursos de computador realizados pelo aplicativo (permitidas ou proibidas). Os relatórios também contêm informações sobre os aplicativos que utilizam cada recurso.

15. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como alterar direitos de aplicativos no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Proteção Contra Ameaças ao Host** → **Prevenção de Intrusão do Host**.

5. No bloco **Direitos de aplicativos e recursos protegidos**, clique no link **Direitos de aplicativos e recursos protegidos**.

   Isso abre a janela de configuração de Direitos de aplicativos e a lista de Recursos protegidos.

6. Vá para a guia **Direitos de aplicativos**.

   Uma lista de Grupos de confiança será exibida no lado esquerdo da janela e suas propriedades no lado direito.

7. Clique **Adicionar**.

   Então, o assistente para adicionar um aplicativo a um grupo de confiança será iniciado.

8. Selecione um grupo de confiança relevante para o aplicativo.

9. Selecione o tipo de **Aplicativo**. Vá para a próxima etapa.

   Caso queira alterar o grupo de confiança para múltiplos aplicativos, selecione o tipo de **Grupo** e defina um nome para o grupo de aplicativos.

10. Na lista de aplicativos aberta, selecione os aplicativos cujos direitos deseja alterar.

    Usar um filtro. É possível inserir o nome do aplicativo ou o nome do fornecedor. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.

11. Conclua o assistente.

    O aplicativo será adicionado ao grupo de confiança.

12. Na parte esquerda da janela, selecione o aplicativo relevante.

13. Na parte direita da janela, na lista suspensa, efetue uma das seguintes opções:

    - Caso queira editar os direitos do grupo de confiança que regem as operações com o registro do sistema operacional, arquivos do usuário e configurações do aplicativo, selecione **Registro do sistema e arquivos**.

    - Caso queira editar os direitos do grupo de confiança que regem o acesso aos processos e objetos do sistema operacional, selecione **Direitos**.

    A atividade de rede dos aplicativos é controlada pelo componente Firewall por meio das *regras de rede*.

14. Para o recurso relevante, na coluna da ação correspondente, selecione a opção necessária: **Herdar**, **Permitir** ( ), **Bloquear** ( ).

15. Caso queira monitorar o uso dos recursos do computador, selecione **Criar log de eventos** (/).

    O Kaspersky Endpoint Security registrará as informações sobre o funcionamento do componente Prevenção de intrusão do host. Os relatórios contêm informações sobre as operações com recursos de computador realizados pelo aplicativo (permitidas ou proibidas). Os relatórios também contêm informações sobre os aplicativos que utilizam cada recurso.

16. Salvar alterações.

Como alterar os direitos de aplicativos na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .

2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.

3. Clique **Gerenciar aplicativos**.

   Aparecerá a lista dos aplicativos instalados.

4. Selecione o aplicativo desejado.

5. No menu de contexto do aplicativo, selecione **Detalhes e regras**.

   Isso abre as propriedades do aplicativo.

6. Realize uma das seguintes ações:

   - Caso queira editar os direitos do grupo de confiança que regem as operações com o registro do sistema operacional, arquivos do usuário e configurações do aplicativo, selecione **Registro do sistema e arquivos**.

   - Caso queira editar os direitos do grupo de confiança que regem o acesso aos processos e objetos do sistema operacional, selecione **Direitos**.

7. Para o recurso relevante, na coluna da ação correspondente, clique com o botão direito do mouse para abrir o menu de contexto e selecionar a opção necessária: **Herdar**, **Permitir** ( ) ou **Negar** ( ).

8. Caso queira monitorar o uso dos recursos do computador, selecione **Registrar eventos** ( ).

   O Kaspersky Endpoint Security registrará as informações sobre o funcionamento do componente Prevenção de intrusão do host. Os relatórios contêm informações sobre as operações com recursos de computador realizados pelo aplicativo (permitidas ou proibidas). Os relatórios também contêm informações sobre os aplicativos que utilizam cada recurso.

9. Selecione a guia **Exclusões** e configure as configurações avançadas do aplicativo (veja a tabela abaixo).

10. Salvar alterações.

Configurações avançadas do aplicativo

Parâmetro	Descrição
Não verificar arquivos abertos por este aplicativo	Todos os arquivos abertos pelo aplicativo são excluídos das verificações pelo Kaspersky Endpoint Security. Por exemplo, se você estiver usando aplicativos para fazer backup de arquivos, este recurso ajuda a reduzir o consumo de recursos pelo Kaspersky Endpoint Security.
Não monitorar a atividade do aplicativo	O Kaspersky Endpoint Security não monitorará os arquivos do aplicativo e a atividade de rede no sistema operacional. Você pode configurar o monitoramento da atividade dos aplicativos para diferentes componentes do Kaspersky Endpoint Security: • **Não monitorar componentes de proteção e controle**. A atividade do aplicativo é monitorada pelos seguintes componentes: Detecção de Comportamento, Prevenção de Exploit, Prevenção de Intrusão do Host, Mecanismo de Remediação e Firewall. • **Não monitorar para Managed Detection and Response e Endpoint Detection and Response**. A atividade do aplicativo é monitorada pelo MDR Agent integrado e pelo EDR (KATA) Agent integrado. • **Não interceptar a entrada interativa do console para o Endpoint Detection and Response**. O Kaspersky Endpoint Security não envia dados de telemetria sobre o gerenciamento do aplicativo no console. Os dados de telemetria são usados pela Kaspersky Anti Targeted Attack Platform (EDR).
Não herdar restrições do processo principal (aplicativo)	As restrições configuradas para o processo pai não serão aplicadas pelo Kaspersky Endpoint Security a um processo filho. O processo pai é iniciado por um aplicativo para o qual os direitos do aplicativo (Prevenção de Intrusão do Host) e as Regras de rede de aplicativos (Firewall) são configurados.
Não monitorar a atividade de aplicativos secundários	O Kaspersky Endpoint 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.
Permitir a interação com a interface do Kaspersky Endpoint Security	A Autodefesa do Kaspersky Endpoint 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 Endpoint Security pela interface do Kaspersky Endpoint Security.
Não verificar tráfego criptografado / Não verificar todo o tráfego	O tráfego de rede iniciado pelo aplicativo será excluído das verificações pelo Kaspersky Endpoint Security. Você pode excluir todo o tráfego ou apenas o tráfego criptografado das verificações. Você também pode excluir endereços IP individuais e números de porta das verificações. O Kaspersky Endpoint Security versão 14.0 ou anterior não é compatível com a exclusão do tráfego de rede se um hash for especificado para um aplicativo confiável em vez de um caminho.

Proteger os recursos do sistema operacional e dados pessoais

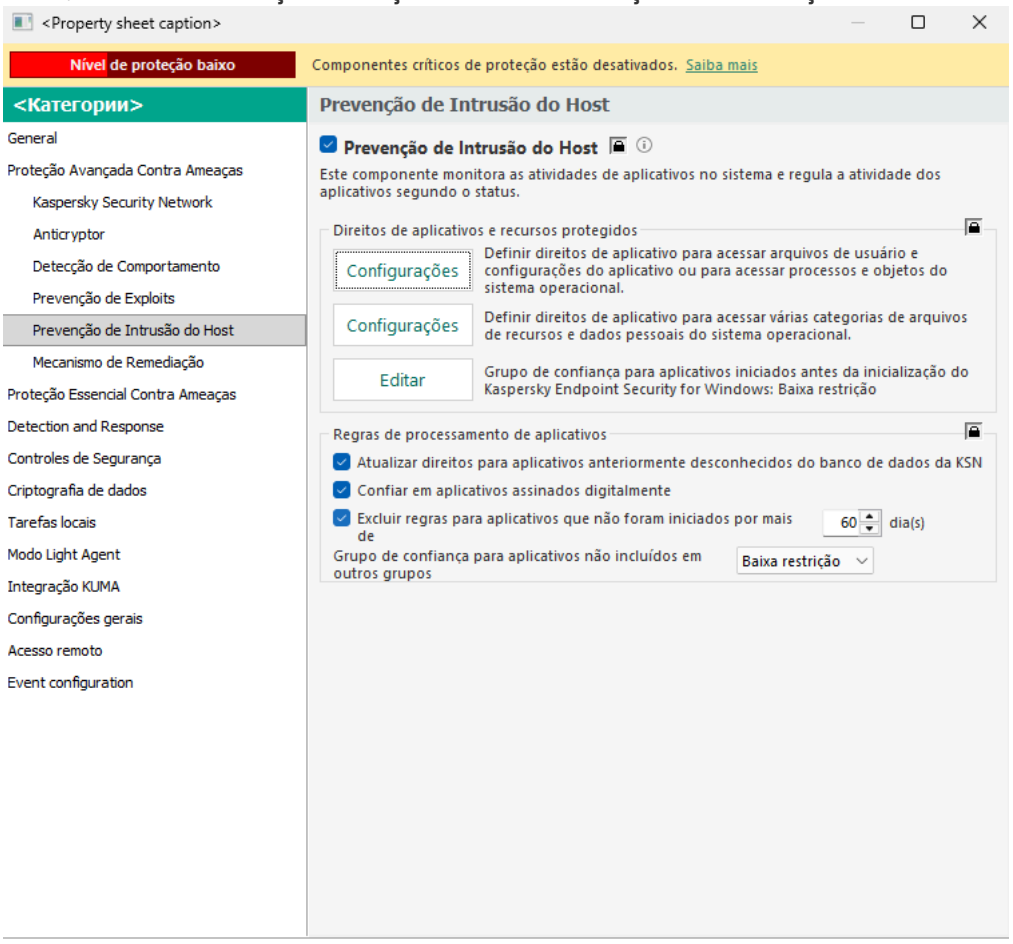
O componente Prevenção de Intrusão do Host gerencia os direitos de aplicativos para executar ações em várias categorias de recursos do sistema operacional e dados pessoais. Os especialistas da Kaspersky criaram categorias predefinidas de recursos protegidos. Por exemplo, a categoria *Sistema operacional* tem uma subcategoria *Configurações de inicialização* que lista todas as chaves de registro associadas à execução automática de aplicativos. As categorias predefinidas de recursos protegidos ou as categorias de recursos protegidos sob estas categorias não podem ser editadas ou excluídas.

Como adicionar um recurso protegido ao Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.



Configurações da Prevenção de Intrusões

4. No bloco **Direitos de aplicativos e recursos protegidos**, clique no botão **Configurações**.

   Isso abre a janela de configuração de Direitos de aplicativos e a lista de Recursos protegidos.

5. Vá para a guia **Recursos protegidos**.

   Uma lista de recursos protegidos aparecerá na parte esquerda da janela, bem como direitos de acesso correspondentes a esses recursos, dependendo do grupo de confiança específico.

6. Selecione a categoria de recursos protegidos aos quais deseja adicionar um novo recurso protegido.

   Caso queira adicionar uma subcategoria, clique em **Adicionar** → **Categoria**.

7. Clique no botão **Adicionar**. Na lista suspensa, selecione o tipo do recurso a ser adicionado: **Arquivo ou pasta** ou **Chave de registro**.

8. Na janela que é aberta, selecione um arquivo, uma pasta ou uma chave de registro.

   Será possível visualizar os direitos de acesso dos aplicativos aos recursos adicionados. Para isso, selecione um recurso adicionado na parte esquerda da janela e o Kaspersky Endpoint Security exibirá os direitos de acesso para cada grupo de confiança. Também é possível desativar o controle da atividade dos aplicativos com recursos usando a caixa de seleção ao lado de um novo recurso.

9. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como adicionar um recurso protegido no Web Console e no Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Proteção Contra Ameaças ao Host** → **Prevenção de Intrusão do Host**.
5. No bloco **Direitos de aplicativos e recursos protegidos**, clique no link **Direitos de aplicativos e recursos protegidos**.

   Isso abre a janela de configuração de Direitos de aplicativos e a lista de Recursos protegidos.
6. Vá para a guia **Recursos protegidos**.

   Uma lista de recursos protegidos aparecerá na parte esquerda da janela, bem como direitos de acesso correspondentes a esses recursos, dependendo do grupo de confiança específico.
7. Clique **Adicionar**.

   O assistente de novo recurso é iniciado.
8. No bloco **Nome do grupo**, selecione a categoria de recursos protegidos à qual pretende adicionar um novo recurso protegido.

   Caso queira adicionar uma subcategoria, selecione a opção **Categoria de recursos protegidos**.
9. Selecione o tipo de recurso a ser adicionado: **Arquivo ou pasta** ou **Chave de registro**.
10. Selecione um arquivo, pasta ou chave de registro.
11. Conclua o assistente.

    Será possível visualizar os direitos de acesso dos aplicativos aos recursos adicionados. Para isso, selecione um recurso adicionado na parte esquerda da janela e o Kaspersky Endpoint Security exibirá os direitos de acesso para cada grupo de confiança. Também é possível usar a caixa de seleção na coluna **Status** para desativar o controle de atividade do aplicativo com recursos.
12. Salvar alterações.

Como adicionar um recurso protegido na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.
3. Clique **Gerenciar recursos**.

   A lista de recursos protegidos é aberta.
4. Selecione a categoria de recursos protegidos aos quais deseja adicionar um novo recurso protegido.

   Caso queira adicionar uma subcategoria, clique em **Adicionar** → **Categoria**.
5. Clique no botão **Adicionar**. Na lista suspensa, selecione o tipo do recurso a ser adicionado: **Arquivo ou pasta** ou **Chave de registro**.

6. Na janela que é aberta, selecione um arquivo, uma pasta ou uma chave de registro.

   Será possível visualizar os direitos de acesso dos aplicativos aos recursos adicionados. Para fazer isso, selecione um recurso adicionado na parte esquerda da janela e o Kaspersky Endpoint Security exibirá uma lista de aplicativos e os direitos de acesso para cada um deles. Também é possível desativar o controle de atividade do aplicativo com recursos usando o botão **Ativar o controle** na coluna **Status**.

7. Salvar alterações.

O Kaspersky Endpoint Security controlará o acesso aos recursos do sistema operacional adicionados e aos dados pessoais. O Kaspersky Endpoint Security controla o acesso de um aplicativo aos recursos com base no grupo de confiança atribuído ao aplicativo. Também é possível alterar o grupo de confiança de um aplicativo.

Exclusão de informações sobre aplicativos não utilizados

O Kaspersky Endpoint Security usa direitos de aplicativos para controlar as atividades dos aplicativos. Os direitos de aplicativos são determinados pelo seu grupo confiável. O Kaspersky Endpoint Security coloca um aplicativo em um grupo de confiança quando ele é iniciado pela primeira vez. Você pode modificar manualmente o grupo confiável de um aplicativo. Você também pode configurar manualmente os direitos de um aplicativo individual. O Kaspersky Endpoint Security armazena as seguintes informações sobre um aplicativo: grupo confiável do aplicativo e direitos do aplicativo.

O Kaspersky Endpoint Security exclui automaticamente as informações sobre aplicativos não utilizados para economizar recursos do computador. O Kaspersky Endpoint Security exclui as informações do aplicativo de acordo com as seguintes regras:

- Se o grupo confiável e os direitos de um aplicativo forem determinados automaticamente, o Kaspersky Endpoint Security exclui as informações sobre esse aplicativo após 30 dias. Não é possível alterar o período de armazenamento para as informações do aplicativo ou desativar a exclusão automática.

- Se você colocar manualmente um aplicativo em um grupo confiável ou configurar seus direitos de acesso, o Kaspersky Endpoint Security excluirá as informações sobre esse aplicativo depois de 60 dias (prazo de armazenamento padrão). Você pode alterar o prazo de armazenamento de informações do aplicativo ou desativar a exclusão automática (veja as instruções abaixo).

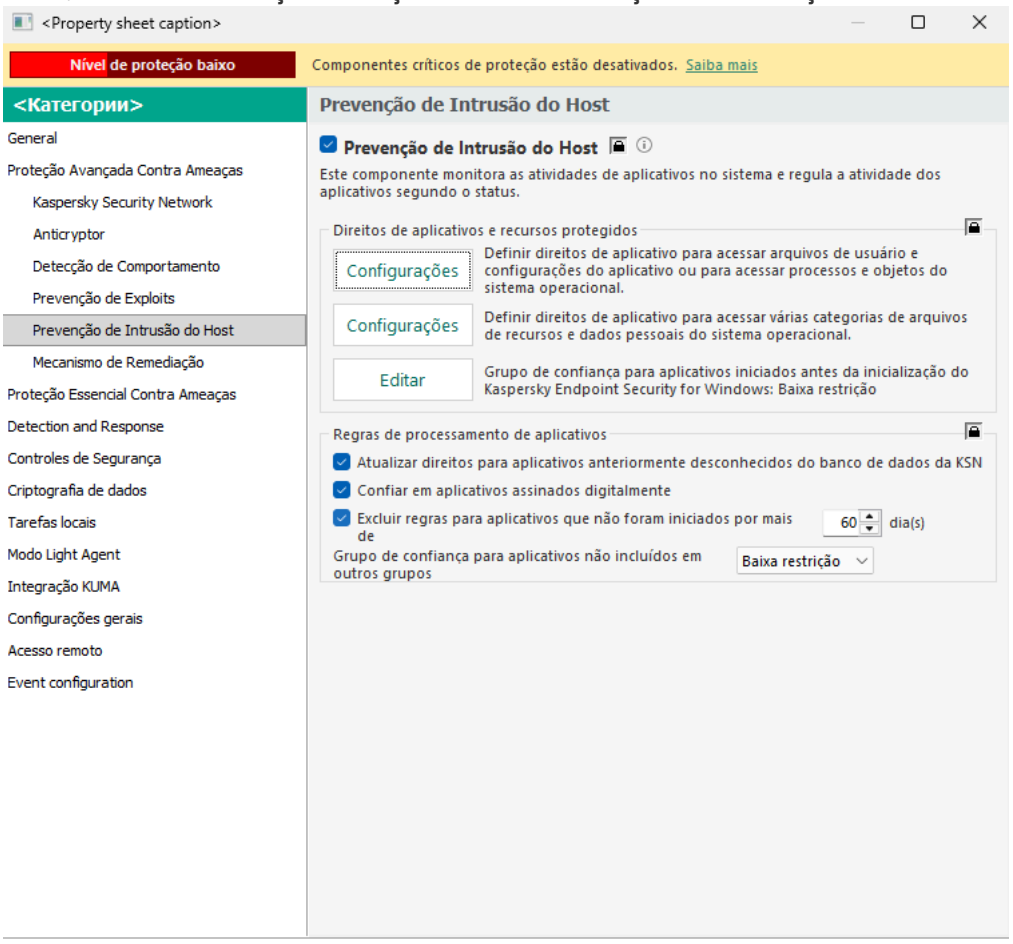
Quando você inicia um aplicativo cujas informações foram excluídas, o Kaspersky Endpoint Security analisa o aplicativo como se estivesse iniciando-o pela primeira vez.

Como configurar a exclusão automática de informações sobre aplicativos não usados no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.



Configurações da Prevenção de Intrusões

4. No bloco **Regras de processamento de aplicativos**, execute uma das seguintes ações:

- Caso queira configurar a exclusão automática, marque a caixa de seleção **Excluir regras para aplicativos que não foram iniciados por mais de N dia(s)** e especifique o número de dias.

  As informações sobre os aplicativos colocados manualmente em um grupo de confiança ou cujos direitos de acesso configurados manualmente serão excluídos pelo Kaspersky Endpoint Security, após o número de dias definidos. As informações sobre aplicativos cujo grupos de confiança e direitos de aplicativos foram determinados automaticamente também serão excluídas pelo Kaspersky Endpoint Security após 30 dias.

- Caso queira desativar a exclusão automática, desmarque a caixa de seleção **Excluir regras para aplicativos que não foram iniciados por mais de N dia(s)**.

  As informações sobre os aplicativos que você coloca manualmente em um grupo confiável ou cujos direitos de acesso configurados manualmente serão armazenados pelo Kaspersky Endpoint Security indefinidamente, sem nenhum limite de prazo de armazenamento. O Kaspersky Endpoint Security excluirá apenas as informações sobre os aplicativos cujo grupo de confiança e direitos de aplicativo foram determinados após 30 dias.

5. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como configurar a exclusão automática de informações sobre aplicativos não usados no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Proteção Contra Ameaças ao Host** → **Prevenção de Intrusão do Host**.

5. No bloco **Regras de processamento de aplicativos**, execute uma das seguintes ações:

   - Caso queira configurar a exclusão automática, marque a caixa de seleção **Excluir regras para aplicativos não iniciados por mais de (dias, 1 a 90)** e insira o número de dias.

     As informações sobre os aplicativos colocados manualmente em um grupo de confiança ou cujos direitos de acesso configurados manualmente serão excluídos pelo Kaspersky Endpoint Security, após o número de dias definidos. As informações sobre aplicativos cujo grupos de confiança e direitos de aplicativos foram determinados automaticamente também serão excluídas pelo Kaspersky Endpoint Security após 30 dias.

   - Caso queira desativar a exclusão automática, desmarque a caixa de seleção **Excluir regras para aplicativos não iniciados por mais de (dias, 1 a 90)**.

     As informações sobre os aplicativos que você coloca manualmente em um grupo confiável ou cujos direitos de acesso configurados manualmente serão armazenados pelo Kaspersky Endpoint Security indefinidamente, sem nenhum limite de prazo de armazenamento. O Kaspersky Endpoint Security excluirá apenas as informações sobre os aplicativos cujo grupo de confiança e direitos de aplicativo foram determinados após 30 dias.

6. Salvar alterações.

Como configurar a exclusão automática de informações sobre aplicativos não usados na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Intrusão do Host**.

3. No bloco **Regras de processamento de aplicativos**, execute uma das seguintes ações:

   - Caso queira configurar a exclusão automática, marque a caixa de seleção **Excluir regras para aplicativos não iniciados por mais de N dias (de 1 a 90)** e especifique o número de dias.

     As informações sobre os aplicativos colocados manualmente em um grupo de confiança ou cujos direitos de acesso configurados manualmente serão excluídos pelo Kaspersky Endpoint Security, após o número de dias definidos. As informações sobre aplicativos cujo grupos de confiança e direitos de aplicativos foram determinados automaticamente também serão excluídas pelo Kaspersky Endpoint Security após 30 dias.

   - Caso queira desativar a exclusão automática, desmarque a caixa de seleção **Excluir regras para aplicativos não iniciados por mais de N dias (de 1 a 90)**.

     As informações sobre os aplicativos que você coloca manualmente em um grupo confiável ou cujos direitos de acesso configurados manualmente serão armazenados pelo Kaspersky Endpoint Security indefinidamente, sem nenhum limite de prazo de armazenamento. O Kaspersky Endpoint Security excluirá apenas as informações sobre os aplicativos cujo grupo de confiança e direitos de aplicativo foram determinados após 30 dias.

4. Salvar alterações.

Monitoramento de Prevenção de Intrusão do Host

É possível receber relatórios sobre o funcionamento do componente de Prevenção de Intrusão do Host. Os relatórios contêm informações sobre as operações com recursos de computador realizados pelo aplicativo (permitidas ou proibidas). Os relatórios também contêm informações sobre os aplicativos que utilizam cada recurso.

Para monitorar as operações de Prevenção de Intrusão do Host, é necessário ativar a gravação de relatórios. Por exemplo, é possível ativar o envio de relatórios para aplicativos individuais nas configurações do componente de Prevenção de Intrusão do Host.

Ao configurar o monitoramento da Prevenção de Intrusão do Host, leve em consideração a carga potencial da rede ao encaminhar eventos para o Kaspersky Security Center. Também é possível ativar a gravação de relatórios somente no log local do Kaspersky Endpoint Security.

Proteção do acesso a áudio e vídeo

A funcionalidade de proteção de sinal de áudio e a funcionalidade de proteção de acesso à webcam não são compatíveis em computadores baseados em Arm.

Os criminosos virtuais podem usar programas especiais para tentar obter acesso a dispositivos que gravam áudio e vídeo (como microfones ou webcams). O Kaspersky Endpoint Security controla quando os aplicativos recebem um fluxo de áudio ou vídeo e protege os dados contra a interceptação não autorizada.

Por padrão, o Kaspersky Endpoint Security permite receber fluxos de áudio e vídeo somente para aplicativos do grupo *Confiável*. Os aplicativos dos grupos *Baixa restrição*, *Alta restrição* e *Não confiável* não têm permissão para receber fluxos de áudio e vídeo de dispositivos. É possível manualmente permitir a recepção do fluxo de áudio de dispositivos de gravação de áudio pelos aplicativos.

Recursos especiais de proteção do fluxo de áudio

A proteção de fluxo de áudio tem as seguintes características especiais:

- O componente Prevenção de Intrusão do Host deve estar ativado para esta funcionalidade funcionar.
- Se o aplicativo começou a receber o fluxo de áudio antes que o componente Prevenção de Intrusão do Host fosse iniciado, o Kaspersky Endpoint Security permitirá ao aplicativo receber o fluxo de áudio e não mostrará nenhuma notificação.
- Se você moveu o aplicativo para o grupo *Não confiável* ou o grupo de *Alta restrição* depois que o aplicativo começou a receber o fluxo de áudio, o Kaspersky Endpoint Security permite ao aplicativo receber o fluxo de áudio e não mostra nenhuma notificação.

- Depois que as configurações de acesso do aplicativo a dispositivos de gravação de som forem modificadas (por exemplo, se a recepção do fluxo de áudio foi bloqueada para o aplicativo), ele deverá ser reiniciado para parar de receber o fluxo de áudio.

- O controle do acesso ao fluxo de áudio de dispositivos de gravação de som não depende de configurações de acesso à câmara da Web de um aplicativo.

- O Kaspersky Endpoint Security protege o acesso somente a microfones integrados e microfones externos. Outros dispositivos de transmissão de fluxo de áudio não são suportados.

- O Kaspersky Endpoint Security não pode garantir a proteção de um fluxo de áudio de tais dispositivos como câmeras DSLR, câmeras de vídeo portáteis, e câmeras de ação.

- Ao executar os aplicativos de gravação ou reprodução de áudio e vídeo pela primeira vez desde a instalação do Kaspersky Endpoint Security, a reprodução ou gravação de áudio e vídeo pode ser interrompida. Isto é necessário para ativar a funcionalidade que controla o acesso a dispositivos de gravação de som por aplicativos. O serviço do sistema que controla o hardware áudio será reiniciado quando o Kaspersky Endpoint Security for executado pela primeira vez.

Recursos especiais de proteção de acesso à webcam para aplicativos

A funcionalidade de proteção de acesso à webcam tem as seguintes considerações especiais e limitações:

- O aplicativo controla vídeo e imagens estáticas derivadas do processamento de dados da webcam.

- O aplicativo controla o fluxo de áudio se ele for parte do fluxo vídeo recebido da webcam.

- O aplicativo controla somente as webcams conectadas via USB ou IEEE1394 exibidas como dispositivos de geração de imagens no Gerenciador de Dispositivos do Windows.

- Kaspersky Endpoint Security suporta as seguintes webcams:

  - Logitech HD Webcam C270

  - Logitech HD Webcam C310

  - Logitech Webcam C210

  - Logitech Webcam Pro 9000

  - Logitech HD Webcam C525

  - Microsoft LifeCam VX-1000

  - Microsoft LifeCam VX-2000

  - Microsoft LifeCam VX-3000

  - Microsoft LifeCam VX-800

  - Microsoft LifeCam Cinema

  A Kaspersky não pode garantir o suporte de webcams que não estão especificadas nessa lista.

Prevenção contra ataque BadUSB

Alguns vírus modificam o firmware dos dispositivos USB para enganar o sistema operacional em detectar o dispositivo USB como um teclado. 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 como um teclado pelo sistema operacional, o aplicativo solicitará que o usuário insira um código numérico gerado pelo próprio aplicativo usando esse teclado ou, se disponível, o teclado virtual (veja a figura abaixo). Esse procedimento é conhecido como autorização do teclado.

Caso o código tenha sido digitado corretamente, o aplicativo salva 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 (ver figura abaixo), a aplicativo bloqueia a entrada a partir do 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.

Autorização do teclado

Ativar e desativar Prevenção contra ataque BadUSB

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 ou desativar o componente Prevenção contra ataque BadUSB no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Prevenção contra ataque BadUSB**.

4. Use a caixa de seleção **Prevenção contra ataque BadUSB** para ativar ou desativar o componente.

5. No bloco **Autorização do dispositivo USB após conexão**, ajuste as configurações de segurança para inserir o código de autorização:

   - **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, se você permitir cinco tentativas para inserir o código de autorização, o aplicativo bloqueará o dispositivo USB após a quinta tentativa malsucedida. O Kaspersky Endpoint Security exibe a duração do bloqueio do dispositivo USB. Após esse tempo, haverá novamente cinco tentativas para inserir o 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 inserir o código de autorização. Os valores válidos são de 1 a 180 (minutos).

6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar ou desativar o componente Prevenção contra ataque BadUSB no Web Console e Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Proteção Contra Ameaças ao Host** → **Prevenção contra ataque BadUSB**.

5. Use o botão de alternância do **Prevenção contra ataque BadUSB ATIVADA** para ativar ou desativar o componente.

6. No bloco **Autorização de dispositivos USB**, ajuste as configurações de segurança para inserir o código de autorização:

   - **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, se você permitir cinco tentativas para inserir o código de autorização, o aplicativo bloqueará o dispositivo USB após a quinta tentativa malsucedida. O Kaspersky Endpoint Security exibe a duração do bloqueio do dispositivo USB. Após esse tempo, haverá novamente cinco tentativas para inserir o código de autorização.

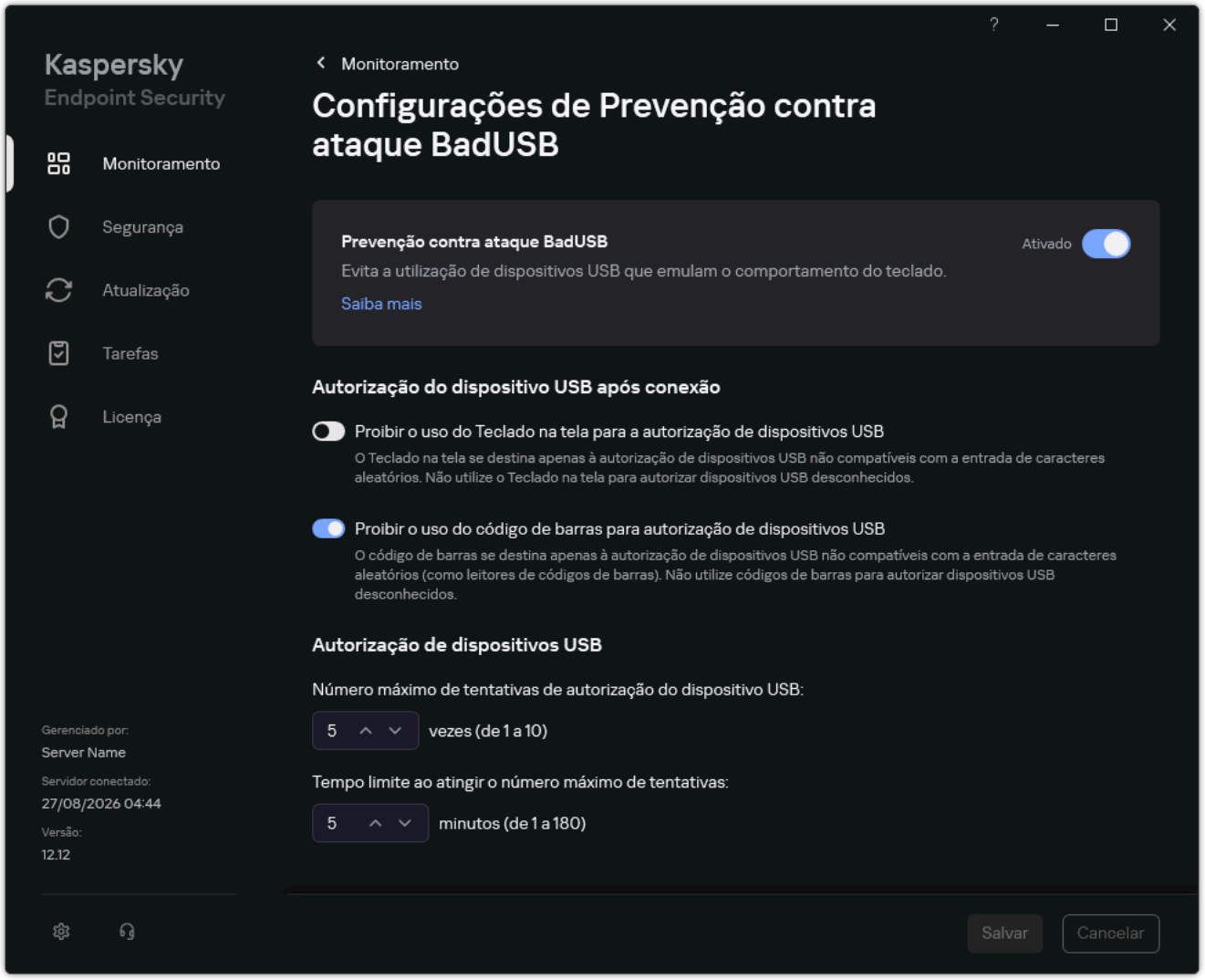
   - **Tempo limite ao atingir o número máximo de tentativas (min)**. Duração do bloqueio do dispositivo USB após o número especificado de tentativas malsucedidas de inserir o código de autorização. Os valores válidos são de 1 a 180 (minutos).

7. Salvar alterações.

Como ativar ou desativar o componente Prevenção contra ataque BadUSB na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Prevenção contra ataque BadUSB**.



Configurações do componente Prevenção contra ataque BadUSB

3. Use o botão de alternância do **Prevenção contra ataque BadUSB** para ativar ou desativar o componente.

4. No bloco **Autorização do dispositivo USB após conexão**, ajuste as configurações de segurança para inserir o código de autorização:

   - **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, se você permitir cinco tentativas para inserir o código de autorização, o aplicativo bloqueará o dispositivo USB após a quinta tentativa malsucedida. O Kaspersky Endpoint Security exibe a duração do bloqueio do dispositivo USB. Após esse tempo, haverá novamente cinco tentativas para inserir o código de autorização.

   - **Tempo limite ao atingir o número máximo de tentativas**. Duração do bloqueio do dispositivo USB após o número especificado de tentativas malsucedidas de inserir o código de autorização. Os valores válidos são de 1 a 180 (minutos).

5. Salvar alterações.

Como resultado, se a Prevenção contra ataque BadUSB estiver ativada, o Kaspersky Endpoint Security exigirá a autorização de um dispositivo USB conectado identificado como um teclado pelo sistema operacional. O usuário não pode utilizar um teclado não autorizado até que ele esteja autorizado.

Uso do teclado na tela para a autorização de dispositivos USB

O Teclado na tela deveria apenas ser utilizado para autorização de dispositivos USB que não suportam a entrada de caracteres aleatórios (leitores de códigos de barras, por exemplo). Não é recomendado utilizar o Teclado Virtual para autorização de dispositivos USB desconhecidos.

Como permitir ou proibir o uso do Teclado na tela para autorização no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Prevenção contra ataque BadUSB**.

4. Use a caixa de seleção **Proibir o uso do Teclado na tela para a autorização de dispositivos USB** para bloquear ou permitir o uso do Teclado Virtual para autorização.

5. Salvar alterações.

Como permitir ou proibir o uso do Teclado na tela para autorização no Web Console e Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Proteção Contra Ameaças ao Host** → **Prevenção contra ataque BadUSB**.

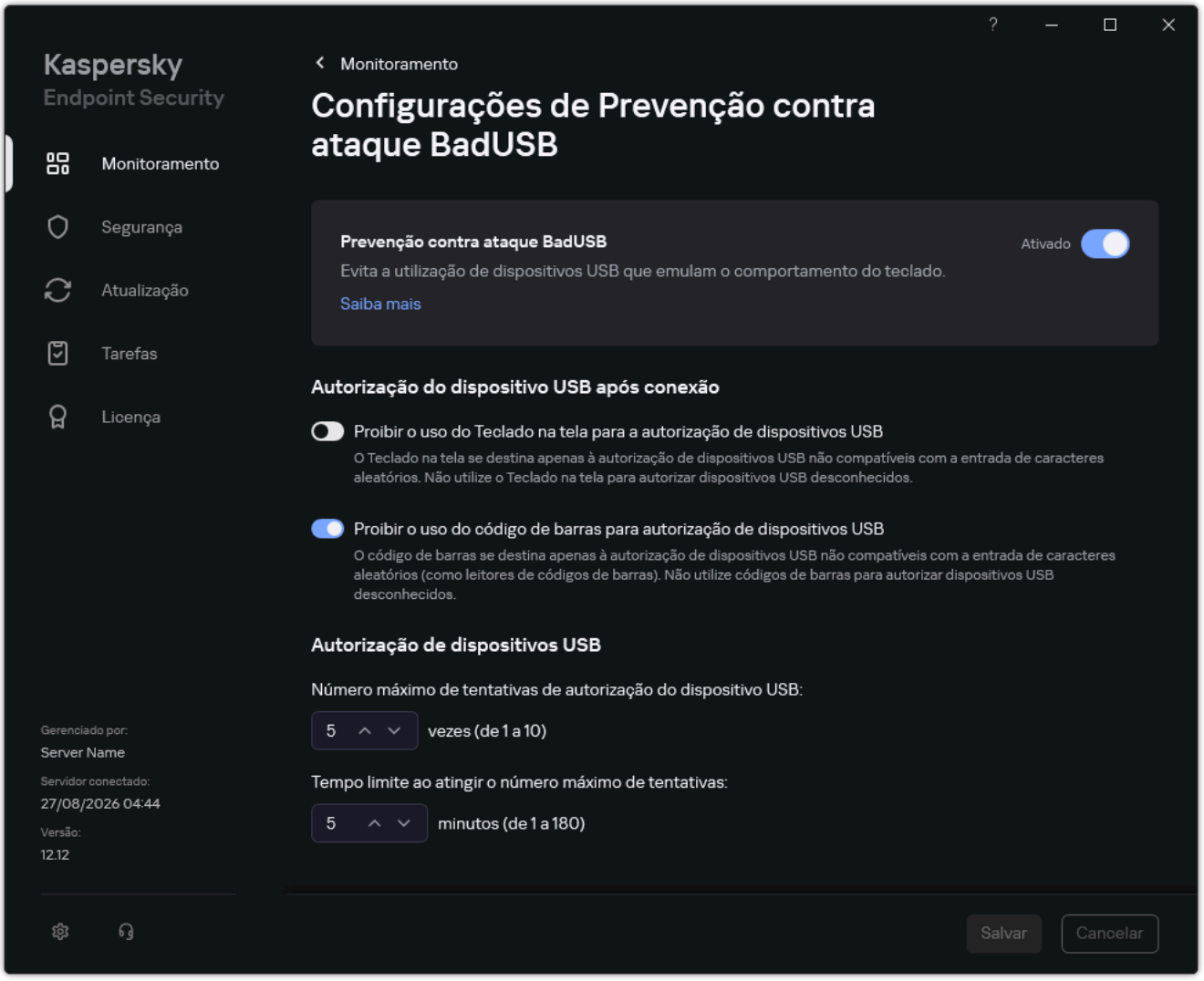
5. Use o botão de alternância **Proibir a utilização do Teclado na tela para autorização de dispositivos USB** para bloquear ou permitir o uso do Teclado na tela para autorização.

6. Salvar alterações.

Como permitir ou proibir o uso do Teclado na tela para autorização na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Prevenção contra ataque BadUSB**.



Configurações do componente Prevenção contra ataque BadUSB

3. Use o botão de alternância **Proibir o uso do Teclado na tela para a autorização de dispositivos USB** para bloquear ou permitir o uso do Teclado na tela para autorização.

4. Salvar alterações.

Autorização de dispositivos USB

Autorização do leitor de código de barras

Ao conectar um leitor de código de barras ao computador, o componente Prevenção contra ataque BadUSB identifica este dispositivo como um dispositivo de entrada e solicita que você execute a autorização. Para autorizar o leitor de código de barras, você deve ler um código de barras exibido na tela. O aplicativo gera um código de barras no formato Code39, que é compatível com a maioria dos leitores de código de barras e QR.

O Kaspersky Endpoint Security também é compatível com outro método de autorização do leitor de código de barras. Se você estiver usando dispositivos com tela sensível ao toque, poderá usar um teclado na tela para digitar um código. Para fazer isso, você precisa permitir o uso do teclado na tela. Este método é conveniente, por exemplo, no caso de leitores de código de barras fixos que estão embutidos em caixas registradoras. Outros métodos de autorização do leitor de código de barras são proibidos.

Por padrão, o aplicativo não usa um código de barras para autorização de dispositivos USB.

Como ativar a autorização do dispositivo USB por meio de código de barras no Console de Administração (MMC)

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

2. Na árvore do console, selecione **Políticas**.

3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

4. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Prevenção contra ataque BadUSB**.

5. Utilize a caixa de seleção **Proibir o uso do código de barras para autorização de dispositivos USB** para bloquear ou permitir o uso de códigos de barra para autorização.

6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar a autorização do dispositivo USB por meio de código de barras no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Proteção Contra Ameaças ao Host** → **Prevenção contra ataque BadUSB**.

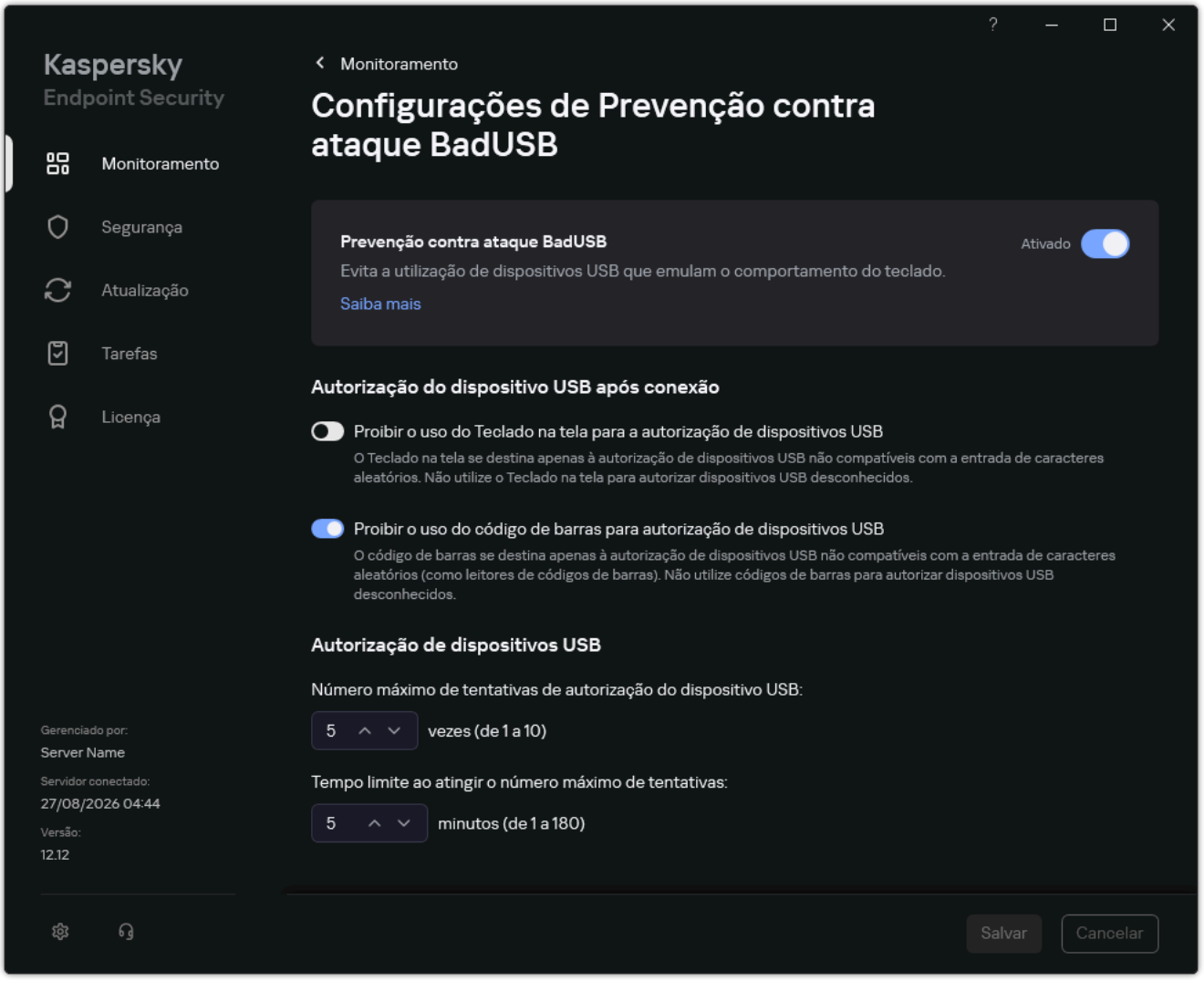
5. Utilize o botão de alternância **Proibir o uso do código de barras para autorização de dispositivos USB** para bloquear ou permitir o uso de códigos de barra para autorização.

6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar a autorização do dispositivo USB por meio de código de barras na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Prevenção contra ataque BadUSB**.



Configurações do componente Prevenção contra ataque BadUSB

3. Utilize o botão de alternância **Proibir o uso do código de barras para autorização de dispositivos USB** para bloquear ou permitir o uso de códigos de barra para autorização.

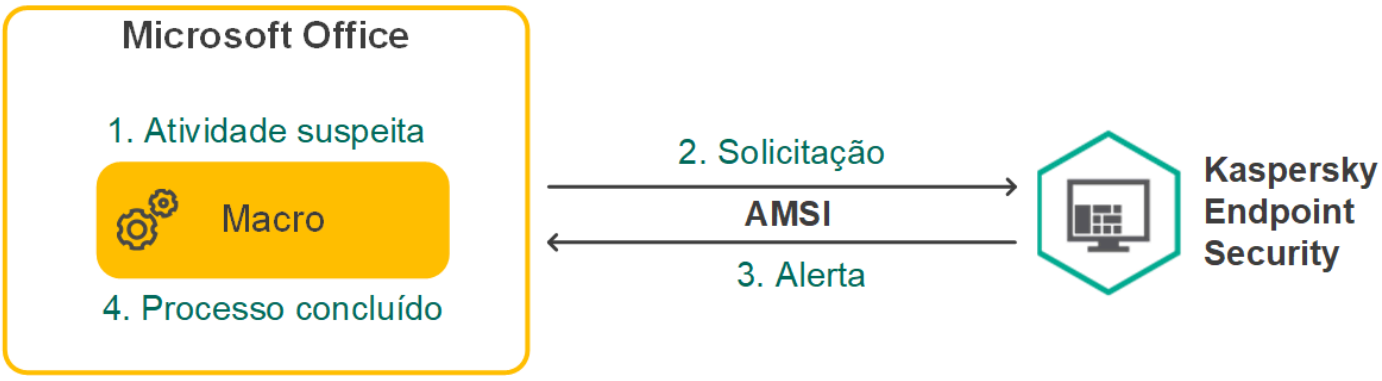
4. Salvar alterações.

Autorização do leitor de código de barras

Proteção AMSI

O componente de Proteção AMSI 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 Endpoint Security para uma verificação adicional e receber os resultados da verificação desses objetos. Aplicativos de terceiros podem incluir, por exemplo, aplicativos do Microsoft Office (veja a figura abaixo). Para obter detalhes sobre a AMSI, consulte a documentação da Microsoft.

A Proteção AMSI pode apenas detectar e notificar aplicativos de terceiros sobre a ameaça. Após receber uma notificação de uma ameaça, o aplicativo de terceiros não permite executar ações maliciosas (por exemplo, encerramentos a ação).



Exemplo de operação AMSI

O componente de Proteção AMSI pode recusar uma solicitação de um aplicativo de terceiros, por exemplo, se esse aplicativo exceder o número máximo de solicitações em um intervalo especificado. O Kaspersky Endpoint Security envia ao Servidor de Administração informações sobre uma solicitação rejeitada de um aplicativo de terceiros. O componente de proteção AMSI não nega as solicitações de aplicativos de terceiros para os quais a integração contínua com o componente de proteção AMSI está ativada.

A Proteção AMSI está disponível para os seguintes sistemas operacionais para estações de trabalho e servidores:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multisessão
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multisessão
- Windows Server 2016 Essentials / Standard / Datacenter (incluindo o modo Server Core)
- Windows Server 2019 Essentials / Standard / Datacenter (incluindo o modo Server Core)
- Windows Server 2022 Standard / Datacenter / Datacenter Azure Edition (incluindo o modo Server Core)
- Windows Server 2025 Standard / Datacenter

Ativar e desativar a proteção AMSI

Por padrão, a Proteção AMSI está ativada e funcionando no modo recomendado pela Kaspersky (consulte a tabela abaixo).

Como ativar ou desativar a Proteção AMSI no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **AMSI Scanner**.
4. Use a caixa de seleção **AMSI Scanner** para ativar ou desativar o componente.
5. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

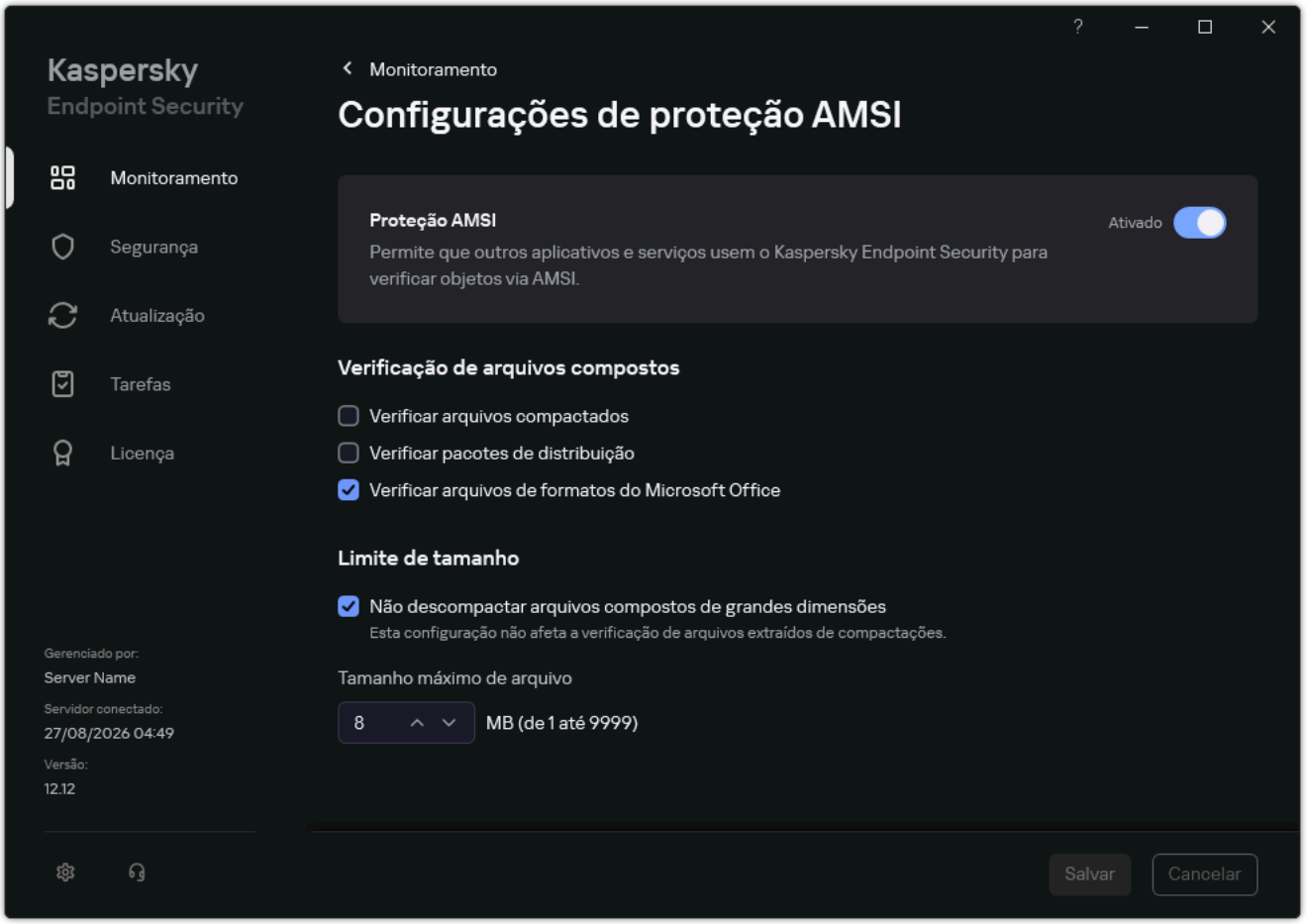
Como ativar ou desativar a Proteção AMSI no Web Console e Cloud Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Proteção Contra Ameaças ao Host** → **Proteção AMSI**.
5. Use o botão de alternância do **Proteção AMSI ATIVADA** para ativar ou desativar o componente.
6. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Como ativar ou desativar a Proteção AMSI na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção AMSI**.



Configurações de Proteção AMSI

3. Use o botão de alternância do **Proteção AMSI** para ativar ou desativar o componente.

4. Salvar alterações.

Configurações de proteção AMSI recomendadas por especialistas da Kaspersky

Parâmetro	Valor	Descrição
Verificar arquivos compactados	**Desativado**	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	**Desativado**	Verificação de pacotes de distribuição de aplicativos de terceiros.
Verificar arquivos de formatos do Microsoft Office	**Ativado**	Verifica arquivos do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Arquivos de formato do Office também incluem objetos OLE. O aplicativo verifica arquivos em formato do Office com menos de 1 MB, independentemente de a caixa de seleção estar marcada ou não.
Não descompactar arquivos compostos de grandes dimensões	**Tamanho máximo de arquivo 8 MB**	Se esta caixa de seleção for marcada, o aplicativo não verificará arquivos compostos se o tamanho deles exceder o valor especificado. Se esta caixa de seleção estiver desmarcada, o aplicativo verificará os arquivos compostos de todos os tamanhos. O aplicativo verifica arquivos grandes extraídos de arquivos compactados independentemente de a caixa de seleção estar selecionada ou não.

Otimização da verificação de arquivos pela Proteção AMSI

Pode otimizar a verificação dos arquivos: reduza o tempo da verificação e aumente a velocidade de processamento do Kaspersky Endpoint Security. É possível selecionar os arquivos compostos que precisam ser verificados: arquivos compactados, pacotes de distribuição ou arquivos em formatos do Office. Também é possível limitar o tamanho dos arquivos compostos a serem verificados. O componente de Proteção AMSI não descompactará arquivos compostos maiores do que o tamanho especificado.

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

Como otimizar a verificando de arquivos pela Proteção AMSI no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **AMSI Scanner**.

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 Proteção AMSI descompacte grandes arquivos compostos, marque a caixa de seleção **Não descompactar arquivos compostos grandes** e especifique o valor requerido. O componente de Proteção AMSI não descompactará arquivos compostos maiores do que o tamanho especificado.

   - Para permitir que o componente de Proteção AMSI descompacte grandes arquivos compostos, desmarque a caixa de seleção **Não descompactar arquivos compostos grandes**.

   O componente de Proteção AMSI verifica os arquivos grandes que foram extraídos dos arquivos, mesmo se a caixa de seleção **Não descompactar arquivos compostos grandes** estiver marcada.

6. Salvar alterações. Para aplicar a política em computadores, feche os cadeados 🔒.

Como otimizar a verificação de arquivos pela Proteção AMSI no Web Console e Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Proteção Contra Ameaças ao Host** → **Proteção AMSI**.

5. 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.

6. No bloco **Otimização da verificação**, execute uma das seguintes ações:

   - Para impedir que o componente de Proteção AMSI descompacte grandes arquivos compostos, marque a caixa de seleção **Limites de tamanho ativados** e especifique o valor requerido. O componente de Proteção AMSI não descompactará arquivos compostos maiores do que o tamanho especificado.

   - Para permitir que o componente de Proteção AMSI descompacte grandes arquivos compostos, desmarque a caixa de seleção **Limites de tamanho ativados**.

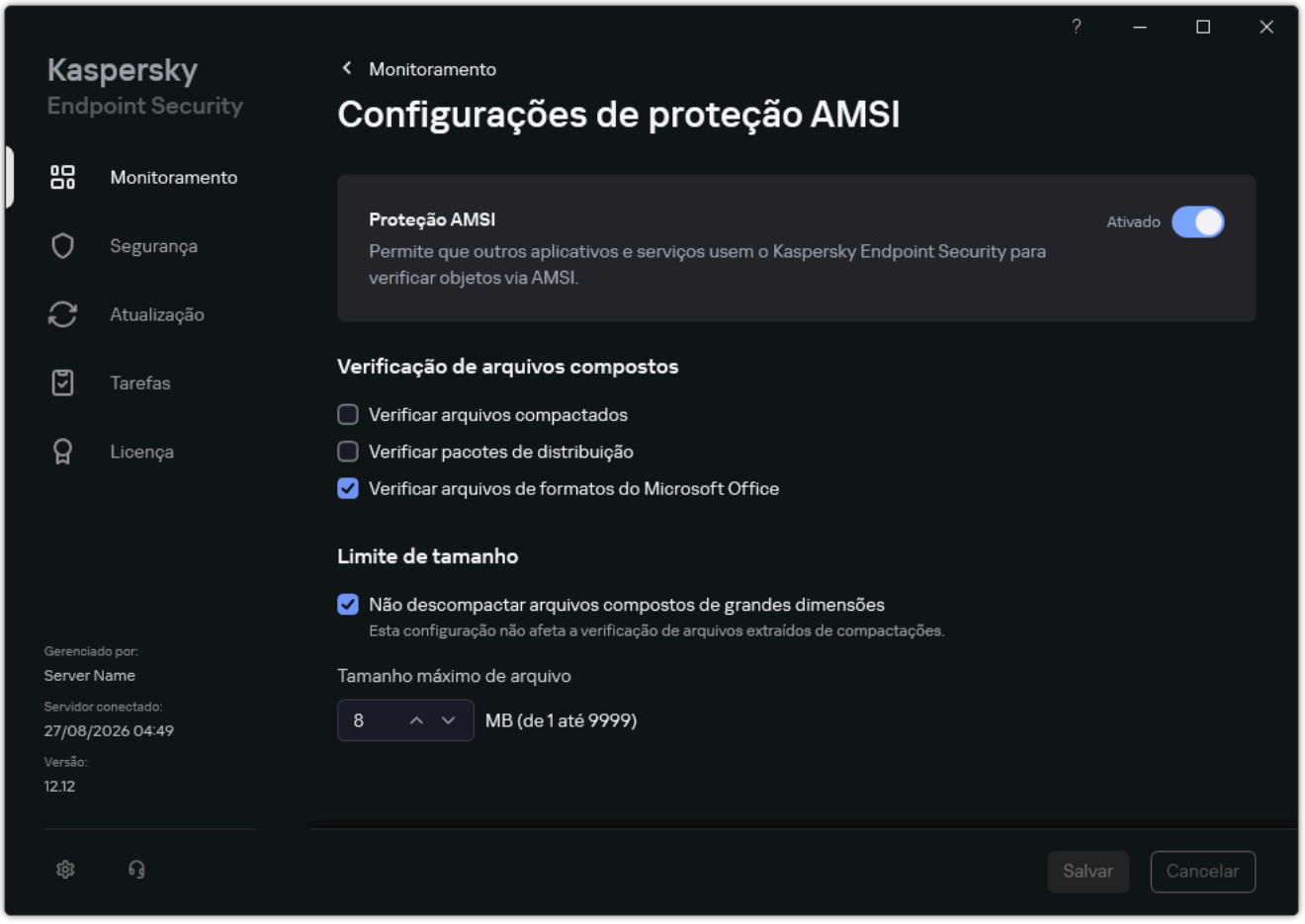
   O componente de Proteção AMSI verifica os arquivos grandes que foram extraídos dos arquivos, mesmo se a caixa de seleção **Limites de tamanho ativados** estiver marcada.

7. Salvar alterações. Para aplicar a política em computadores, feche os cadeados 🔒.

Como otimizar a verificação de arquivos pela Proteção AMSI na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças → Proteção AMSI**.



Configurações de Proteção AMSI

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 Proteção AMSI descompacte grandes arquivos compostos, marque a caixa de seleção **Não descompactar arquivos compostos de grandes dimensões** e especifique o valor requerido. O componente de Proteção AMSI não descompactará arquivos compostos maiores do que o tamanho especificado.

   - Para permitir que o componente de Proteção AMSI descompacte grandes arquivos compostos, desmarque a caixa de seleção **Não descompactar arquivos compostos de grandes dimensões**.

   O componente de Proteção AMSI verifica os arquivos grandes que foram extraídos dos arquivos, mesmo se a caixa de seleção **Não descompactar arquivos compostos de grandes dimensões** estiver marcada.

5. Salvar alterações.

Proteção Contra Ameaças da Web

O componente Proteção Contra Ameaças da Web impede o download de arquivos maliciosos da Internet e também bloqueia a conexão com sites maliciosos e de phishing. O componente fornece proteção ao computador com a ajuda de bancos de dados de antivírus, o serviço na nuvem Kaspersky Security Network e análise heurística.

O Kaspersky Endpoint Security verifica o tráfego HTTP, HTTPS e FTP. O Kaspersky Endpoint Security verifica URLs e endereços IP.

Para usar a Proteção Contra Ameaças da Web, você deve concluir a configuração inicial do aplicativo:

- Para o monitoramento de tráfego HTTPS, ative a verificação de conexões criptografadas (ativada por padrão).

- Selecione as portas que o Kaspersky Endpoint Security deve monitorar (por padrão, o aplicativo monitora todas as portas).

- Selecione os aplicativos cujo tráfego você deseja que o Kaspersky Endpoint Security monitore. A maioria dos navegadores já está presente na lista de aplicativos recomendados pela Kaspersky. Se o seu navegador não estiver na lista, adicione-o manualmente.

- Recomendamos injetar um script de interação de página da web no tráfego da Web (por padrão, a injeção de script está desabilitada). Esse script ativa o registro de eventos da Proteção Contra Ameaças da Web para o log de eventos do aplicativo, log de eventos do SO e relatórios.

Quando um usuário tenta abrir um site malicioso ou de phishing, o Kaspersky Endpoint Security bloqueará o acesso e exibirá um aviso.

Ativar e desativar a Proteção Contra Ameaças da Web

Por padrão, o componente Proteção Contra Ameaças da Web é ativado e executado no modo recomendado por especialistas da Kaspersky. Para Proteção Contra Ameaças da Web, o aplicativo pode aplicar diferentes grupos de configurações. Estes grupos de configurações armazenados no aplicativo são denominados *níveis de segurança*: **Alto**, **Recomendado**, **Baixo**. As configurações do nível de segurança **Recomendado** para tráfego da Web são consideradas as configurações ideais recomendadas pelos especialistas da Kaspersky (veja a tabela abaixo). Você pode selecionar um dos níveis de segurança de tráfego da Web predefinidos que é recebido e transmitido através dos protocolos HTTP e FTP, ou configurar um nível de segurança de tráfego da Web personalizado. A alteração das configurações do nível de segurança do nível de segurança de tráfego da Web não impede a reversão para o nível recomendado quando desejado.

É possível selecionar ou configurar o nível de segurança apenas no Console de Administração (MMC) ou na interface local do aplicativo. Não é possível selecionar ou configurar o nível de segurança no Web Console ou no Cloud Console.

Como ativar ou desativar o componente Proteção Contra Ameaças da Web no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças da Web**.
4. Use a caixa de seleção **Proteção Contra Ameaças da Web** para ativar ou desativar o componente.
5. Caso tenha ativado o componente, execute uma das seguintes operações no bloco **Nível de segurança**:
   - Caso queira aplicar um dos níveis de segurança pré-configurados, selecione-o com o controle deslizante:
     - **Alto**. O nível de segurança sob o qual o componente Proteção Contra Ameaças da Web executa a verificação máxima do tráfego da web que o computador recebe através dos protocolos de FTP e HTTP. A Proteção Contra Ameaças da Web verifica detalhadamente todos os objetos de tráfego da web, usando o conjunto completo de bancos de dados do aplicativo, e executa a análise heurística mais profunda possível.
     - **Recomendado**. O nível de segurança que fornece o equilíbrio ideal entre o desempenho do aplicativo e a segurança do tráfego da Web. O componente Proteção Contra Ameaças da Web executa a análise heurística no nível de verificação média. Esse nível de segurança do tráfego da Web é recomendado pelos especialistas da Kaspersky. Os valores das configurações para o nível de segurança recomendado são fornecidos na tabela abaixo.
     - **Baixo**. As configurações deste nível de segurança de tráfego da web asseguram a velocidade máxima de verificação de tráfego da web. O componente Proteção Contra Ameaças da Web executa a análise heurística no nível de verificação leve.
   - Caso queira configurar um nível de segurança personalizado, clique no botão **Configurações** e defina suas próprias configurações do componente (consulte a tabela abaixo).

     É possível restaurar os valores dos níveis de segurança predefinidos clicando no botão **Por padrão**.

6. No bloco **Ação ao detectar ameaça**, selecione a ação que o Kaspersky Endpoint Security deve executar em objetos maliciosos de tráfego da Web:

   - **Bloquear**. Se esta opção for selecionada, quando o componente Proteção Contra Ameaças da Web detectar um objeto infectado no tráfego da Web, ele bloqueará o acesso ao objeto e exibirá uma notificação no navegador.

   - **Informar**. Se essa opção estiver selecionada e um objeto infectado for detectado no tráfego da Web, o Kaspersky Endpoint Security permitirá que esse objeto seja baixado no computador, mas adicionará informações sobre o objeto infectado à lista de ameaças ativas.

7. Salvar alterações.

Como ativar ou desativar o componente Proteção Contra Ameaças da Web no Web Console

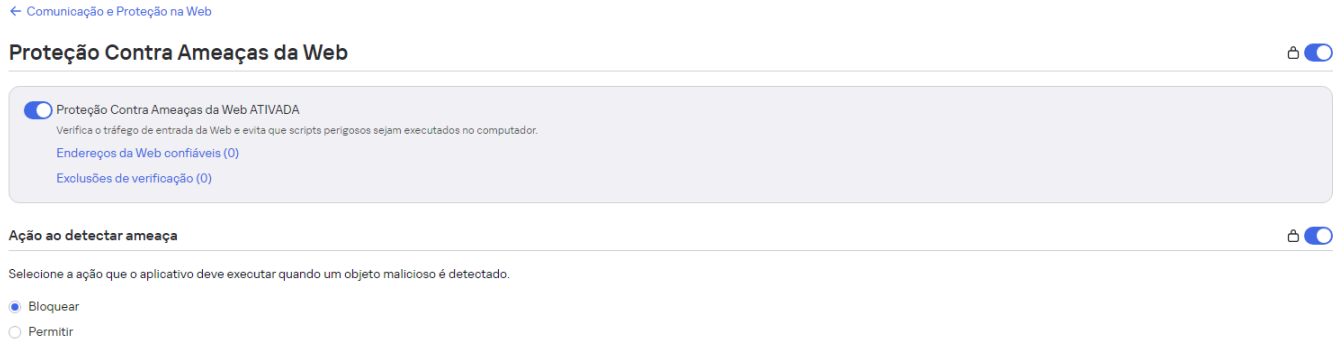
1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Comunicação e Proteção na Web** → **Proteção Contra Ameaças da Web**.



Configurações de Proteção Contra Ameaças da Web

5. Use o botão de alternância do **Proteção Contra Ameaças da Web ATIVADA** para ativar ou desativar o componente.

6. No bloco **Ação ao detectar ameaça**, selecione a ação que o Kaspersky Endpoint Security deve executar em objetos maliciosos de tráfego da Web:

   - **Bloquear**. Se esta opção for selecionada, quando o componente Proteção Contra Ameaças da Web detectar um objeto infectado no tráfego da Web, ele bloqueará o acesso ao objeto e exibirá uma notificação no navegador.

   - **Permitir, informar ou perguntar o que fazer (depende do SO)**. Se essa opção estiver selecionada e um objeto infectado for detectado no tráfego da Web, o Kaspersky Endpoint Security permitirá que esse objeto seja baixado no computador, mas adicionará informações sobre o objeto infectado à lista de ameaças ativas.

7. Caso seja necessário, faça uma lista de endereços da Web confiáveis.

8. Para aplicar a política aos computadores, feche os ícones de cadeado 🔒 e salve as alterações.

Como ativar ou desativar o componente Proteção Contra Ameaças da Web

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças da Web**.

3. Use o botão de alternância do **Proteção Contra Ameaças da Web** para ativar ou desativar o componente.

4. Caso tenha ativado o componente, execute uma das seguintes operações no bloco **Nível de segurança**:

   - Caso queira aplicar um dos níveis de segurança pré-configurados, selecione-o com o controle deslizante:

     - **Alto**. O nível de segurança sob o qual o componente Proteção Contra Ameaças da Web executa a verificação máxima do tráfego da web que o computador recebe através dos protocolos de FTP e HTTP. A Proteção Contra Ameaças da Web verifica detalhadamente todos os objetos de tráfego da web, usando o conjunto completo de bancos de dados do aplicativo, e executa a análise heurística mais profunda possível.

     - **Recomendado**. O nível de segurança que fornece o equilíbrio ideal entre o desempenho do aplicativo e a segurança do tráfego da Web. O componente Proteção Contra Ameaças da Web executa a análise heurística no nível de verificação média. Esse nível de segurança do tráfego da Web é recomendado pelos especialistas da Kaspersky. Os valores das configurações para o nível de segurança recomendado são fornecidos na tabela abaixo.

     - **Baixo**. As configurações deste nível de segurança de tráfego da web asseguram a velocidade máxima de verificação de tráfego da web. O componente Proteção Contra Ameaças da Web executa a análise heurística no nível de verificação leve.

   - Caso queira configurar um nível de segurança personalizado, clique no botão **Configurações avançadas** e defina suas próprias configurações do componente (consulte a tabela abaixo).

     É possível restaurar os valores dos níveis de segurança predefinidos clicando no botão **Restaurar nível de segurança recomendado**.

5. No bloco **Ação ao detectar ameaça**, selecione a ação que o Kaspersky Endpoint Security deve executar em objetos maliciosos de tráfego da Web:

   - **Bloquear**. Se esta opção for selecionada, quando o componente Proteção Contra Ameaças da Web detectar um objeto infectado no tráfego da Web, ele bloqueará o acesso ao objeto e exibirá uma notificação no navegador.

   - **Informar**. Se essa opção estiver selecionada e um objeto infectado for detectado no tráfego da Web, o Kaspersky Endpoint Security permitirá que esse objeto seja baixado no computador, mas adicionará informações sobre o objeto infectado à lista de ameaças ativas.

6. Salvar alterações.

Configurações de Proteção Contra Ameaças da Web recomendadas pelos especialistas da Kaspersky (nível de segurança recomendado)

Parâmetro	Valor	Descrição
Verificar se o endereço está no banco de dados de endereços da Web maliciosos	**Ativado**	A verificação de links para determinar se estão incluídos no banco de dados de endereços da Web maliciosos permite rastrear sites que foram incluídos na lista de bloqueio. O banco de dados de endereços Web maliciosos é mantido pela Kaspersky, incluído no pacote de instalação do aplicativo e atualizado durante as atualizações do banco de dados do Kaspersky Endpoint Security.
Verificar se o endereço está no banco de dados de endereços da Web de phishing	**Ativado**	O banco de dados de endereços Web de phishing inclui os endereços Web de sites atualmente conhecidos que são usados para iniciar ataques de phishing. A Kaspersky complementa esse banco de dados de links de phishing com endereços obtidos da organização internacional Anti-Phishing Working Group. O banco de dados de endereços de phishing está incluído no pacote de instalação do aplicativo e é complementado com atualizações de banco de dados do Kaspersky Endpoint Security.
Usar a análise heurística (Proteção Contra Ameaças da Web)	**Verificação média**	A tecnologia foi desenvolvida para detectar ameaças que não podem ser detectadas usando a versão atual dos bancos de dados do aplicativo Kaspersky. Detecta arquivos que podem estar infectados por um vírus desconhecido ou por uma nova variedade de um vírus conhecido. Quando o tráfego da Web for verificado quanto a vírus e outros aplicativos que apresentam uma ameaça, o analisador heurístico executará instruções nos arquivos executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível de análise heurística assegura um equilíbrio entre a eficácia da verificação quanto a novas ameaças, a carga nos recursos do sistema operacional e a duração da análise heurística.
Usar a análise heurística (Antiphishing)	**Ativado**	A tecnologia foi desenvolvida para detectar ameaças que não podem ser detectadas usando a versão atual dos bancos de dados do aplicativo Kaspersky. Detecta arquivos que podem estar infectados por um vírus desconhecido ou por uma nova variedade de um vírus conhecido.
Ação ao detectar ameaça	**Bloquear**	Se esta opção for selecionada, quando o componente Proteção Contra Ameaças da Web detectar um objeto infectado no tráfego da Web, ele bloqueará o acesso ao objeto e exibirá uma notificação no navegador.

Configurar métodos de detecção de endereços da Web maliciosos

A Proteção Contra Ameaças da Web detecta endereços da Web maliciosos usando bancos de dados antivírus, o serviço na nuvem da Kaspersky Security Network e a análise heurística.

É possível selecionar métodos de detecção de endereços da Web maliciosos apenas no Console de Administração (MMC) ou na interface local do aplicativo. Não é possível selecionar métodos de detecção de endereços da Web maliciosos no Web Console ou no Cloud Console. A opção padrão é verificar se o endereço está no banco de dados de endereços da Web maliciosos com a análise heurística (verificação média).

Verificação usando o banco de dados de endereços maliciosos

A verificação de links para determinar se estão incluídos no banco de dados de endereços da Web maliciosos permite rastrear sites que foram incluídos na lista de bloqueio. O banco de dados de endereços Web maliciosos é mantido pela Kaspersky, incluído no pacote de instalação do aplicativo e atualizado durante as atualizações do banco de dados do Kaspersky Endpoint Security.

O Kaspersky Endpoint Security verifica todos os links para determinar se eles estão listados em bancos de dados de endereços da web maliciosos. As configurações de verificação de conexão segura do aplicativo não afetam a funcionalidade de verificação de links. Em outras palavras, caso a verificação de conexões criptografadas esteja desativada, o Kaspersky Endpoint Security verifica se os links estão nos bancos de dados de endereços da Web maliciosos, mesmo se o tráfego de rede for transmitido por uma conexão criptografada.

Como ativar ou desativar a opção de verificar se os endereços estão no banco de dados de endereços da Web maliciosos usando o Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças da Web**.
4. No bloco **Nível de segurança**, clique no botão **Configurações**.
5. Na janela aberta, no bloco **Métodos de verificação**, marque ou desmarque a caixa de seleção **Verificar se o endereço está no banco de dados de endereços da Web maliciosos** para ativar ou desativar a opção de verificar se os endereços estão no banco de dados de endereços da Web maliciosos.
6. Salvar alterações.

Como ativar ou desativar a opção de verificar se os endereços estão no banco de dados de endereços maliciosos na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças da Web**.

3. Clique **Configurações avançadas**.

4. No bloco **Métodos de verificação**, marque ou desmarque a caixa de seleção **Verificar se o endereço está no banco de dados de endereços da Web maliciosos** para ativar ou desativar a opção de verificar se os endereços estão no banco de dados de endereços da Web maliciosos.

5. Salvar alterações.

Análise heurística

Durante a análise heurística, o Kaspersky Endpoint Security analisa a atividade dos aplicativos no sistema operacional. A análise heurística consegue detectar ameaças que ainda não tenham registros nos bancos de dados do Kaspersky Endpoint Security.

Quando o tráfego da Web for verificado quanto a vírus e outros aplicativos que apresentam uma ameaça, o analisador heurístico executará instruções nos arquivos executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível de análise heurística assegura um equilíbrio entre a eficácia da verificação quanto a novas ameaças, a carga nos recursos do sistema operacional e a duração da análise heurística.

Como ativar ou desativar o uso da análise heurística no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças da Web**.

4. No bloco **Nível de segurança**, clique no botão **Configurações**.

5. Na janela que é aberta, no bloco **Métodos de verificação**, selecione a caixa de seleção **Usar a análise heurística** caso queira que o aplicativo utilize a análise heurística ao verificar o tráfego da Web em busca de vírus e outros malwares.

6. Use o controle deslizante para definir o nível de análise heurística: **verificação superficial**, **verificação média** ou **verificação profunda**.

   Quando o tráfego da Web for verificado quanto a vírus e outros aplicativos que apresentam uma ameaça, o analisador heurístico executará instruções nos arquivos executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível de análise heurística assegura um equilíbrio entre a eficácia da verificação quanto a novas ameaças, a carga nos recursos do sistema operacional e a duração da análise heurística.

7. Salvar alterações.

Como ativar ou desativar o uso da análise heurística na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças da Web**.

3. Clique **Configurações avançadas**.

4. No bloco **Métodos de verificação**, marque a caixa de seleção **Usar a análise heurística** caso queira que o aplicativo utilize a análise heurística ao verificar o tráfego da web em busca de vírus e outros malwares.

   Quando o tráfego da Web for verificado quanto a vírus e outros aplicativos que apresentam uma ameaça, o analisador heurístico executará instruções nos arquivos executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível de análise heurística assegura um equilíbrio entre a eficácia da verificação quanto a novas ameaças, a carga nos recursos do sistema operacional e a duração da análise heurística.

5. Salvar alterações.

Antiphishing

A Proteção Contra Ameaças da Web verifica os links para ver se pertencem a endereços de phishing. Isso ajuda a prevenir *ataques de phishing*. Um ataque de phishing pode ser disfarçado, por exemplo, como uma mensagem de e-mail supostamente do seu banco, com um link para o site oficial do banco. Ao clicar no link, você é direcionado para uma cópia exata do site do banco e pode até ver o endereço real no navegador, embora, na verdade, esteja em um site falso. Desse momento em diante, todas as suas ações no site são rastreadas e podem ser usadas para roubá-lo.

Uma vez que links para sites de phishing podem ser recebidos não só por e-mail, mas também de outras fontes, como serviços de mensagens, o componente Proteção Contra Ameaças da Web monitora as tentativas de acessar um site de phishing no nível de verificação de tráfego da Web e bloqueia o acesso a esses sites. O kit de distribuição do Kaspersky Endpoint Security contém as listas de URLs de phishing.

É possível configurar o Antiphishing apenas no Console de administração (MMC) ou na interface local do aplicativo. Não é possível configurar o Anti-Phishing no Web Console ou no Cloud Console. Por padrão, o Anti-Phishing com análise heurística está ativado.

Como ativar ou desativar o Anti-Phishing no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças da Web**.

4. No bloco **Nível de segurança**, clique no botão **Configurações**.

5. Na janela aberta, no bloco **Configurações de Antiphishing**, marque ou desmarque a caixa de seleção **Verificar se o endereço está no banco de dados de endereços da Web de phishing** para ativar ou desativar o Antiphishing.

   O banco de dados de endereços Web de phishing inclui os endereços Web de sites atualmente conhecidos que são usados para iniciar ataques de phishing. A Kaspersky complementa esse banco de dados de links de phishing com endereços obtidos da organização internacional Anti-Phishing Working Group. O banco de dados de endereços de phishing está incluído no pacote de instalação do aplicativo e é complementado com atualizações de banco de dados do Kaspersky Endpoint Security.

6. Marque a caixa de seleção **Usar a análise heurística** se desejar que o aplicativo use a análise heurística ao verificar as páginas da Web em busca de links de phishing.

   Durante a análise heurística, o Kaspersky Endpoint Security analisa a atividade dos aplicativos no sistema operacional. A análise heurística consegue detectar ameaças que ainda não tenham registros nos bancos de dados do Kaspersky Endpoint Security.

   Para verificar links, além do banco de dados antivírus e da análise heurística, é possível usar os bancos de dados de reputação da Kaspersky Security Network.

7. Salvar alterações.

Como ativar ou desativar o Anti-Phishing na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças da Web**.

3. Clique **Configurações avançadas**.

4. Caso deseje que o componente de Proteção Contra Ameaças da Web verifique os links nos bancos de dados de endereços de phishing, marque a caixa de seleção **Verificar se o endereço está no banco de dados de endereços da Web de phishing** no bloco **Antiphishing**. O banco de dados de endereços Web de phishing inclui os endereços Web de sites atualmente conhecidos que são usados para iniciar ataques de phishing. A Kaspersky complementa esse banco de dados de links de phishing com endereços obtidos da organização internacional Anti-Phishing Working Group. O banco de dados de endereços de phishing está incluído no pacote de instalação do aplicativo e é complementado com atualizações de banco de dados do Kaspersky Endpoint Security.

5. Marque a caixa de seleção **Usar a análise heurística** se desejar que o aplicativo use a análise heurística ao verificar as páginas da Web em busca de links de phishing.

   Durante a análise heurística, o Kaspersky Endpoint Security analisa a atividade dos aplicativos no sistema operacional. A análise heurística consegue detectar ameaças que ainda não tenham registros nos bancos de dados do Kaspersky Endpoint Security.

   Para verificar links, além do banco de dados antivírus e da análise heurística, é possível usar os bancos de dados de reputação da Kaspersky Security Network.

6. Salvar alterações.

Criar lista de Endereços da Web confiáveis

Além de sites maliciosos e de phishing, a Proteção Contra Ameaças da Web pode bloquear outros sites. Por exemplo, a Proteção Contra Ameaças da Web bloqueia o tráfego HTTP que não atenda aos padrões RFC. Você pode criar uma lista de URLs em cujo conteúdo confia. O componente Proteção Contra Ameaças da Web não analisa informações de Endereços da Web confiáveis para verificar se eles contêm vírus ou outras ameaças. Esta opção poderá ser útil, por exemplo, se o componente Proteção Contra Ameaças da Web interferir no download de um arquivo de um site conhecido.

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

Como adicionar um endereço da Web confiável usando o Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças da Web**.
5. No bloco **Nível de segurança**, clique no botão **Configurações**.
6. Na janela que é aberta, selecione a guia **Endereços da Web confiáveis**.
7. Marque a caixa de seleção **Não verificar tráfego da web de endereços confiáveis**.

   Caso esta opção seja selecionada, o componente Proteção Contra Ameaças da Web não verificará o conteúdo de páginas da Web ou sites cujos endereços estão incluídos na lista endereços da Web confiáveis. Você pode adicionar tanto o endereço especifico como a máscara de endereço de uma página da Web/site à lista de endereços da Web confiáveis.
8. Crie uma lista de URLs/páginas em cujo conteúdo você confia.

   O Kaspersky Endpoint Security tem suporte aos caracteres `*` e `?` ao inserir uma máscara.

   Também é possível importar uma lista de endereços da Web confiáveis de um arquivo XML.
9. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como adicionar um endereço da Web confiável no Web Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Ir para a seção **Zona Confiável**.
5. Na janela aberta, clique no link **Endereços da Web**.

   Essa ação abre uma janela que contém uma lista de endereços da Web confiáveis.

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

   O Kaspersky Endpoint Security tem suporte aos caracteres `*` e `?` ao inserir uma máscara.

   Também é possível importar uma lista de endereços da Web confiáveis de um arquivo JSON.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como adicionar um endereço da Web confiável na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças da Web**.

3. Clique **Configurações avançadas**.

4. Marque a caixa de seleção **Não verificar o tráfego da web de URLs confiáveis**.

   Caso esta opção seja selecionada, o componente Proteção Contra Ameaças da Web não verificará o conteúdo de páginas da Web ou sites cujos endereços estão incluídos na lista endereços da Web confiáveis. Você pode adicionar tanto o endereço especifico como a máscara de endereço de uma página da Web/site à lista de endereços da Web confiáveis.

5. Crie uma lista de URLs/páginas em cujo conteúdo você confia.

   O Kaspersky Endpoint Security tem suporte aos caracteres `*` e `?` ao inserir uma máscara.

   Também é possível importar uma lista de endereços da Web confiáveis de um arquivo XML.

6. Salvar alterações.

Como resultado, a Proteção Contra Ameaças da Web não verifica o tráfego de endereços da Web confiáveis. O usuário sempre pode abrir um site confiável e baixar um arquivo desse site. Caso não tenha conseguido acessar o site, verifique as configurações dos componentes Verificação de conexões criptografadas, Controle da Web e Monitoramento de portas de rede. Se o Kaspersky Endpoint Security detectar que um arquivo baixado de um site confiável é malicioso, é possível adicionar esse arquivo às exclusões.

Também é possível criar uma lista geral de exclusões para conexões criptografadas. Nesse caso, o Kaspersky Endpoint Security não verifica o tráfego HTTPS de endereços da Web confiáveis quando os componentes Proteção Contra Ameaças da Web, Proteção Contra Ameaças ao Correio e Controle da Web estão fazendo seu trabalho.

Exportar e importar a lista de Endereços da Web confiáveis

Você pode exportar a lista de Endereços da Web confiáveis para um arquivo XML. Em seguida, você pode modificar o arquivo para, por exemplo, adicionar um grande número de endereços da web do mesmo tipo. Você também pode usar a função de exportação/importação para fazer backup da lista de Endereços da Web confiáveis ou para migrar a lista para um servidor diferente.

Como exportar e importar uma lista de Endereços da Web confiáveis no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças da Web**.

4. No bloco **Nível de segurança**, clique no botão **Configurações**.

5. Na janela que é aberta, selecione a guia **Endereços da Web confiáveis**.

6. Para exportar a Lista de Endereços da Web confiáveis:

   a. Selecione as Endereços da Web confiáveis que deseja exportar. Para selecionar várias portas, use as teclas **CTRL** ou **SHIFT**.

      Se você não selecionou nenhum endereço confiável, o Kaspersky Endpoint Security exportará todos os endereços da web.

   b. Clique no link **Exportar**.

   c. Na janela exibida, especifique o nome do arquivo XML para o qual você quer exportar a lista de Endereços da Web confiáveis e selecione a pasta na qual você quer salvar este arquivo.

   d. Salvar o arquivo.

      O Kaspersky Endpoint Security exporta toda a lista de Endereços da Web confiáveis para o arquivo XML.

7. Para importar a lista de Endereços da Web confiáveis:

   a. Clique no link **Importar**.

      Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de endereços confiáveis.

   b. Abra o arquivo.

      Se o computador já tiver uma lista de endereços confiáveis, o Kaspersky Endpoint 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 uma lista de Endereços da Web confiáveis no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Comunicação e Proteção na Web** → **Proteção Contra Ameaças da Web**.

5. Para exportar a lista de exclusões, na seção **Lista de regras**:

   a. Selecione as Endereços da Web confiáveis que deseja exportar.

   b. Clique no botão → **Exportar**.

      O Kaspersky Endpoint Security exporta a lista de endereços da Web confiáveis para um arquivo JSON na pasta de downloads padrão.

6. Para importar uma lista de exclusões, no bloco **Lista de regras**:

   a. Clique no botão → **Importar**.

      Na janela exibida, selecione o arquivo JSON do qual deseja importar a lista de endereços confiáveis.

b. Abra o arquivo.

Se o computador já tiver uma lista de endereços confiáveis, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo JSON.

7. Salvar alterações.

Proteção Contra Ameaças ao Correio

O componente Proteção contra ameaças de correio verifica os anexos das mensagens de e-mail recebidas e enviadas para detectar vírus e outras ameaças. O componente fornece proteção ao computador com a ajuda de bancos de dados de antivírus, o serviço na nuvem Kaspersky Security Network e análise heurística.

A Proteção Contra Ameaças ao Correio pode verificar as mensagens recebidas e enviadas. O aplicativo é compatível com POP3, SMTP, IMAP e NNTP nos seguintes clientes de e-mail:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- Correio do MyOffice
- R7-Office Organizer

Para verificar o tráfego nos programas de e-mail Mozilla Thunderbird, MyOffice Mail e R7-Office Organizer, é necessário adicionar o certificado da Kaspersky ao armazenamento de certificados e selecionar o armazenamento de certificados próprio.

A Proteção Contra Ameaças ao Correio não oferece suporte a outros protocolos e clientes de e-mail.

A Proteção Contra Ameaças ao Correio pode nem sempre ser capaz de obter acesso a mensagens no *nível de protocolo* (por exemplo, ao usar a solução Microsoft Exchange). Por essa razão, a Proteção Contra Ameaças ao Correio inclui uma extensão para Microsoft Office Outlook. A extensão permite verificar mensagens no *nível do cliente de e-mail*. A extensão Proteção Contra Ameaças ao Correio é compatível com as versões de 32 e 64 bits do Outlook 2010, 2013, 2016, 2019, 2021, 2024 e 365. Em computadores baseados em Arm, a extensão Proteção Contra Ameaças ao Correio é compatível com as versões de 32 e 64 bits do Outlook 2016, Outlook 2021, Outlook 2024 e Outlook 365 para Arm64.

O componente Proteção Contra Ameaças ao Correio não verifica as mensagens se o programa de e-mail estiver aberto em um navegador.

Quando um arquivo malicioso for detectado em um anexo, o Kaspersky Endpoint Security adiciona informações sobre a ação executada ao assunto da mensagem, por exemplo, *[Message has been processed]<assunto da mensagem>*.

Ativar e desativar a Proteção Contra Ameaças ao Correio

Por padrão, o componente Proteção Contra Ameaças ao Correio é ativado e executado no modo recomendado por especialistas da Kaspersky. Para a Proteção Contra Ameaças ao Correio, o aplicativo poderá aplicar diferentes grupos de configurações. Estes grupos de configurações armazenados no aplicativo são denominados *níveis de segurança*: **Alto**, **Recomendado**, **Baixo**. As configurações do nível de segurança **Recomendado** para correio são consideradas as configurações ideais recomendadas pelos especialistas da Kaspersky (veja a tabela abaixo). Selecione um dos níveis de segurança de e-mails predefinidos ou configure um nível de segurança personalizado. A alteração das configurações do nível de segurança de e-mails não impede a reversão para o nível recomendado quando desejado.

Ao trabalhar com o programa de e-mail Mozilla Thunderbird, o componente Proteção Contra Ameaças ao Correio não verificará as mensagens transmitidas por meio do protocolo IMAP em relação a vírus e outras ameaças se os filtros forem utilizados para mover as mensagens da pasta caixa de entrada.

Como ativar ou desativar o componente Proteção Contra Ameaças ao Correio no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Correio**.

4. Use a caixa de seleção **Proteção Contra Ameaças ao Correio** para ativar ou desativar o componente.

5. Caso tenha ativado o componente, execute uma das seguintes operações no bloco **Nível de segurança**:

   - Caso queira aplicar um dos níveis de segurança pré-configurados, selecione-o com o controle deslizante:

     - **Alto**. Quando este nível de segurança de e-mail é selecionado, o componente Proteção Contra Ameaças ao Correio verifica as mensagens de e-mail mais detalhadamente. O componente Proteção Contra Ameaças ao Correio verifica mensagens de e-mail enviadas e recebidas e realiza uma análise heurística profunda. O nível de segurança de e-mails alto é recomendado para ambientes de alto risco. Um exemplo desse tipo de ambiente é uma conexão com um serviço de e-mail gratuito, de uma rede doméstica que não tem uma proteção de e-mail centralizada.

     - **Recomendado**. O nível de segurança do e-mail que fornece o equilíbrio ideal entre o desempenho do aplicativo e a segurança do e-mail. O componente Proteção Contra Ameaças ao Correio verifica mensagens de e-mail enviadas e recebidas e realiza uma análise heurística de nível médio. Esse nível de segurança de tráfego de e-mail é recomendado por especialistas da Kaspersky. Os valores das configurações para o nível de segurança recomendado são fornecidos na tabela abaixo.

     - **Baixo**. Quando este nível de segurança de e-mail é selecionado, o componente Proteção Contra Ameaças ao Correio verifica apenas mensagens de e-mail recebidas, executa a análise heurística superficial e não verifica arquivos compactados anexados a mensagens de e-mail. Nesse nível de segurança de e-mail, o componente Proteção Contra Ameaças ao Correio verifica mensagens de e-mail na velocidade máxima e usa um mínimo de recursos do sistema operacional. O nível de segurança de e-mail baixo é recomendado para utilização em um ambiente bem protegido. Um exemplo desse ambiente poderia ser uma LAN corporativa com segurança de e-mail centralizada.

- Caso queira configurar um nível de segurança personalizado, clique no botão **Configurações** e defina suas próprias configurações do componente (consulte a tabela abaixo).

  É possível restaurar os valores dos níveis de segurança predefinidos clicando no botão **Por padrão**.

6. No bloco **Ação ao detectar ameaça**, selecione a ação que o Kaspersky Endpoint Security deve executar em objetos maliciosos:

   - **Desinfectar e excluir se a desinfecção falhar**. Quando um objeto infectado é detectado em uma mensagem de entrada ou saída, o aplicativo tenta desinfectar o objeto detectado. O usuário poderá acessar a mensagem com um anexo seguro. Caso o objeto não possa ser desinfectado, o aplicativo excluirá o objeto infectado. O aplicativo adiciona informações sobre a ação executada ao assunto da mensagem: *[A mensagem foi processada] <assunto da mensagem>*.

   - **Desinfectar e bloquear se a desinfecção falhar**. Quando um objeto infectado é detectado em uma mensagem de entrada, o aplicativo tenta desinfectar o objeto detectado. O usuário poderá acessar a mensagem com um anexo seguro. Caso o objeto não possa ser desinfectado, o aplicativo adicionará um aviso ao assunto da mensagem. O usuário poderá acessar a mensagem com o anexo original. Quando um objeto infectado é detectado em uma mensagem de saída, o aplicativo tenta desinfectar o objeto detectado. Caso o objeto não possa ser desinfectado, o aplicativo bloqueará a transmissão da mensagem e o programa de e-mail exibirá um erro.

   - **Bloquear**. Caso um objeto infectado seja detectado em uma mensagem recebida, o aplicativo adiciona um aviso ao assunto da mensagem. O usuário poderá acessar a mensagem com o anexo original. Caso um objeto infectado seja detectado em uma mensagem de saída, o aplicativo bloqueará a transmissão da mensagem e o programa de e-mail exibirá um erro.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar ou desativar o componente Proteção Contra Ameaças ao Correio no Web Console

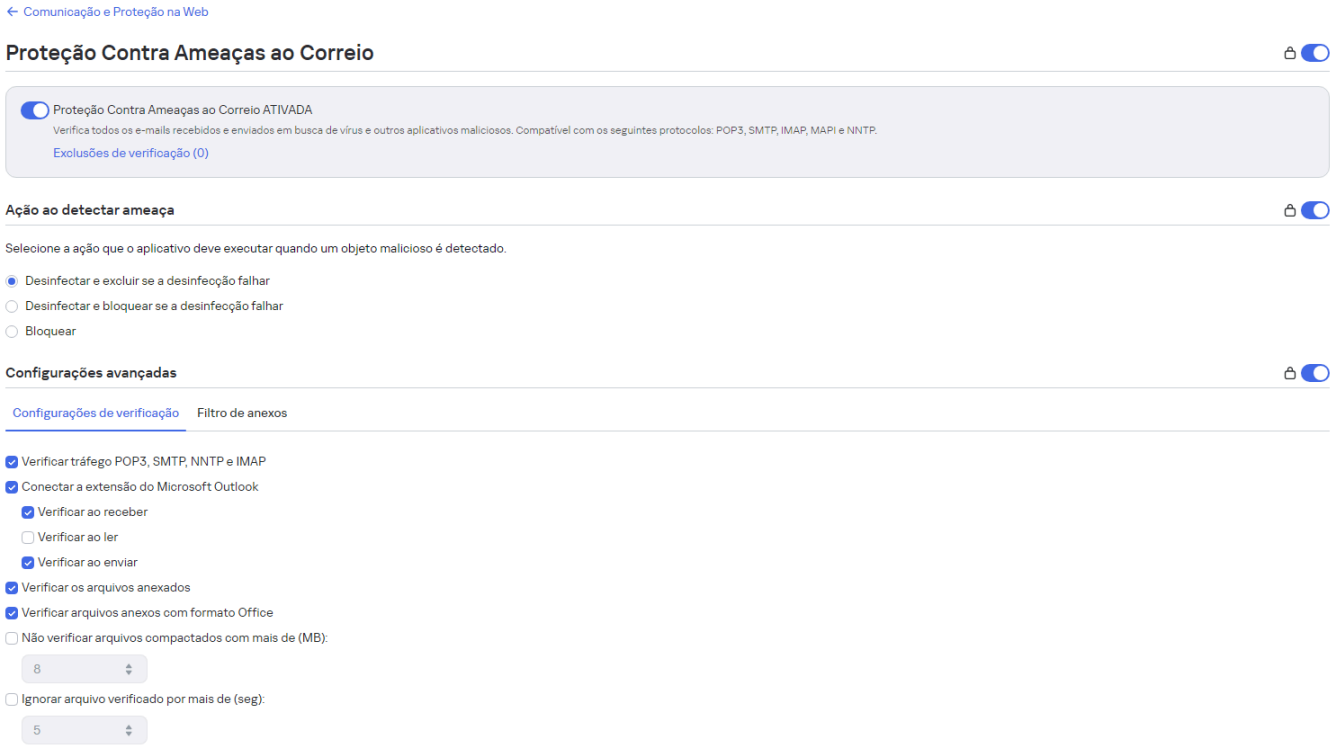
1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

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



Configurações de Proteção Contra Ameaças ao Correio

5. Use o botão de alternância do **Proteção Contra Ameaças ao Correio ATIVADA** para ativar ou desativar o componente.

6. No bloco **Ação ao detectar ameaça**, selecione a ação que o Kaspersky Endpoint Security deve executar em objetos maliciosos:

   - **Desinfectar e excluir se a desinfecção falhar**. Quando um objeto infectado é detectado em uma mensagem de entrada ou saída, o aplicativo tenta desinfectar o objeto detectado. O usuário poderá acessar a mensagem com um anexo seguro. Caso o objeto não possa ser desinfectado, o aplicativo excluirá o objeto infectado. O aplicativo adiciona informações sobre a ação executada ao assunto da mensagem: *[A mensagem foi processada] <assunto da mensagem>*.

   - **Desinfectar e bloquear se a desinfecção falhar**. Quando um objeto infectado é detectado em uma mensagem de entrada, o aplicativo tenta desinfectar o objeto detectado. O usuário poderá acessar a mensagem com um anexo seguro. Caso o objeto não possa ser desinfectado, o aplicativo adicionará um aviso ao assunto da mensagem. O usuário poderá acessar a mensagem com o anexo original. Quando um objeto infectado é detectado em uma mensagem de saída, o aplicativo tenta desinfectar o objeto detectado. Caso o objeto não possa ser desinfectado, o aplicativo bloqueará a transmissão da mensagem e o programa de e-mail exibirá um erro.

   - **Bloquear**. Caso um objeto infectado seja detectado em uma mensagem recebida, o aplicativo adiciona um aviso ao assunto da mensagem. O usuário poderá acessar a mensagem com o anexo original. Caso um objeto infectado seja detectado em uma mensagem de saída, o aplicativo bloqueará a transmissão da mensagem e o programa de e-mail exibirá um erro.

7. Caso seja necessário, edite as configurações avançadas da Proteção Contra Ameaças ao Correio.

8. Para aplicar a política aos computadores, feche os ícones de cadeado 🔒 e salve as alterações.

Como ativar ou desativar o componente Proteção Contra Ameaças ao Correio na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Correio**.

3. Use o botão de alternância do **Proteção Contra Ameaças ao Correio** para ativar ou desativar o componente.

4. Caso tenha ativado o componente, execute uma das seguintes operações no bloco **Nível de segurança**:

   - Caso queira aplicar um dos níveis de segurança pré-configurados, selecione-o com o controle deslizante:

     - **Alto**. Quando este nível de segurança de e-mail é selecionado, o componente Proteção Contra Ameaças ao Correio verifica as mensagens de e-mail mais detalhadamente. O componente Proteção Contra Ameaças ao Correio verifica mensagens de e-mail enviadas e recebidas e realiza uma análise heurística profunda. O nível de segurança de e-mails alto é recomendado para ambientes de alto risco. Um exemplo desse tipo de ambiente é uma conexão com um serviço de e-mail gratuito, de uma rede doméstica que não tem uma proteção de e-mail centralizada.

     - **Recomendado**. O nível de segurança do e-mail que fornece o equilíbrio ideal entre o desempenho do aplicativo e a segurança do e-mail. O componente Proteção Contra Ameaças ao Correio verifica mensagens de e-mail enviadas e recebidas e realiza uma análise heurística de nível médio. Esse nível de segurança de tráfego de e-mail é recomendado por especialistas da Kaspersky. Os valores das configurações para o nível de segurança recomendado são fornecidos na tabela abaixo.

     - **Baixo**. Quando este nível de segurança de e-mail é selecionado, o componente Proteção Contra Ameaças ao Correio verifica apenas mensagens de e-mail recebidas, executa a análise heurística superficial e não verifica arquivos compactados anexados a mensagens de e-mail. Nesse nível de segurança de e-mail, o componente Proteção Contra Ameaças ao Correio verifica mensagens de e-mail na velocidade máxima e usa um mínimo de recursos do sistema operacional. O nível de segurança de e-mail baixo é recomendado para utilização em um ambiente bem protegido. Um exemplo desse ambiente poderia ser uma LAN corporativa com segurança de e-mail centralizada.

   - Caso queira configurar um nível de segurança personalizado, clique no botão **Configurações avançadas** e defina suas próprias configurações do componente (consulte a tabela abaixo).

     É possível restaurar os valores dos níveis de segurança predefinidos clicando no botão **Restaurar nível de segurança recomendado**.

5. No bloco **Ação ao detectar ameaça**, selecione a ação que o Kaspersky Endpoint Security deve executar em objetos maliciosos:

   - **Desinfectar e excluir se a desinfecção falhar**. Quando um objeto infectado é detectado em uma mensagem de entrada ou saída, o aplicativo tenta desinfectar o objeto detectado. O usuário poderá acessar a mensagem com um anexo seguro. Caso o objeto não possa ser desinfectado, o aplicativo excluirá o objeto infectado. O aplicativo adiciona informações sobre a ação executada ao assunto da mensagem: *[A mensagem foi processada] <assunto da mensagem>*.

   - **Desinfectar e bloquear se a desinfecção falhar**. Quando um objeto infectado é detectado em uma mensagem de entrada, o aplicativo tenta desinfectar o objeto detectado. O usuário poderá acessar a mensagem com um anexo seguro. Caso o objeto não possa ser desinfectado, o aplicativo adicionará um aviso ao assunto da mensagem. O usuário poderá acessar a mensagem com o anexo original. Quando um objeto infectado é detectado em uma mensagem de saída, o aplicativo tenta desinfectar o objeto detectado. Caso o objeto não possa ser desinfectado, o aplicativo bloqueará a transmissão da mensagem e o programa de e-mail exibirá um erro.

   - **Bloquear**. Caso um objeto infectado seja detectado em uma mensagem recebida, o aplicativo adiciona um aviso ao assunto da mensagem. O usuário poderá acessar a mensagem com o anexo original. Caso um objeto infectado seja detectado em uma mensagem de saída, o aplicativo bloqueará a transmissão da mensagem e o programa de e-mail exibirá um erro.

6. Salvar alterações.

Configurações de Proteção Contra Ameaças ao Correio recomendadas pelos especialistas da Kaspersky (nível de segurança recomendado)

Parâmetro	Valor	Descrição
Escopo de proteção	**Mensagens enviadas e recebidas**	O *Escopo da proteção* inclui objetos que o componente verifica ao ser executado: mensagens recebidas e enviadas ou apenas mensagens recebidas. Para proteger seus computadores, você precisa apenas verificar as mensagens recebidas. É possível ativar a verificação de mensagens enviadas para impedir que arquivos infectados sejam enviados em arquivos compactados. Também é possível ativar a verificação de mensagens enviadas se quiser impedir que arquivos em formatos específicos sejam enviados, tais como arquivos de áudio e vídeo, por exemplo.
Conectar a extensão do Microsoft Outlook	**Ativado**	Se a caixa de seleção estiver marcada, a verificação de mensagens de e-mail transmitidas através dos protocolos POP3, SMTP, NNTP e IMAP será ativada no lado da extensão integrada ao Microsoft Outlook. Se o e-mail for verificado por meio da extensão para o Microsoft Outlook, recomenda-se utilizar o Cached Exchange Mode. Para obter informações mais detalhadas sobre o Modo de cache do Exchange e recomendações sobre seu uso, consulte a Base de Dados de Conhecimento Microsoft.
Verificar arquivos compactados anexados	**Ativado**	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 arquivos anexos com formato Microsoft Office	**Ativado**	Verifica arquivos do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Arquivos de formato do Office também incluem objetos OLE. O aplicativo verifica arquivos em formato do Office com menos de 1 MB, independentemente de a caixa de seleção estar marcada ou não.
Filtro de anexos	**Renomear anexos dos tipos selecionados**	Se você selecionar essa opção, o componente de Proteção Contra Ameaças ao Correio substituirá o último caractere da extensão encontrado nos arquivos anexados dos tipos especificados pelo caractere de sublinhado (por exemplo, anexo.doc_). Portanto, para abrir o arquivo, o usuário deve renomeá-lo.

Parâmetro	Valor	Descrição
Análise heurística	**Verificação média**	A tecnologia foi desenvolvida para detectar ameaças que não podem ser detectadas usando a versão atual dos bancos de dados do aplicativo Kaspersky. Detecta arquivos que podem estar infectados por um vírus desconhecido ou por uma nova variedade de um vírus conhecido. Ao verificar arquivos em busca de códigos maliciosos, o analisador heurístico executa instruções nos arquivos executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível de análise heurística assegura um equilíbrio entre a eficácia da verificação quanto a novas ameaças, a carga nos recursos do sistema operacional e a duração da análise heurística.
Ação ao detectar ameaça	**Desinfectar e excluir se a desinfecção falhar**	Quando um objeto infectado é detectado em uma mensagem de entrada ou saída, o aplicativo tenta desinfectar o objeto detectado. O usuário poderá acessar a mensagem com um anexo seguro. Caso o objeto não possa ser desinfectado, o aplicativo excluirá o objeto infectado. O aplicativo adiciona informações sobre a ação executada ao assunto da mensagem: *[A mensagem foi processada] <assunto da mensagem>*.

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

Por padrão, o componente Proteção Contra Ameaças ao Correio tentará desinfectar automaticamente todas as mensagens por e-mail infectadas detectadas. Se a desinfeção falhar, o componente Proteção Contra Ameaças ao Correio exclui as mensagens de e-mail infectadas.

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

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Correio**.

3. No bloco **Ação ao detectar ameaça**, selecione a ação que o Kaspersky Endpoint Security deve executar ao detectar uma mensagem infectada:

   - **Desinfectar e excluir se a desinfecção falhar**. Quando um objeto infectado é detectado em uma mensagem de entrada ou saída, o aplicativo tenta desinfectar o objeto detectado. O usuário poderá acessar a mensagem com um anexo seguro. Caso o objeto não possa ser desinfectado, o aplicativo excluirá o objeto infectado. O aplicativo adiciona informações sobre a ação executada ao assunto da mensagem: *[A mensagem foi processada] <assunto da mensagem>*.

   - **Desinfectar e bloquear se a desinfecção falhar**. Quando um objeto infectado é detectado em uma mensagem de entrada, o aplicativo tenta desinfectar o objeto detectado. O usuário poderá acessar a mensagem com um anexo seguro. Caso o objeto não possa ser desinfectado, o aplicativo adicionará um aviso ao assunto da mensagem. O usuário poderá acessar a mensagem com o anexo original. Quando um objeto infectado é detectado em uma mensagem de saída, o aplicativo tenta desinfectar o objeto detectado. Caso o objeto não possa ser desinfectado, o aplicativo bloqueará a transmissão da mensagem e o programa de e-mail exibirá um erro.

   - **Bloquear**. Caso um objeto infectado seja detectado em uma mensagem recebida, o aplicativo adiciona um aviso ao assunto da mensagem. O usuário poderá acessar a mensagem com o anexo original. Caso um objeto infectado seja detectado em uma mensagem de saída, o aplicativo bloqueará a transmissão da mensagem e o programa de e-mail exibirá um erro.

4. Salvar alterações.

Formar o escopo de proteção do componente Proteção Contra Ameaças ao Correio

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

Para formar o escopo de proteção do componente Proteção Contra Ameaças ao Correio:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Correio**.

3. Clique **Configurações avançadas**.

4. No bloco **Escopo de proteção**, selecione as mensagens a serem verificadas:

   - **Mensagens enviadas e recebidas**.

   - **Somente mensagens recebidas**.

   Para proteger seus computadores, você precisa apenas verificar as mensagens recebidas. É possível ativar a verificação de mensagens enviadas para impedir que arquivos infectados sejam enviados em arquivos compactados. Também é possível ativar a verificação de mensagens enviadas se quiser impedir que arquivos em formatos específicos sejam enviados, tais como arquivos de áudio e vídeo, por exemplo.

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

5. No bloco **Conectividade**, faça o seguinte:

   - Caso queira que o componente de Proteção Contra Ameaças ao Correio verifique as mensagens transmitidas por meio dos protocolos POP3, SMTP, NNTP e IMAP antes de chegarem ao computador do usuário, marque a caixa de seleção **Verificar tráfego POP3, SMTP, NNTP e IMAP**.

     Caso não queira que o componente de Proteção Contra Ameaças ao Correio verifique as mensagens transmitidas por meio dos protocolos POP3, SMTP, NNTP e IMAP antes de chegarem ao computador do usuário, desmarque a caixa de seleção **Verificar tráfego POP3, SMTP, NNTP e IMAP**. Nesse caso, as mensagens são verificadas pela extensão da Proteção Contra Ameaças ao Correio incorporada no cliente de e-mail do Microsoft Office Outlook depois que são recebidas no computador do usuário se a caixa de seleção **Conectar a extensão do Microsoft Outlook** estiver marcada.

Caso use um cliente de e-mail diferente do Microsoft Office Outlook, o componente de Proteção Contra Ameaças ao Correio não verificará as mensagens transmitidas pelos protocolos POP3, SMTP, NNTP e IMAP se a caixa de seleção **Verificar tráfego POP3, SMTP, NNTP e IMAP** estiver desmarcada.

- Para permitir o acesso às configurações do componente Proteção Contra Ameaças ao Correio a partir do Microsoft Office Outlook e ativar a verificação de mensagens transmitidas por meio dos protocolos POP3, SMTP, NNTP, IMAP e MAPI após chegarem ao computador usando a extensão incorporada no Microsoft Office Outlook, marque a caixa de seleção **Conectar a extensão do Microsoft Outlook**.

  Para bloquear o acesso às configurações do componente Proteção Contra Ameaças ao Correio a partir do Microsoft Office Outlook e desativar a verificação de mensagens transmitidas por meio dos protocolos POP3, SMTP, NNTP, IMAP e MAPI após chegarem ao computador usando uma extensão incorporada no Microsoft Office Outlook, desmarque a caixa de seleção **Conectar a extensão do Microsoft Outlook**.

  A extensão da Proteção Contra Ameaças ao Correio é incorporada no programa de e-mail do Microsoft Office Outlook durante a instalação do Kaspersky Endpoint Security.

6. Salvar alterações.

Verificar arquivos compostos anexados a mensagens de e-mail

Você pode ativar ou desativar a verificação de anexos de mensagem, limitar o tamanho máximo de anexos de mensagem a verificar e limitar a duração de verificação de anexo de mensagem máxima.

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

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Correio**.

3. Clique **Configurações avançadas**.

4. No bloco **Verificação de arquivos compostos**, defina as configurações de verificação:

   - **Verificar arquivos anexos com formato 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 aplicativo verifica arquivos em formato do Office com menos de 1 MB, independentemente de a caixa de seleção estar marcada ou não.

   - **Verificar arquivos compactados anexados**. 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).

     Se, durante a verificação, o aplicativo detectar uma senha para um arquivo compactado no texto da mensagem, essa senha será usada para verificar o conteúdo do arquivo compactado em busca de aplicativos maliciosos. Nesse caso, a senha não é salva. O arquivo compactado é descompactado durante a verificação. Caso ocorra um erro de aplicativo durante o processo de descompactação, será possível excluir manualmente os arquivos descompactados salvos no seguinte caminho: %systemroot%\temp. Os arquivos têm o prefixo PR.

- **Não verificar arquivos compactados com mais de N MB (de 1 até 9999)**. Se esta caixa de seleção for marcada, o componente Proteção contra ameaças de correio excluirá arquivos compactados anexados a mensagens de e-mail da verificação se o seu tamanho exceder o valor especificado. Se a caixa de seleção for desmarcada, o componente Proteção contra ameaças de correio verificará arquivos compactados de anexo de e-mail de qualquer tamanho.

- **Limitar o tempo para a verificação de arquivos compactados a N s (de 1 até 9999)**. Se a caixa de seleção for marcada, o tempo alocado para verificar arquivos compactados anexados a mensagens de e-mail será limitado ao período especificado.

5. Salvar alterações.

Filtragem de anexos de mensagens de e-mail

O filtro de anexos não é aplicado a mensagens de e-mail enviadas.

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

Para configurar a filtragem de anexos:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Correio**.

3. Clique **Configurações avançadas**.

4. No bloco **Filtro de anexos**, execute uma das seguintes ações:

   - **Desativar a filtragem**. Se esta opção for selecionada, o componente de Proteção Contra Ameaças ao Correio não filtrará arquivos anexados a mensagens de e-mail.

   - **Renomear anexos dos tipos selecionados**. Se você selecionar essa opção, o componente de Proteção Contra Ameaças ao Correio substituirá o último caractere da extensão encontrado nos arquivos anexados dos tipos especificados pelo caractere de sublinhado (por exemplo, anexo.doc_). Portanto, para abrir o arquivo, o usuário deve renomeá-lo.

   - **Excluir anexos dos tipos selecionados**. Se esta opção for selecionada, o componente Proteção Contra Ameaças ao Correio excluirá arquivos anexados dos tipos especificados de mensagens de e-mail.

5. Se você selecionou a opção **Renomear anexos dos tipos selecionados** ou a opção **Excluir anexos dos tipos selecionados** na etapa anterior, marque as caixas de seleção diante dos tipos de arquivo relevantes.

6. Salvar alterações.

Exportar e importar extensões para filtragem de anexos

Você pode exportar a lista de extensões de filtro de anexos para um arquivo XML. Você pode usar a função de exportação/importação para fazer backup da lista de extensões ou para migrar a lista para um servidor diferente.

Como exportar e importar uma lista de extensões de filtro de anexos no Console de Administração (MMC)

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Comunicação e Proteção na Web** → **Proteção Contra Ameaças ao Correio**.
5. Para exportar a lista de extensões, na seção **Filtro de anexos**:
   a. Selecione as extensões que você deseja exportar.
   b. Clique no link **Exportar**.
   c. Na janela exibida, especifique o nome do arquivo XML para o qual você quer exportar a lista de extensões e selecione a pasta na qual você quer salvar este arquivo.
   d. Salvar o arquivo.

      O Kaspersky Endpoint Security exporta toda a lista de extensões para o arquivo XML.
6. Para importar a lista de extensões, no bloco **Filtro de anexos**:
   a. Clique no link **Importar**.
   b. Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de extensões.
   c. Abra o arquivo.

      Se o computador já tiver uma lista de extensões, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.
7. Salvar alterações.

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Correio**.
4. No bloco **Nível de segurança**, clique no botão **Configurações**.
5. Uma janela será aberta; nessa janela, selecione a guia **Filtro de anexos**.

6. Para exportar a lista de extensões:

   a. Selecione as extensões que você deseja exportar. Para selecionar várias portas, use as teclas **CTRL** ou **SHIFT**.

   b. Clique no link **Exportar**.

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

   d. Salvar o arquivo.

      O Kaspersky Endpoint Security exporta toda a lista de extensões para o arquivo XML.

7. Para importar a lista de extensões:

   a. Clique no link **Importar**.

   b. Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de extensões.

   c. Abra o arquivo.

      Se o computador já tiver uma lista de extensões, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

8. Salvar alterações.

Verificar e-mails no Microsoft Office Outlook

Durante a instalação do Kaspersky Endpoint Security, a extensão da Proteção Contra Ameaças ao Correio é integrada no Microsoft Office Outlook (daqui em diante também referido como Outlook). A extensão permite a verificação de mensagens no nível de um cliente de e-mail em vez do nível de protocolo. Além das mensagens, a extensão permite verificar objetos recebidos por meio da interface MAPI dos repositórios do Microsoft Exchange (por exemplo, objetos do calendário). Essa verificação ocorre no cliente de e-mail.

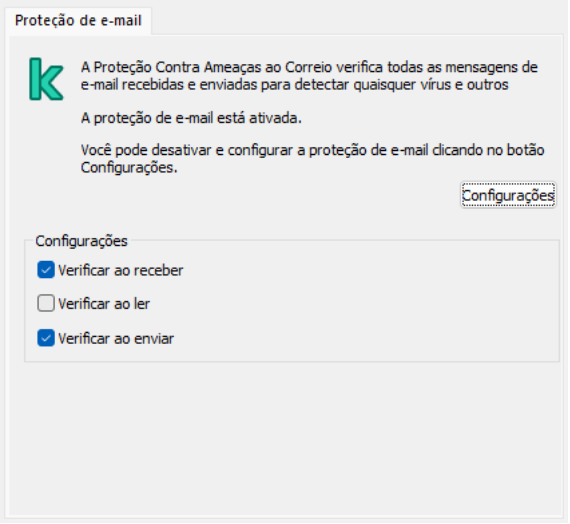
É possível abrir as configurações do componente Proteção Contra Ameaças ao Correio internamente no Outlook e especificar o momento da verificação das mensagens de e-mail para detectar vírus e outras ameaças.

A extensão Proteção Contra Ameaças ao Correio é compatível com as versões de 32 e 64 bits do Outlook 2010, 2013, 2016, 2019, 2021, 2024 e 365.

Em computadores baseados em Arm, a extensão Proteção Contra Ameaças ao Correio é compatível com as versões de 32 e 64 bits do Outlook 2016, Outlook 2021, Outlook 2024 e Outlook 365 para Arm64.

No Outlook, as mensagens recebidas são verificadas primeiramente pelo componente Proteção Contra Ameaças ao Correio (se a caixa de seleção Selecionar tráfego POP3, SMTP, NNTP e IMAP estiver marcada na interface do Kaspersky Endpoint Security) e, em seguida, pela extensão da Proteção Contra Ameaças ao Correio para Outlook. Se o componente Proteção Contra Ameaças ao Correio detectar um objeto malicioso em uma mensagem, você será alertado sobre esse evento.

As configurações do componente de Proteção Contra Ameaças ao Correio podem ser configuradas diretamente no Outlook se a extensão do Microsoft Outlook estiver conectada na interface do Kaspersky Endpoint Security (veja a figura abaixo).



Configurações do componente Proteção Contra Ameaças ao Correio no Outlook

As mensagens enviadas são verificadas primeiramente pela extensão da Proteção Contra Ameaças ao Correio para Outlook e, em seguida, pelo componente Proteção Contra Ameaças ao Correio.

> Ao verificar e-mails com a extensão Proteção Contra Ameaças ao Correio para Outlook, recomendamos usar o Modo em Cache do Exchange Server (Use Cached Exchange Mode). Para obter informações mais detalhadas sobre o Modo de cache do Exchange e recomendações sobre seu uso, consulte a Base de Dados de Conhecimento Microsoft.

Como configurar o modo de operação da extensão da Proteção Contra Ameaças ao Correio para Outlook no Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Correio**.
5. No bloco **Nível de segurança**, clique no botão **Configurações**.
6. Na janela que é aberta, no bloco **Conectividade**, marque a caixa de seleção **Conectar a extensão do Microsoft Outlook**.
7. Clique **Configurações**.

8. Na janela **Proteção de e-mail**, faça o seguinte:

   - Marque a caixa de seleção **Verificar ao receber** se desejar que a extensão da Proteção Contra Ameaças ao Correio para Outlook verifique mensagens de entrada conforme elas chegam à caixa do correio.

   - Marque a caixa de seleção **Verificar ao ler** se quiser que a extensão da Proteção Contra Ameaças ao Correio para Outlook verifique mensagens de entrada no momento em que o usuário as abre.

   - Marque a caixa de seleção **Verificar ao enviar** se quiser que a extensão da Proteção Contra Ameaças ao Correio para Outlook verifique mensagens de saída quando elas são enviadas.

9. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como configurar o modo de operação da extensão da Proteção Contra Ameaças ao Correio para Outlook no Web Console

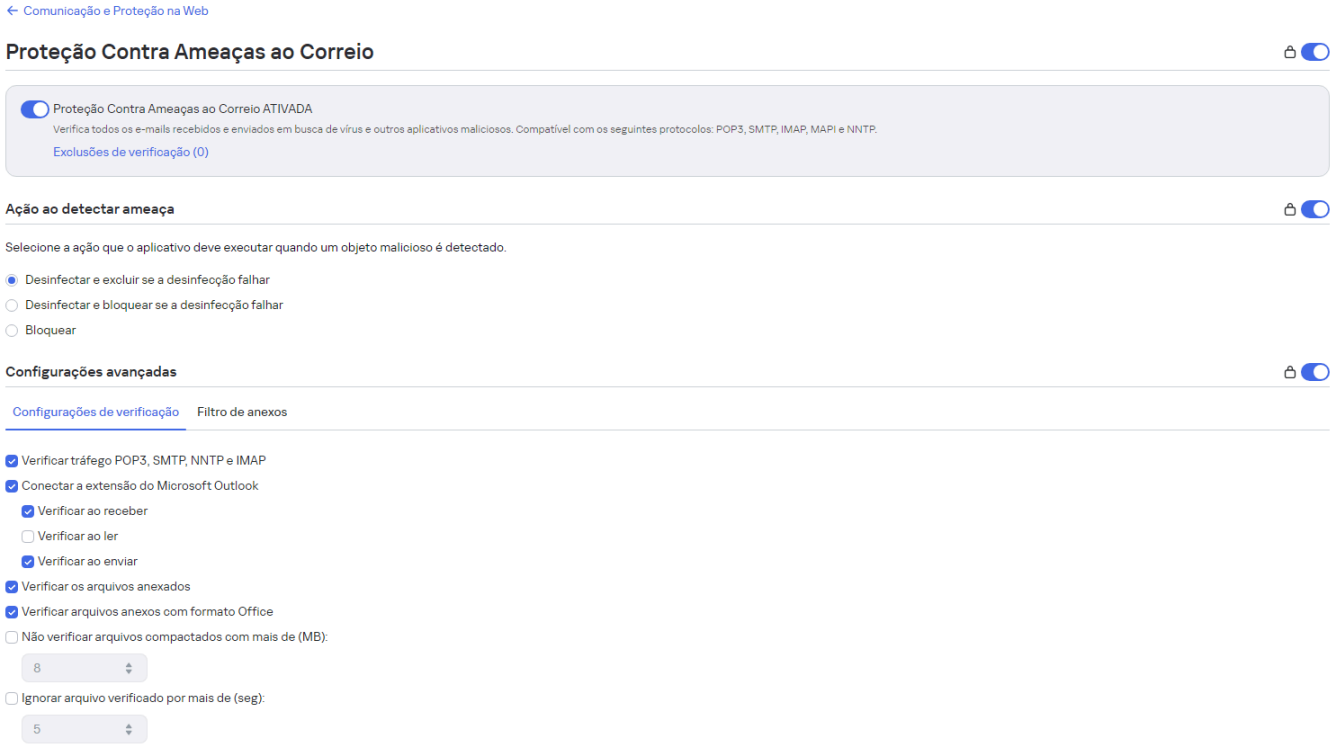
1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

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



Configurações de Proteção Contra Ameaças ao Correio

5. Em **Configurações avançadas**, selecione a guia **Configurações de verificação**.

6. Marque a caixa de seleção **Conectar a extensão do Microsoft Outlook**.

7. Configure o modo de operação da extensão:

- Marque a caixa de seleção **Verificar ao receber** se desejar que a extensão da Proteção Contra Ameaças ao Correio para Outlook verifique mensagens de entrada conforme elas chegam à caixa do correio.
- Marque a caixa de seleção **Verificar ao ler** se quiser que a extensão da Proteção Contra Ameaças ao Correio para Outlook verifique mensagens de entrada no momento em que o usuário as abre.
- Marque a caixa de seleção **Verificar ao enviar** se quiser que a extensão da Proteção Contra Ameaças ao Correio para Outlook verifique mensagens de saída quando elas são enviadas.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Verificação de e-mails no Thunderbird, MyOffice e R7-Office

O componente Proteção contra ameaças de correio verifica os anexos das mensagens de e-mail recebidas e enviadas para detectar vírus e outras ameaças. Para os programas de e-mail Mozilla Thunderbird, MyOffice Mail e R7-Office Organizer, o aplicativo obtém acesso às mensagens somente no *nível de protocolo* (POP3, SMTP, IMAP, NNTP).

Para verificar o tráfego nos programas de e-mail Mozilla Thunderbird, MyOffice Mail e R7-Office Organizer, é necessário adicionar o certificado da Kaspersky ao armazenamento de certificados e selecionar o armazenamento de certificados próprio.

O componente Proteção Contra Ameaças ao Correio não verifica as mensagens se o programa de e-mail estiver aberto em um navegador.

Proteção Contra Ameaças ao Correio em tempo real

A Proteção Contra Ameaças ao Correio pode verificar as mensagens recebidas e enviadas. Por padrão, o componente Proteção Contra Ameaças ao Correio tentará desinfectar automaticamente todas as mensagens por e-mail infectadas detectadas. Se a desinfeção falhar, o componente Proteção Contra Ameaças ao Correio exclui as mensagens de e-mail infectadas. Quando um arquivo malicioso for detectado em um anexo, o Kaspersky Endpoint Security adiciona informações sobre a ação executada ao assunto da mensagem, por exemplo, *[Message has been processed]<assunto da mensagem>*.

Ao trabalhar com o programa de e-mail Mozilla Thunderbird, o componente Proteção Contra Ameaças ao Correio não verificará as mensagens transmitidas por meio do protocolo IMAP em relação a vírus e outras ameaças se os filtros forem utilizados para mover as mensagens da pasta caixa de entrada.

Verificação de malware em bancos de dados de e-mail

A Proteção Contra Ameaças ao Correio evita a infecção do computador no nível do protocolo, mas, se o computador tiver sido infectado antes da instalação do Kaspersky Endpoint Security, o aplicativo poderá detectar a ameaça nos bancos de dados de e-mail usando a tarefa *Verificação de malware*. O aplicativo não desinfecta nem exclui arquivos infectados nos bancos de dados de e-mail, independentemente das configurações da tarefa. Isso ocorre porque o Kaspersky Endpoint Security não divide as mensagens do Thunderbird, MyOffice e P7-Office em suas partes (cabeçalho, corpo e anexos) da mesma forma que faz com as mensagens do Microsoft Office Outlook. O aplicativo adiciona somente informações sobre os objetos detectados à lista de ameaças ativas.

Para eliminar ameaças ativas:

1. Localize e exclua manualmente a mensagem com o objeto detectado na interface do programa de e-mail.

   O aplicativo exibe as informações sobre o objeto detectado na lista de ameaças ativas.

   Exemplo de cartão de objeto detectado:

!	**HEUR:Trojan.PDF.Phish.gen** Objeto: `C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\ov56jpz0.default-release\Mail\mail.company.ru\Inbox//` `[From USER NAME <company@mail.com>][Date 25 Sep 2025 20:05:36] [Subj Mail title X] Object.pdf`

2. Execute a operação de compactação do banco de dados.

   Quando uma mensagem for excluída na interface do usuário, o programa de e-mail adicionará apenas uma marca de exclusão. O programa de e-mail realmente exclui a mensagem apenas após a compactação do banco de dados. Para obter informações sobre a compactação do banco de dados, consulte a ajuda do programa de e-mail (por exemplo, Mozilla Thunderbird).

3. Execute novamente a tarefa *Verificação de malware* e verifique se a ameaça não está mais presente.

Se, por algum motivo, não for possível excluir mensagens com arquivos infectados no momento, você poderá processar essas ameaças na interface do usuário do Kaspersky Endpoint Security. Para arquivos de clientes de e-mail, há duas opções para processar uma ameaça: **Ignorar** e **Adicionar às exclusões**. Para impedir que o aplicativo adicione esses objetos à lista de ameaças ativas durante uma nova verificação, adicione-os à lista de exclusões da verificação.

Proteção Contra Ameaças à Rede

O componente *Proteção Contra Ameaças à Rede* (também chamado de Intrusion Detection System, IDS) monitora o tráfego de rede de entrada em busca de atividades com características de ataques de rede. Quando o aplicativo detecta uma tentativa de ataque de rede no computador do usuário, ele bloqueia a conexão de rede com o computador atacante. 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.

Ativar e desativar a Proteção Contra Ameaças à Rede

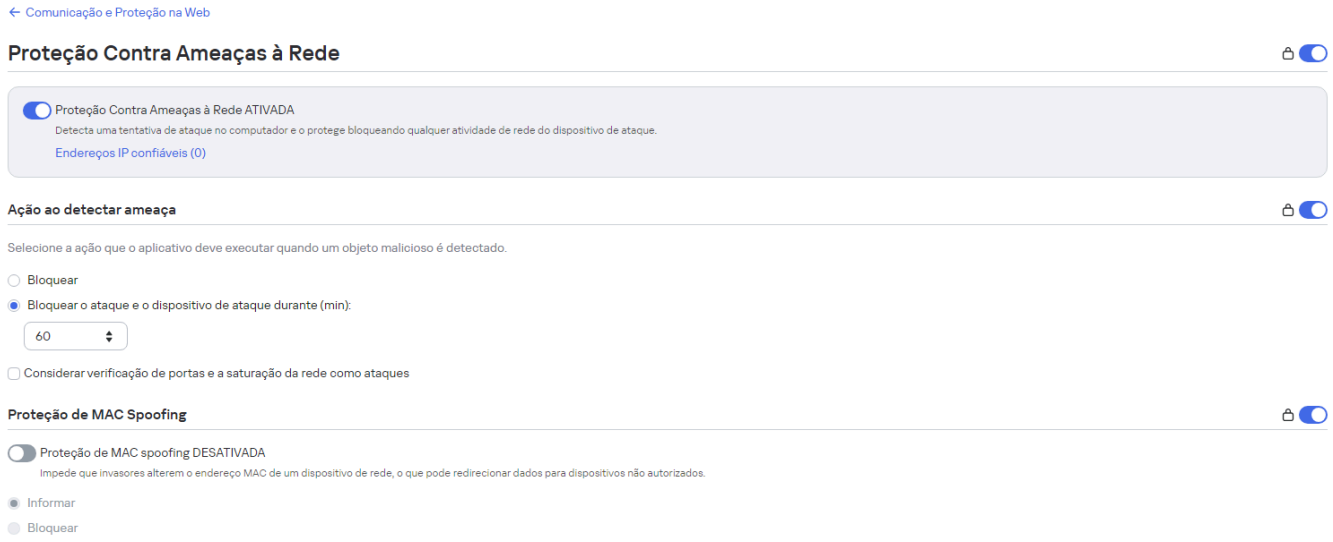
Por padrão, a Proteção Contra Ameaças à Rede é ativada e funciona no modo ideal. O Kaspersky Endpoint Security monitora o tráfego de rede de entrada em busca de atividades com características de ataques de rede e bloqueia os ataques.

Como ativar ou desativar a Proteção Contra Ameaças à Rede no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças à Rede**.
4. Use a caixa de seleção **Proteção Contra Ameaças à Rede** para ativar ou desativar o componente.
5. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar ou desativar a Proteção Contra Ameaças à Rede no Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Comunicação e Proteção na Web** → **Proteção Contra Ameaças à Rede**.



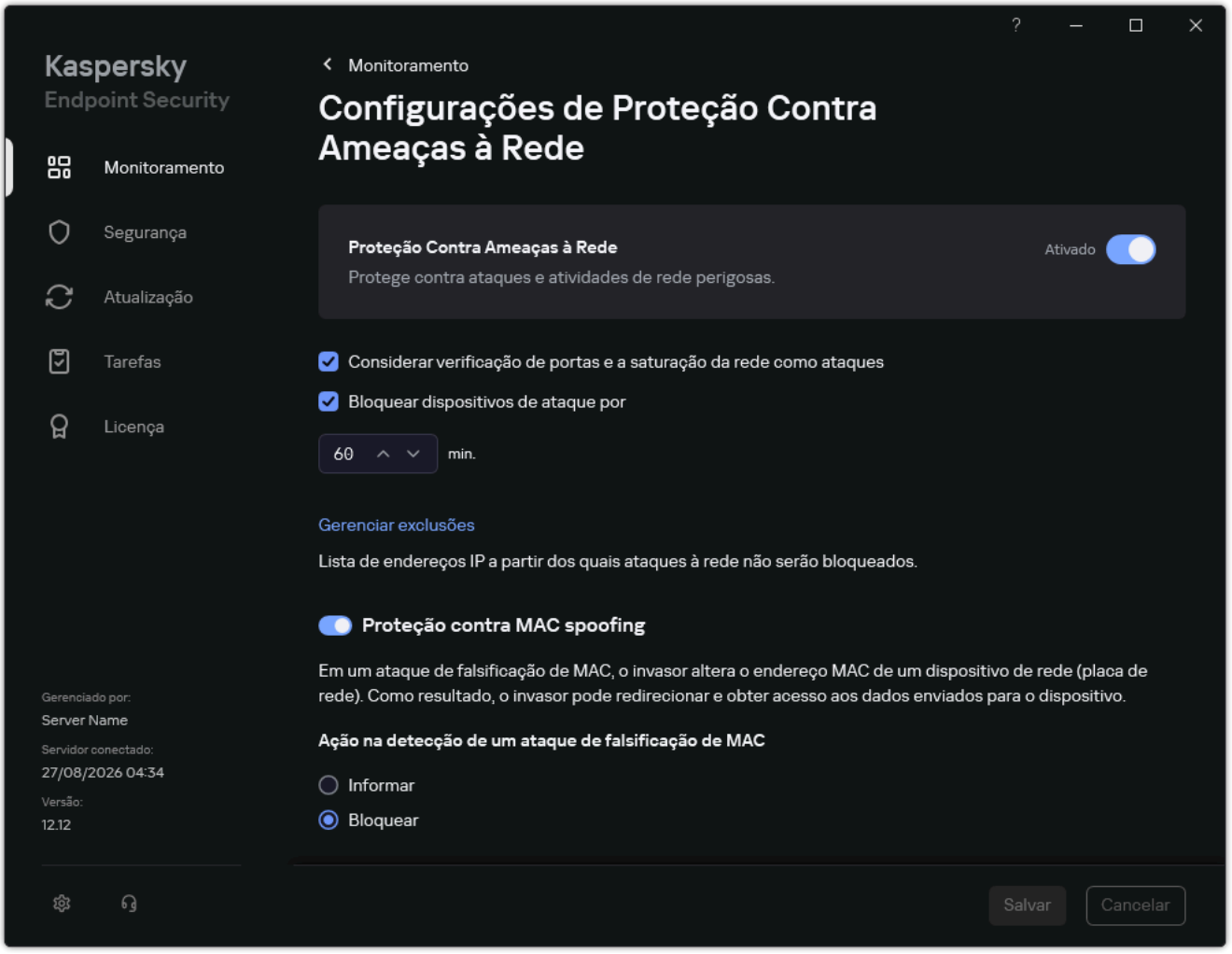
Configurações de Proteção contra ameaças à rede

5. Use o botão de alternância do **Proteção Contra Ameaças à Rede ATIVADA** para ativar ou desativar o componente.
6. Salvar alterações.

Como ativar ou desativar a Proteção Contra Ameaças à Rede na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças à Rede**.



Configurações de Proteção contra ameaças à rede

3. Use o botão de alternância do **Proteção Contra Ameaças à Rede** para ativar ou desativar o componente.

4. Salvar alterações.

Bloquear um computador atacante

Se o componente Proteção Contra Ameaças à Rede estiver ativado, o Kaspersky Endpoint Security bloqueia automaticamente as ameaças à rede. Além disso, o aplicativo pode bloquear o computador atacante e restringir o envio de pacotes de rede por um determinado período de tempo. Por padrão, o Kaspersky Endpoint Security bloqueia o computador por uma hora.

Como bloquear um computador atacante no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças à Rede**.

4. Em **Configurações de Proteção Contra Ameaças à Rede**, marque a caixa de seleção **Bloquear dispositivos de ataque por N min**.

   Caso esta opção seja ativada, o componente Proteção Contra Ameaças à Rede adicionará o computador atacante à lista bloqueada. Isso significa que o componente Proteção Contra Ameaças à Rede bloqueia a conexão de rede com o computador de ataque depois da primeira tentativa de ataque de rede pelo período de tempo especificado. Esse bloqueio protege automaticamente o computador do usuário contra a ocorrência de ataques de rede futuros que se originem do mesmo endereço. O tempo mínimo que um computador atacante deve gastar na lista de bloqueio é um minuto. O tempo máximo é de 999 minutos.

5. Defina uma duração de bloqueio diferente para um computador de ataque no campo à direita da caixa de seleção **Bloquear dispositivos de ataque por N min**.

6. Salvar alterações.

Como bloquear um computador atacante no Web Console

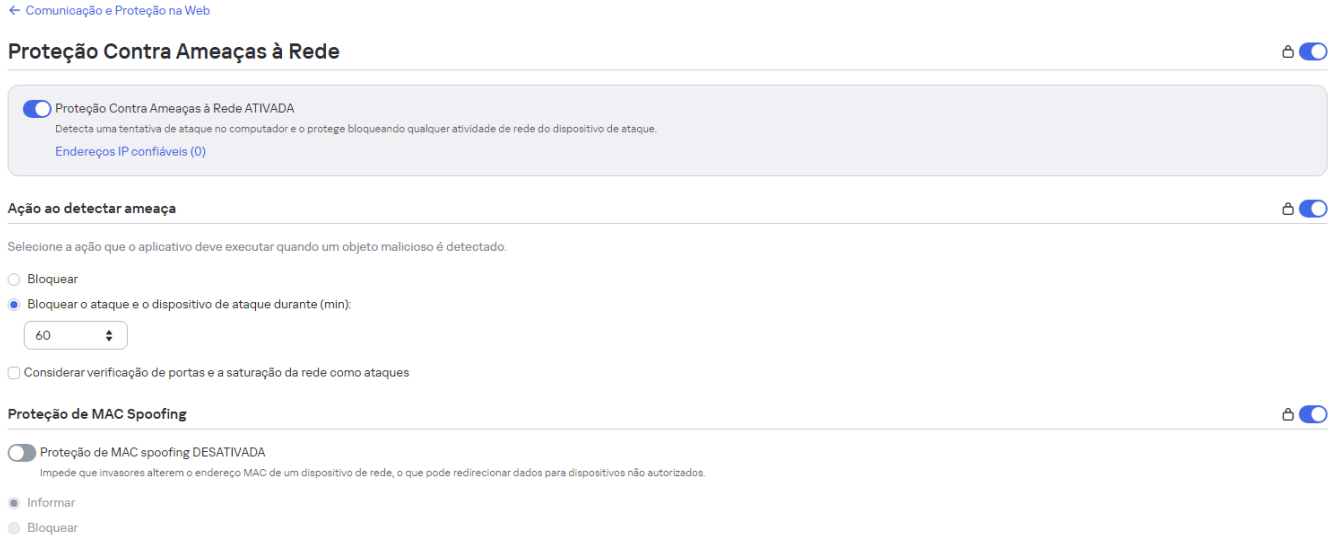
1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Comunicação e Proteção na Web** → **Proteção Contra Ameaças à Rede**.



Configurações de Proteção contra ameaças à rede

5. No bloco **Ação ao detectar ameaça**, marque a caixa de seleção **Bloquear o ataque e o dispositivo de ataque durante (min)**.

   Caso esta opção seja ativada, o componente Proteção Contra Ameaças à Rede adicionará o computador atacante à lista bloqueada. Isso significa que o componente Proteção Contra Ameaças à Rede bloqueia a conexão de rede com o computador de ataque depois da primeira tentativa de ataque de rede pelo período de tempo especificado. Esse bloqueio protege automaticamente o computador do usuário contra a ocorrência de ataques de rede futuros que se originem do mesmo endereço. O tempo mínimo que um computador atacante deve gastar na lista de bloqueio é um minuto. O tempo máximo é de 999 minutos.

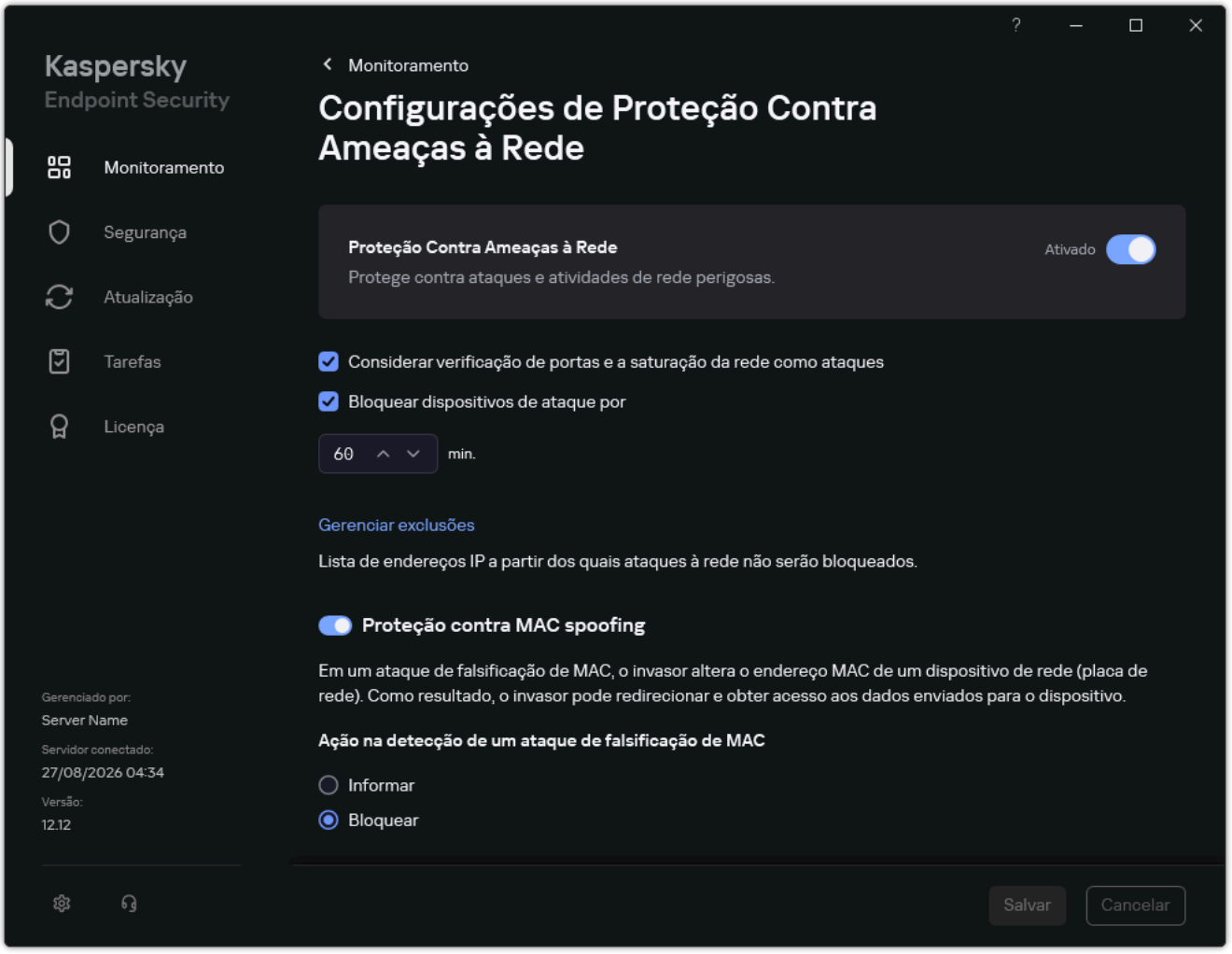
6. Altere a duração do bloqueio do computador atacante.

7. Salvar alterações.

Como bloquear um computador atacante na interface do usuário do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças à Rede**.



Configurações de Proteção contra ameaças à rede

3. Ative o botão de alternância **Bloquear dispositivos de ataque por N min**.

   Caso esta opção seja ativada, o componente Proteção Contra Ameaças à Rede adicionará o computador atacante à lista bloqueada. Isso significa que o componente Proteção Contra Ameaças à Rede bloqueia a conexão de rede com o computador de ataque depois da primeira tentativa de ataque de rede pelo período de tempo especificado. Esse bloqueio protege automaticamente o computador do usuário contra a ocorrência de ataques de rede futuros que se originem do mesmo endereço. O tempo mínimo que um computador atacante deve gastar na lista de bloqueio é um minuto. O tempo máximo é de 999 minutos.

4. Defina uma duração de bloqueio diferente para um computador atacante no campo abaixo do botão de alternância **Bloquear dispositivos de ataque por N min**.

5. Salvar alterações.

Como resultado, quando o Kaspersky Endpoint Security detecta uma tentativa de ataque de rede no computador de um usuário, ele bloqueia todas as conexões com o computador atacante. O Kaspersky Endpoint Security cria os eventos *Ataque de rede detectado*. O evento contém as informações sobre o computador atacante: Endereços IP e MAC.

É possível visualizar o endereço MAC do computador atacante na interface do usuário do aplicativo ou no console do Kaspersky Security Center versão 15.1 ou posterior.

Notificação sobre detecção de ataque à rede

O Kaspersky Endpoint Security desbloqueia o computador quando o tempo especificado se esgota. O console do Kaspersky Security Center não fornece ferramentas para monitorar computadores bloqueados além dos eventos no relatório *Ataque de rede detectado*. É possível visualizar a lista de computadores bloqueadores apenas na interface do aplicativo. Essa funcionalidade é fornecida pela ferramenta *Monitor de rede*. Também é possível usar a ferramenta Monitor de Rede para desbloquear um computador.

Para desbloquear um computador:

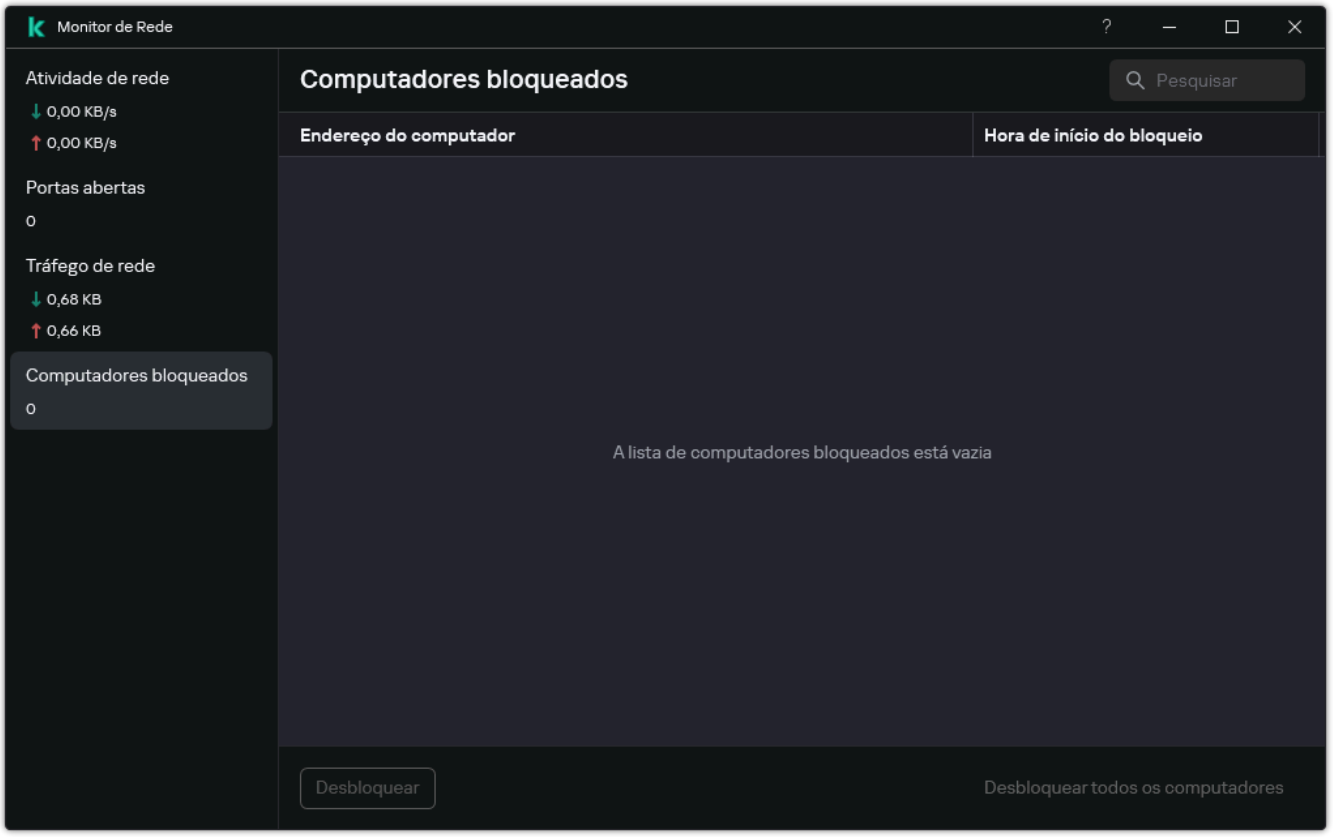
1. Na janela principal do aplicativo, na seção **Monitoramento**, clique no bloco **Monitor de Rede**.

2. Vá para a guia **Computadores bloqueados**.

   Isso abre uma lista de computadores bloqueados (veja a figura abaixo).

   O Kaspersky Endpoint Security limpa a lista de bloqueio quando o aplicativo é reiniciado e quando as configurações de proteção contra ameaças à rede são alteradas.

3. Selecione o computador que deseja desbloquear e clique em **Desbloquear**.



Lista de computadores bloqueados

Configurar endereços de exclusões de bloqueio

O Kaspersky Endpoint 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.

Como configurar endereços de exclusões de bloqueio no Console de Administração (MMC)

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

2. Na árvore do console, selecione **Políticas**.

3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

4. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças à Rede**.

5. No bloco **Configurações de Proteção Contra Ameaças à Rede**, clique no botão **Exclusões**.

6. Na janela que é aberta, clique no botão **Adicionar**.

7. Insira o endereço IP do computador a partir do qual os ataques de rede não devem ser bloqueados.

   Se necessário, selecione o protocolo e as portas pelas quais os dados são transmitidos.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

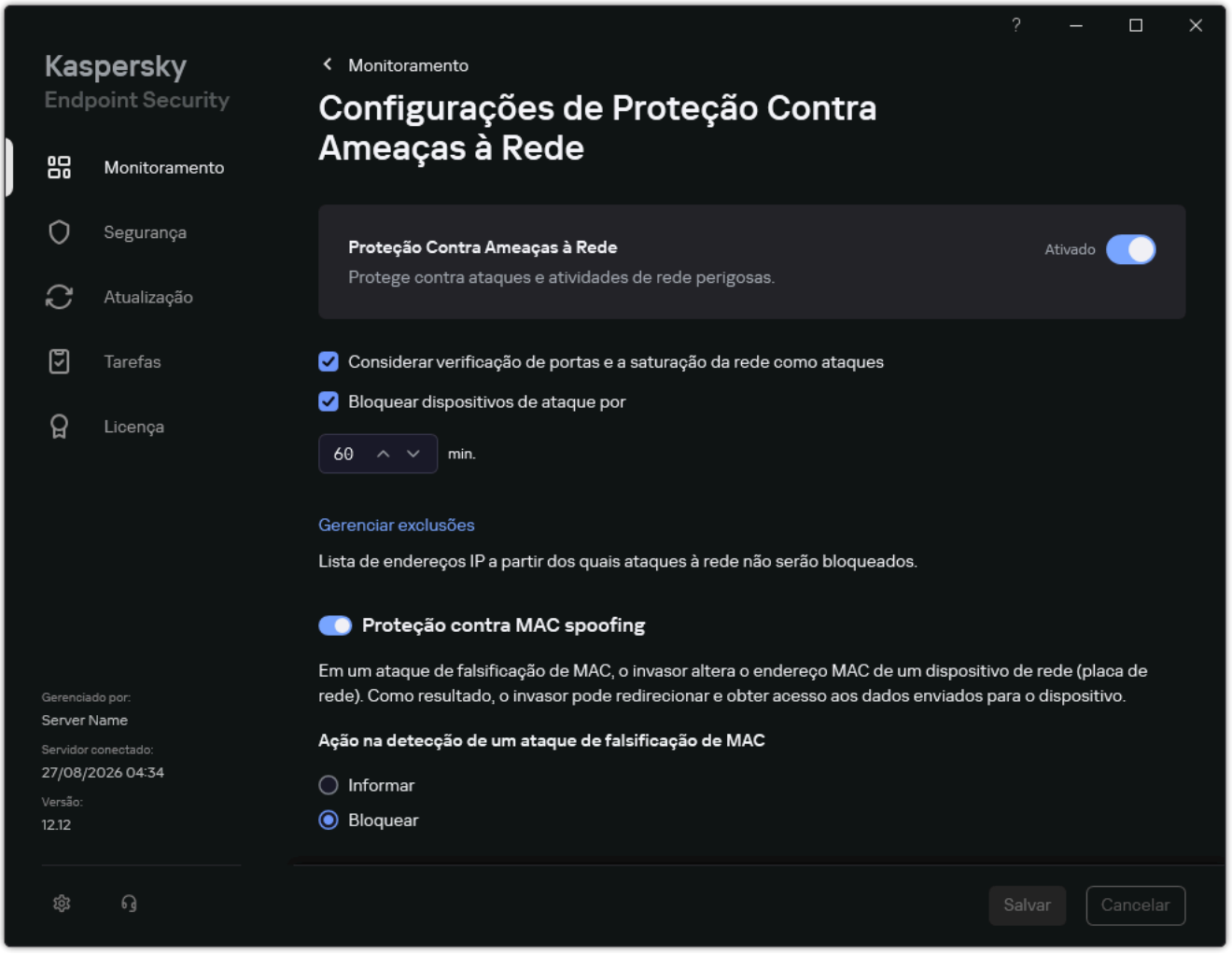
Como configurar endereços excluídos do bloqueio no Web Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Ir para a seção **Zona Confiável**.
5. Na janela aberta, clique no link **Endereços IP**.
   Essa ação abre uma janela que contém uma lista de endereços IP confiáveis.
6. Na janela que é aberta, clique no botão **Adicionar**.
7. Insira o endereço IP do computador a partir do qual os ataques de rede não devem ser bloqueados.
   Caso necessário, especifique a sub-rede.
8. Para aplicar a política aos computadores, feche os ícones de cadeado 🔒 e salve as alterações.

Como configurar endereços de exclusões de bloqueio na interface do usuário do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças à Rede**.



Configurações de Proteção contra ameaças à rede

3. Clique no link **Gerenciar exclusões**.

4. Na janela que é aberta, clique no botão **Adicionar**.

5. Insira o endereço IP do computador a partir do qual os ataques de rede não devem ser bloqueados.

   Se necessário, selecione o protocolo e as portas pelas quais os dados são transmitidos.

6. Salvar alterações.

Exportar e importar a lista de exclusões do bloqueio

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 (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças à Rede**.
4. No bloco **Configurações de Proteção Contra Ameaças à Rede**, clique no botão **Exclusões**.
5. Para exportar a lista de regras:
   a. Selecione as exclusões que deseja exportar. Para selecionar várias portas, use as teclas **CTRL** ou **SHIFT**.
      Se você não selecionou nenhuma exclusão, o Kaspersky Endpoint Security exportará todas as exclusões.
   b. Clique no botão → **Exportar**.
   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 Endpoint Security exporta toda a lista de exclusões para o arquivo XML.
6. Para importar a lista de exclusões:
   a. Clique no botão → **Importar**.
   b. Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de exclusões.
   c. Abra o arquivo.
      Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint 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 exclusões no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Comunicação e Proteção na Web** → **Proteção Contra Ameaças à Rede**.
5. Na parte superior da janela, clique no link **Endereços IP confiáveis**.
   A lista de exclusões é aberta.

6. Para exportar a lista de regras:

   a. Selecione as exclusões que deseja exportar.

   b. Clique no botão → **Exportar**.

      O Kaspersky Endpoint Security exporta a lista de exclusões para um arquivo JSON na pasta de downloads padrão.

7. Para importar a lista de exclusões:

   a. Clique no botão → **Importar**.

      Na janela exibida, selecione o arquivo JSON do qual deseja importar a lista de exclusões.

   b. Abra o arquivo.

      Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo JSON.

8. Salvar alterações.

Configurar a Proteção Contra Ameaças à Rede por tipo

O Kaspersky Endpoint Security permite gerenciar a proteção contra os seguintes tipos de ataques de rede:

- *Saturação de rede* é um ataque aos recursos de rede de uma organização (como servidores da web). Esse ataque consiste no envio de um grande número de solicitações para sobrecarregar a largura de banda dos recursos de rede. Quando isso acontece, os usuários não conseguem acessar os recursos de rede da organização.

- Um ataque de *verificação de portas* consiste em varrer portas UDP, portas TCP e serviços de rede no computador. Esse ataque permite ao atacante identificar o grau de vulnerabilidade do computador antes de efetuar outros tipos mais perigosos de ataques de rede. A verificação de portas também permite ao invasor identificar o sistema operacional no computador e selecionar os ataques de rede apropriados para esse sistema operacional.

- Um *ataque de falsificação de MAC* consiste em alterar o endereço MAC de um dispositivo de rede (placa de rede). Como resultado, um invasor pode redirecionar dados enviados para um dispositivo para outro dispositivo e obter acesso a esses dados. O Kaspersky Endpoint Security permite bloquear ataques de MAC spoofing e receber notificações sobre os ataques.

É possível desativar a detecção desses tipos de ataques caso alguns dos aplicativos permitidos realizem operações típicas desses tipos de ataques. Isso ajudará a evitar alarmes falsos.

Por padrão, o Kaspersky Endpoint Security não monitora ataques de saturação de rede, verificação de portas e falsificação de MAC.

Não é possível configurar exclusões separadas para esses tipos de ataques. Isso significa que, mesmo que endereços IP individuais sejam adicionados à zona confiável, o Kaspersky Endpoint Security bloqueará o computador invasor se detectar um ataque desse tipo. Você pode ativar ou desativar a detecção desses ataques.

Não recomendamos ativar a proteção contra MAC spoofing em máquinas virtuais na infraestrutura Microsoft Hyper-V. Devido às especificidades da plataforma Microsoft Hyper-V, o Kaspersky Industrial CyberSecurity for Nodes pode bloquear o hipervisor por causa de resultados falsos positivos.

Como configurar a Proteção Contra Ameaças à Rede por tipo no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças à Rede**.
4. Use a caixa de seleção **Considerar verificação de portas e a saturação da rede como ataques** para ativar ou desativar a detecção desses ataques.

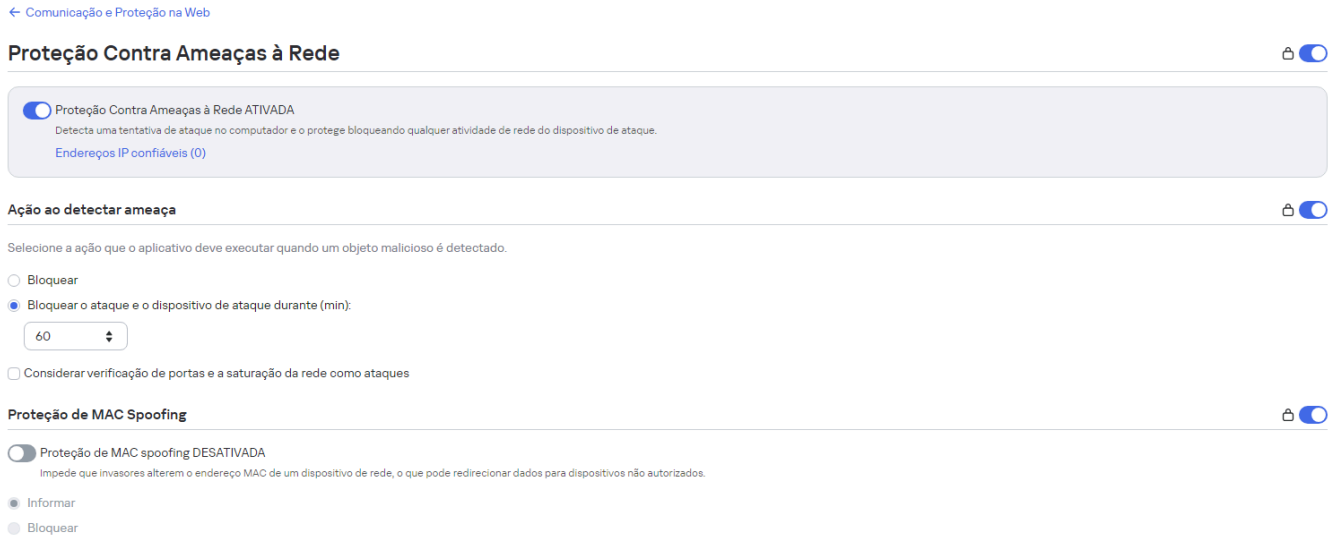
   Caso a funcionalidade esteja ativada, o Kaspersky Endpoint Security monitora o tráfego de rede em busca de varredura de porta e saturação de rede. Caso esse comportamento seja detectado, o aplicativo notifica o usuário e envia o evento correspondente ao Kaspersky Security Center. O aplicativo fornece as informações sobre o computador que está fazendo as requisições. Essa informação é necessária para uma pronta resposta. Entretanto, o Kaspersky Endpoint Security não bloqueia o computador que está fazendo as requisições, pois esse tráfego pode ser uma ocorrência normal na rede corporativa.
5. No bloco **Modo de proteção de MAC spoofing**, escolha uma das seguintes opções:
   - **Não rastrear MAC spoofing**.
   - **Informar**.
   - **Bloquear**.
6. Salvar alterações.

Como configurar a Proteção Contra Ameaças à Rede por tipo no Web Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.

4. Selecione **Comunicação e Proteção na Web** → **Proteção Contra Ameaças à Rede**.



Configurações de Proteção contra ameaças à rede

5. Use a caixa de seleção **Considerar verificação de portas e a saturação da rede como ataques** para ativar ou desativar a detecção desses ataques.

   Caso a funcionalidade esteja ativada, o Kaspersky Endpoint Security monitora o tráfego de rede em busca de varredura de porta e saturação de rede. Caso esse comportamento seja detectado, o aplicativo notifica o usuário e envia o evento correspondente ao Kaspersky Security Center. O aplicativo fornece as informações sobre o computador que está fazendo as requisições. Essa informação é necessária para uma pronta resposta. Entretanto, o Kaspersky Endpoint Security não bloqueia o computador que está fazendo as requisições, pois esse tráfego pode ser uma ocorrência normal na rede corporativa.

6. Em **Proteção de MAC Spoofing**, configure a detecção de ataques de MAC spoofing:

   a. Utilize o botão de alternância **Proteção de MAC spoofing ATIVADA** para ativar ou desativar a detecção desses ataques.

   b. Selecione a ação a ser executada quando um ataque de MAC spoofing for detectado:

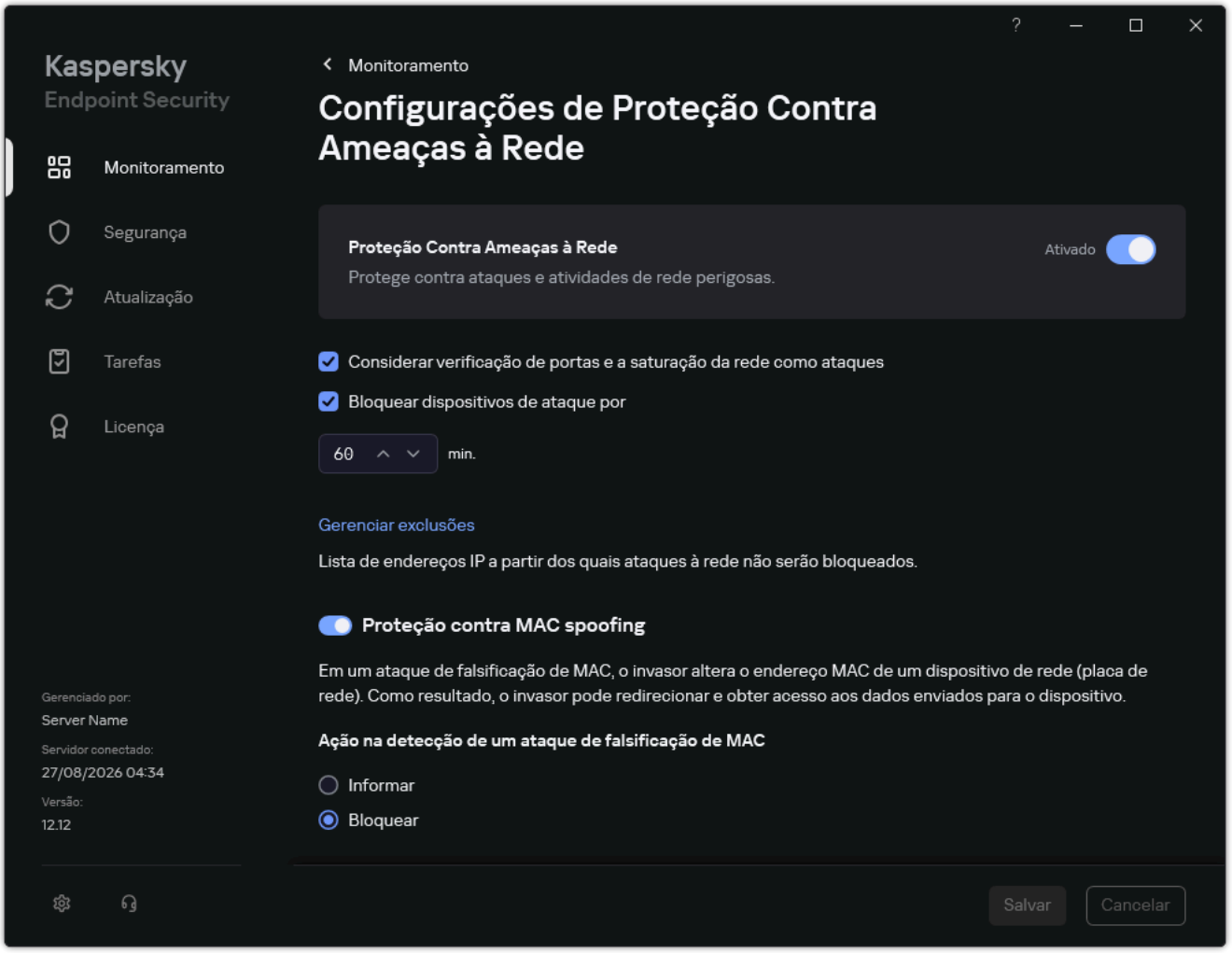
      - **Informar**.
      - **Bloquear**.

7. Salvar alterações.

Como configurar a Proteção Contra Ameaças à Rede por tipo na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças à Rede**.



Configurações de Proteção contra ameaças à rede

3. Utilize o botão de alternância **Considerar verificação de portas e a saturação da rede como ataques** para ativar ou desativar a detecção desses ataques.

   Caso a funcionalidade esteja ativada, o Kaspersky Endpoint Security monitora o tráfego de rede em busca de varredura de porta e saturação de rede. Caso esse comportamento seja detectado, o aplicativo notifica o usuário e envia o evento correspondente ao Kaspersky Security Center. O aplicativo fornece as informações sobre o computador que está fazendo as requisições. Essa informação é necessária para uma pronta resposta. Entretanto, o Kaspersky Endpoint Security não bloqueia o computador que está fazendo as requisições, pois esse tráfego pode ser uma ocorrência normal na rede corporativa.

4. Utilize o botão de alternância **Proteção contra MAC spoofing** para ativar ou desativar a detecção desses ataques.

5. No bloco **Ação na detecção de um ataque de falsificação de MAC**, escolha uma das seguintes opções:

   - **Informar**.
   - **Bloquear**.

6. Salvar alterações.

Firewall

O componente Firewall bloqueia conexões não autorizadas ao computador enquanto conectado na Internet ou na rede local. O Firewall também controla a atividade de rede dos aplicativos no computador. Isso permite proteger sua LAN contra roubo de identidade e outros ataques. O componente fornece proteção ao computador com a ajuda de bancos de dados antivírus, o serviço na nuvem da Kaspersky Security Network e *regras de rede* predefinidas.

O agente de rede é usado para interação com o Kaspersky Security Center. O Firewall cria automaticamente as regras de rede necessárias para que o aplicativo e o agente de rede funcionem. Como resultado, o Firewall abre várias portas no computador. Quais portas serão abertas depende da função do computador (por exemplo, ponto de distribuição). Para saber mais sobre as portas que serão abertas no computador, consulte a Ajuda do Kaspersky Security Center.

Regras de rede

Você pode configurar regras de rede nos seguintes níveis:

- *Regras de pacotes de rede*. As regras de pacotes de rede impõem restrições a pacotes de rede, seja qual for o aplicativo. Estas regras restringem o tráfego de rede de entrada e de saída através de portas específicas do protocolo de dados selecionado. O Kaspersky Endpoint Security predefiniu regras de pacotes de rede com permissões recomendadas por especialistas da Kaspersky.

- *Regras de rede de aplicativos*. As regras de rede de aplicativos impõem restrições à atividade de rede de um aplicativo específico. Elas têm em conta não só as características do pacote de rede, mas também o aplicativo específico para o qual este pacote de rede é direcionado ou que emitiu este pacote de rede.

O acesso controlado de aplicativos aos recursos, processos e dados pessoais do sistema operacional é fornecido pelo componente Prevenção de Intrusão do Host usando *direitos de aplicativo*.

Durante a primeira inicialização do aplicativo, o Firewall executa as seguintes ações:

1. Verifica a segurança do aplicativo usando bancos de dados de antivírus baixados.

2. Verifica a segurança do aplicativo na Kaspersky Security Network.

   A participação na Kaspersky Security Network é recomendada para ajudar o Firewall a funcionar de maneira mais eficiente.

3. Coloca o aplicativo em um dos grupos de confiança: *Confiável*, *Baixa restrição*, *Alta restrição*, *Não confiável*.

   Um grupo confiável define os direitos aos quais o Kaspersky Endpoint Security se refere ao controlar a atividade do aplicativo. O Kaspersky Endpoint Security coloca um aplicativo em um grupo de confiança, dependendo do nível de perigo que esse aplicativo pode representar para o computador.

O Kaspersky Endpoint Security coloca um aplicativo em um grupo de confiança para os componentes Firewall e Prevenção de Intrusão do Host. Você não pode alterar o grupo de confiança apenas para o Firewall ou Prevenção de Intrusão do Host.

Se você se recusou a participar do KSN ou não há rede, o Kaspersky Endpoint Security coloca o aplicativo em um grupo de confiança, dependendo das configurações do componente Prevenção de Intrusão do Host. Após receber a reputação do aplicativo da KSN, o grupo de confiança pode ser alterado automaticamente.

4. Bloqueia a atividade de rede do aplicativo, dependendo do grupo de confiança. Por exemplo, os aplicativos no grupo de confiança de *Alta restrição* não têm permissão para usar nenhuma conexão de rede.

Na próxima vez em que o aplicativo for iniciado, a Prevenção de Intrusão do Host verificará sua integridade. Se o aplicativo não estiver modificado, o componente usará as regras de rede atuais para ele. Se o aplicativo foi modificado, o Kaspersky Endpoint Security o analisará como se estivesse sendo iniciado pela primeira vez.

Prioridades de regra de rede

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

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

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

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

Tipos da conexão de rede

O Firewall permite controlar a atividade da rede, dependendo do tipo da conexão de rede. O Kaspersky Endpoint Security recebe o tipo da conexão de rede do sistema operacional do computador. O tipo da conexão de rede no sistema operacional é definido pelo usuário ao configurar a conexão. Você pode alterar o tipo da conexão de rede nas configurações do Kaspersky Endpoint Security. O firewall monitorará a atividade da rede, dependendo do tipo de rede, especificado nas configurações do Kaspersky Endpoint Security, e não do sistema operacional.

Os seguintes tipos de conexão de rede estão disponíveis:

- **Rede pública**. A rede não está protegida por aplicativos antivírus, firewalls ou filtros (como Wi-Fi em um café). Quando o usuário utiliza um computador que está conectado a uma rede desse tipo, o Firewall bloqueia o acesso a arquivos e impressoras desse computador. Os usuários externos também não podem acessar dados por meio de pastas compartilhadas e acesso remoto à área de trabalho deste computador. O Firewall filtra a atividade de rede de cada aplicativo, de acordo com as regras de rede definidas para cada uma.

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

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

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

Compatibilidade com o Firewall do Windows Defender

O sistema operacional tem um firewall integrado próprio, o *Firewall do Windows Defender*. O aplicativo se comporta de maneira diferente dependendo do tipo de sistema operacional:

- **Estação de trabalho**. Usar o Firewall da Kaspersky em paralelo com o Firewall do Windows Defender pode causar o funcionamento incorreto do sistema operacional. Portanto, o Kaspersky Endpoint Security tem um mecanismo que impede que ambos os firewalls sejam usados simultaneamente. Quando você ativa o Firewall da Kaspersky, o sistema operacional desativa automaticamente o Firewall do Windows Defender. Quando você desativa o Firewall da Kaspersky, o sistema operacional reativa automaticamente o Firewall do Windows Defender para manter o computador protegido.

- **Servidor**. O Firewall da Kaspersky e o Firewall do Windows Defender são incompatíveis entre si. O instalador do Kaspersky Endpoint Security remove automaticamente o Firewall do Windows Defender durante a instalação do aplicativo.

Ativar ou desativar o Firewall

Por padrão, o Firewall está ativado e funciona no modo normal.

Como ativar ou desativar o firewall no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.

4. Use a caixa de seleção **Firewall** para ativar ou desativar o componente.

5. Salvar alterações.

Como ativar ou desativar o Firewall no Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Comunicação e Proteção na Web** → **Firewall**.
5. Use o botão de alternância do **Firewall ATIVADO** para ativar ou desativar o componente.
6. Salvar alterações.

Como ativar ou desativar o firewall na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.
3. Use o botão de alternância do **Firewall** para ativar ou desativar o componente.
4. Salvar alterações.

Como resultado, se o Firewall estiver ativado, o Kaspersky Endpoint Security controla a atividade de rede e bloqueia conexões de rede não autorizadas ao computador, além de bloquear atividades de rede não autorizadas de aplicativos no computador. A atividade da rede também é controlada pelo componente de Proteção Contra Ameaças à Rede. O componente Proteção Contra Ameaças à Rede (também chamado de Intrusion Detection System, IDS) monitora o tráfego de rede de entrada em busca de atividades com características de ataques de rede.

O Kaspersky Endpoint Security registra eventos de ataque de rede em seus relatórios, independentemente das configurações do Firewall. Mesmo que o Firewall bloqueie a conexão de rede usando regras e, assim, evite um ataque à rede, o componente Proteção Contra Ameaças à Rede registra os eventos de ataque à rede. Ele é necessário para gerar informações estatísticas sobre ataques de rede nos computadores da organização.

Alterar o tipo de conexão de rede

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

Para alterar o tipo da conexão de rede:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.
3. Clique **Redes disponíveis**.
4. Selecione a conexão de rede cujo tipo deseja alterar.

5. Na coluna **Tipo de rede**, selecione o tipo da conexão de rede:

   - **Rede pública**. A rede não está protegida por aplicativos antivírus, firewalls ou filtros (como Wi-Fi em um café). Quando o usuário utiliza um computador que está conectado a uma rede desse tipo, o Firewall bloqueia o acesso a arquivos e impressoras desse computador. Os usuários externos também não podem acessar dados por meio de pastas compartilhadas e acesso remoto à área de trabalho deste computador. O Firewall filtra a atividade de rede de cada aplicativo, de acordo com as regras de rede definidas para cada uma.

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

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

6. Salvar alterações.

Gerenciar regras de pacotes de rede

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

- Criar uma nova regra de pacotes de rede.

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

- Ativar ou desativar uma regra de pacotes de rede.

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

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

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

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

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

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

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

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

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

- Excluir uma regra de pacotes de rede.

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

Criar uma regra de pacote de rede

O Firewall filtra todas as atividades de rede no computador de acordo com as regras de pacotes de rede. As regras de pacotes de rede incluem condições, como direção e protocolo, que o Firewall aplica para controlar as conexões de rede do computador. As regras de pacotes de rede também definem se o Firewall permitirá ou bloqueará a conexão correspondente (permitir ou bloquear a conexão).

Recomendações para criar regras de pacotes de rede

É possível especificar um endereço IP ou um intervalo de endereços IP para filtrar a atividade da rede. Você também pode especificar um nome DNS.

Se um nome DNS for usado em uma regra, o Kaspersky Endpoint Security resolverá esse nome DNS para um endereço IP e, posteriormente, tratará a regra como se esse endereço IP estivesse especificado nela.

O Kaspersky Endpoint Security pode resolver nomes DNS nos seguintes casos:

- Inicialização do aplicativo
- Alteração das configurações do Firewall

Quando o aplicativo resolve nomes DNS no computador em que está instalado, um grande número de consultas pode ser enviado ao servidor DNS. Para evitar isso, recomendamos usar endereços IP em vez de nomes DNS ao criar regras.

Em alguns casos, o uso de nomes DNS em nomes de pacotes de rede pode não ser seguro, pois o proprietário do servidor DNS pode alterar os parâmetros do registro DNS. Um agente malicioso também pode falsificar mensagens DNS e burlar as regras do Firewall.

É possível controlar as conexões de rede por nomes DNS com o uso das regras de Controle da Web. Caso necessite especificar um nome DNS nas regras do Firewall:

- Garanta a segurança da rede local corporativa.
- Garanta a segurança do armazenamento em cache e servidores DNS autoritativos.
- Ative a proteção do registro DNS contra modificação.

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

Métodos de criação de regras de pacotes de rede

É possível criar uma regra de pacote de rede das seguintes maneiras:

- Usar a ferramenta Monitor de Rede.

  O *Monitor de Rede* é uma ferramenta desenvolvida para exibir as informações sobre a atividade do computador de um usuário em tempo real. O procedimento é conveniente porque não é preciso definir todas as configurações de regras. Algumas configurações do Firewall serão inseridas automaticamente a partir dos dados do Monitor de Rede. O Monitor de Rede está disponível somente na interface do aplicativo.

- Defina as configurações do firewall.

  Isso permite refinar as configurações do Firewall. É possível criar regras para qualquer atividade de rede, mesmo que não haja nenhuma atividade de rede no momento atual.

Como usar a ferramenta Monitor de Rede para criar uma regra de pacote de rede na interface do aplicativo

1. Na janela principal do aplicativo, na seção **Monitoramento**, clique no bloco **Monitor de Rede**.

2. Vá para a guia **Atividade de rede**.

   A guia **Atividade de rede** exibe todas as conexões de rede atuais estabelecidas com o computador. São exibidos o tráfego de entrada e de saída das conexões de rede.

3. No menu de contexto de uma conexão de rede, selecione **Criar uma regra de pacote de rede**.

   As propriedades da regra de pacotes aparecerão.

4. Defina o status **Ativo** para a regra de pacote.

5. Insira manualmente o nome do serviço de rede no campo **Nome**.

6. Configure as definições da regra de rede (consulte a tabela abaixo).

   É possível selecionar um modelo de regra predefinido clicando no link **Modelo de regra de rede**. Os modelos de regras descrevem as conexões de rede usadas com mais frequência.

   Todas as configurações de regras de rede serão preenchidas automaticamente.

7. Se desejar que as ações da regra de rede sejam refletidas no relatório, marque a caixa de seleção **Registrar eventos**.

8. Clique **Salvar**.

   A regra de rede será adicionada à lista.

9. Use os botões **Acima**/**Abaixo** para definir a prioridade da regra de rede.

10. Salvar alterações.

Como usar as configurações do Firewall para criar uma regra de pacote de rede na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.

3. Clique **Regras de pacotes**.

   Isso abrirá a lista de regras de rede padrão definidas pelo Firewall.

4. Ao usar a lista suspensa **Adicionar**, selecione o local da regra na lista: na parte superior, na parte inferior da lista ou ao lado da regra selecionada.

   A posição da regra na lista determina a prioridade da regra. A regra no topo da lista tem a prioridade mais alta.

5. Defina o status **Ativo** para a regra de pacote.

6. Insira manualmente o nome do serviço de rede no campo **Nome**.

7. Configure as definições da regra de rede (consulte a tabela abaixo).

   É possível selecionar um modelo de regra predefinido clicando no link **Modelo de regra de rede**. Os modelos de regras descrevem as conexões de rede usadas com mais frequência.

   Todas as configurações de regras de rede serão preenchidas automaticamente.

8. Se desejar que as ações da regra de rede sejam refletidas no relatório, marque a caixa de seleção **Registrar eventos**.

9. Clique **Salvar**.

   A regra de rede será adicionada à lista.

10. Use os botões **Acima**/**Abaixo** para definir a prioridade da regra de rede.

11. Salvar alterações.

Como criar uma regra de pacote de rede no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.

4. No bloco **Configurações do Firewall**, clique no botão **Configurações**.

   Isso abre a lista de regras de pacotes de rede e a lista de regras de rede de aplicativos.

5. Vá para a guia **Regras de pacotes de rede**.

   Isso abrirá a lista de regras de rede padrão definidas pelo Firewall.

6. Ao usar a lista suspensa **Adicionar**, selecione o local da regra na lista: na parte superior, na parte inferior da lista ou ao lado da regra selecionada.

   A posição da regra na lista determina a prioridade da regra. A regra no topo da lista tem a prioridade mais alta.

7. Insira manualmente o nome do serviço de rede no campo **Nome**.

8. Configure as definições da regra de rede (consulte a tabela abaixo).

   É possível selecionar um modelo de regra predefinido ao clicar no botão . Os modelos de regras descrevem as conexões de rede usadas com mais frequência.

   Todas as configurações de regras de rede serão preenchidas automaticamente.

9. Se desejar que as ações da regra de rede sejam refletidas no relatório, marque a caixa de seleção **Criar log de eventos**.

10. Salve a nova regra de rede.

11. Use os botões **Para cima**/**Para baixo** para definir a prioridade da regra de rede.

12. Salvar alterações.

O Firewall controlará os pacotes de rede de acordo com a regra. É possível desativar uma regra de pacote a partir da operação do Firewall sem exclui-la da lista. Para fazer isso, desmarque a caixa de seleção ao lado do objeto.

Como criar uma regra de pacotes de rede na Web Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Comunicação e Proteção na Web** → **Firewall**.

5. Selecione a guia **Regras de pacotes de rede**.

   Isso abrirá a lista de regras de rede padrão definidas pelo Firewall.

6. Clique **Adicionar**.

   Isso abre o formulário para uma nova regra de rede.

7. Insira manualmente o nome do serviço de rede no campo **Nome da regra**.

8. Configure as definições da regra de rede (consulte a tabela abaixo).

   É possível selecionar um modelo de regra predefinido clicando no link **Selecionar o modelo de regra**. Os modelos de regras descrevem as conexões de rede usadas com mais frequência.

   Todas as configurações de regras de rede serão preenchidas automaticamente.

9. Se desejar que as ações da regra de rede sejam refletidas no relatório, marque a caixa de seleção **Criar log de eventos**.

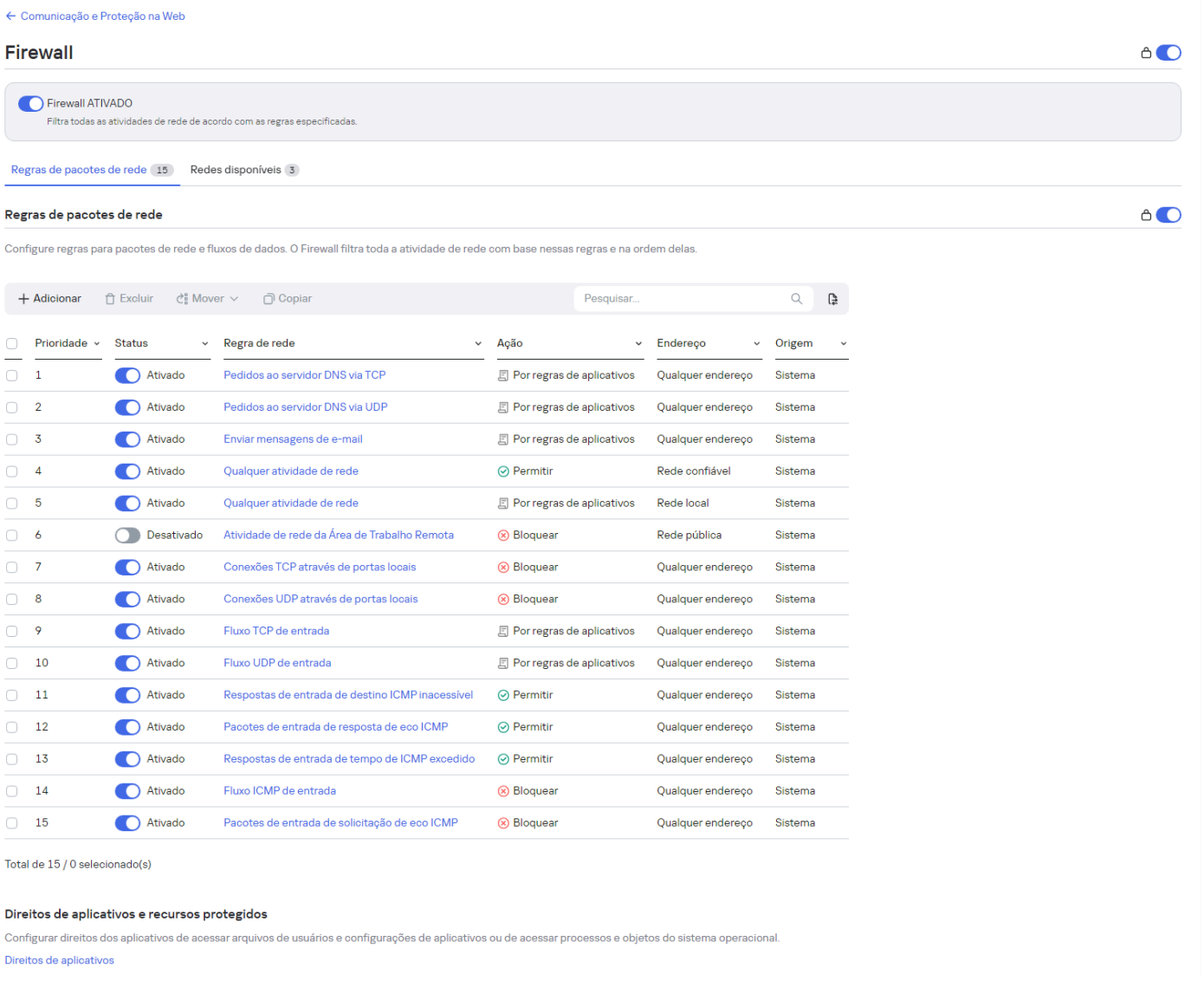
10. Salvar a regra de rede.

    A regra de rede será adicionada à lista.

11. Use o botão **Mover** para definir a prioridade da regra de rede.

12. Salvar alterações.

O Firewall controlará os pacotes de rede de acordo com a regra. É possível desativar uma regra de pacote a partir da operação do Firewall sem exclui-la da lista. Use o botão de alternância na coluna **Status** para ativar ou desativar a regra.



Regras de pacotes do Firewall

Configurações da regra de pacote de rede

Parâmetro	Descrição
Ação	**Permitir**. **Bloquear**. **Por regras de aplicativo**. Se essa opção for selecionada, o Firewall aplica as Regras de rede de aplicativos à conexão de rede.
Protocolo	Controlar a atividade da rede sobre o protocolo selecionado: TCP, UDP, ICMP, ICMPv6, IGMP e GRE. Ao selecionar os protocolos do tipo ICMP ou ICMPv6, especifique o tipo e o código do pacote ICMP. Ao selecionar os protocolos TCP ou UDP, especifique as portas dos computadores local e remoto entre as quais ocorrerá o monitoramento da conexão. Intervalo de valores possíveis para os números de porta: 0-65535. Em cada campo, é possível inserir diversos valores separados por `,` ou especifique um intervalo de valores usando `-`. Por exemplo: • `100,101` • `100-130` • `100,110-130`

Parâmetro	Descrição
Direção	**Entrada (pacote)**. O Firewall aplica a regra de rede a todos os pacotes de rede de entrada. **Entrada**. O Firewall aplica a regra de rede para todos os pacotes de rede enviados por uma conexão iniciada por um computador remoto. **Entrada/Saída**. O Firewall aplica a regra de rede a todos os pacotes de rede de entrada e saída. **Saída (pacote)**. O Firewall aplica a regra de rede para todos os pacotes de rede de saída. **Saída**. O Firewall aplica a regra de rede a todos os pacotes de rede enviados por uma conexão iniciada pelo computador do usuário.
Adaptadores de rede	Os adaptadores de rede que podem enviar e/ou receber pacotes de rede. A especificação das configurações de adaptadores de rede permite diferenciar entre pacotes de rede enviados ou recebidos por adaptadores de rede com endereços IP idênticos.
Vida útil (TTL)	Limitação do controle de pacotes de rede por seu tempo de vida (Time to Live, TTL).
Endereços remotos	Os endereços de rede dos computadores remotos que podem enviar ou receber pacotes de rede. O Firewall aplica uma regra de rede ao intervalo especificado de endereços de rede remotos. É possível incluir todos os endereços IP em uma regra de rede, criar uma lista separada de endereços IP ou especificar um intervalo de endereços IP (redes confiáveis, redes locais, redes públicas). Também é possível especificar um nome DNS de um computador em vez de seu endereço IP. Deve-se usar os nomes DNS apenas para computadores da LAN ou serviços internos. A interação com serviços na nuvem (como o Microsoft Azure) e outros recursos da Internet deve ser tratada pelo componente controle da Web. Se na regra de pacote de rede foi adicionado um nome DNS para o qual o endereço IP não pôde ser determinado, o Kaspersky Endpoint Security exibirá um aviso. Na lista de regras de pacote de rede no Web Console, uma coluna é adicionada com uma descrição do erro. A descrição do erro não está disponível no Console de Administração (MMC). Essas regras de pacotes são destacadas em cores.
Endereços locais	Os endereços de rede dos computadores que podem enviar ou receber pacotes de rede. O Firewall aplica uma regra de rede ao intervalo especificado de endereços de rede locais. É possível incluir todos os endereços IP em uma regra de rede, criar uma lista separada de endereços IP ou especificar um intervalo de endereços IP. O aplicativo armazena endereços locais somente se uma lista de endereços remotos for especificada. Ou seja, se o valor **Endereços da lista** foi selecionado para **Endereços remotos** e pelo menos um endereço foi adicionado. Algumas vezes o endereço local não pode ser obtido para aplicativos. Nesse caso, o parâmetro é ignorado.

Ativar ou desativar uma regra de pacotes de rede

Para ativar ou desativar uma regra de pacotes de rede:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.
3. Clique **Regras de pacotes**.
   Esta guia exibe uma lista de regras de pacotes de rede definidas pelo firewall.
4. Selecione a regra de pacotes de rede necessária na lista.
5. Use o botão de alternância na coluna **Status** para habilitar ou desabilitar a regra.
6. Salvar alterações.

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

Para alterar a ação do Firewall aplicada a uma regra de pacotes de rede:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.
3. Clique **Regras de pacotes**.

   Esta guia exibe uma lista de regras de pacotes de rede definidas pelo firewall.
4. Selecione-a na lista de regras de pacotes de rede e clique no botão **Editar**.
5. Na lista suspensa **Ação**, selecione a ação a ser executada pelo Firewall ao detectar este tipo de atividade de rede:
   - **Permitir**.
   - **Bloquear**.
   - **Por regras de aplicativo**. Se essa opção for selecionada, o Firewall aplica as Regras de rede de aplicativos à conexão de rede.
6. Salvar alterações.

Alterar a prioridade de uma regra de pacotes de rede

A prioridade de uma regra de pacotes de rede é determinada pela sua posição na lista de regras de pacotes de rede. A regra de rede no topo da lista de regras de rede tem prioridade em relação às demais.

Todas as regras de pacotes de rede criadas manualmente são adicionadas ao fim da lista de regras de pacotes de rede, sendo estas precedidas pelas demais.

O Firewall executa as regras na ordem em que aparecem na lista de regras de pacotes de rede, ou seja, de cima para baixo. De acordo com cada regra de rede processada aplicada a uma conexão de rede específica, o Firewall permite ou bloqueia o acesso à rede ao endereço e à porta que estão indicados nas configurações desta conexão de rede.

Para alterar a prioridade das regras de pacotes de rede:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.
3. Clique **Regras de pacotes**.

   Esta guia exibe uma lista de regras de pacotes de rede definidas pelo firewall.
4. Na lista, selecione a regra do pacote de rede cuja prioridade você deseja alterar.

5. Use os botões **Acima**/**Abaixo** para definir a prioridade da regra de rede.

6. Salvar alterações.

Exportar e importar regras de pacotes de rede

Você pode exportar a lista de regras de pacotes de rede para um arquivo XML. Em seguida, você pode modificar o arquivo para, por exemplo, adicionar um grande número de regras do mesmo tipo. Você pode usar a função de exportação/importação para fazer backup da lista de regras de pacotes de rede ou para migrar a lista para um servidor diferente.

Como exportar e importar uma lista de regras de pacotes de rede no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.

4. No bloco **Configurações do Firewall**, clique no botão **Configurações**.

   Isso abre a lista de regras de pacotes de rede e a lista de regras de rede de aplicativos.

5. Vá para a guia **Regras de pacotes de rede**.

6. Para exportar a lista de regras de pacotes de rede:

   a. Selecione as regras que deseja exportar. Para selecionar várias portas, use as teclas `CTRL` ou `SHIFT`.

      Se você não selecionou nenhuma regra, o Kaspersky Endpoint Security exportará todas as regras.

   b. Clique no link **Exportar**.

   c. 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.

   d. Salvar o arquivo.

      O Kaspersky Endpoint Security exporta toda a lista de regras para o arquivo XML.

7. Para importar uma lista de regras de pacotes de rede:

   a. Clique no link **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 Endpoint 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 uma lista de regras de pacotes de rede no Web Console e no Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Comunicação e Proteção na Web** → **Firewall**.
5. Para exportar a lista de regras, na seção **Regras de pacotes de rede**:

   a. Selecione as regras que deseja exportar.

   b. Clique no botão → **Exportar**.

   O Kaspersky Endpoint Security exporta a lista de regras para um arquivo JSON na pasta de downloads padrão.
6. Para importar a lista de regras, na seção **Regras de pacotes de rede**:

   a. Clique no botão → **Importar**.

   Na janela exibida, selecione o arquivo JSON do qual deseja importar a lista de regras.

   b. Abra o arquivo.

   Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo JSON.
7. Salvar alterações.

Definição das regras de pacote de rede no XML

O firewall permite exportar regras de pacote de rede no formato XML. Em seguida, você pode modificar o arquivo para, por exemplo, adicionar um grande número de regras do mesmo tipo.

O arquivo XML contém dois nós principais: `Rules` e `Resources`. O nó `Rules` lista as regras de pacote de rede. Este nó contém regras configuradas por padrão (*regras predefinidas*) bem como regras adicionadas pelo usuário (*regras personalizadas*).

Marcação de regra de pacote de rede

```
<key name="0000">
        <tDWORD name="RuleId">100</tDWORD>
        <tDWORD name="RuleState">1</tDWORD>
        <tDWORD name="RuleTypeId">4</tDWORD>
        <tQWORD name="AppIdEx">0</tQWORD>
        <tDWORD name="ResIdEx">812</tDWORD>
        <tDWORD name="ResIdEx2">0</tDWORD>
        <tDWORD name="AccessFlag">2</tDWORD>
</key>
```

Parâmetro	Descrição	Valor
`<key name="0000">`	Prioridade da regra. Quanto menor o valor, maior será a prioridade.	Número inteiro O valor da prioridade deve consistir em 4 dígitos. Os nós no arquivo XML devem ser organizados por valor de prioridade, começando com `0000`.
`RuleId`	ID a regra.	**Regras predefinidas** `100` – **Pedidos ao servidor DNS via TCP**. `101` – **Pedidos ao servidor DNS via UDP**. `102` – **Enviar mensagens de e-mail**. `110` – **Qualquer atividade de rede** (Redes confiáveis). `125` – **Qualquer atividade de rede** (Redes locais). `130` – **Atividade de rede da Área de Trabalho Remota**. `131` – **Conexões TCP através de portas locais**. `132` – **Conexões UDP através de portas locais**. `133` – **Fluxo TCP de entrada**. `134` – **Fluxo UDP de entrada**. `137` – **Respostas de entrada de destino ICMP inacessível**. `138` – **Pacotes de entrada de resposta de eco ICMP**. `140` – **Respostas de entrada de tempo de ICMP excedido**. `142` – **Fluxo ICMP de entrada**. `266` – **Pacotes de entrada de solicitação de eco ICMPv6**.
`RuleState`	Status da regra.	`0`: a regra predefinida está desativada `1`: a regra predefinida está ativada `2`: a regra personalizada está desativada `3`: a regra personalizada está ativada
`RuleTypeId`	ID do tipo de regra.	`4` – regra de pacote de rede.
`AppIdEx`	ID do aplicativo ao qual a regra de pacote de rede pertence.	Se a regra não pertencer a nenhum aplicativo, o valor será `0`.
`ResIdEx`	ID principal do recurso com configurações de regras. É possível usar esse identificador para localizar um bloco com configurações de regra no nó `Resources`.	Número inteiro
`ResIdEx2`	ID do tipo de rede.	`0` – **Qualquer endereço**. `50` – **Redes confiáveis**. `51` – **Redes locais**. `52` – **Redes públicas**. `<Network Identifier>` – **Endereços da lista** (os endereços são definidos manualmente).
`AccessFlag`	Valor do parâmetro **Ação**.	`0` – **Permitir**. `2` – **Por regras de aplicativos**. `3` – **Bloquear**. `4` – **Permitir** e **Criar log de eventos**. `6` – **Por regras de aplicativos** e **Criar log de eventos**. `7` – **Bloquear** e **Criar log de eventos**.
`</key>`		

O nó `Resources` contém configurações da regra de pacote de rede. As configurações da regra de pacote de rede personalizado são listadas no bloco `<key name="0004">`.

Marcação da regra de pacote de rede personalizada

```
<key name="0026">
        <key name="Data">
                <key name="RemotePorts"> </key>
                <key name="LocalPorts"> </key>
                <key name="AdapterBindings">
                        <key name="0000">
                                <key name="IpAddresses">
                                        <key name="0000">
                                                <key name="IP">
                                                        <key name="V6">
                                                                <tQWORD name="Hi">0</tQWORD>
                                                                <tQWORD name="Lo">0</tQWORD>
                                                                <tDWORD name="Zone">0</tDWORD>
                                                                <tSTRING name="ZoneStr"/>
                                                        </key>
                                                        <tBYTE name="Version">4</tBYTE>
                                                        <tDWORD name="V4">16909060</tDWORD>
                                                        <tBYTE name="Mask">32</tBYTE>
                                                </key>
                                                <key name="AddressIP"> </key>
                                                <tSTRING name="Address"/>
                                        </key>
                                </key>
                                <key name="MacAddresses">
                                        <key name="0000">
                                                <tDWORD name="Type">0</tDWORD>
                                                <tQWORD name="AddressData0">1108152157446</tQWORD>
                                                <tQWORD name="AddressData1">0</tQWORD>
                                        </key>
                                </key>
                                <tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
                                <tDWORD name="InterfaceType">3</tDWORD>
                        </key>
                </key>
                <tTYPE_ID name="unique">3213697024</tTYPE_ID>
                <tBYTE name="Proto">2</tBYTE>
                <tBYTE name="Direction">2</tBYTE>
                <tBYTE name="IcmpType">0</tBYTE>
                <tBYTE name="IcmpCode">0</tBYTE>
                <tDWORD name="Flags">1</tDWORD>
                <tBYTE name="TTL">255</tBYTE>
        </key>
        <key name="Childs"> </key>
        <tDWORD name="Id">1073747214</tDWORD>
        <tDWORD name="ParentID">7</tDWORD>
        <tDWORD name="Flags">38</tDWORD>
        <tSTRING name="Name">TEST1</tSTRING>
</key>
```

Configurações da regra de pacote de rede personalizada

Parâmetro	Descrição	Valor
`<key name="Data">`	ID do bloco do parâmetro.	Número inteiro
`RemotePorts`	Valor do parâmetro **Portas remotas**.	Lista de intervalos de portas remotas.
`LocalPorts`	Valor do parâmetro **Portas locais**.	Lista de intervalos de portas locais.

Parâmetro	Descrição	Valor
`AdapterBindings`	Valor do parâmetro **Adaptadores de rede**.	`IpAddresses` – valor do parâmetro **Endereços IP**. `MacAddresses` – valor do parâmetro **Endereços MAC**. `AdapterName` – nome do adaptador de rede. `InterfaceType` – valor do parâmetro **Tipo de interface**: • `0` – **Outro**. • `1` – **LoopBack**. • `2` – **Rede com fio (Ethernet)**. • `3` – **Rede Wi-Fi (Wi-Fi)**. • `4` – **Túnel**. • `5` – **Conexão PPP**. • `6` – **Conexão PPPoE**. • `7` – **Conexão VPN**. • `8` – **Conexão de modem**.
`unique`	ID interno da estrutura.	Número inteiro Recomenda-se deixar este parâmetro inalterado.
`Proto`	Valor do parâmetro **Protocolo**.	`0` – desativado. `1` – **ICMP**. `2` – **IGMP**. `6` – **TCP**. `17` – **UDP**. `47` – **GRE**. `58` – **ICMPv6**.
`Direction`	Valor do parâmetro **Direção**.	`1` – **Entrada (pacote)**. `2` – **Saída (pacote)**. `3` – **Entrada/Saída**. `4` – **Entrada**. `5` – **Saída**.

Parâmetro	Descrição	Valor
`IcmpType`	Valor do parâmetro **Tipo de ICMP**.	**Protocolo ICMP** `0` – **Resposta de eco** (ICMP) ou desativado. `3` – **Destino não accessível** (ICMP). `4` – **Atenuação de origem**. `5` – **Redirecionar**. `6` – **Endereço de Host alternativo**. `8` – **Solicitação de eco**. `9` – **Anúncio de roteador**. `10` – **Solicitação de roteador**. `11` – **Tempo excedido**. `12` – **Problema de parâmetro**. `13` – **Marca de hora**. `14` – **Resposta de marca de hora**. `15` – **Solicitação de informação**. `16` – **Resposta de informação**. `17` – **Solicitação de máscara de endereço**. `18` – **Resposta de máscara de endereço**. `30` – **Rota de rastreio**. `31` – **Erro de conversão de datagrama**. `32` – **Redirecionamento de Host móvel**. `33` – **IPv6 Where-Are-You**. `34` – **IPv6 I-Am-Here**. `35` – **Solicitação de registro móvel**. `36` – **Resposta de registro móvel**. `37` – **Solicitação de nome de domínio**. `38` – **Resposta de nome de domínio**. `40` – **Photuris**. **Protocolo ICMPv6** `1` – **Destino não accessível**. `2` – **Pacote demasiado grande**. `3` – **Tempo excedido**. `4` – **Problema de parâmetro**. `128` – **Solicitação de eco**. `129` – **Resposta de eco**. `130` – **Consulta de ouvinte multicast**. `131` – **Relatório de ouvinte multicast**. `132` – **Ouvinte de multicast concluído**. `133` – **Solicitação de roteador**. `134` – **Anúncio de roteador**. `135` – **Solicitação de vizinho**. `136` – **Anúncio de vizinho**. `137` – **Redirecionamento de mensagem**. `138` – **Renumeração de roteador**. `139` – **Consulta de informação de nó ICMP**. `141` – **Mensagem de solicitação de descoberta inversa de vizinho**. `142` – **Mensagem de anúncio de descoberta inversa de vizinho**. `143` – **Relatório de ouvinte multicast Versão 2**.

Parâmetro	Descrição	Valor
		`144` – **Mensagem de solicitação de descoberta de endereço de agente doméstico**. `145` – **Mensagem de resposta de descoberta de endereço de agente doméstico**. `146` – **Solicitação de prefixo móvel**. `147` – **Anúncio de prefixo móvel**. `148` – **Mensagem de solicitação de caminho de certificação**. `149` – **Mensagem de anúncio de caminho de certificação**. `151` – **Anúncio de roteador multicast**. `152` – **Solicitação de roteador multicast**. `153` – **Encerramento de roteador multicast**.
`IcmpCode`	Valor do parâmetro **Código ICMP**.	`0` – **Código 0** ou desativado. `1` – **Código 1**. `2` – **Código 2**.
`Flags`	Ponteiro de atributo de estrutura.	Número inteiro Recomenda-se deixar este parâmetro inalterado.
`TTL`	Valor do parâmetro **Vida útil (TTL)**.	Valor em segundos. Se desativado, o valor é `0`.
`</key>`		
`Id`	ID principal do recurso (consulte o nó `Rules`).	Número inteiro
`ParentID`	ID do grupo principal.	Número inteiro Recomenda-se deixar este parâmetro inalterado.
`Flags`	Status da regra.	`6` – a regra está desativada. `38` – a regra está ativada.
`Name`	Nome da regra de pacote de rede.	Texto

Gerenciar as regras de rede de aplicativos

Por padrão, o Kaspersky Endpoint Security reúne todos os aplicativos instalados no computador do usuário pelo nome do fornecedor do aplicativo cujo arquivo ou atividade de rede é monitorado. Os grupos de aplicativos são, por sua vez, categorizados em grupos confiáveis. Todos os aplicativos e grupos de aplicativos herdam as propriedades do seu grupo pai: regras de controle de aplicativos, regras de rede para aplicativos e prioridade de execução.

Assim como o componente Prevenção de Intrusão do Host, o componente Firewall aplica por padrão as regras de rede a um grupo de aplicativos ao filtrar a atividade de rede de todos os aplicativos no grupo. As regras de rede de grupo de aplicativos definem os direitos de aplicativos dentro do grupo para acessar diferentes conexões de rede.

Por padrão, o Firewall cria um conjunto de regras de rede para cada grupo de aplicativos detectado pelo Kaspersky Endpoint Security no computador. É possível alterar a ação do Firewall aplicada às regras de rede de grupo de aplicativos criadas por padrão. Não é possível editar, remover, desativar ou alterar a prioridade das regras de rede de grupo de aplicativos criadas por padrão.

Você também pode criar uma regra de rede para um aplicativo individual. Tal regra terá uma prioridade mais alta do que a regra de rede do grupo ao qual o aplicativo pertence.

Criar uma nova regra de rede

Por padrão, a atividade de aplicativos é controlada por regras de rede definidas para o grupo de confiança ao qual o Kaspersky Endpoint Security atribuiu o aplicativo na primeira inicialização. Se necessário, é possível criar regras de rede para todo o grupo de confiança, para um aplicativo individual ou para um grupo de aplicativos em um grupo de confiança.

As regras de rede definidas manualmente têm prioridade mais alta do que as regras de rede que foram determinadas para um grupo de confiança. Em outras palavras, se as regras de aplicativo definidas manualmente diferirem das regras de aplicativo determinadas para um grupo de confiança, o firewall controla a atividade de aplicativos de acordo com as regras para aplicativos definidas manualmente.

Por padrão, o Firewall cria as seguintes regras de rede para cada aplicativo:

- Qualquer atividade de rede em Redes confiáveis.
- Qualquer atividade de rede em Redes locais.
- Qualquer atividade de rede em Redes públicas.

O Kaspersky Endpoint Security controla a atividade de aplicativos de rede de acordo com regras de rede predefinidas da seguinte forma:

- Confiáveis e Baixa restrição: todas as atividades de rede são autorizadas.
- Alta restrição e Não confiáveis: todas as atividades de rede são bloqueadas.

As regras de aplicativo predefinidas não podem ser editadas ou excluídas.

É possível criar uma regra de aplicativo de rede das seguintes maneiras:

- Usar a ferramenta Monitor de Rede.

  O *Monitor de Rede* é uma ferramenta desenvolvida para exibir as informações sobre a atividade do computador de um usuário em tempo real. O procedimento é conveniente porque não é preciso definir todas as configurações de regras. Algumas configurações do Firewall serão inseridas automaticamente a partir dos dados do Monitor de Rede. O Monitor de Rede está disponível somente na interface do aplicativo.

- Defina as configurações do firewall.

  Isso permite refinar as configurações do Firewall. É possível criar regras para qualquer atividade de rede, mesmo que não haja nenhuma atividade de rede no momento atual.

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

Como usar a ferramenta Monitor de Rede para criar uma regra de aplicativo de rede na interface do aplicativo

1. Na janela principal do aplicativo, na seção **Monitoramento**, clique no bloco **Monitor de Rede**.

2. Vá para a guia **Atividade de rede** ou **Portas abertas**.

   A guia **Atividade de rede** exibe todas as conexões de rede atuais estabelecidas com o computador. São exibidos o tráfego de entrada e de saída das conexões de rede.

   A guia **Portas abertas** lista todas as portas de rede abertas do computador.

3. No menu de contexto de uma conexão de rede, selecione **Criar uma regra de aplicativo de rede**.

   A janela de propriedades e regras de aplicativo é exibida.

4. Selecione a guia **Regras de rede**.

   Isso abrirá a lista de regras de rede padrão definidas pelo Firewall.

5. Clique **Adicionar**.

   As propriedades da regra de pacotes aparecerão.

6. Insira manualmente o nome do serviço de rede no campo **Nome**.

7. Configure as definições da regra de rede (consulte a tabela abaixo).

   É possível selecionar um modelo de regra predefinido clicando no link **Modelo de regra de rede**. Os modelos de regras descrevem as conexões de rede usadas com mais frequência.

   Todas as configurações de regras de rede serão preenchidas automaticamente.

8. Se desejar que as ações da regra de rede sejam refletidas no relatório, marque a caixa de seleção **Registrar eventos**.

9. Clique **Salvar**.

   A regra de rede será adicionada à lista.

10. Use os botões **Acima**/**Abaixo** para definir a prioridade da regra de rede.

11. Salvar alterações.

Como usar as configurações do Firewall para criar uma regra de aplicativo de rede na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.

3. Clique **Regras para aplicativos**.

   Isso abrirá a lista de regras de rede padrão definidas pelo Firewall.

4. Na lista de aplicativos, selecione o aplicativo ou grupo de aplicativos para o qual deseja criar uma regra de rede.

5. Clique com o botão direito para abrir o menu de contexto e selecione **Detalhes e regras**.

   A janela de propriedades e regras de aplicativo é exibida.

6. Selecione a guia **Regras de rede**.

7. Clique **Adicionar**.

   As propriedades da regra de pacotes aparecerão.

8. Insira manualmente o nome do serviço de rede no campo **Nome**.

9. Configure as definições da regra de rede (consulte a tabela abaixo).

   É possível selecionar um modelo de regra predefinido clicando no link **Modelo de regra de rede**. Os modelos de regras descrevem as conexões de rede usadas com mais frequência.

   Todas as configurações de regras de rede serão preenchidas automaticamente.

10. Se desejar que as ações da regra de rede sejam refletidas no relatório, marque a caixa de seleção **Registrar eventos**.

11. Clique **Salvar**.

    A regra de rede será adicionada à lista.

12. Use os botões **Acima**/**Abaixo** para definir a prioridade da regra de rede.

13. Salvar alterações.

Como criar uma regra de aplicativo de rede no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.

4. No bloco **Configurações do Firewall**, clique no botão **Configurações**.

   Isso abre a lista de regras de pacotes de rede e a lista de regras de rede de aplicativos.

5. Vá para a guia **Regras de rede de aplicativos**.

6. Clique **Adicionar**.

7. Na janela que é aberta, insira os critérios para buscar o aplicativo para o qual deseja criar uma regra de rede.

   É possível inserir o nome do aplicativo ou o nome do fornecedor. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.

8. Clique **Atualizar**.

   O Kaspersky Endpoint Security pesquisará o aplicativo na lista consolidada de aplicativos instalados em computadores gerenciados. O Kaspersky Endpoint Security exibirá uma lista de aplicativos que satisfazem os critérios de pesquisa.

9. Selecione o aplicativo desejado.

10. Na lista suspensa **Adicionar o aplicativo selecionado ao grupo de confiança**, selecione **Grupos padrão** e clique em **OK**.

    O aplicativo será adicionado ao grupos padrão.

11. Selecione o aplicativo relevante e, então, selecione os **Direitos de aplicativos** a partir do menu de contexto do aplicativo.

    A janela de propriedades e regras de aplicativo é exibida.

12. Selecione a guia **Regras de rede**.

    Isso abrirá a lista de regras de rede padrão definidas pelo Firewall.

13. Clique **Adicionar**.

    As propriedades da regra de pacotes aparecerão.

14. Insira manualmente o nome do serviço de rede no campo **Nome**.

15. Configure as definições da regra de rede (consulte a tabela abaixo).

    É possível selecionar um modelo de regra predefinido ao clicar no botão . Os modelos de regras descrevem as conexões de rede usadas com mais frequência.

    Todas as configurações de regras de rede serão preenchidas automaticamente.

16. Se desejar que as ações da regra de rede sejam refletidas no relatório, marque a caixa de seleção **Criar log de eventos**.

17. Salve a nova regra de rede.

18. Use os botões **Para cima**/**Para baixo** para definir a prioridade da regra de rede.

19. Salvar alterações.

Como criar uma regra de aplicativo de rede no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Comunicação e Proteção na Web** → **Firewall**.

5. No bloco **Direitos de aplicativos e recursos protegidos**, clique no link **Direitos de aplicativos**.

   Isso abre a janela de configuração de Direitos de aplicativos e a lista de Recursos protegidos.

6. Vá para a guia **Direitos de aplicativos**.

   Uma lista de Grupos de confiança será exibida no lado esquerdo da janela e suas propriedades no lado direito.

7. No bloco **Aplicativos**, clique no botão **Adicionar**.

   Então, o assistente para adicionar um aplicativo a um grupo de confiança será iniciado.

8. Selecione um grupo de confiança relevante para o aplicativo.

9. Selecione o tipo de **Aplicativo**. Vá para a próxima etapa.

   Caso deseje criar uma regra de rede para múltiplos aplicativos, selecione o tipo de **Grupo** e defina um nome para o grupo de aplicativos.

10. Na lista de aplicativos aberta, selecione os aplicativos para os quais deseja criar uma regra de rede.

    Usar um filtro. É possível inserir o nome do aplicativo ou o nome do fornecedor. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.

11. Conclua o assistente.

    O aplicativo será adicionado ao grupo de confiança.

12. Na parte esquerda da janela, selecione o aplicativo relevante.

13. Na parte direita da janela, selecione **Regras de rede** a partir da lista suspensa.

    Isso abrirá a lista de regras de rede padrão definidas pelo Firewall.

14. Clique **Adicionar**.

    Isso abre as propriedades da regra de aplicativo.

15. Insira manualmente o nome do serviço de rede no campo **Nome da regra**.

16. Configure as definições da regra de rede (consulte a tabela abaixo).

    É possível selecionar um modelo de regra predefinido clicando no link **Selecionar o modelo de regra**. Os modelos de regras descrevem as conexões de rede usadas com mais frequência.

    Todas as configurações de regras de rede serão preenchidas automaticamente.

17. Se desejar que as ações da regra de rede sejam refletidas no relatório, marque a caixa de seleção **Criar log de eventos**.

18. Salvar a regra de rede.

    A regra de rede será adicionada à lista.

19. Use o botão **Mover** para definir a prioridade da regra de rede.

20. Salvar alterações.

Configurações de regras de rede de aplicativos

Parâmetro	Descrição
Ação	**Permitir**. **Bloquear**.
Protocolo	Controlar a atividade da rede sobre o protocolo selecionado: TCP, UDP, ICMP, ICMPv6, IGMP e GRE. Ao selecionar os protocolos do tipo ICMP ou ICMPv6, especifique o tipo e o código do pacote ICMP. Ao selecionar os protocolos TCP ou UDP, especifique as portas dos computadores local e remoto entre as quais ocorrerá o monitoramento da conexão. Intervalo de valores possíveis para os números de porta: 0-65535. Em cada campo, é possível inserir diversos valores separados por `,` ou especifique um intervalo de valores usando `-`. Por exemplo: • `100,101` • `100-130` • `100,110-130`
Direção	**Entrada**. **Entrada/Saída**. **Saída**.

Parâmetro	Descrição
Endereços remotos	Os endereços de rede dos computadores remotos que podem enviar ou receber pacotes de rede. O Firewall aplica uma regra de rede ao intervalo especificado de endereços de rede remotos. É possível incluir todos os endereços IP em uma regra de rede, criar uma lista separada de endereços IP ou especificar um intervalo de endereços IP (redes confiáveis, redes locais, redes públicas). Também é possível especificar um nome DNS de um computador em vez de seu endereço IP. Deve-se usar os nomes DNS apenas para computadores da LAN ou serviços internos. A interação com serviços na nuvem (como o Microsoft Azure) e outros recursos da Internet deve ser tratada pelo componente controle da Web. Se na regra de pacote de rede foi adicionado um nome DNS para o qual o endereço IP não pôde ser determinado, o Kaspersky Endpoint Security exibirá um aviso. Na lista de regras de pacote de rede no Web Console, uma coluna é adicionada com uma descrição do erro. A descrição do erro não está disponível no Console de Administração (MMC). Essas regras de pacotes são destacadas em cores.
Endereços locais	Os endereços de rede dos computadores que podem enviar ou receber pacotes de rede. O Firewall aplica uma regra de rede ao intervalo especificado de endereços de rede locais. É possível incluir todos os endereços IP em uma regra de rede, criar uma lista separada de endereços IP ou especificar um intervalo de endereços IP. O aplicativo armazena endereços locais somente se uma lista de endereços remotos for especificada. Ou seja, se o valor **Endereços da lista** foi selecionado para **Endereços remotos** e pelo menos um endereço foi adicionado. Algumas vezes o endereço local não pode ser obtido para aplicativos. Nesse caso, o parâmetro é ignorado.

Ativar e desativar uma regra de rede de aplicativo

Para ativar ou desativar uma regra de rede de um aplicativo:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.
3. Clique **Regras para aplicativos**.

   Abrirá a lista de regras de aplicativo.
4. Na lista de aplicativos, selecione o aplicativo ou grupo de aplicativos em que deseja criar ou editar de uma regra de rede.
5. Clique com o botão direito para abrir o menu de contexto e selecione **Detalhes e regras**.

   A janela de propriedades e regras de aplicativo é exibida.
6. Selecione a guia **Regras de rede**.
7. Na lista de regras de rede para grupos de aplicativos, selecione a regra de rede relevante.

   A janela de propriedades de regras de rede é exibida.
8. Defina o status **Ativo** ou **Inativo** para a regra de rede.

   Não é possível desativar uma regra de rede de grupo de aplicativos criada pelo Firewall por padrão.
9. Salvar alterações.

Alterar a ação do Firewall para uma regra de rede de um aplicativo

É possível alterar a ação do Firewall que é aplicada a todas as regras de rede para um aplicativo ou grupo de aplicativos que foi criado por padrão; e alterar a ação do Firewall para uma única regra de rede personalizada para um aplicativo ou grupo de aplicativos.

Para modificar a ação de Firewall de todas as regras de rede de um aplicativo ou o grupo de aplicativos:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.
3. Clique **Regras para aplicativos**.

   Abrirá a lista de regras de aplicativo.
4. Se desejar modificar a ação do Firewall que é aplicada a todas as regras de rede que são criadas por padrão, selecione um aplicativo ou grupo de aplicativos na lista. As regras de rede criadas manualmente não são alteradas.
5. Clique com o botão direito para abrir o menu de contexto, selecione **Regras de rede** e selecione a ação que deseja atribuir:
   - **Herdar**.
   - **Permitir**.
   - **Bloquear**.
6. Salvar alterações.

Para modificar a resposta do Firewall a uma regra de rede de um aplicativo ou grupo de aplicativos:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.
3. Clique **Regras para aplicativos**.

   Abrirá a lista de regras de aplicativo.
4. Na lista, selecione o aplicativo ou o grupo de aplicativos para os quais você deseja modificar a ação de uma regra de rede.
5. Clique com o botão direito para abrir o menu de contexto e selecione **Detalhes e regras**.

   A janela de propriedades e regras de aplicativo é exibida.
6. Selecione a guia **Regras de rede**.
7. Selecione a regra de rede para a qual você deseja modificar a ação do Firewall.

8. Na coluna **Permissão**, clique com o botão direito do mouse para exibir o menu de contexto e selecione a ação que você pretende atribuir:
   - **Herdar**.
   - **Permitir**.
   - **Negar**.
   - **Registrar eventos**.
9. Salvar alterações.

Alterar a prioridade de uma regra de rede de um aplicativo

A prioridade de uma regra de rede é determinada pela sua posição na lista de regras de rede. O Firewall executa as regras na ordem em que aparecem na lista de regras de rede, de cima para baixo. De acordo com cada regra de rede processada aplicada a uma conexão de rede específica, o Firewall ou permite ou bloqueia o acesso ao endereço e à porta que estão indicados nas configurações desta conexão de rede.

As regras de rede criadas manualmente têm uma prioridade mais alta do que regras de rede padrão.

Não é possível alterar a prioridade das regras de rede de grupo de aplicativos criadas por padrão.

Para alterar a prioridade de uma regra de rede:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.
3. Clique **Regras para aplicativos**.

   Abrirá a lista de regras de aplicativo.
4. Na lista de aplicativos, selecione o aplicativo ou grupo de aplicativos em que deseja alterar a prioridade de uma regra de rede.
5. Clique com o botão direito para abrir o menu de contexto e selecione **Detalhes e regras**.

   A janela de propriedades e regras de aplicativo é exibida.
6. Selecione a guia **Regras de rede**.
7. Selecione a regra de rede cuja prioridade deseja alterar.
8. Use os botões **Acima**/**Abaixo** para definir a prioridade da regra de rede.
9. Salvar alterações.

Monitor de Rede

O *Monitor de Rede* é uma ferramenta desenvolvida para exibir as informações sobre a atividade do computador de um usuário em tempo real.

Para iniciar o Monitor de Rede:

Na janela principal do aplicativo, na seção **Monitoramento**, clique no bloco **Monitor de Rede**.

A janela Monitor de Rede é aberta. Nesta janela, as informações sobre a atividade de rede são exibidas em quatro guias:

- A guia **Atividade de rede** exibe todas as conexões de rede atuais estabelecidas com o computador. São exibidos o tráfego de entrada e de saída das conexões de rede. Nesta guia, também é possível criar regras de pacotes de rede para a operação do firewall.
- A guia **Portas abertas** lista todas as portas de rede abertas do computador. Nesta guia, também é possível criar regras de pacotes de rede e regras de aplicativos para a operação do firewall.
- A guia **Tráfego de rede** exibe o volume do tráfego de entrada e de saída entre o computador do usuário e outros computadores da rede nos quais o usuário está conectado atualmente.
- A guia **Computadores bloqueados** lista os endereços IP de computadores remotos cuja atividade de rede foi bloqueada pelo componente Proteção Contra Ameaças à Rede ao detectar tentativas de ataque de rede destes endereços IP.

Prevenção de 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, os exploits podem utilizar um ataque de estouro de buffer. Para isso, o exploit envia uma grande quantidade de dados para um aplicativo vulnerável. Ao processar esses dados, o aplicativo vulnerável executa um código malicioso. Como resultado desse ataque, o exploit pode iniciar uma instalação não autorizada de malware. Quando há uma tentativa de executar um arquivo executável de um aplicativo vulnerável que não foi realizada pelo usuário, o Kaspersky Endpoint Security bloqueia a execução do arquivo ou notifica o usuário.

O componente Prevenção de Exploits também monitora as portas de rede quanto a processos de aplicativos que possam ameaçar a segurança do computador. O aplicativo obtém informações sobre esses processos em bancos de dados de antivírus.

Ativar e desativar a Prevenção de Exploit

Por padrão, a Prevenção de Exploit é ativada e funciona no modo ideal. O Kaspersky Endpoint Security monitora os arquivos executáveis que estão sendo executados por aplicativos vulneráveis. Se o Kaspersky Endpoint Security detectar que um arquivo executável de um aplicativo vulnerável foi executado por outra coisa além do usuário, o Kaspersky Endpoint Security executará a ação selecionada (por exemplo, bloqueará a operação).

Como ativar ou desativar a Prevenção de Exploit no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Exploits**.
4. Use a caixa de seleção **Prevenção de Exploits** para ativar ou desativar o componente.
5. Selecione a ação relevante na seção **Na detecção de exploit**:
   - **Bloquear**. Se esse item for selecionado ao detectar uma exploit, o Kaspersky Endpoint Security bloqueará as operações dessa exploit e registrará as informações sobre ela.
   - **Informar**. Se esse item for selecionado, quando o Kaspersky Endpoint Security detectar um exploit, ele registrará uma entrada contendo as informações sobre o exploit e adicionará informações sobre ele na lista de ameaças ativas.
6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar ou desativar a Prevenção de Exploit no Web Console e no Cloud Console

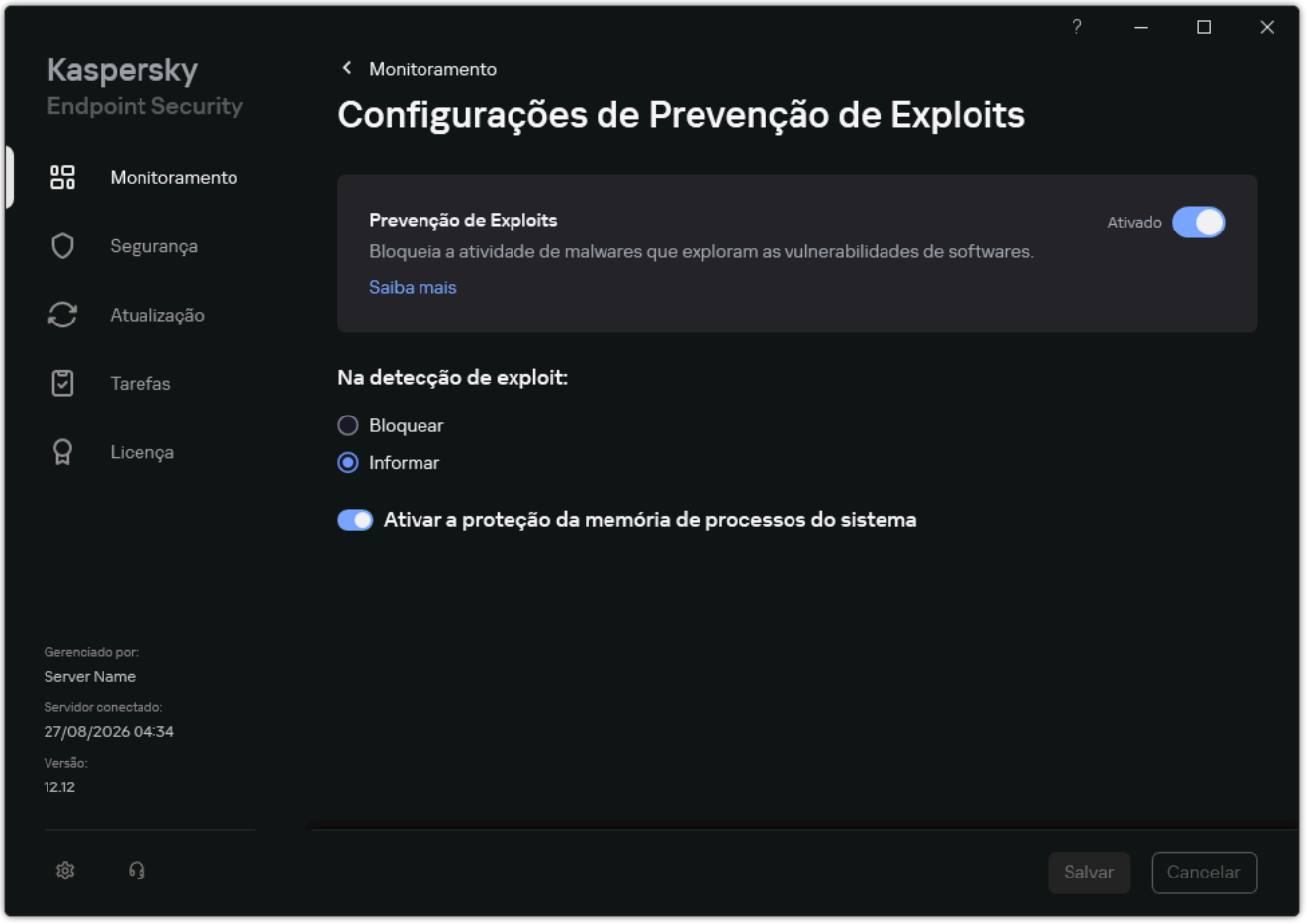
1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Proteção Contra Ameaças ao Host** → **Análise de comportamento** → **Prevenção de Exploits**.
5. Use o botão de alternância do **Prevenção de Exploits** para ativar ou desativar o componente.
6. Selecione a ação relevante na seção **Ação ao detectar ameaça**:
   - **Bloquear**. Se esse item for selecionado ao detectar uma exploit, o Kaspersky Endpoint Security bloqueará as operações dessa exploit e registrará as informações sobre ela.
   - **Informar**. Se esse item for selecionado, quando o Kaspersky Endpoint Security detectar um exploit, ele registrará uma entrada contendo as informações sobre o exploit e adicionará informações sobre ele na lista de ameaças ativas.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar ou desativar a Prevenção de Exploit na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Exploits**.



Configurações de Prevenção de exploit

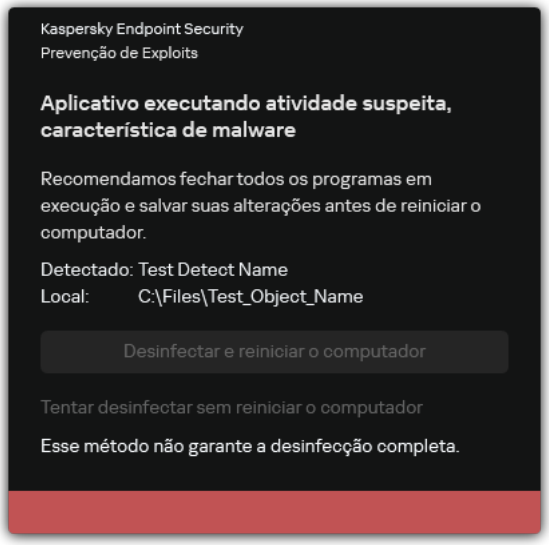
3. Use o botão de alternância do **Prevenção de Exploits** para ativar ou desativar o componente.

4. Selecione a ação relevante na seção **Na detecção de exploit**:

   - **Bloquear**. Se esse item for selecionado ao detectar uma exploit, o Kaspersky Endpoint Security bloqueará as operações dessa exploit e registrará as informações sobre ela.

   - **Informar**. Se esse item for selecionado, quando o Kaspersky Endpoint Security detectar um exploit, ele registrará uma entrada contendo as informações sobre o exploit e adicionará informações sobre ele na lista de ameaças ativas.

5. Salvar alterações.



Notificação sobre ameaça ativa

Proteção da memória de processos do sistema

Por padrão, a proteção da memória de processos do sistema está ativada. O Kaspersky Endpoint Security bloqueia processos externos que tentam obter acesso aos processos do sistema.

Como ativar ou desativar a proteção da memória de processos do sistema no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Exploits**.

4. Use a caixa de seleção **Ativar a proteção da memória de processos do sistema** para ativar ou desativar a opção.

5. Salvar alterações.

Como ativar ou desativar a proteção de memória de processos do sistema no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Proteção Contra Ameaças ao Host** → **Análise de comportamento** → **Prevenção de Exploits**.

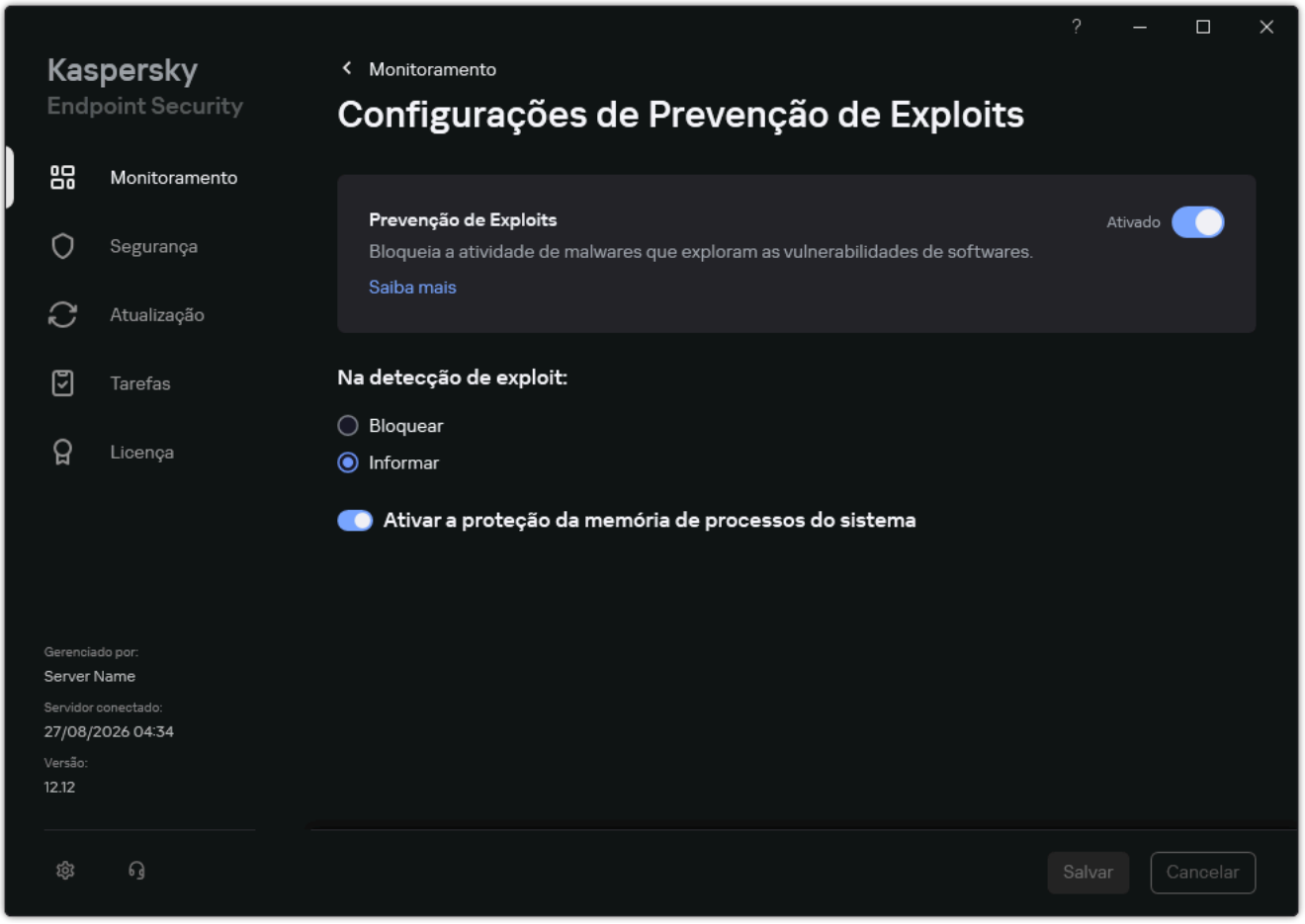
5. Use o botão de alternância **Proteção da memória de processos do sistema ATIVADA** para ativar ou desativar esse recurso.

6. Salvar alterações.

Como ativar ou desativar a proteção de memória de processos do sistema na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Prevenção de Exploits**.



Configurações de Prevenção de exploit

3. Use o botão de alternância **Ativar a proteção da memória de processos do sistema** para ativar ou desativar esse recurso.

4. Salvar alterações.

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 Endpoint Security executará a ação de resposta selecionada. A funcionalidade do Kaspersky Endpoint Security com base em padrões de atividades perigosas fornece defesa proativa ao computador.

O componente Detecção de Comportamento também monitora as portas de rede quanto aos processos de aplicativos que possam ameaçar a segurança do computador. O aplicativo obtém informações sobre esses processos em bancos de dados de antivírus.

Por padrão, a Detecção de Comportamento é ativada e executada no modo recomendado por especialistas da Kaspersky. Quando uma atividade maliciosa é detectada, o Kaspersky Endpoint Security exclui o arquivo executável do aplicativo malicioso.

Não se recomenda desativar a Detecção de Comportamento a menos que absolutamente necessário, uma vez que isso reduziria a eficiência dos componentes de proteção. Os componentes de proteção podem solicitar dados coletados pelo componente Detecção de Comportamento para detectar ameaças.

Como ativar ou desativar a Detecção de Comportamento no Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Detecção de Comportamento**.
5. Use a caixa de seleção **Detecção de Comportamento** para ativar ou desativar o componente.
6. 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 Endpoint 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 Endpoint Security encerrará este aplicativo.
   - **Informar**. Se este item for selecionado e a atividade de malware de um aplicativo for detectada, o Kaspersky Endpoint Security adiciona informações sobre a atividade de malware do aplicativo à lista de ameaças ativas.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar ou desativar a Detecção de Comportamento no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Proteção Contra Ameaças ao Host** → **Análise de comportamento** → **Detecção de Comportamento**.

5. Use o botão de alternância do **Detecção de Comportamento ATIVADA** para ativar ou desativar o componente.

6. Selecione a ação relevante na seção **Ação ao detectar ameaça**:

   - **Excluir**. Se este item for selecionado, ao detectar uma atividade maliciosa, o Kaspersky Endpoint 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 Endpoint Security encerrará este aplicativo.

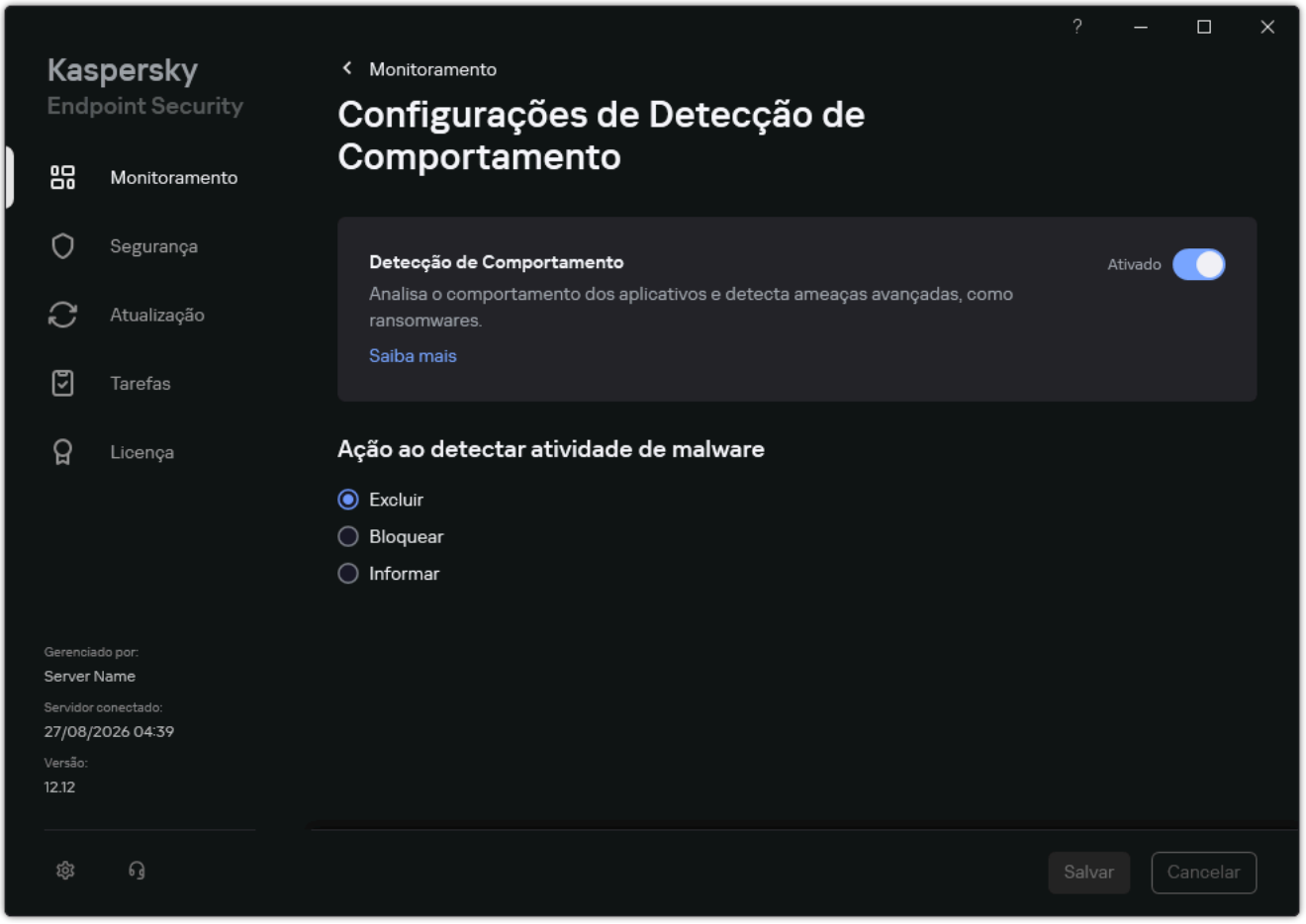
   - **Informar**. Se este item for selecionado e a atividade de malware de um aplicativo for detectada, o Kaspersky Endpoint Security adiciona informações sobre a atividade de malware do aplicativo à lista de ameaças ativas.

7. Para aplicar a política aos computadores, feche os ícones de cadeado 🔒 e salve as alterações.

Como ativar ou desativar a Detecção de Comportamento na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Detecção de Comportamento**.



Configurações de Detecção de Comportamento

3. Use o botão de alternância do **Detecção de Comportamento** para ativar ou desativar o componente.

4. 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 Endpoint 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 Endpoint Security encerrará este aplicativo.

   - **Informar**. Se este item for selecionado e a atividade de malware de um aplicativo for detectada, o Kaspersky Endpoint Security adiciona informações sobre a atividade de malware do aplicativo à lista de ameaças ativas.

5. Salvar alterações.

Como resultado, se a Detecção de Comportamento estiver ativada, o Kaspersky Endpoint Security usará assinaturas de fluxo de comportamento para analisar a atividade dos aplicativos no sistema operacional.

Anticryptor

A partir do Kaspersky Endpoint Security 12.12 for Windows, a proteção de pastas compartilhadas contra criptografia externa que costumava fazer parte do componente Detecção de Comportamento passou a ser um componente separado, o Anticryptor.

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.

O componente Anticryptor analisa a atividade em pastas compartilhadas. Se esta atividade combinar com uma assinatura de fluxo de comportamento que é típica para a criptografia externa, o Kaspersky Endpoint Security executa a ação selecionada.

Para que o componente Anticryptor funcione, é necessário ativar o componente Detecção de Comportamento.

Se o Kaspersky Endpoint Security detectar uma tentativa de modificar arquivos em pastas compartilhadas, ele 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 conforme recomendado pelos especialistas da Kaspersky. Para configurar essa funcionalidade, é possível criar um escopo de proteção e configurar exclusões, se necessário. Por padrão, o aplicativo identifica automaticamente as pastas compartilhadas e monitora a atividade de arquivos em todas as pastas. Quando uma tentativa de criptografar arquivos externamente em pastas compartilhadas é detectada, o Kaspersky Endpoint Security bloqueia a sessão do usuário remoto por uma hora (por padrão).

Depois que o Kaspersky Endpoint 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 (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Anticryptor**.

4. Use a caixa de seleção **Anticryptor** para ativar ou desativar a detecção de atividade típica da criptografia externa.

5. Selecione a ação relevante que o aplicativo executará quando uma tentativa de modificar arquivos em pastas compartilhadas for detectada:

   - **Bloquear conexão por N min**. Caso esta opção seja selecionada, ao detectar uma tentativa de modificação dos arquivos em pastas compartilhadas, o Kaspersky Endpoint Security bloqueia o acesso à modificação de arquivo 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 esteja selecionada, ao detectar uma tentativa de modificação de arquivos em pastas compartilhadas, o Kaspersky Endpoint Security adicionará as informações sobre a tentativa na lista de ameaças ativas, adicionará uma entrada nos relatórios da interface do aplicativo local e enviará as informações sobre a atividade maliciosa detectada ao Kaspersky Security Center.

6. Se necessário, edite um escopo de proteção e defina exclusões.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar ou desativar a proteção de pastas compartilhadas contra criptografia externa no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Proteção Contra Ameaças ao Host** → **Análise de comportamento** → **Anticryptor**.

5. Use o botão **Anticryptor ATIVADO** para ativar ou desativar a detecção de atividade típica da criptografia externa.

6. Selecione a ação relevante que o aplicativo executará quando uma tentativa de modificar arquivos em pastas compartilhadas for detectada:

   - **Bloquear conexão por (min) N min**. Caso esta opção seja selecionada, ao detectar uma tentativa de modificação dos arquivos em pastas compartilhadas, o Kaspersky Endpoint Security bloqueia o acesso à modificação de arquivo 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 (min) N min** seja selecionada, os arquivos modificados são restaurados a partir das cópias de backup.

   - **Informar**. Caso essa opção esteja selecionada, ao detectar uma tentativa de modificação de arquivos em pastas compartilhadas, o Kaspersky Endpoint Security adicionará as informações sobre a tentativa na lista de ameaças ativas, adicionará uma entrada nos relatórios da interface do aplicativo local e enviará as informações sobre a atividade maliciosa detectada ao Kaspersky Security Center.

7. Se necessário, edite um escopo de proteção e defina exclusões.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar ou desativar a proteção de pastas compartilhadas contra criptografia externa na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .

2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Anticryptor**.

3. Use a caixa de seleção **Proteção de pastas compartilhadas contra criptografia externa** para ativar ou desativar a detecção de atividade típica da criptografia externa.

4. Use a caixa de seleção **Proteção de pastas compartilhadas contra criptografia externa** para ativar ou desativar a detecção de atividade típica da criptografia externa.

5. Selecione a ação relevante que o aplicativo executará quando uma tentativa de modificar arquivos em pastas compartilhadas for detectada:

   - **Bloquear conexão por (min) N min**. Caso esta opção seja selecionada, ao detectar uma tentativa de modificação dos arquivos em pastas compartilhadas, o Kaspersky Endpoint Security bloqueia o acesso à modificação de arquivo 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 (min) N min** seja selecionada, os arquivos modificados são restaurados a partir das cópias de backup.

   - **Informar**. Caso essa opção esteja selecionada, ao detectar uma tentativa de modificação de arquivos em pastas compartilhadas, o Kaspersky Endpoint Security adicionará as informações sobre a tentativa na lista de ameaças ativas, adicionará uma entrada nos relatórios da interface do aplicativo local e enviará as informações sobre a atividade maliciosa detectada ao Kaspersky Security Center.

6. Se necessário, edite um escopo de proteção e defina exclusões.

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 Endpoint Security bloqueia a sessão do usuário remoto por uma hora. Quando o período de bloqueio expira, o Kaspersky Endpoint 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 (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Anticryptor**.
4. No bloco **Ação ao detectar ameaça**, selecione **Bloquear conexão por N min**.
5. Configure o período de bloqueio de um computador não confiável que esteja envolvido em atividades maliciosas ou criptografia de dados.
6. Salvar alterações.

Como configurar o período de bloqueio de um computador não confiável no Web Console e no Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Proteção Contra Ameaças ao Host** → **Análise de comportamento** → **Anticryptor**.
5. Em **Ação ao detectar ameaça**, configure o período de bloqueio de um computador não confiável que esteja envolvido em atividades maliciosas ou criptografia de dados.
6. Salvar alterações.

Como configurar o período de bloqueio de um computador não confiável na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Anticryptor**.
3. No bloco **Ação ao detectar ameaça**, selecione **Bloquear conexão por (min)**.
4. Configure o período de bloqueio de um computador não confiável que esteja envolvido em atividades maliciosas ou criptografia de dados.
5. Salvar alterações.

Como resultado, o computador remoto será bloqueado. Para desbloquear o computador remoto, reinicie o Kaspersky Endpoint Security.

Editar o escopo de proteção

O *escopo de proteção* é uma lista de caminhos para pastas compartilhadas nas quais o Kaspersky Endpoint Security monitora a atividade do arquivo. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara. Por padrão, o aplicativo identifica automaticamente as pastas compartilhadas e monitora 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, a 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 dos quais as tentativas de criptografia externa não devem ser processadas.

Como editar um escopo de proteção no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Anticryptor**.
4. No bloco **Escopo de proteção**, selecione **Somente pastas especificadas compartilhadas**.
5. Na lista de pastas, clique em **Adicionar**.
6. 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.

7. Clique **OK**.
8. Se necessário, defina as exclusões do escopo de proteção:

   a. No bloco **Exclusões de verificação**, clique no botão **Por máscara**.

   b. Na janela que é aberta, clique no botão **Adicionar**.

   c. Na janela exibida, especifique uma extensão de arquivo no formato `*.<file extension>` ou um caminho de pasta. O Kaspersky Endpoint Security tem suporte aos caracteres `*` e `?` ao inserir uma máscara.

   O aplicativo não é compatível com algumas extensões de arquivo de exclusão. Assim, é possível especificar uma exclusão como `*.docx` ou `**\Folder\**`.

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.

9. Salvar alterações.

Como editar um escopo de proteção no Web Console e no Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Proteção Contra Ameaças ao Host** → **Análise de comportamento** → **Anticryptor**.
5. No bloco **Escopo de proteção**, selecione **Somente pastas compartilhadas especificadas**.
6. Na lista de pastas, clique em **Adicionar**.
7. 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.

8. Clique **OK**.
9. Se necessário, defina as exclusões do escopo de proteção:

   a. Na parte superior da janela, clique no link **Exclusões de verificação**.

   b. Na janela que é aberta, clique no botão **Adicionar**.

   c. Na janela exibida, especifique uma extensão de arquivo no formato `*.<file extension>` ou um caminho de pasta. O Kaspersky Endpoint Security tem suporte aos caracteres `*` e `?` ao inserir uma máscara.

   O aplicativo não é compatível com algumas extensões de arquivo de exclusão. Assim, é possível especificar uma exclusão como `*.docx` ou `**\Folder\**`.

   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.

10. Salvar alterações.

Como editar um escopo de proteção na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Anticryptor**.
3. No bloco **Escopo de proteção**, selecione **Somente pastas especificadas compartilhadas**.
4. Na lista de pastas, clique em **Adicionar**.

5. 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.

6. Clique **OK**.

7. Se necessário, defina as exclusões do escopo de proteção:

   a. Na parte superior da janela, clique no link **Exclusões por máscara**.

   b. Na janela que é aberta, clique no botão **Adicionar**.

   c. Na janela exibida, especifique uma extensão de arquivo no formato `*.<file extension>` ou um caminho de pasta. O Kaspersky Endpoint Security tem suporte aos caracteres `*` e `?` ao inserir uma máscara.

      O aplicativo não é compatível com algumas extensões de arquivo de exclusão. Assim, é possível especificar uma exclusão como `*.docx` ou `**\Folder\**`.

   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.

8. Salvar alterações.

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Exclusões e tipos de objetos detectados**.

3. No bloco **Exclusões**, clique no link **Gerenciar exclusões**.

4. Clique **Adicionar**.

5. Clique em **Procurar** e selecione a pasta compartilhada.

   Também é possível inserir o caminho manualmente. O Kaspersky Endpoint Security é compatível com os 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.

   - `?` (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. Na seção **Componentes de proteção**, selecione o componente **Detecção de Comportamento**.

7. Se necessário, no campo **Comentário**, insira uma breve observação sobre a exclusão de verificação que está sendo criada.

8. Selecione o status **Ativo** para a exclusão.

   Você pode usar o botão de alternância para interromper uma exclusão a qualquer momento.

9. Salvar alterações.

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

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

   A janela de propriedades da política é exibida.

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

4. Ir para a seção **Zona Confiável**.

5. Na janela aberta, clique no link **Exclusões de Verificação de malware**.

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 Endpoint 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 Endpoint Security adiciona uma nova exclusão de verificação à raiz da lista.

   - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Endpoint Security nos servidores SQL, Microsoft Exchange e System Center Configuration Manager, o aplicativo inclui as *exclusões de verificação predefinidas*. Também foram adicionadas exclusões de verificação predefinidas para dar suporte à configuração do aplicativo em ambientes virtuais Citrix e VMware. É necessário selecionar as exclusões predefinidas de verificação dependendo da finalidade do servidor protegido.

9. Selecione como deseja adicionar a exclusão **Caminho para o arquivo ou pasta**.

10. Insira o caminho para a pasta compartilhada.

Também é possível inserir o caminho manualmente. O Kaspersky Endpoint Security é compatível com os 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.

- `?` (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 `C:\Users\*\Folder\`.

11. Na seção **Aplicar exclusão a**, selecione o componente **Detecção de Comportamento**.

12. Se necessário, no campo **Comentário**, insira uma breve observação sobre a exclusão de verificação que está sendo criada.

13. Selecione o status **Adicionar às exclusões** para a exclusão.

    Você pode usar o botão de alternância para interromper uma exclusão a qualquer momento.

14. Salvar alterações.

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Configurações gerais** → **Exclusões e tipos de objetos**.

4. No bloco **Exclusões de verificação e aplicativos confiáveis** → **Exclusões de verificação**, clique no botão **Configurações**.

   Aparecerá uma janela com uma lista de exclusões.

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 Endpoint 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 Endpoint Security adiciona uma nova exclusão de verificação à raiz da lista.

   - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Endpoint Security nos servidores SQL, Microsoft Exchange e System Center Configuration Manager, o aplicativo inclui as *exclusões de verificação predefinidas*. Também foram adicionadas exclusões de verificação predefinidas para dar suporte à configuração do aplicativo em ambientes virtuais Citrix e VMware. É necessário selecionar as exclusões predefinidas de verificação dependendo da finalidade do servidor protegido.

8. Clique **Adicionar**.

9. No bloco **Propriedades**, marque a caixa de seleção **Arquivo ou pasta**.

10. Clique no link **Selecionar arquivo ou pasta** no bloco **Descrição da exclusão de verificação (clique nos itens sublinhados para editá-los)** para abrir a janela **Nome do arquivo ou pasta**.

11. Clique em **Procurar** e selecione a pasta compartilhada.

    Também é possível inserir o caminho manualmente. O Kaspersky Endpoint Security é compatível com os 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.

    - `?` (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\`.

12. Se necessário, no campo **Comentário**, insira uma breve observação sobre a exclusão de verificação que está sendo criada.

13. Clique no bloco **Descrição da exclusão de verificação (clique nos itens sublinhados para editá-los)** para abrir a janela **Componentes de proteção**.

14. Marque a caixa de seleção ao lado do componente **Detecção de Comportamento**.

15. Salvar alterações.

Adicionar computadores confiáveis para criptografia externa de dados

Se sua organização usa criptografia externa de dados no fluxo de trabalho de troca de arquivos, é necessário criar uma lista de computadores confiáveis. O Kaspersky Endpoint Security não monitora a criptografia de dados por 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 Endpoint Security. Você pode reiniciar esse computador remoto depois que o Kaspersky Endpoint 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 (MMC)

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

2. Na árvore do console, selecione **Políticas**.

3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

4. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Anticryptor**.

5. No bloco **Exclusões de verificação**, clique no botão **Por nome ou endereço IP**.

6. Na janela que é aberta, clique no botão **Por nome ou endereço IP**.

7. Insira endereços IP, intervalos de endereços IP ou nomes dos computadores a partir dos quais as tentativas de criptografia externa não devem ser processadas.

   Exemplos:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`

- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como adicionar um computador confiável para criptografia externa de dados no Kaspersky Security Center Web Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Ir para a seção **Zona Confiável**.
5. Na parte direita da janela, clique no link **Exclusões do Anticryptor**.
6. Na janela que é aberta, clique no botão **Adicionar**.
7. Insira endereços IP, intervalos de endereços IP ou nomes dos computadores a partir dos quais as tentativas de criptografia externa não devem ser processadas.

   Exemplos:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como adicionar um computador confiável para criptografia externa de dados na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .
2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Anticryptor**.
3. Na parte superior da janela, clique no link **Exclusões por nome ou endereço IP**.
4. Na janela que é aberta, clique no botão **Adicionar**.
5. Insira endereços IP, intervalos de endereços IP ou nomes dos computadores a partir dos quais as tentativas de criptografia externa não devem ser processadas.

   Exemplos:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`

- `192.168.2-3.0-128`
- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

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 (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Anticryptor**.
4. No bloco **Exclusões de verificação**, clique no botão **Por nome ou endereço IP**.
5. Para exportar a lista de regras:
   a. Selecione as exclusões que deseja exportar. Para selecionar várias portas, use as teclas **CTRL** ou **SHIFT**.
      Se você não selecionou nenhuma exclusão, o Kaspersky Endpoint Security exportará todas as exclusões.
   b. Clique no botão → **Exportar**.
   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 Endpoint Security exporta toda a lista de exclusões para o arquivo XML.
6. Para importar a lista de exclusões:
   a. Clique no botão → **Importar**.
   b. Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de exclusões.
   c. Abra o arquivo.
      Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint 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 exclusões no Web Console e no Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Proteção Contra Ameaças ao Host** → **Análise de comportamento** → **Anticryptor**.
5. Clique no link **Exclusões por nome ou endereço IP**.
6. Para exportar a lista de regras:

   a. Selecione as exclusões que deseja exportar.

   b. Clique no botão → **Exportar**.

   O Kaspersky Endpoint Security exporta a lista de exclusões para um arquivo JSON na pasta de downloads padrão.
7. Para importar a lista de exclusões:

   a. Clique no botão → **Importar**.

   Na janela exibida, selecione o arquivo JSON do qual deseja importar a lista de exclusões.

   b. Abra o arquivo.

   Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo JSON.
8. Salvar alterações.

Mecanismo de Remediação

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

Ao reverter a atividade de Malware no sistema operacional, o Kaspersky Endpoint Security processa os seguintes tipos da atividade de Malware:

- **Atividade de arquivo**

  O Kaspersky Endpoint Security executa as seguintes ações:

  - Exclui arquivos executáveis que foram criados por malware (em todas as mídias, exceto unidades de rede).
  - Exclui arquivos executáveis que foram criados por programas infiltrados por malware.
  - Restaura arquivos que foram modificados ou excluídos por malware.

  O recurso de recuperação de arquivo tem algumas limitações.

- **Atividade de registro**

  O Kaspersky Endpoint Security executa as seguintes ações:

  - Exclui chaves do registro que foram criadas pelo malware.
  - Não restaura chaves do registro que foram modificadas ou excluídas pelo malware.

- **Atividade de sistema**

  O Kaspersky Endpoint Security executa as seguintes ações:

  - Encerra os processos que foram iniciados por malware.
  - Encerra os processos nos quais um aplicativo malicioso foi injetado.
  - Não retoma processos que foram interrompidos por malware.

- **Atividade de rede**

  O Kaspersky Endpoint Security executa as seguintes ações:

  - Bloqueia a atividade de rede do malware.
  - Bloqueia a atividade de rede de processos que foram invadidos pelo malware.

Uma reversão das ações do malware pode ser iniciada pelo componente Proteção Contra Ameaças ao Arquivo ou Detecção de Comportamento ou durante uma verificação de malware.

O procedimento de reverter operações de malware afeta um conjunto de dados definido rigidamente. A reversão não tem efeitos adversos no sistema operacional ou na integridade dos dados do computador.

Como ativar ou desativar o componente Mecanismo de remediação no console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Mecanismo de Remediação**.
4. Use a caixa de seleção **Mecanismo de Remediação** para ativar ou desativar o componente.
5. Salvar alterações.

Como ativar ou desativar o componente Mecanismo de Remediação no Web Console e no Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Proteção Contra Ameaças ao Host** → **Análise de comportamento** → **Mecanismo de Remediação**.
5. Use o botão de alternância do **Mecanismo de Remediação ATIVADO** para ativar ou desativar o componente.
6. Salvar alterações.

Como ativar ou desativar o componente do Mecanismo de Remediação na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Mecanismo de Remediação**.
3. Use o botão de alternância do **Mecanismo de Remediação** para ativar ou desativar o componente.
4. Salvar alterações.

Como resultado, se o Mecanismo de Remediação estiver ativado, o Kaspersky Endpoint Security reverterá as ações executadas por aplicativos maliciosos no sistema operacional.

Kaspersky Security Network

Para melhorar a proteção do computador, o Kaspersky Endpoint 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 Endpoint Security a novas ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos positivos. Caso participe da Kaspersky Security Network, os serviços da KSN fornecem à Kaspersky Endpoint Security informações sobre a reputação dos endereços da Web verificados, além de informações sobre a categoria e a reputação dos arquivos verificados. Para obter mais detalhes sobre a configuração de acesso à KSN, consulte a Ajuda do Kaspersky Security Center.

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 Endpoint 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 Endpoint 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 LAN corporativa é proibida por lei ou restrita pelas políticas de segurança corporativa.

Ativar e desativar o uso do Kaspersky Security Network

Por padrão, o Kaspersky Endpoint Security usa o modo KSN estendido. O *modo KSN estendido* é um modo no qual o Kaspersky Endpoint Security envia dados adicionais para a Kaspersky.

Como ativar ou desativar o Uso da KSN no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Kaspersky Security Network**.

4. Use o botão de alternância do **Kaspersky Security Network** para ativar ou desativar o componente.

   Se você habilitou o uso da KSN, o Kaspersky Endpoint 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.

5. Caso seja necessário, desmarque a caixa de seleção **Ativar modo KSN estendido**. Por padrão, o modo KSN estendido está ativado.

6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar ou desativar o Uso da KSN no Web Console e Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Kaspersky Security Network**.

5. Use o botão de alternância do **Uso da Kaspersky Security Network (KSN) ATIVADO** para ativar ou desativar o componente.

   Se você habilitou o uso da KSN, o Kaspersky Endpoint 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.

6. Caso necessário, desative a opção **Usar modo KSN estendido**. Por padrão, o modo KSN estendido está ativado.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar ou desativar o Uso da KSN na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .

2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Kaspersky Security Network**.

3. Use o botão de alternância do **Kaspersky Security Network** para ativar ou desativar o componente.

   Se você habilitou o uso da KSN, o Kaspersky Endpoint 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.

4. Caso necessário, desative a opção **Ativar modo KSN estendido**. Por padrão, o modo KSN estendido está ativado.

5. Salvar alterações.

Como resultado, se o uso da KSN estiver habilitado, o Kaspersky Endpoint Security usa informações sobre a reputação de arquivos, recursos da Web e aplicativos recebidos da Kaspersky Security Network.

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 Endpoint 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 Endpoint Security está verificando um computador e solicita a reputação de um arquivo na KSN/KPSN. Se o arquivo tiver uma reputação *Não confiável* no banco de dados de reputação local, mas tiver uma reputação *Confiável* na KSN/KPSN, o Kaspersky Endpoint Security detectará o arquivo como *Não confiável* e executará a ação definida para ameaças detectadas.

No entanto, em alguns casos, o Kaspersky Endpoint Security pode não solicitar a reputação de um objeto na KSN/KPSN. Se for esse o caso, o Kaspersky Endpoint Security não receberá dados do banco de dados de reputação local da KPSN. O Kaspersky Endpoint 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. Você também pode definir as configurações de otimização da verificação na interface do aplicativo, por exemplo, para o componente Proteção Contra Ameaças ao Arquivo.

- O Kaspersky Endpoint Security no modo Light Agent se comunica com os servidores da KSN por meio de um servidor proxy da KSN. Não suporte para a comunicação direta com a KSN.

Ativar e desativar o modo na nuvem para os componentes de proteção

O *Modo nuvem* refere-se ao modo operacional do aplicativo no qual o Kaspersky Endpoint Security usa uma versão simplificada dos bancos de dados de antivírus. A Kaspersky Security Network oferece suporte ao funcionamento do aplicativo quando bancos de dados de antivírus leves estão em uso. A versão leve dos bancos de dados de antivírus permite usar aproximadamente metade da RAM do computador que, de outra forma, seria usada nos bancos de dados comuns. Se você não participa da Kaspersky Security Network ou se o modo de nuvem está desativado, o Kaspersky Endpoint Security faz o download da versão completa dos bancos de dados antivírus dos servidores da Kaspersky.

Ao usar o Kaspersky Private Security Network, a funcionalidade do modo na nuvem fica disponível, começando pelo Kaspersky Private Security Network versão 3.0.

Se o aplicativo estiver funcionando em modo Light Agent, o modo na nuvem não estará disponível.

Como ativar ou desativar o Modo na nuvem para os componentes de proteção no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Kaspersky Security Network**.

4. Use a caixa de seleção **Ativar modo na nuvem** para ativar ou desativar o componente.

5. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar ou desativar o Modo na nuvem para os componentes de proteção no Web Console e Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Kaspersky Security Network**.

5. Use o botão de alternância do **Usar o modo na nuvem** para ativar ou desativar o componente.

6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar ou desativar o Modo na nuvem para os componentes de proteção na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .

2. Na janela de configurações do aplicativo, selecione **Proteção Avançada Contra Ameaças** → **Kaspersky Security Network**.

3. Use o botão de alternância do **Ativar modo na nuvem** para ativar ou desativar o componente.

4. Salvar alterações.

Como resultado, o Kaspersky Endpoint Security baixa uma versão light ou uma versão completa dos bancos de dados de antivírus durante a próxima atualização.

> Se a versão leve dos bancos de dados de antivírus não estiver disponível para uso, o Kaspersky Endpoint Security alternará automaticamente para a versão premium de bancos de dados de antivírus.

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 KSN Proxy.

> Se o aplicativo estiver em execução no modo Light Agent, não há suporte para a comunicação direta com a KSN. O Kaspersky Endpoint Security se comunica com os servidores da KSN por meio de um servidor proxy da KSN.

O serviço de KSN Proxy 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 o 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. Portanto, se o Proxy da KSN não estiver disponível, será preciso 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 KSN Proxy da seguinte forma: ative ou desative o KSN Proxy e configure a porta para a conexão. Para fazer isso, é preciso abrir as propriedades do Servidor de Administração. Para obter mais detalhes sobre a configuração do KSN Proxy, consulte a Ajuda do Kaspersky Security Center. Também é possível ativar ou desativar o KSN Proxy para computadores individuais na política do Kaspersky Endpoint Security.

Como ativar ou desativar o Proxy da KSN no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Proteção Avançada Contra Ameaças** → **Kaspersky Security Network**.
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 Endpoint Security usará os servidores da KSN quando o serviço KSN Proxy estiver indisponível. Os servidores da KSN podem ser localizados no lado da Kaspersky e no lado de terceiros (quando a Kaspersky Private Security Network for usada).
6. Salvar alterações.

Como habilitar ou desabilitar o Proxy da KSN no Web Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Kaspersky Security Network**.
5. Use a caixa de seleção **Usar o Servidor de Administração como um servidor proxy da KSN** para ativar ou desativar o KSN Proxy.

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 Endpoint Security usará os servidores da KSN quando o serviço KSN Proxy estiver indisponível. Os servidores da KSN podem ser localizados no lado da Kaspersky e no lado de terceiros (quando a Kaspersky Private Security Network for usada). Por padrão, a caixa de seleção está desmarcada.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

O endereço do KSN Proxy 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 KSN Proxy.

Para configurar o endereço do Proxy da KSN:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione a pasta **Avançado** → **Instalação remota** → **Pacotes de instalação**.
3. No menu de contexto da pasta **Pacotes de instalação**, selecione **Propriedades**.
4. Na guia **Geral** na janela aberta, especifique o novo endereço do servidor proxy da KSN.
5. Salvar alterações.

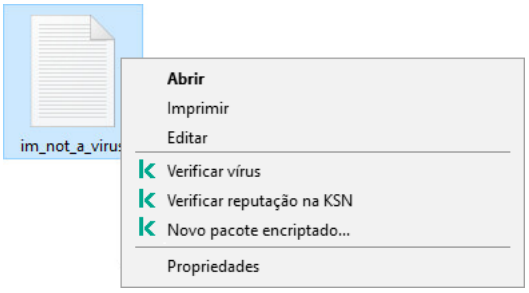
Verificar a reputação de um arquivo np Kaspersky Security Network

Se você duvida da segurança de um arquivo, pode verificar sua reputação no Kaspersky Security Network.

> Você pode verificar a reputação de um arquivo se tiver aceito os termos da Declaração da Kaspersky Security Network.

Para verificar a reputação de um arquivo no Kaspersky Security Network:

Abra o menu de contexto do arquivo e selecione a opção **Verificar a reputação na KSN** (veja a figura abaixo).



Menu de contexto do arquivo

O Kaspersky Endpoint Security exibe a reputação do arquivo:

Confiável (Kaspersky Security Network). O aplicativo considera um arquivo confiável se uma ou mais das seguintes condições forem atendidas:

- o arquivo é assinado digitalmente por um fornecedor confiável;
- o arquivo tem uma reputação confiável na Kaspersky Security Network;
- O usuário colocou o arquivo no Grupo confiável.

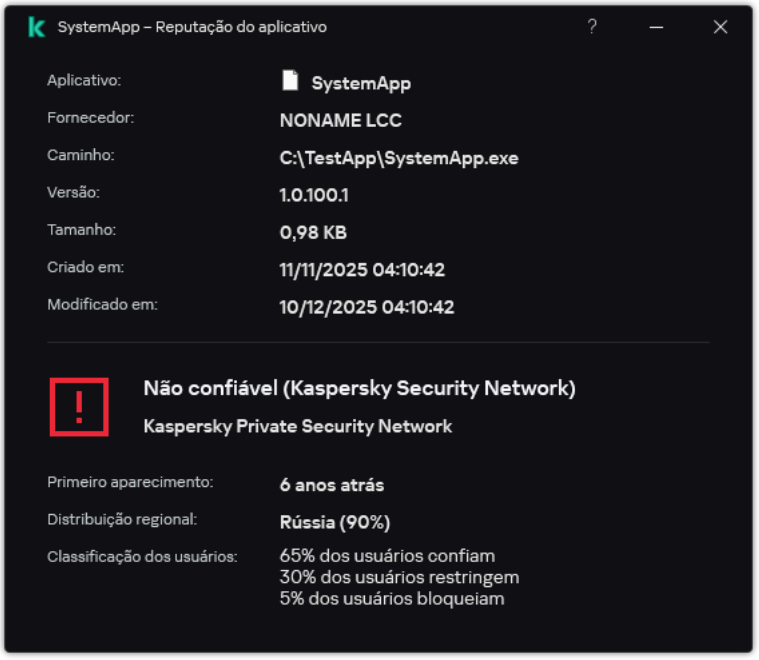
Software legítimo que pode ser usado por intrusos para danificar seu computador ou dados pessoais. Para obter detalhes sobre o software legítimo que pode ser usado por criminosos para danificar o computador ou os dados pessoais de um usuário, visite o site da Kaspersky IT Encyclopedia. Você pode adicionar esses aplicativos à lista confiável.

Não confiável (Kaspersky Security Network). Um vírus ou outro aplicativo que representa uma ameaça.

Desconhecido (Kaspersky Security Network). O Kaspersky Security Network não possui nenhuma informação sobre o arquivo. Você pode verificar um arquivo usando bancos de dados de antivírus (a opção **Verificar Vírus** no menu de contexto).

O Kaspersky Endpoint Security exibe a solução KSN usada para determinar a reputação do arquivo: *Kaspersky Security Network* ou *Kaspersky Private Security Network*.

O Kaspersky Endpoint Security também exibe informações adicionais sobre o arquivo (veja a figura abaixo).



Reputação de um arquivo na Kaspersky Security Network

Verificação de conexões criptografadas

Após a instalação, o Kaspersky Endpoint Security adiciona um certificado Kaspersky ao armazenamento do sistema para certificados confiáveis (armazenamento de certificados do Windows). O Kaspersky Endpoint Security usa esse certificado para verificar conexões criptografadas. O Kaspersky Endpoint Security também inclui o uso do armazenamento do sistema de certificados confiáveis no Firefox e Thunderbird para verificar o tráfego desses aplicativos.

Os componentes Controle da Web, Proteção Contra Ameaças ao Correio, Proteção Contra Ameaças da Web, Detecção de comportamento e Prevenção de Exploits podem descriptografar e verificar o tráfego de rede transmitido por conexões criptografadas por meio dos seguintes protocolos:

- SSL 3.0.
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Ativar a verificação de conexões criptografadas

Por padrão, o Kaspersky Endpoint Security verifica as conexões criptografadas apenas quando solicitado pelos componentes de proteção.

Como ativar a verificação de conexões criptografadas no Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Configurações gerais** → **Configurações de rede**.
5. No bloco **Verificação de conexões criptografadas**, selecione o modo da verificação de conexões criptografadas:
   - **Verificar conexões criptografadas**. O Kaspersky Endpoint Security não terá acesso ao conteúdo de sites cujos endereços comecem com `https://`.
   - **Verificar conexões criptografadas após solicitação de componentes de proteção**. O Kaspersky Endpoint Security verificará o tráfego criptografado apenas quando solicitado pelos componentes Proteção Contra Ameaças da Web, Proteção Contra Ameaças ao Correio e Controle da Web.
   - **Sempre verificar conexões criptografadas**. O Kaspersky Endpoint Security verificará o tráfego de rede criptografado mesmo se os componentes de proteção estiverem desativados.

O Kaspersky Endpoint Security não verifica conexões criptografadas estabelecidas por aplicativos confiáveis para os quais a verificação de tráfego está desativada. O Kaspersky Endpoint Security não verifica conexões criptografadas da lista predefinida de sites confiáveis. A lista predefinida de sites confiáveis é criada por especialistas da Kaspersky. Esta lista é atualizada com os bancos de dados de antivírus do aplicativo. É possível visualizar a lista predefinida de sites confiáveis apenas na interface do Kaspersky Endpoint Security. Não é possível visualizar a lista no Console do Kaspersky Security Center.

6. Se necessário, adicione exclusões de verificação: endereços e aplicativos confiáveis.

7. Defina as configurações para verificar as conexões criptografadas (consulte a tabela abaixo).

8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar a verificação de conexões criptografadas no Web Console e Cloud Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Configurações de rede**.

5. Em **Verificação de conexões criptografadas**, ative o botão de alternância **Verificação de conexões criptografadas ATIVADA**.

   Caso o botão de alternância esteja desativado, o Kaspersky Endpoint Security não terá acesso ao conteúdo de sites cujos endereços comecem com `https://`.

6. Clique em **Configurações** e selecione o modo da verificação de conexões criptografadas:

   - **Verificar conexões criptografadas após solicitação de componentes de proteção**. O Kaspersky Endpoint Security verificará o tráfego criptografado apenas quando solicitado pelos componentes Proteção Contra Ameaças da Web, Proteção Contra Ameaças ao Correio e Controle da Web.

   - **Sempre verificar conexões criptografadas**. O Kaspersky Endpoint Security verificará o tráfego de rede criptografado mesmo se os componentes de proteção estiverem desativados.

O Kaspersky Endpoint Security não verifica conexões criptografadas estabelecidas por aplicativos confiáveis para os quais a verificação de tráfego está desativada. O Kaspersky Endpoint Security não verifica conexões criptografadas da lista predefinida de sites confiáveis. A lista predefinida de sites confiáveis é criada por especialistas da Kaspersky. Esta lista é atualizada com os bancos de dados de antivírus do aplicativo. É possível visualizar a lista predefinida de sites confiáveis apenas na interface do Kaspersky Endpoint Security. Não é possível visualizar a lista no Console do Kaspersky Security Center.

7. Se necessário, adicione exclusões de verificação: endereços e aplicativos confiáveis.

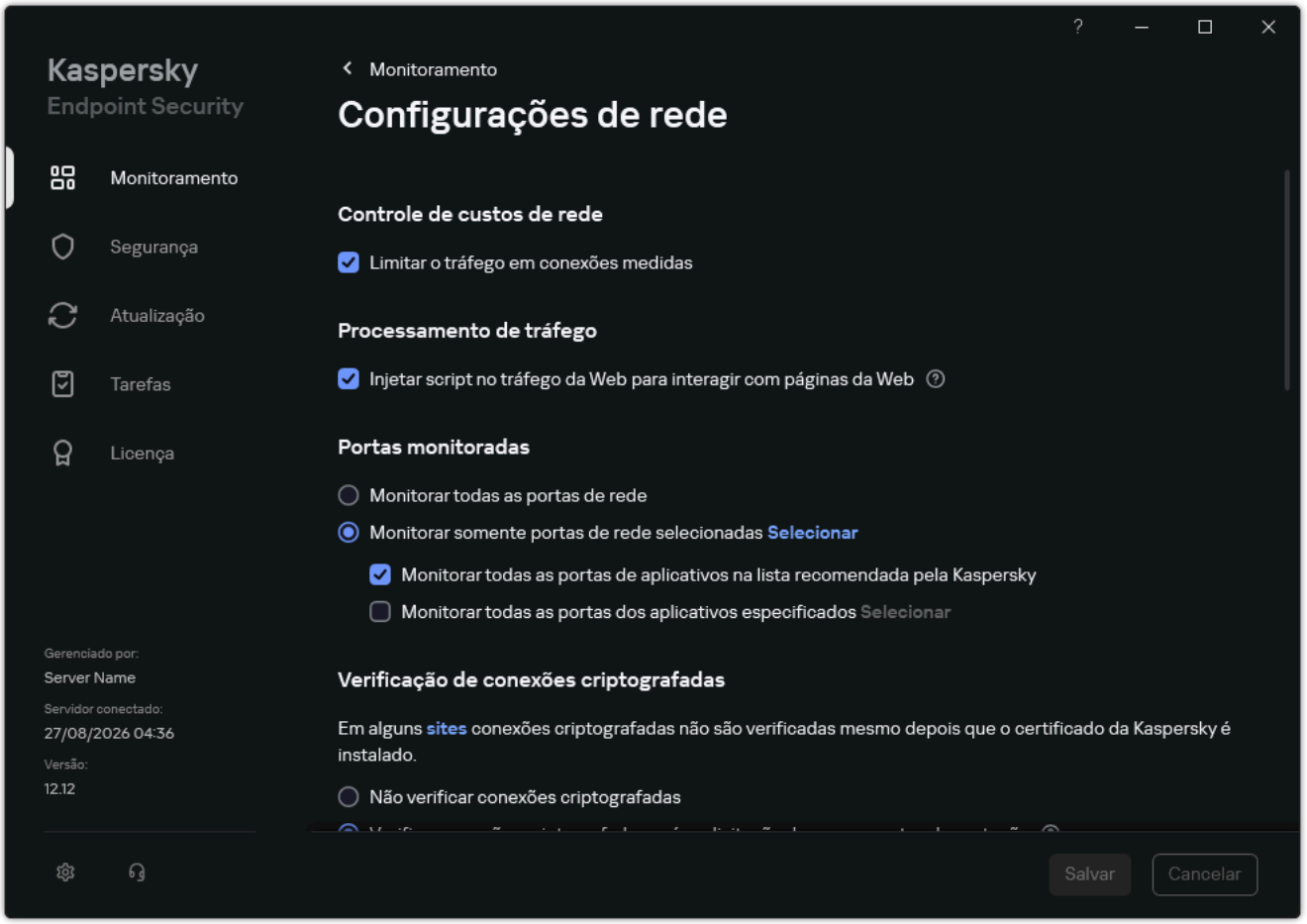
8. Defina as configurações para verificar as conexões criptografadas (consulte a tabela abaixo).

9. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar a verificação de conexões criptografadas na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações de rede**.



Configurações da Verificação de conexões criptografadas

3. No bloco **Verificação de conexões criptografadas**, selecione o modo da verificação de conexões criptografadas:

   - **Não verificar conexões criptografadas**. O Kaspersky Endpoint Security não terá acesso ao conteúdo de sites cujos endereços comecem com `https://`.

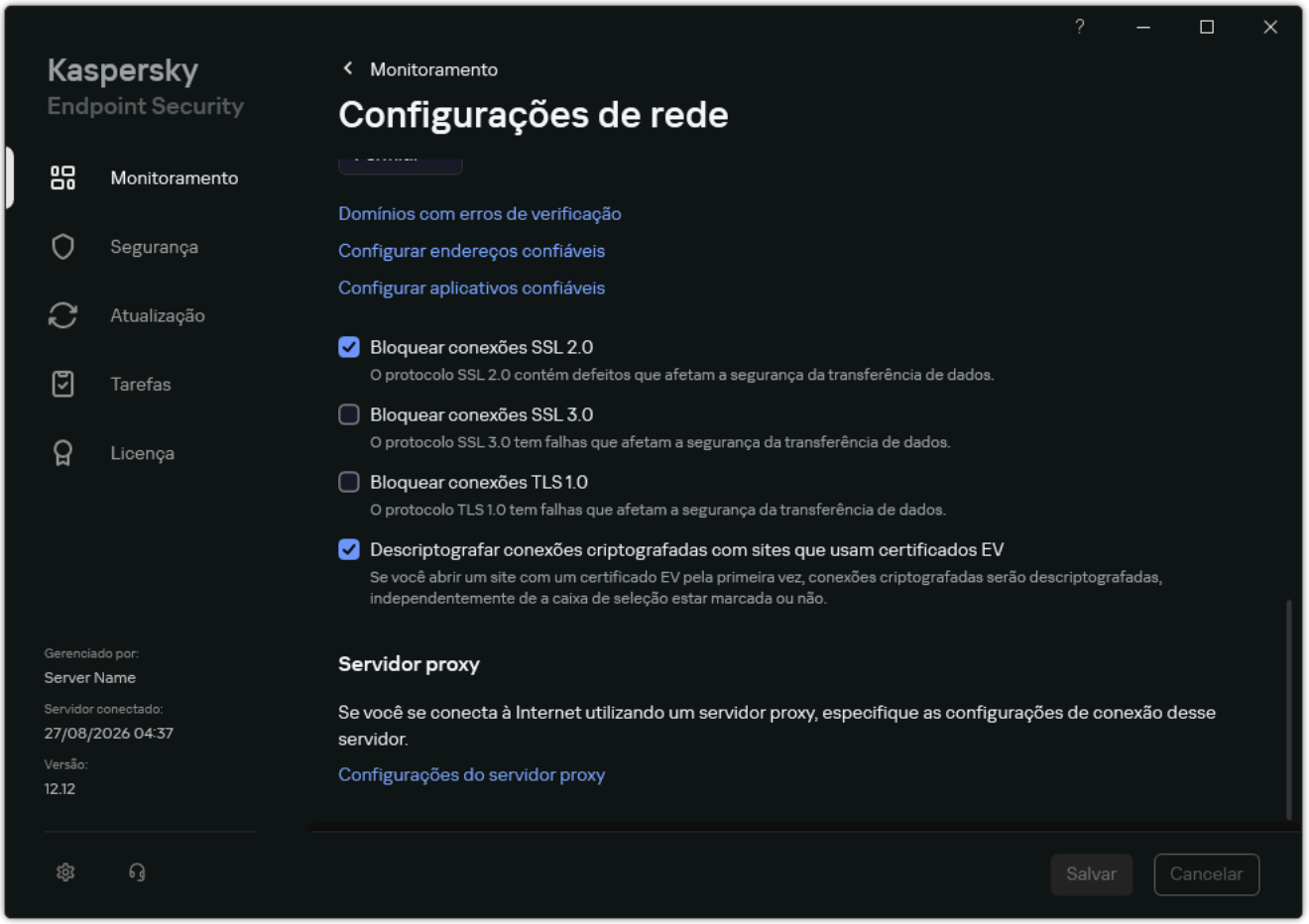
   - **Verificar conexões criptografadas após solicitação de componentes de proteção**. O Kaspersky Endpoint Security verificará o tráfego criptografado apenas quando solicitado pelos componentes Proteção Contra Ameaças da Web, Proteção Contra Ameaças ao Correio e Controle da Web.

   - **Sempre verificar conexões criptografadas**. O Kaspersky Endpoint Security verificará o tráfego de rede criptografado mesmo se os componentes de proteção estiverem desativados.

O Kaspersky Endpoint Security não verifica conexões criptografadas estabelecidas por aplicativos confiáveis para os quais a verificação de tráfego está desativada. O Kaspersky Endpoint Security não verifica conexões criptografadas da lista predefinida de sites confiáveis. A lista predefinida de sites confiáveis é criada por especialistas da Kaspersky. Esta lista é atualizada com os bancos de dados de antivírus do aplicativo. É possível visualizar a lista predefinida de sites confiáveis apenas na interface do Kaspersky Endpoint Security. Não é possível visualizar a lista no Console do Kaspersky Security Center.

4. Se necessário, adicione exclusões de verificação: endereços e aplicativos confiáveis.

5. Defina as configurações para verificar as conexões criptografadas (consulte a tabela abaixo).



Configurações adicionais para verificação de conexões criptografadas

6. Salvar alterações.

Configurações da Verificação de conexões criptografadas

Parâmetro	Descrição
Certificados raiz confiáveis	Lista de certificados raiz confiáveis. O Kaspersky Endpoint Security permite a instalação de certificados raiz confiáveis nos computadores dos usuários caso, por exemplo, seja necessário implementar um novo centro de certificação. O aplicativo permite adicionar um certificado para uma loja especial de certificado Kaspersky Endpoint Security. Neste caso, o certificado é considerado confiável somente para o aplicativo Kaspersky Endpoint Security. Em outras palavras, o usuário pode ter acesso a um site com um novo certificado no navegador. Caso outro aplicativo tente acessar o site, é possível ocorrer um erro de conexão devido a um problema de certificado. Para adicionar ao sistema de armazenamento de certificados, é possível usar as políticas do grupo do Active Directory.
Acesso a um domínio com um certificado não confiável	• **Permitir**. Ao visitar um domínio com um certificado não confiável, o Kaspersky Endpoint Security permitirá a conexão da rede. Ao abrir um domínio com um certificado não confiável em um navegador, o Kaspersky Endpoint Security exibe uma página HTML com um aviso e o motivo de o acesso ao domínio não ser recomendado. Um usuário pode clicar no link da página de aviso HTML para obter o acesso ao recurso da Web solicitado. Se um aplicativo ou serviço de terceiros estabelecer conexão com um domínio com um certificado não confiável, o Kaspersky Endpoint Security cria seu próprio certificado para verificar o tráfego. O novo certificado possui o status *Não confiável*. Isso é necessário para avisar o aplicativo de terceiros sobre a conexão não confiável, pois a página HTML não pode ser exibida nesse caso e a conexão pode ser estabelecida em modo de segundo plano. • **Bloquear**. Ao visitar um domínio com um certificado não confiável, o Kaspersky Endpoint Security bloqueará a conexão da rede. Ao abrir um domínio com um certificado não confiável em um navegador, o Kaspersky Endpoint Security exibe uma página HTML com o motivo pelo qual o domínio está bloqueado.
Acesso a um domínio com um erro de verificação de conexões criptografadas	• **Bloquear**. Caso um erro de verificação de conexão criptografada ocorra, o Kaspersky Endpoint Security bloqueará a conexão de rede. • **Permitir e adicionar domínio às exclusões**. Caso um erro de verificação de conexão criptografada ocorra, o Kaspersky Endpoint Security adicionará o domínio que resultou no erro à lista de domínios com erros de verificação e não monitorará o tráfego de rede criptografado quando este domínio for acessado. É possível visualizar uma lista de domínios com erros de verificação de conexões criptografadas apenas na interface local do aplicativo. Para limpar o conteúdo da lista, você precisa selecionar **Bloquear**. O Kaspersky Endpoint Security também gera um evento para o erro de verificação de conexões criptografadas.

Parâmetro	Descrição
Bloquear conexões SSL 2.0	Se a caixa de seleção estiver marcada, o aplicativo monitora e bloqueia as conexões de rede estabelecidas por meio do protocolo SSL 2.0. Se a caixa de seleção for desmarcada, o aplicativo não bloqueará as conexões de rede estabelecidas por meio do protocolo SSL 2.0. No entanto, o aplicativo não monitora o tráfego de rede por meio desse protocolo.
Bloquear conexões SSL 3.0	Se a caixa de seleção for marcada, o aplicativo bloqueará as conexões de rede estabelecidas por meio do protocolo SSL 3.0. Se a caixa de seleção for desmarcada, o aplicativo não bloqueará as conexões de rede estabelecidas por meio do protocolo SSL 3.0. O aplicativo monitora o tráfego de rede por meio desse protocolo. Todos os componentes do aplicativo funcionam sem restrições.
Bloquear conexões TLS 1.0	Se a caixa de seleção for marcada, o aplicativo bloqueará as conexões de rede estabelecidas por meio do protocolo TLS 1.0. Se a caixa de seleção for desmarcada, o aplicativo não bloqueará as conexões de rede estabelecidas por meio do protocolo TLS 1.0. O aplicativo monitora o tráfego de rede por meio desse protocolo. Todos os componentes do aplicativo funcionam sem restrições.
Descriptografar conexões criptografadas com sites que usam certificados EV	Os certificados EV (Extended Validation Certificate) confirmam a autenticidade dos sites e aumentam a segurança da conexão. Os navegadores usam um ícone de fechadura na sua barra de endereço para indicar que um site possui um certificado EV. Os navegadores também podem colorir total ou parcialmente a barra de endereço em verde. Se a caixa de seleção estiver selecionada, o aplicativo descriptografa e monitora as conexões criptografadas que usam um certificado EV. Se a caixa de seleção estiver desmarcada, o aplicativo não tem acesso ao conteúdo do tráfego HTTPS. Por esse motivo, o aplicativo monitora o tráfego HTTPS apenas com base no endereço do site, por exemplo, `https://bing.com`. Se você estiver abrindo um site com um certificado EV pela primeira vez, a conexão criptografada será descriptografada independentemente se a caixa foi ou não marcada.

Instalação dos certificados raiz confiáveis

O Kaspersky Endpoint Security permite a instalação de certificados raiz confiáveis nos computadores dos usuários caso, por exemplo, seja necessário implementar um novo centro de certificação. O aplicativo permite adicionar um certificado para uma loja especial de certificado Kaspersky Endpoint Security. Neste caso, o certificado é considerado confiável somente para o aplicativo Kaspersky Endpoint Security. Em outras palavras, o usuário pode ter acesso a um site com um novo certificado no navegador. Caso outro aplicativo tente acessar o site, é possível ocorrer um erro de conexão devido a um problema de certificado. Para adicionar ao sistema de armazenamento de certificados, é possível usar as políticas do grupo do Active Directory.

Como instalar certificados raiz confiáveis no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Configurações de rede**.
4. No bloco **Certificados raiz confiáveis**, clique no botão **Adicionar**.
5. Isso abre uma janela; nessa janela selecione um certificado de raiz confiável.
   O Kaspersky Endpoint Security dá suporte a certificados com extensões PEM, DER e CRT.
6. Salvar alterações.

Como instalar certificados raiz confiáveis no Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Configurações de rede**.
5. Clique no link **Certificados raiz confiáveis**.
6. Isso abre uma janela; nessa janela clique em **Adicionar** e selecione um certificado de raiz confiável.
   O Kaspersky Endpoint Security dá suporte a certificados com extensões PEM, DER e CRT.
7. Salvar alterações.

Como instalar certificados raiz confiáveis na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações de rede**.
3. No bloco **Verificação de conexões criptografadas**, clique no botão **Mostrar certificados**.
4. Isso abre uma janela; nessa janela clique em **Adicionar** e selecione um certificado de raiz confiável.
   O Kaspersky Endpoint Security dá suporte a certificados com extensões PEM, DER e CRT.
5. Salvar alterações.

Como resultado, ao verificar o tráfego, além do armazenamento de certificados do sistema, o Kaspersky Endpoint Security usa o seu próprio armazenamento de certificados.

Verificar conexões criptografadas com um certificado não confiável

Após a instalação, o Kaspersky Endpoint Security adiciona um certificado Kaspersky ao armazenamento do sistema para certificados confiáveis (armazenamento de certificados do Windows). O Kaspersky Endpoint Security usa esse certificado para verificar conexões criptografadas. Ao visitar um domínio com um certificado não confiável, é possível permitir ou negar o acesso do usuário a esse domínio (consulte as instruções abaixo).

Caso tenha permitido que o usuário visite domínios com certificados não confiáveis, o Kaspersky Endpoint Security executará as seguintes ações:

- Ao visitar um domínio com um certificado não confiável no *navegador*, o Kaspersky Endpoint Security usa o certificado da Kaspersky para verificar o tráfego. O Kaspersky Endpoint Security exibe uma página HTML com um aviso e informações sobre o motivo pelo qual não é recomendado visitar o domínio relevante (veja a figura abaixo). Um usuário pode clicar no link da página de aviso HTML para obter o acesso ao recurso da Web solicitado. Depois de seguir este link, durante a próxima hora o Kaspersky Endpoint Security não exibirá avisos sobre um certificado não confiável ao visitar outros recursos neste mesmo domínio. O Kaspersky Endpoint Security também gera um evento sobre o estabelecimento de uma conexão criptografada com um certificado não confiável.

  Em alguns casos, o Kaspersky Endpoint Security não pode exibir tecnicamente uma página HTML com um aviso no navegador (veja a figura abaixo). Por exemplo, se um recurso da Web utilizar uma versão desatualizada de um protocolo de rede e uma porta fora do padrão. Nesses casos, o Kaspersky Endpoint Security bloqueará o acesso a esse domínio e o navegador exibirá a janela `ERR_CONNECTION_RESET` padrão. Para acessar um recurso da Web, você pode adicionar o domínio às exclusões ou usar um certificado confiável.

- Se *um aplicativo ou serviço de terceiros* estabelecer conexão com um domínio com um certificado não confiável, o Kaspersky Endpoint Security cria seu próprio certificado para verificar o tráfego. O novo certificado possui o status *Não confiável*. Isso é necessário para avisar o aplicativo de terceiros sobre a conexão não confiável, pois a página HTML não pode ser exibida nesse caso e a conexão pode ser estabelecida em modo de segundo plano. Portanto, se um aplicativo de terceiros tiver ferramentas de verificação de certificado integradas, a conexão poderá ser encerrada. Nesse caso, é necessário entrar em contato com o proprietário do domínio e configurar uma conexão confiável. Se for impossível configurar uma conexão confiável, você pode adicionar esse aplicativo de terceiros à lista de aplicativos confiáveis. O Kaspersky Endpoint Security também gera um evento sobre o estabelecimento de uma conexão criptografada com um certificado não confiável.

Como configurar a verificação de conexões criptografadas com um certificado não confiável no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Configurações de rede**.
4. No bloco **Verificação de conexões criptografadas**, clique no botão **Configurações avançadas**.
5. Na janela aberta, selecione o modo de operação do aplicativo ao visitar um domínio com um certificado não confiável: **Permitir** ou **Bloquear**.
6. Salvar alterações.

Como configurar a verificação de conexões criptografadas com um certificado não confiável no Web Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.

4. Selecione **Configurações gerais** → **Configurações de rede**.

5. No bloco **Verificação de conexões criptografadas**, clique no link **Configurações**.

6. Na janela aberta, selecione o modo de operação do aplicativo ao visitar um domínio com um certificado não confiável: **Permitir conexão** ou **Bloquear conexão**.

7. Salvar alterações.

Como configurar a verificação de conexões criptografadas com um certificado não confiável na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações de rede**.

3. No bloco **Verificação de conexões criptografadas**, selecione o modo de operação do aplicativo ao visitar um domínio com um certificado não confiável: **Permitir** ou **Bloquear**.

4. Salvar alterações.

Aviso sobre visitar um domínio com um certificado não confiável

Adicionar o certificado da Kaspersky ao armazenamento de certificados próprio

Navegadores e programas de e-mail usam o certificado para confirmar a segurança e a autenticidade de recurso da Web. O certificado também fornece criptografia de dados entre os recursos da Web e o usuário. A maioria dos navegadores e dos programas de e-mail usam o armazenamento de certificados confiável (armazenamento de certificados do Windows). Por exemplo, Google Chrome. Alguns navegadores e programas de e-mail usam seu próprio armazenamento de certificados, por padrão, em vez do armazenamento de certificados do Windows. Por exemplo, Firefox e Thunderbird.

Após a instalação, o Kaspersky Endpoint Security adiciona um certificado Kaspersky ao armazenamento do sistema para certificados confiáveis (armazenamento de certificados do Windows). Se o Kaspersky Security Center for implantado em sua organização e uma política estiver sendo aplicada a um computador, o Kaspersky Endpoint Security ativa automaticamente o uso do armazenamento de certificados do Windows nos navegadores e nos programas de e-mail para verificar o tráfego desses aplicativos. Se uma política não estiver sendo aplicada ao computador, você poderá escolher o armazenamento de certificados que será usado pelos navegadores e pelos programas de e-mail. Se você tiver selecionado o armazenamento de certificados próprio, adicione o certificado da Kaspersky ao armazenamento manualmente. Isso ajudará a evitar erros ao trabalhar com tráfego HTTPS.

Para verificar o tráfego no navegador Mozilla Firefox e o cliente de correio Thunderbird, é necessário ativar a verificação de conexões criptografadas. Caso a verificação de conexões criptografadas esteja desativada, o aplicativo não verifica o tráfego no navegador Mozilla Firefox e no cliente de correio Thunderbird. A verificação de conexões criptografadas também deve ser ativada para verificar o tráfego nos programas de e-mail MyOffice Mail e R7-Office Organizer.

Antes de adicionar um certificado ao armazenamento de certificados do navegador ou do próprio agente de e-mail, exporte o certificado da Kaspersky pelo painel de controle do Windows (propriedades da Internet). Você pode saber mais sobre como adicionar um certificado ao armazenamento, por exemplo, no site de suporte técnico do Mozilla.

Você pode escolher o armazenamento de certificados apenas na interface local do aplicativo.

Para escolher um armazenamento de certificados para verificar conexões criptografadas em navegadores e programas de e-mail:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações de rede**.
3. No bloco **Verificação de conexões criptografadas**, marque a caixa de seleção **Para verificar conexões criptografadas em aplicativos com armazenamento de certificados próprio, use**.
4. Selecione um armazenamento de certificados:
   - **Repositório de certificados do Windows (recomendado)**. O certificado raiz da Kaspersky é adicionado a este repositório durante a instalação do Kaspersky Endpoint Security.
   - **Armazenamento de certificados próprio**. Mozilla Firefox e Thunderbird usam seus próprios repositórios de certificados. Se o armazenamento de certificados do Mozilla for selecionado, você precisará adicionar manualmente o certificado raiz da Kaspersky a este armazenamento por meio das propriedades do navegador.

     Os programas de e-mail MyOffice Mail e R7-Office Organizer também usam armazenamentos de certificados próprios.
5. Salvar alterações.

Excluindo conexões criptografadas da verificação

A maioria dos recursos da web usa conexões criptografadas. Os especialistas da Kaspersky recomendam que você ative a verificação de conexões criptografadas. Caso a verificação de conexões criptografadas interfira na atividade relacionada ao trabalho, é possível adicionar um site a exclusões conhecidas como *endereços confiáveis*. Nesse caso, o Kaspersky Endpoint Security não verifica o tráfego HTTPS de endereços da Web confiáveis quando os componentes Proteção Contra Ameaças da Web, Proteção Contra Ameaças ao Correio e Controle da Web estão fazendo seu trabalho.

Se um aplicativo confiável usar uma conexão criptografada, você poderá desativar a verificação de conexões criptografadas para esse aplicativo. Por exemplo, você pode desativar a verificação de conexões criptografadas para aplicativos de armazenamento em nuvem que usam autenticação de dois fatores com seu próprio certificado.

Como excluir um endereço da Web das verificações de conexões criptografadas no Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Configurações gerais** → **Configurações de rede**.
5. No bloco **Verificação de conexões criptografadas**, clique no botão **Configurar endereços confiáveis**.
6. Clique **Adicionar**.
7. Digite um nome de domínio ou endereço IP, se não quiser que o Kaspersky Endpoint Security verifique as conexões criptografadas estabelecidas ao visitar esse domínio.

   O Kaspersky Endpoint Security é compatível com o caractere `*` para inserção de uma máscara no nome de domínio.

   > O Kaspersky Endpoint Security não é compatível com o símbolo `*` para endereços IP. É possível selecionar um intervalo de endereços IP usando uma máscara de sub-rede (por exemplo, 198.51.100.0/24).

   Exemplos:

   - `domain.com`: o registro inclui os seguintes endereços: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. O registro é exclusivo de subdomínios (por exemplo, `subdomain.domain.com`).
   - `subdomain.domain.com`: o registro inclui os seguintes endereços: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. O registro é exclusivo do domínio `domain.com`.
   - `*.domain.com`: o registro inclui os seguintes endereços: `https://movies.domain.com`, `https://images.domain.com/page123`. O registro é exclusivo do domínio `domain.com`.
8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como excluir um endereço da Web das verificações de conexões criptografadas no Web Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Configurações de rede**.
5. No bloco **Verificação de conexões criptografadas**, clique no botão **Domínios confiáveis**.
6. Clique **Adicionar**.
7. Digite um nome de domínio ou endereço IP, se não quiser que o Kaspersky Endpoint Security verifique as conexões criptografadas estabelecidas ao visitar esse domínio.

   O Kaspersky Endpoint Security é compatível com o caractere `*` para inserção de uma máscara no nome de domínio.

   > O Kaspersky Endpoint Security não é compatível com o símbolo `*` para endereços IP. É possível selecionar um intervalo de endereços IP usando uma máscara de sub-rede (por exemplo, 198.51.100.0/24).

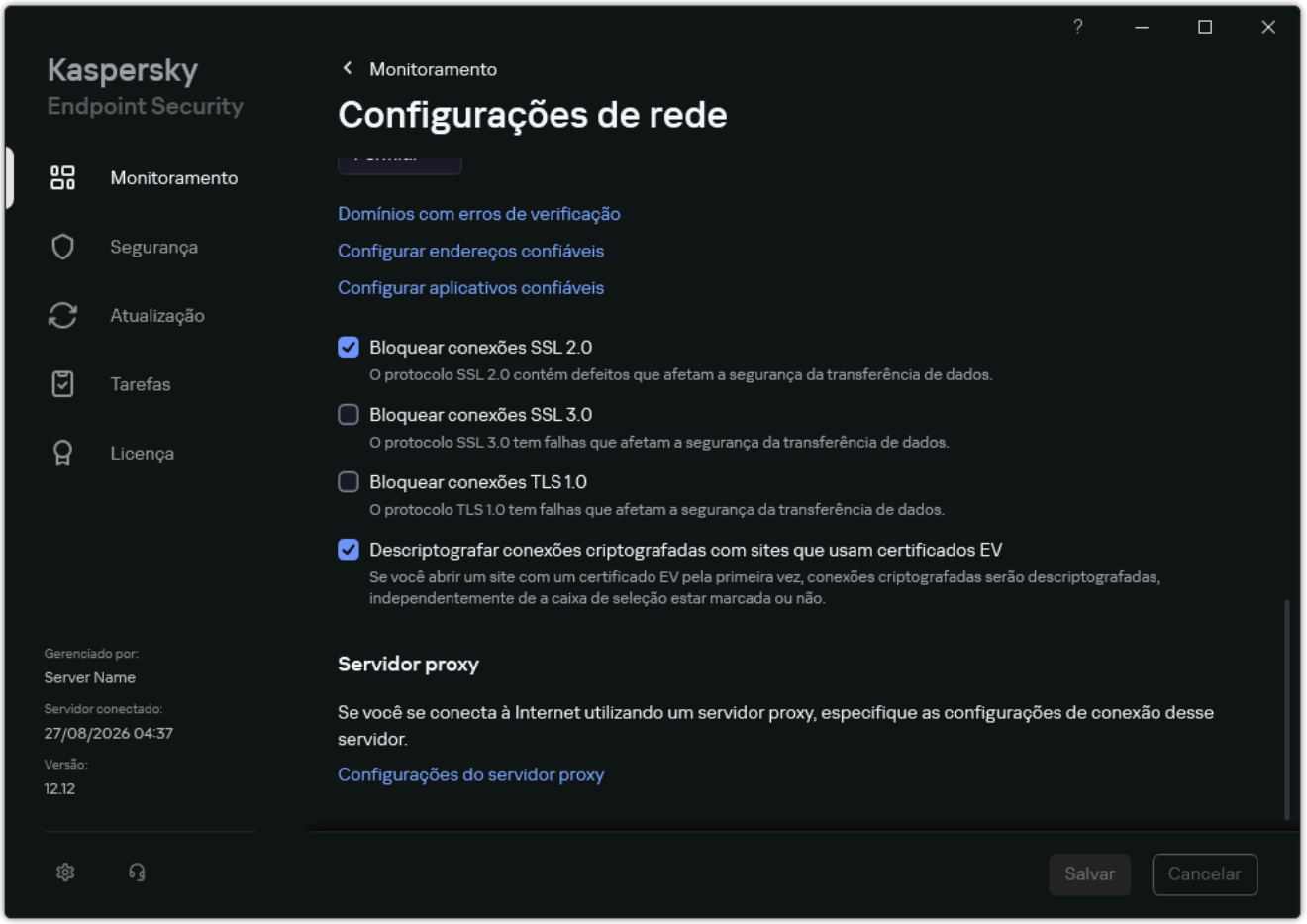
   Exemplos:

   - `domain.com`: o registro inclui os seguintes endereços: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. O registro é exclusivo de subdomínios (por exemplo, `subdomain.domain.com`).
   - `subdomain.domain.com`: o registro inclui os seguintes endereços: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. O registro é exclusivo do domínio `domain.com`.
   - `*.domain.com`: o registro inclui os seguintes endereços: `https://movies.domain.com`, `https://images.domain.com/page123`. O registro é exclusivo do domínio `domain.com`.
8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como excluir um endereço da Web de verificações de conexões criptografadas na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações de rede**.



Configurações de aplicativo rede

3. No bloco **Verificação de conexões criptografadas**, clique no botão **Configurar endereços confiáveis**.

4. Clique **Adicionar**.

5. Digite um nome de domínio ou endereço IP, se não quiser que o Kaspersky Endpoint Security verifique as conexões criptografadas estabelecidas ao visitar esse domínio.

   O Kaspersky Endpoint Security é compatível com o caractere `*` para inserção de uma máscara no nome de domínio.

   > O Kaspersky Endpoint Security não é compatível com o símbolo `*` para endereços IP. É possível selecionar um intervalo de endereços IP usando uma máscara de sub-rede (por exemplo, 198.51.100.0/24).

Exemplos:

- `domain.com`: o registro inclui os seguintes endereços: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. O registro é exclusivo de subdomínios (por exemplo, `subdomain.domain.com`).
- `subdomain.domain.com`: o registro inclui os seguintes endereços: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. O registro é exclusivo do domínio `domain.com`.
- `*.domain.com`: o registro inclui os seguintes endereços: `https://movies.domain.com`, `https://images.domain.com/page123`. O registro é exclusivo do domínio `domain.com`.

6. Salvar alterações.

Por padrão, o Kaspersky Endpoint Security não verifica conexões criptografadas quando ocorrem erros e adiciona o site a uma lista especial de *Domínios com erros de verificação*. O Kaspersky Endpoint Security compila uma lista separada para cada usuário e não envia dados para o Kaspersky Security Center. Você pode ativar o bloqueio da conexão quando ocorrer um erro de verificação. É possível visualizar uma lista de domínios com erros de verificação de conexões criptografadas apenas na interface local do aplicativo.

Para visualizar a lista de domínios com erros de verificação:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações de rede**.
3. No bloco **Verificação de conexões criptografadas**, clique no botão **Domínios com erros de verificação**.

   Uma lista de domínios com erros de verificação é aberta. Para redefinir a lista, ative o bloqueio de conexão quando ocorrerem erros de varredura na política, aplique a política, redefina o parâmetro para seu valor inicial e aplique a política novamente.

Os especialistas da Kaspersky fazem uma lista de *exceções globais* - sites confiáveis que o Kaspersky Endpoint Security não verifica, independentemente das configurações do aplicativo.

Para exibir as exclusões globais das verificações de tráfego criptografado:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações de rede**.
3. No bloco **Verificação de conexões criptografadas**, clique na lista do link de sites confiáveis.

   Aparecerá uma lista de sites compilada por especialistas da Kaspersky. O Kaspersky Endpoint Security não verifica conexões protegidas para sites da lista. A lista pode ser atualizada quando os bancos de dados e os módulos do Kaspersky Endpoint Security são atualizados.

Bloquear o acesso a domínios com certificados não confiáveis

Em alguns casos, ao bloquear o acesso a um domínio com certificado não confiável, o Kaspersky Endpoint Security exibe no navegador uma página de aviso HTML sem o link para o recurso da Web solicitado.

Isso pode acontecer pelos seguintes motivos:

- O administrador bloqueou o acesso a um domínio com certificado não confiável.
- O domínio tem um certificado não confiável ou inválido, e o servidor da Web usa o mecanismo HTTP Strict Transport Security (HSTS). O *HSTS* é um mecanismo de segurança que impõe o uso do protocolo HTTPS seguro para a comunicação entre um cliente e um servidor da Web. Nesse caso, não é possível acessar o domínio, mesmo que ele tenha sido adicionado à lista de endereços confiáveis. O mecanismo HSTS é descrito na RFC 6797.

  Em alguns casos, o site pode ser aberto diretamente em um navegador sem usar o Kaspersky Endpoint Security. Os navegadores nem sempre detectam certificados revogados, enquanto o Kaspersky Endpoint Security realiza uma verificação on-line da revogação do certificado ao estabelecer uma conexão. Isso permite que o aplicativo detecte um problema no certificado antes do navegador e exiba a mensagem de erro correspondente.

Aviso sobre visitar um domínio com um certificado não confiável

Limpar dados

O Kaspersky Endpoint Security permite que você use uma tarefa para excluir remotamente dados dos computadores dos usuários.

O Kaspersky Endpoint Security exclui dados da seguinte maneira:

- No modo silencioso;
- Em discos rígidos e unidades removíveis;
- Para todas as contas de usuários no computador.

O Kaspersky Endpoint Security executa a tarefa *Limpar dados* independentemente do tipo de licenciamento que está sendo usado, mesmo depois que a licença expirar.

Modos de limpeza de dados

Esta tarefa permite excluir dados nos seguintes modos:

- Exclusão imediata de dados.

  Nesse modo, você pode, por exemplo, excluir dados desatualizados para liberar espaço em disco.

- Exclusão de dados adiada.

  Este modo destina-se, por exemplo, a proteger dados em um laptop, caso sejam perdidos ou roubados. Você pode configurar a exclusão automática de dados se o laptop ultrapassar os limites da rede corporativa e não tiver sido sincronizado com o Kaspersky Security Center há muito tempo.

Não é possível definir um agendamento para excluir dados nas propriedades da tarefa. Você só pode excluir dados imediatamente após iniciar a tarefa manualmente ou configurar a exclusão de dados com atraso se não houver conexão com o Kaspersky Security Center.

Limitações

A Limpeza de dados tem as seguintes limitações:

- Somente um administrador do Kaspersky Security Center pode gerenciar a tarefa de *Limpar dados*. Você não pode configurar ou iniciar uma tarefa na interface local do Kaspersky Endpoint Security.

- Para o sistema de arquivos NTFS, o Kaspersky Endpoint Security exclui apenas os nomes dos principais fluxos de dados. Nomes de fluxo de dados alternativos não podem ser excluídos.

- Quando você exclui um arquivo de link simbólico, o Kaspersky Endpoint Security também exclui os arquivos cujos caminhos são especificados no link simbólico.

Criando uma tarefa de limpeza de dados

Para excluir dados nos computadores dos usuários:

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Limpar dados**.

c. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Limpar dados (antirroubo)*.

d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Vá para a próxima etapa.

> Se novos computadores forem adicionados a um grupo de administração dentro do escopo da tarefa, a tarefa de exclusão imediata de dados será executada nos novos computadores apenas se a tarefa for concluída dentro de 5 minutos após a adição dos novos computadores.

5. Conclua o assistente.

   Uma nova tarefa será exibida na lista de tarefas.

6. Clique na tarefa **Limpar dados** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

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

8. Selecione o método de exclusão de dados:

   - **Remover através do sistema operacional**. O Kaspersky Endpoint Security usa os recursos do sistema operacional para excluir arquivos sem enviá-los para a lixeira.

   - **Remover completamente, nenhuma recuperação é possível**. O Kaspersky Endpoint Security substitui arquivos várias vezes com dados aleatórios. É praticamente impossível restaurar dados depois de excluídos.

9. Caso queira adiar a exclusão de dados, marque a caixa de seleção **Limpa os dados automaticamente quando não há conexão com o Kaspersky Security Center por mais de N dias**. Defina o número de dias.

   > A tarefa de exclusão de dados adiada será executada toda vez que uma conexão com o Kaspersky Security Center estiver ausente pelo período definido.

   Ao configurar a exclusão de dados adiada, lembre-se de que os funcionários podem ter horários de trabalho diferentes. Considere também o cronograma de trabalho dos usuários off-line. Para obter mais detalhes sobre como trabalhar com computadores offline e usuários ausentes, consulte a Ajuda do Kaspersky Security Center.

   > Se o computador estiver desligado e a conexão não puder ser feita durante o período que tiver sido definido, o Kaspersky Endpoint Security não excluirá os dados imediatamente após o computador ser ligado. O aplicativo aguardará a sincronização com o Kaspersky Security Center por uma hora. Isso é necessário para impedir a exclusão não autorizada de dados em computadores que tiverem sido desligados por usuários que entraram em férias, por exemplo.

   Se a caixa de seleção estiver desmarcada, a tarefa será executada imediatamente após a sincronização com o Kaspersky Security Center.

10. Gerar uma lista de objetos para excluir:

    - **Pasta**. O Kaspersky Endpoint Security exclui todos os arquivos da pasta e suas subpastas. O Kaspersky Endpoint Security não oferece suporte à máscaras e variáveis de ambiente para a inserção de um caminho de pasta.

    - **Arquivos por extensão**. O Kaspersky Endpoint Security procura arquivos com as extensões especificadas em todas as unidades do computador, inclusive nas unidades removíveis. Use o caractere "`;`" ou "`,`" para especificar várias extensões.

    - **Escopo predefinido**. O Kaspersky Endpoint Security excluirá arquivos das seguintes áreas:

        - **Documentos**. Arquivos na pasta *Documentos* padrão do sistema operacional e suas subpastas.

        - **Cookies**. Arquivos nos quais o navegador salva dados dos sites visitados pelo usuário (como dados de autorização do usuário).

        - **Área de trabalho**. Arquivos na pasta da *Área de trabalho* padrão do sistema operacional e suas subpastas.

        - **Arquivos temporários do Internet Explorer**. Arquivos temporários relacionados ao funcionamento do Internet Explorer, como cópias de páginas da web, imagens e arquivos de mídia.

        - **Arquivos temporários**. Arquivos temporários relacionados ao funcionamento de aplicativos instalados no computador. Por exemplo, os aplicativos do Microsoft Office criam arquivos temporários que contêm cópias de backup dos documentos.

        - **Arquivos do Outlook**. Arquivos relacionados ao funcionamento do cliente de e-mail do Outlook: arquivos de dados (PST), arquivos de dados off-line (OST), arquivos de catálogo de endereços off-line (OAB) e arquivos de catálogo de endereços pessoal (PAB).

        - **Perfil de usuário**. Conjunto de arquivos e pastas que armazenam configurações do sistema operacional para a conta de usuário local.

    Você pode criar uma lista de objetos para excluir em cada guia. O Kaspersky Endpoint Security criará uma lista consolidada e apagará arquivos desta lista quando uma tarefa for concluída.

    > Você não pode excluir arquivos necessários para a operação do Kaspersky Endpoint Security.

11. Salvar alterações.

12. Marque a caixa de seleção ao lado da tarefa.

13. Clique **Iniciar**.

    Como resultado, os dados nos computadores dos usuários serão excluídos de acordo com o modo selecionado: imediato ou quando não houver conexão. Se o Kaspersky Endpoint Security não puder excluir um arquivo, por exemplo, quando um usuário estiver usando um arquivo, ele não tentará excluí-lo novamente. Para concluir a exclusão de dados, execute a tarefa novamente.

Controle do computador

Controle da Web

O Controle da Web gerencia o acesso dos usuários aos recursos da Web. Isso ajuda a reduzir o tráfego e o uso inadequado do tempo de trabalho. Quando um usuário tenta abrir um site proibido pelo Controle da Web, o Kaspersky Endpoint Security bloqueará o acesso e exibirá um aviso (veja a figura abaixo).

Para usar o Controle da Web, você deve concluir a configuração inicial do aplicativo:

- Para o monitoramento de tráfego HTTPS, ative a verificação de conexões criptografadas (ativada por padrão).
- Selecione as portas que o Kaspersky Endpoint Security deve monitorar (por padrão, o aplicativo monitora todas as portas).
- Selecione os aplicativos cujo tráfego você deseja que o Kaspersky Endpoint Security monitore. A maioria dos navegadores já está presente na lista de aplicativos recomendados pela Kaspersky. Se o seu navegador não estiver na lista, adicione-o manualmente.
- Recomendamos injetar um script de interação de página da web no tráfego da Web (por padrão, a injeção de script está desabilitada). Esse script permite o registro de eventos do Controle da Web para o log de eventos do aplicativo, log de eventos do sistema operacional e relatórios.

Métodos de gerenciamento de acesso à sites

O Controle da Web permite que você configure o acesso à sites usando os seguintes métodos:

- **Categoria do site**. Os sites são categorizados de acordo com o serviço de nuvem Kaspersky Security Network, análise heurística e o banco de dados de sites conhecidos (incluídos nos bancos de dados de aplicativos). Por exemplo, é possível restringir o acesso do usuário à categoria *Redes sociais* ou a outras categorias.
- **Tipo de dados**. É possível restringir o acesso dos usuários aos dados de um site e ocultar imagens, por exemplo. O Kaspersky Endpoint Security determina o tipo de dados com base no formato do arquivo e não na sua extensão.

  O Kaspersky Endpoint Security não verifica arquivos dentro de arquivos. Por exemplo, se os arquivos de imagem foram colocados em um arquivo, o Kaspersky Endpoint Security identifica o tipo de dados *Arquivos compactados* e não como *Gráficos*.

- **Endereço individual**. Você pode inserir um endereço web ou usar máscaras.

Você pode usar simultaneamente vários métodos para regular o acesso à sites. Por exemplo, é possível restringir o acesso ao tipo de dado dos *Arquivos dos aplicativos do Office* apenas para a categoria de site *E-mail baseado na Web*.

Regras de acesso de site

O Controle da Web gerencia o acesso do usuário a sites usando *regras de acesso*. Você pode definir as seguintes configurações avançadas para uma regra de acesso à site:

- Usuários aos quais se aplica a regra.

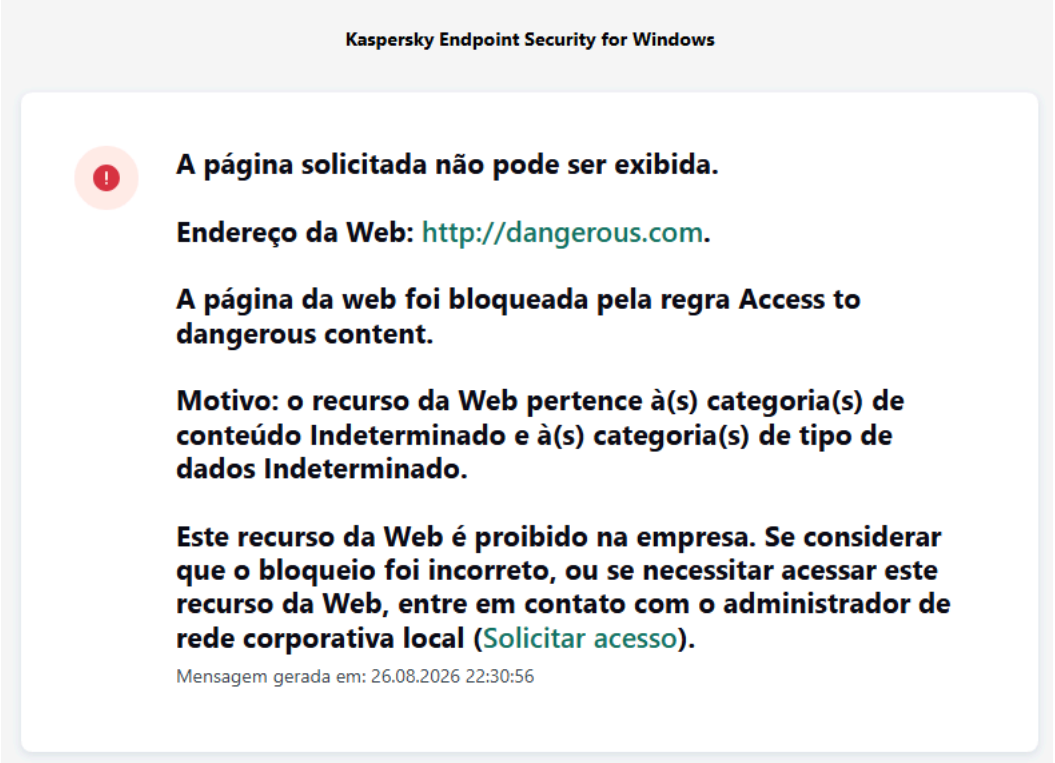
  Por exemplo, é possível restringir o acesso à Internet através de um navegador para todos os usuários da empresa, exceto os do departamento de TI.

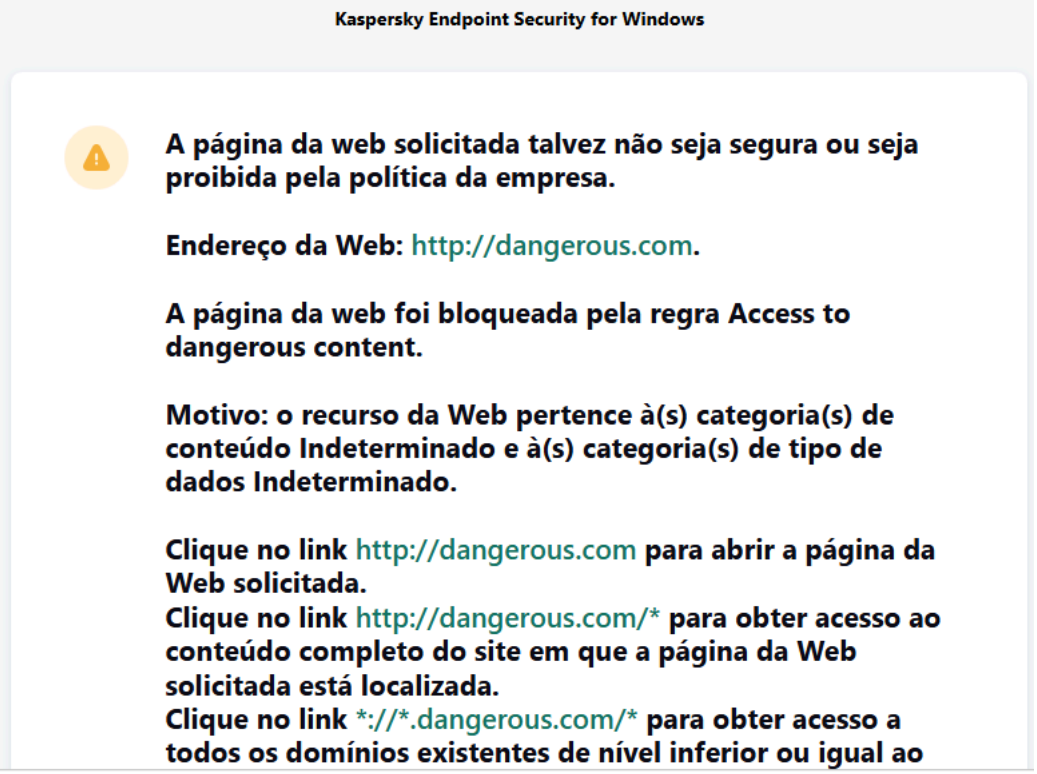
- Agendamento da regra.

  Por exemplo, é possível restringir o acesso à Internet por meio de um navegador apenas durante o horário de trabalho.

Prioridades da regra de acesso

Cada regra tem uma prioridade. Quanto mais alta uma regra estiver na lista, mais alta será sua prioridade. Se um site foi adicionado a várias regras, o Controle da Web regula o acesso ao site com base na regra com a maior prioridade. Por exemplo, o Kaspersky Endpoint Security pode identificar um portal corporativo como uma rede social. Para restringir o acesso às redes sociais e dar acesso ao portal corporativo, crie duas regras: uma regra de bloqueio para a categoria *Redes sociais* e uma regra de permissão para o portal corporativo. A regra de acesso ao portal web corporativo deve ter uma prioridade maior do que a regra de acesso para redes sociais.





Mensagens de Controle da Web

Adicionar uma regra de acesso a recursos da web

Uma *regra de acesso a recursos da Web* é um conjunto de filtros e ações aplicados pelo Kaspersky Endpoint Security quando os usuários visitam recursos da Web. As regras de acesso podem incluir agendamento de regra.

Não se recomenda criar mais de 1000 regras de acesso a recursos da Web, uma vez que isso pode tornar o sistema instável.

A regra de acesso de recurso da Web é um conjunto de filtros e ações que o Kaspersky Endpoint Security executa quando o usuário visita os recursos da Web descritos na regra durante o período indicado no agendamento da regra. Os filtros permitem especificar de forma precisa um grupo de recursos da Web cujo acesso é controlado pelo componente de Controle da Web.

Os seguintes filtros estão disponíveis:

- **Filtro por conteúdo**. O Controle da Web categoriza recursos da Web por conteúdo e tipo de dados. Você pode controlar o acesso dos usuários aos recursos da Web, com conteúdo e dados dentro dos tipos definidos por essas categorias. Quando usuários visitam recursos da Web que pertencem à categoria de conteúdo selecionada e/ou de tipo de dados, o Kaspersky Endpoint Security executa a ação especificada na regra.

- **Filtro por endereços de recurso da Web**. Você pode controlar o acesso do usuário a todos os endereços de recurso da Web ou a endereços de recurso da Web individuais e a endereços de /ou grupos de endereços de recurso da Web.

  Ao especificar o filtro por conteúdo e por endereços de recurso da Web, e os endereços de recurso da Web e/ou grupos de endereços de recurso da Web especificados pertencem às categorias de conteúdo ou tipo de dados selecionadas, o Kaspersky Endpoint Security não controla o acesso de todos os recursos da Web nas categorias de conteúdo e/ou tipos de dados selecionadas. Em vez disso, o aplicativo controla o acesso somente dos endereços de recurso da Web e/ou grupos de endereços de recurso da Web especificados.

- **Filtrar por nomes de usuários e grupo de usuários**. Você pode especificar os nomes de usuários e / ou grupos de usuários com acesso a recursos da Web controlados segundo a regra.

- **Agendamento da regra**. É possível especificar a regra de agendamento. O agendamento da regra determina o período de tempo durante o qual o Kaspersky Endpoint Security monitora o acesso de recursos da Web abrangidos pela regra.

Após o Kaspersky Endpoint Security ser instalado, a lista de regras do componente de Controle da Web não fica vazia. A *Regra padrão* é predefinida. Essa regra é aplicada a qualquer recurso da Web que não é coberto por outras regras, e permite ou bloqueia o acesso a esses recursos da Web para todos os usuários.

Cada regra tem uma prioridade. Quanto mais alta uma regra estiver na lista, mais alta será sua prioridade. Se um site foi adicionado a várias regras, o Controle da Web regula o acesso ao site com base na regra com a maior prioridade. Por exemplo, o Kaspersky Endpoint Security pode identificar um portal corporativo como uma rede social. Para restringir o acesso às redes sociais e dar acesso ao portal corporativo, crie duas regras: uma regra de bloqueio para a categoria *Redes sociais* e uma regra de permissão para o portal corporativo. A regra de acesso ao portal web corporativo deve ter uma prioridade maior do que a regra de acesso para redes sociais.

Como adicionar uma regra de acesso a recursos da Web no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Controles de Segurança** → **Controle da Web**.

4. Marque a caixa de seleção **Controle da Web**.

5. No bloco **Configurações do controle da web**, clique no botão **Adicionar**.

   A janela **Regra de acesso a recursos da Web** é aberta.

6. Configure a regra de acesso a recursos da Web (consulte a tabela abaixo).

7. Se quiser que o Controle da Web encerre a conexão com o recurso da Web proibido imediatamente após a aplicação da política, marque a caixa de seleção **Encerrar as sessões de navegador ativas após a aplicação da regra**.

   > O Controle da Web permite a desconexão imediata de recursos da Web somente em navegadores da Web. Para outros aplicativos, o Controle da Web apenas restringe novas conexões.

   Caso a caixa de seleção esteja desmarcada, o Controle da Web restringirá somente as novas conexões aos recursos da Web proibidos. O Controle da Web não encerra conexões ativas.

8. Salvar alterações.

Como adicionar uma regra de acesso a recursos da Web no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Controle da Web**.

5. Ative o botão de alternância **Controle da Web ATIVADO**.

6. No bloco **Lista de regras**, clique no botão **Adicionar**.

7. Configure a regra de acesso a recursos da Web (consulte a tabela abaixo).

8. Se quiser que o Controle da Web encerre a conexão com o recurso da Web proibido imediatamente após a aplicação da política, marque a caixa de seleção **Encerrar as sessões de navegador ativas após a aplicação da regra**.

   O Controle da Web permite a desconexão imediata de recursos da Web somente em navegadores da Web. Para outros aplicativos, o Controle da Web apenas restringe novas conexões.

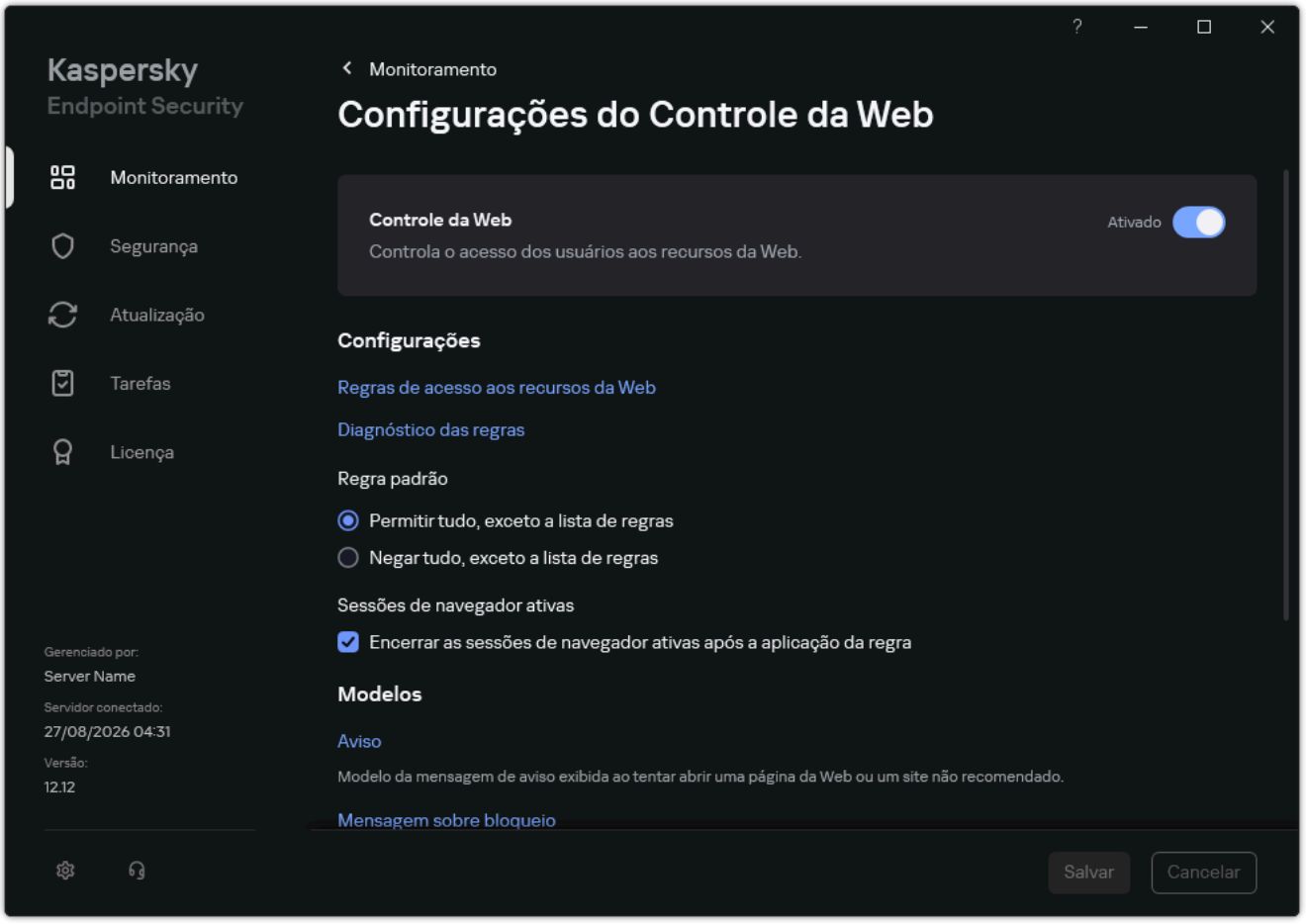
   Caso a caixa de seleção esteja desmarcada, o Controle da Web restringirá somente as novas conexões aos recursos da Web proibidos. O Controle da Web não encerra conexões ativas.

9. Salvar alterações.

Como adicionar uma regra de acesso aos recursos na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle da Web**.



Configurações do Controle da Web

3. Ative o botão de alternância **Controle da Web**.

4. No bloco **Configurações**, clique no botão **Regras de acesso aos recursos da Web**.

5. Na janela que é aberta, clique no botão **Adicionar**.

   A janela **Regra de acesso a recursos da Web** é aberta.

6. Configure a regra de acesso a recursos da Web (consulte a tabela abaixo).

7. Se quiser que o Controle da Web encerre a conexão com o recurso da Web proibido imediatamente após a aplicação da política, marque a caixa de seleção **Encerrar as sessões de navegador ativas após a aplicação da regra**.

   O Controle da Web permite a desconexão imediata de recursos da Web somente em navegadores da Web. Para outros aplicativos, o Controle da Web apenas restringe novas conexões.

   Caso a caixa de seleção esteja desmarcada, o Controle da Web restringirá somente as novas conexões aos recursos da Web proibidos. O Controle da Web não encerra conexões ativas.

8. Salvar alterações.

Como resultado, a nova regra de Controle da Web é adicionada à lista. Caso necessário, altere a prioridade da regra de Controle da Web. Também é possível usar o botão de alternância para desativar a regra de acesso a recursos da Web a qualquer momento sem ter que removê-la da lista.

Parâmetros da regra de Controle da Web

Parâmetro	Descrição
Nome da regra	Nome da regra de Controle da Web.
Estado	• **Ativado**. • **Desativado**. É possível usar o botão de alternância para desativar a regra de acesso a recursos da Web a qualquer momento.
Ação	• **Permitir**. O Controle da Web permite o acesso aos recursos da Web que correspondem aos parâmetros da regra. • **Bloquear**. O Controle da Web bloqueia o acesso aos recurso da Web que correspondem aos parâmetros da regra e exibe uma mensagem de acesso negado ao site. • **Avisar**. Quando o usuário tenta obter acesso a um recurso da Web que corresponde à regra, o Controle da Web exibe um aviso informando que não é aconselhável visitá-lo. O usuário consegue obter o acesso ao recurso da Web desejado ao usar os links da mensagem de aviso.
Conteúdo do filtro	• **Por categorias de conteúdo**. É possível controlar o acesso do usuário aos recursos da Web por categoria (por exemplo, a categoria *Redes sociais*). • **Por tipos de dados**. Você pode controlar o acesso do usuário a recursos da Web com base no tipo de dados específico dos dados publicados (por exemplo, *Gráficos*).
Endereços	• **Para todos os endereços**. O Controle da Web não filtrará recursos da Web por endereço. • **Para endereços individuais**. O Controle da Web filtrará apenas endereços de recursos da Web da lista. Você pode inserir um endereço web ou usar máscaras. Você também pode exportar uma lista de endereços de recursos da Web de um arquivo TXT. 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. Se a Verificação de Conexões Criptografadas for desativada para o protocolo HTTPS, você poderá filtrar apenas pelo nome do servidor.
Usuários	• **A todos os usuários**. O Controle da Web não filtrará recursos da Web para usuários específicos. • **Aplicar a usuários individuais e/ou grupos**. O Controle da Web filtrará recursos da Web apenas para usuários específicos. 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.
Agendamento de regra	O agendamento da regra determina o período de tempo durante o qual o Kaspersky Endpoint Security monitora o acesso de recursos da Web abrangidos pela regra. Por exemplo, é possível restringir o acesso à Internet por meio de um navegador apenas durante o horário de trabalho.

Filtrar por endereços de recursos da Web

Para controlar o acesso a recursos da Web individuais, é necessário criar uma regra de Controle da Web, uma lista de endereços da Web e selecionar uma ação no Controle da Web. Durante a criação de uma lista de endereço da Web, é possível inserir endereços URL ou usar máscaras.

As regras podem incluir um agendamento de regra e uma lista de usuários aos quais a regra se aplica. Por exemplo, é possível restringir o acesso a sites apenas durante o horário de trabalho ou permitir a visita a sites para usuários de certos grupos.

Como ativar a filtragem de endereços de recursos da Web no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Controles de Segurança** → **Controle da Web**.
4. Marque a caixa de seleção **Controle da Web**.
5. No bloco **Configurações do controle da web**, clique no botão **Adicionar**.
   A janela **Regra de acesso a recursos da Web** é aberta.
6. Configure a regra de acesso a recursos da Web:
   a. No campo **Nome**, insira ou edite o nome da regra.
   b. Na lista suspensa **Aplicar aos endereços**, selecione **Para endereços individuais**.
   c. Crie uma lista de endereços de recursos da Web. Você pode inserir um endereço web ou usar máscaras. Você também pode exportar uma lista de endereços de recursos da Web de um arquivo TXT.

      Se a Verificação de Conexões Criptografadas for desativada para o protocolo HTTPS, você poderá filtrar apenas pelo nome do servidor.

   d. Na lista suspensa **Aplicar aos usuários**, selecione a filtragem pertinente para os usuários:
      - **A todos os usuários**. O Controle da Web não filtrará recursos da Web por endereço.
      - **A usuários individuais ou grupos**. O Controle da Web filtrará apenas endereços de recursos da Web da lista. Você pode inserir um endereço web ou usar máscaras. Você também pode exportar uma lista de endereços de recursos da Web de um arquivo TXT. 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.

e. Na lista suspensa **Ação**, selecione uma opção:

- **Permitir**. O Controle da Web permite o acesso aos recursos da Web que correspondem aos parâmetros da regra.
- **Bloquear**. O Controle da Web bloqueia o acesso aos recurso da Web que correspondem aos parâmetros da regra e exibe uma mensagem de acesso negado ao site.
- **Avisar**. Quando o usuário tenta obter acesso a um recurso da Web que corresponde à regra, o Controle da Web exibe um aviso informando que não é aconselhável visitá-lo. O usuário consegue obter o acesso ao recurso da Web desejado ao usar os links da mensagem de aviso.

f. Na lista suspensa **Agendamento de regra**, selecione um agendamento ou crie um novo agendamento.

7. Se quiser que o Controle da Web encerre a conexão com o recurso da Web proibido imediatamente após a aplicação da política, marque a caixa de seleção **Encerrar as sessões de navegador ativas após a aplicação da regra**.

   O Controle da Web permite a desconexão imediata de recursos da Web somente em navegadores da Web. Para outros aplicativos, o Controle da Web apenas restringe novas conexões.

   Caso a caixa de seleção esteja desmarcada, o Controle da Web restringirá somente as novas conexões aos recursos da Web proibidos. O Controle da Web não encerra conexões ativas.

8. Salvar alterações.

Como ativar a filtragem de endereços de recursos da Web no Web Console e no Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Controles de segurança** → **Controle da Web**.
5. Ative o botão de alternância **Controle da Web ATIVADO**.
6. No bloco **Lista de regras**, clique no botão **Adicionar**.
7. Configure a regra de acesso a recursos da Web:

   a. No campo **Nome da regra**, insira ou edite o nome da regra.

   b. Selecione o status **Ativado** para a regra de acesso aos recursos da Web.

   É possível usar o botão de alternância para desativar a regra de acesso a recursos da Web a qualquer momento sem ter que removê-la da lista.

c. No bloco **Ação**, selecione a opção pertinente:

- **Permitir**. O Controle da Web permite o acesso aos recursos da Web que correspondem aos parâmetros da regra.
- **Bloquear**. O Controle da Web bloqueia o acesso aos recurso da Web que correspondem aos parâmetros da regra e exibe uma mensagem de acesso negado ao site.
- **Informar**. Quando o usuário tenta obter acesso a um recurso da Web que corresponde à regra, o Controle da Web exibe um aviso informando que não é aconselhável visitá-lo. O usuário consegue obter o acesso ao recurso da Web desejado ao usar os links da mensagem de aviso.

d. Em **Escopo**, selecione **Sites individuais**.

e. Configure o filtro de conteúdo:

- **Endereço individual**. Crie uma lista de endereços de recursos da Web. Você pode inserir um endereço web ou usar máscaras. Você também pode exportar uma lista de endereços de recursos da Web de um arquivo TXT.

  Se a Verificação de Conexões Criptografadas for desativada para o protocolo HTTPS, você poderá filtrar apenas pelo nome do servidor.

- **Tipo de dados**. Você pode controlar o acesso do usuário a recursos da Web com base no tipo de dados específico dos dados publicados (por exemplo, *Gráficos*).

f. Em **Usuário ou grupo**, selecione os usuários aos quais você deseja que o Controle da Web aplique a regra.

O Controle da Web filtrará apenas endereços de recursos da Web da lista. Você pode inserir um endereço web ou usar máscaras. Você também pode exportar uma lista de endereços de recursos da Web de um arquivo TXT. 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.

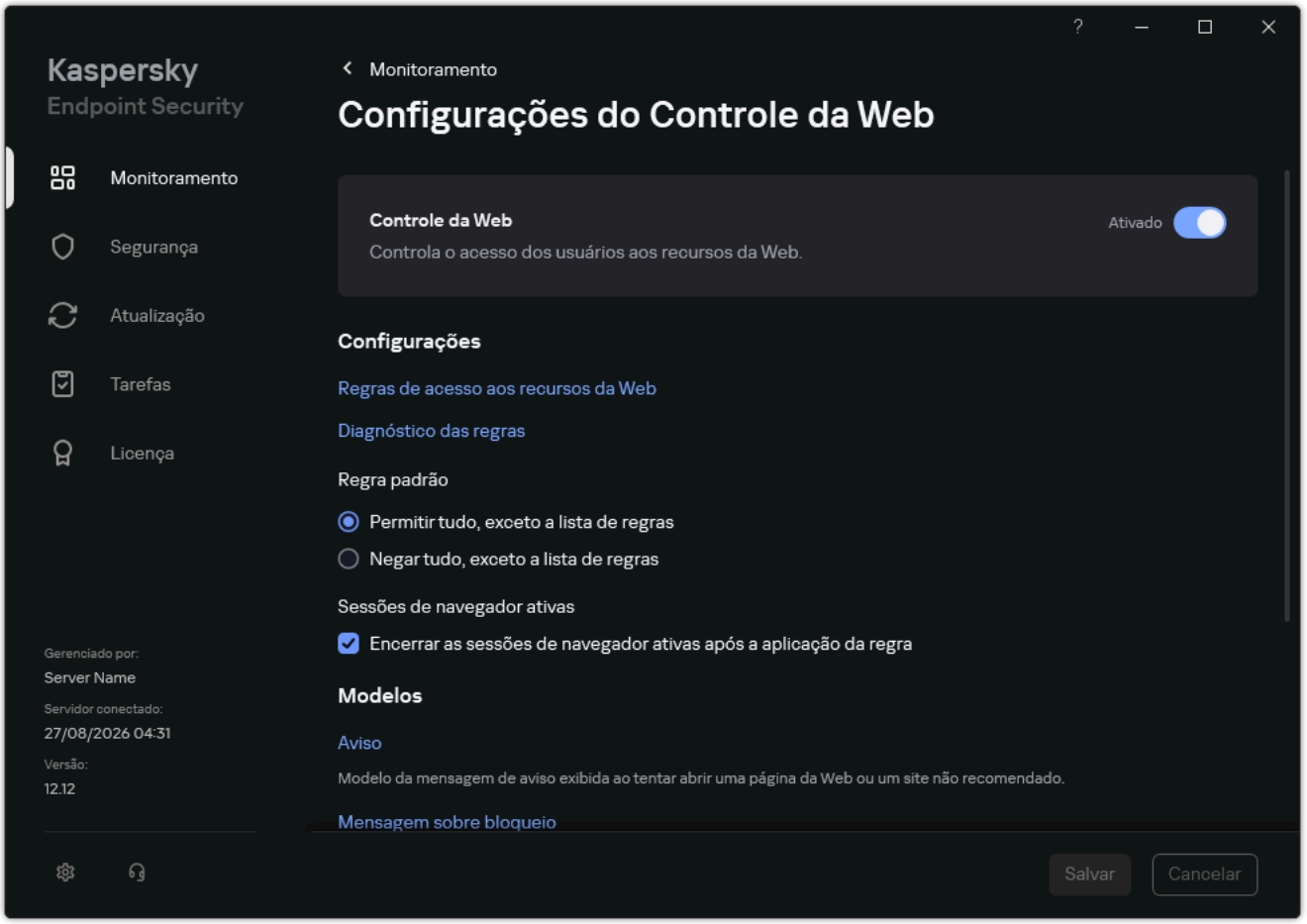
g. No bloco **Agendamento do acesso**, selecione um agendamento ou crie um novo agendamento.

8. Salvar alterações.

Como ativar a filtragem de endereço do recurso da Web na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle da Web**.



Configurações do Controle da Web

3. No bloco **Configurações**, clique no botão **Regras de acesso aos recursos da Web**.

4. Na janela que é aberta, clique no botão **Adicionar**.

   A janela **Regra de acesso a recursos da Web** é aberta.

5. No campo **Nome da regra**, insira ou edite o nome da regra.

6. Selecione o status **Ativado** para a regra de acesso aos recursos da Web.

   É possível usar o botão de alternância para desativar a regra de acesso a recursos da Web a qualquer momento.

7. No bloco **Ação**, selecione a opção pertinente:

   - **Permitir**. O Controle da Web permite o acesso aos recursos da Web que correspondem aos parâmetros da regra.

   - **Bloquear**. O Controle da Web bloqueia o acesso aos recurso da Web que correspondem aos parâmetros da regra e exibe uma mensagem de acesso negado ao site.

   - **Avisar**. Quando o usuário tenta obter acesso a um recurso da Web que corresponde à regra, o Controle da Web exibe um aviso informando que não é aconselhável visitá-lo. O usuário consegue obter o acesso ao recurso da Web desejado ao usar os links da mensagem de aviso.

8. Em **Endereços**, selecione **Para endereços individuais**.

   Crie uma lista de endereços de recursos da Web. Você pode inserir um endereço web ou usar máscaras. Você também pode exportar uma lista de endereços de recursos da Web de um arquivo TXT.

   > Se a Verificação de Conexões Criptografadas for desativada para o protocolo HTTPS, você poderá filtrar apenas pelo nome do servidor.

9. Na seção **Usuários**, selecione o filtro relevante para usuários:

   - **A todos os usuários**. O Controle da Web não filtrará recursos da Web para usuários específicos.
   - **Aplicar a usuários individuais e/ou grupos**. O Controle da Web filtrará apenas endereços de recursos da Web da lista. Você pode inserir um endereço web ou usar máscaras. Você também pode exportar uma lista de endereços de recursos da Web de um arquivo TXT. 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.

10. Na lista suspensa **Agendamento de regra**, selecione um agendamento ou crie um novo agendamento.

11. Se quiser que o Controle da Web encerre a conexão com o recurso da Web proibido imediatamente após a aplicação da política, marque a caixa de seleção **Encerrar as sessões de navegador ativas após a aplicação da regra**.

    > O Controle da Web permite a desconexão imediata de recursos da Web somente em navegadores da Web. Para outros aplicativos, o Controle da Web apenas restringe novas conexões.

    Caso a caixa de seleção esteja desmarcada, o Controle da Web restringirá somente as novas conexões aos recursos da Web proibidos. O Controle da Web não encerra conexões ativas.

12. Salvar alterações.

Como resultado, a nova regra de Controle da Web é adicionada à lista. Caso necessário, altere a prioridade da regra de Controle da Web. Também é possível usar o botão de alternância para desativar a regra de acesso a recursos da Web a qualquer momento sem ter que removê-la da lista.

Filtrar por conteúdo do recurso da Web

Para controlar o acesso por conteúdo do recurso da Web, o Controle da Web fornece um filtro de categoria e um filtro de tipo de dados.

Os sites são categorizados de acordo com o serviço de nuvem Kaspersky Security Network, análise heurística e o banco de dados de sites conhecidos (incluídos nos bancos de dados de aplicativos). Por exemplo, é possível restringir o acesso do usuário à categoria *Redes sociais* ou a outras categorias.

É possível restringir o acesso do usuário a um site de acordo com o tipo de dados, por exemplo, para ocultar imagens. O Kaspersky Endpoint Security determina o tipo de dados com base no formato do arquivo e não na sua extensão. O Controle da Web distingue os seguintes tipos de dados:

- Vídeo
- Áudio
- Arquivos dos aplicativos do Office
- Arquivos executáveis
- Arquivos compactados
- Gráficos
- Scripts

O Kaspersky Endpoint Security não verifica arquivos dentro de arquivos. Por exemplo, se os arquivos de imagem foram colocados em um arquivo, o Kaspersky Endpoint Security identifica o tipo de dados *Arquivos compactados* e não como *Gráficos*.

As regras podem incluir um agendamento de regra e uma lista de usuários aos quais a regra se aplica. Por exemplo, é possível restringir o acesso a sites apenas durante o horário de trabalho ou permitir a visita a sites para usuários de certos grupos.

Como ativar a filtragem de conteúdo do recurso da Web no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Controles de Segurança** → **Controle da Web**.
4. Marque a caixa de seleção **Controle da Web**.
5. No bloco **Configurações do controle da web**, clique no botão **Adicionar**.

   A janela **Regra de acesso a recursos da Web** é aberta.
6. Configure a regra de acesso a recursos da Web:

   a. No campo **Nome**, insira ou edite o nome da regra.

   b. Na lista suspensa **Filtrar conteúdo**, selecione a filtragem de conteúdo pertinente:

   - **Por categorias de conteúdo**. É possível controlar o acesso do usuário aos recursos da Web por categoria (por exemplo, a categoria *Redes sociais*).
   - **Por tipos de dados**. Você pode controlar o acesso do usuário a recursos da Web com base no tipo de dados específico dos dados publicados (por exemplo, *Gráficos*).
   - **Por categorias de conteúdo e tipos de dados**. A filtragem por categorias de conteúdo e tipos de dados está ativada.

Após selecionar os filtros, configure os parâmetros de filtragem.

c. Na lista suspensa **Aplicar aos usuários**, selecione a filtragem pertinente para os usuários:

- **A todos os usuários**. O Controle da Web não filtrará recursos da Web por endereço.
- **A usuários individuais ou grupos**. O Controle da Web filtrará apenas endereços de recursos da Web da lista. Você pode inserir um endereço web ou usar máscaras. Você também pode exportar uma lista de endereços de recursos da Web de um arquivo TXT. 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. Na lista suspensa **Ação**, selecione uma opção:

- **Permitir**. O Controle da Web permite o acesso aos recursos da Web que correspondem aos parâmetros da regra.
- **Bloquear**. O Controle da Web bloqueia o acesso aos recurso da Web que correspondem aos parâmetros da regra e exibe uma mensagem de acesso negado ao site.
- **Avisar**. Quando o usuário tenta obter acesso a um recurso da Web que corresponde à regra, o Controle da Web exibe um aviso informando que não é aconselhável visitá-lo. O usuário consegue obter o acesso ao recurso da Web desejado ao usar os links da mensagem de aviso.

e. Na lista suspensa **Agendamento de regra**, selecione um agendamento ou crie um novo agendamento.

7. Se quiser que o Controle da Web encerre a conexão com o recurso da Web proibido imediatamente após a aplicação da política, marque a caixa de seleção **Encerrar as sessões de navegador ativas após a aplicação da regra**.

   O Controle da Web permite a desconexão imediata de recursos da Web somente em navegadores da Web. Para outros aplicativos, o Controle da Web apenas restringe novas conexões.

   Caso a caixa de seleção esteja desmarcada, o Controle da Web restringirá somente as novas conexões aos recursos da Web proibidos. O Controle da Web não encerra conexões ativas.

8. Salvar alterações.

Como ativar a filtragem de conteúdo do recurso da Web no Web Console e no Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Controles de segurança** → **Controle da Web**.
5. Ative o botão de alternância **Controle da Web ATIVADO**.
6. No bloco **Lista de regras**, clique no botão **Adicionar**.

7. Configure a regra de acesso a recursos da Web:

   a. No campo **Nome da regra**, insira ou edite o nome da regra.

   b. Selecione o status **Ativado** para a regra de acesso aos recursos da Web.

      É possível usar o botão de alternância para desativar a regra de acesso a recursos da Web a qualquer momento.

   c. No bloco **Ação**, selecione a opção pertinente:

      - **Permitir**. O Controle da Web permite o acesso aos recursos da Web que correspondem aos parâmetros da regra.
      - **Bloquear**. O Controle da Web bloqueia o acesso aos recurso da Web que correspondem aos parâmetros da regra e exibe uma mensagem de acesso negado ao site.
      - **Informar**. Quando o usuário tenta obter acesso a um recurso da Web que corresponde à regra, o Controle da Web exibe um aviso informando que não é aconselhável visitá-lo. O usuário consegue obter o acesso ao recurso da Web desejado ao usar os links da mensagem de aviso.

   d. Em **Escopo**, selecione **Categoria de conteúdo**.

   e. Configure o filtro de conteúdo:

      - **Categoria de conteúdo**. É possível controlar o acesso do usuário aos recursos da Web por categoria (por exemplo, a categoria *Redes sociais*).
      - **Tipo de dados**. Você pode controlar o acesso do usuário a recursos da Web com base no tipo de dados específico dos dados publicados (por exemplo, *Gráficos*).

   f. Em **Usuário ou grupo**, selecione os usuários aos quais você deseja que o Controle da Web aplique a regra.

      O Controle da Web filtrará apenas endereços de recursos da Web da lista. Você pode inserir um endereço web ou usar máscaras. Você também pode exportar uma lista de endereços de recursos da Web de um arquivo TXT. 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.

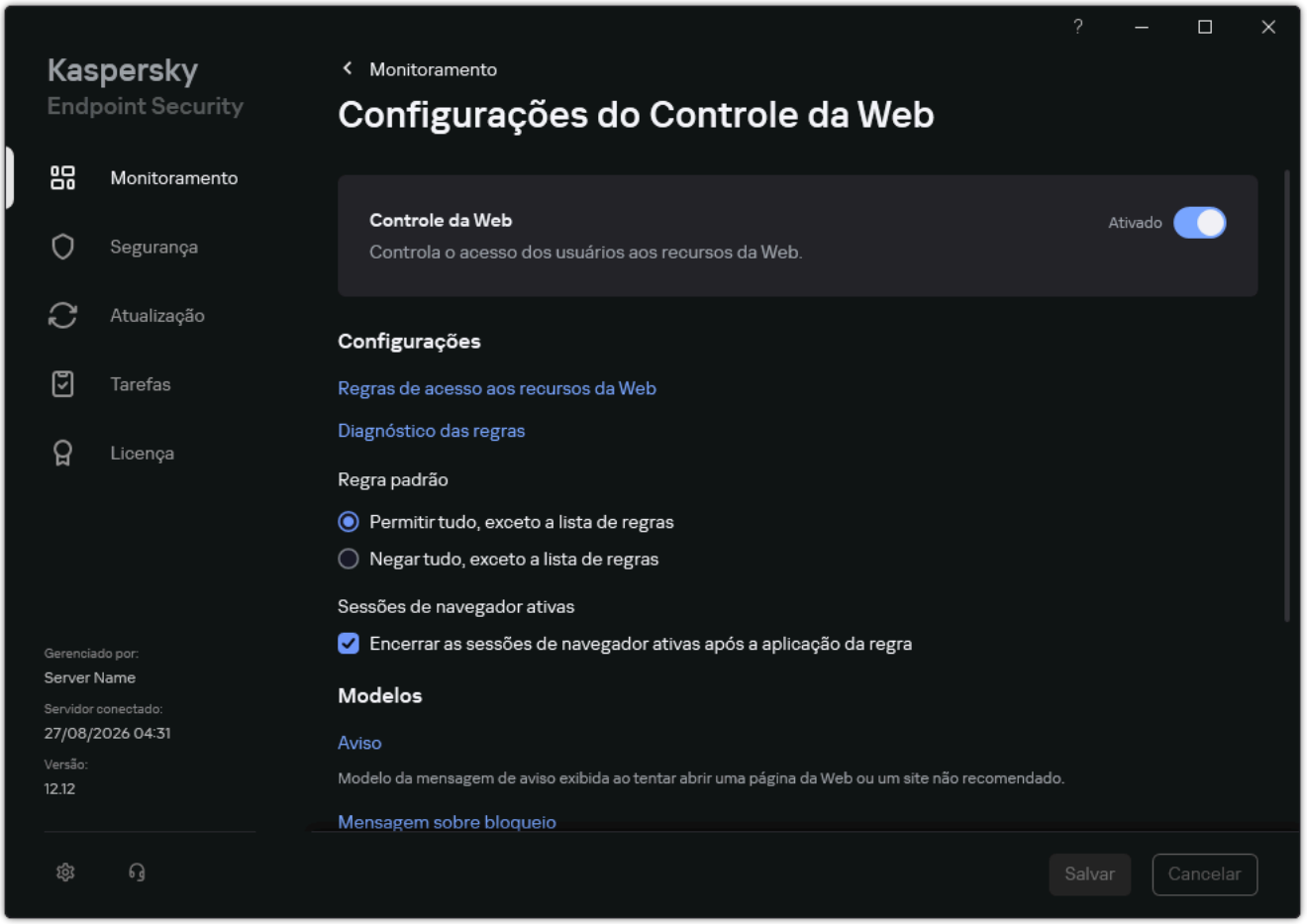
   g. No bloco **Agendamento do acesso**, selecione um agendamento ou crie um novo agendamento.

8. Salvar alterações.

Como ativar a filtragem de conteúdo do recurso da Web na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle da Web**.



Configurações do Controle da Web

3. No bloco **Configurações**, clique no botão **Regras de acesso aos recursos da Web**.

4. Na janela que é aberta, clique no botão **Adicionar**.

   A janela **Regra de acesso a recursos da Web** é aberta.

5. No campo **Nome da regra**, insira ou edite o nome da regra.

6. Selecione o status **Ativado** para a regra de acesso aos recursos da Web.

   É possível usar o botão de alternância para desativar a regra de acesso a recursos da Web a qualquer momento.

7. No bloco **Ação**, selecione a opção pertinente:

   - **Permitir**. O Controle da Web permite o acesso aos recursos da Web que correspondem aos parâmetros da regra.

   - **Bloquear**. O Controle da Web bloqueia o acesso aos recurso da Web que correspondem aos parâmetros da regra e exibe uma mensagem de acesso negado ao site.

   - **Avisar**. Quando o usuário tenta obter acesso a um recurso da Web que corresponde à regra, o Controle da Web exibe um aviso informando que não é aconselhável visitá-lo. O usuário consegue obter o acesso ao recurso da Web desejado ao usar os links da mensagem de aviso.

8. No bloco **Conteúdo do filtro**, selecione o filtro de conteúdo relevante:

   - **Por categorias de conteúdo**. É possível controlar o acesso do usuário aos recursos da Web por categoria (por exemplo, a categoria *Redes sociais*).

   - **Por tipos de dados**. Você pode controlar o acesso do usuário a recursos da Web com base no tipo de dados específico dos dados publicados (por exemplo, *Gráficos*).

   Para configurar o filtro de conteúdo:

   a. Clique no link **Configurações**.

   b. Marque as caixas de seleção junto aos nomes das categorias de conteúdo necessárias e/ou de tipo de dados.

      Ao marcar as caixas de seleção junto aos nomes de uma categoria de conteúdo e/ou tipo de dados, o Kaspersky Endpoint Security aplica a regra para controlar o acesso a recursos da Web que pertencem às categorias de conteúdo e/ou tipos de dados selecionados.

   c. Retorne à janela para configurar a regra de acesso a recursos da Web.

9. Na seção **Usuários**, selecione o filtro relevante para usuários:

   - **A todos os usuários**. O Controle da Web não filtrará recursos da Web por endereço.

   - **Aplicar a usuários individuais e/ou grupos**. O Controle da Web filtrará apenas endereços de recursos da Web da lista. Você pode inserir um endereço web ou usar máscaras. Você também pode exportar uma lista de endereços de recursos da Web de um arquivo TXT. 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. Para criar uma lista de usuários aos quais deseja aplicar a regra:

     a. Clique **Adicionar**.

     b. Na janela que é aberta, selecione os usuários ou grupos de usuários aos quais deseja aplicar a regra de acesso a recursos da Web.

     c. Retorne à janela para configurar a regra de acesso a recursos da Web.

10. Na lista suspensa **Agendamento de regra**, selecione o nome do agendamento desejado ou crie um novo com base no agendamento da regra selecionada. Para fazer isso:

    a. Clique **Editar ou adicionar novo**.

    b. Na janela que é aberta, clique no botão **Adicionar**.

    c. Na janela que é aberta, insira o nome do agendamento da regra.

    d. Configure o agendamento de acesso a recursos da Web para usuários.

    e. Retorne à janela para configurar a regra de acesso a recursos da Web.

11. Se quiser que o Controle da Web encerre a conexão com o recurso da Web proibido imediatamente após a aplicação da política, marque a caixa de seleção **Encerrar as sessões de navegador ativas após a aplicação da regra**.

O Controle da Web permite a desconexão imediata de recursos da Web somente em navegadores da Web. Para outros aplicativos, o Controle da Web apenas restringe novas conexões.

Caso a caixa de seleção esteja desmarcada, o Controle da Web restringirá somente as novas conexões aos recursos da Web proibidos. O Controle da Web não encerra conexões ativas.

12. Salvar alterações.

Como resultado, a nova regra de Controle da Web é adicionada à lista. Caso necessário, altere a prioridade da regra de Controle da Web. Também é possível usar o botão de alternância para desativar a regra de acesso a recursos da Web a qualquer momento sem ter que removê-la da lista.

Testar as regras de acesso de recurso da Web

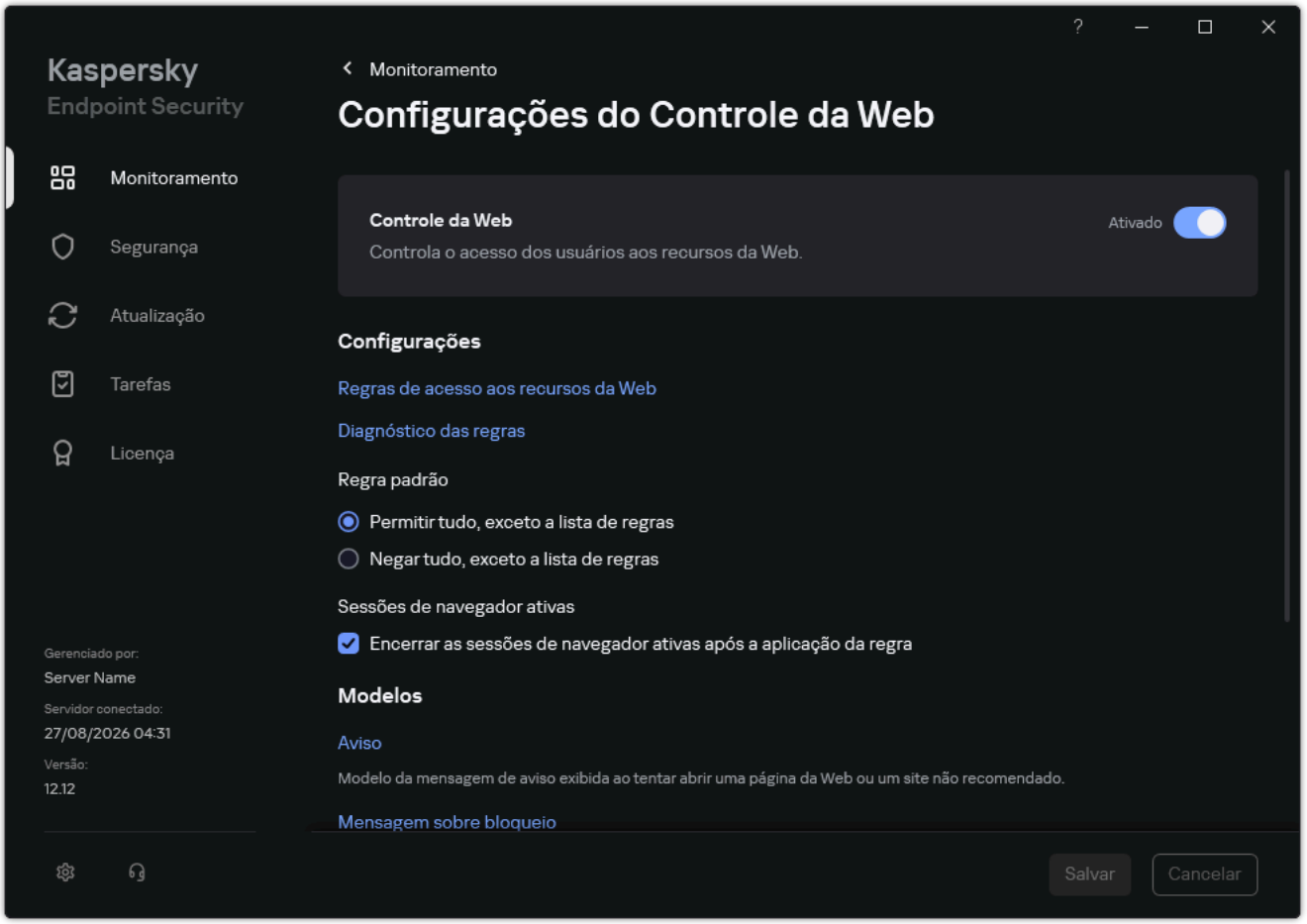
Ao configurar o controle da Web, o acesso a recursos da Web que os usuários precisam para trabalhar pode ser inadvertidamente bloqueado. Para descobrir que regra de Controle da Web está bloqueando o acesso aos recursos da Web, é possível usar a ferramenta de *diagnóstico das regras de Controle da Web*. O diagnóstico das regras de Controle da Web está disponível apenas na interface do Kaspersky Endpoint Security. No console do Kaspersky Security Center, não é possível descobrir qual regra do Controle da Web inclui um dado recurso.

Se o usuário considerar que o recurso da Web foi bloqueado por engano, ele pode clicar no link na mensagem de notificação de bloqueio de recurso da Web para enviar uma mensagem pré-gerada ao administrador da rede corporativa local.

Para testar as regras de acesso a recursos da Web:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle da Web**.



Configurações do Controle da Web

3. No bloco **Configurações**, clique no link **Diagnóstico das regras**.

   A janela **Diagnóstico das regras** é aberta.

4. Se deseja testar as regras que o Kaspersky Endpoint Security usa para controlar o acesso a um recurso específico da Web, selecione a caixa de seleção **Especificar endereço**. Digite o endereço do recurso da Web no campo abaixo.

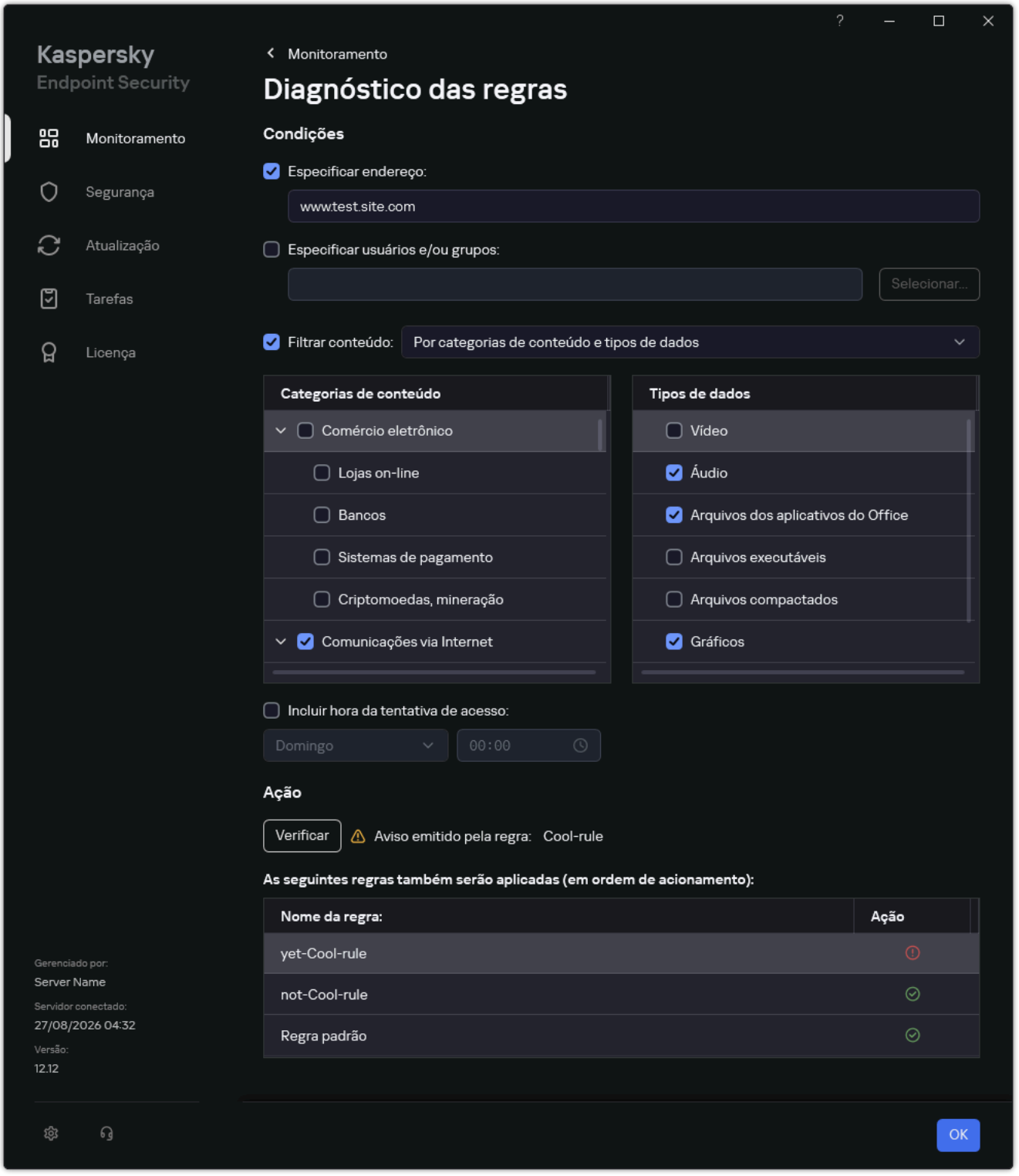
5. Se desejar testar as regras usadas pelo Kaspersky Endpoint Security para controlar o acesso a recursos da Web por usuários e/ou grupos de usuários especificados, especifique a lista de usuários e/ou grupos de usuários.

6. Caso deseje testar as regras usadas pelo Kaspersky Endpoint Security para controlar o acesso a recursos da web de certas categorias de conteúdo e/ou as categorias de tipo de dados, selecione **Filtrar conteúdo** e escolha a opção desejada na lista suspensa (**Por categorias de conteúdo**, **Por tipos de dados** ou **Por categorias de conteúdo e tipos de dados**).

7. Se desejar testar as regras incluindo a hora e dia da semana em que a tentativa é feita para acessar o(s) recurso(s) da Web especificado(s) nas condições de diagnóstico das regras, marque a caixa de seleção **Incluir hora da tentativa de acesso**. Especifique o dia da semana e a hora.

8. Clique **Verificar**.

A conclusão do teste é seguida de uma mensagem informando a ação realizada pelo Kaspersky Endpoint Security de acordo com a primeira regra acionada na tentativa de acessar o recurso da web especificado (permitir, bloquear ou aviso). A primeira regra acionada é aquela que tem prioridade na lista de regras do Controle da Web que são aplicadas segundo as condições de diagnóstico. A mensagem é exibida à direita do botão **Verificar**. A tabela a seguir lista as regras acionadas existentes, especificando a ação do Kaspersky Endpoint Security. As regras são listadas em ordem decrescente de prioridade.



Resultado do teste de acesso do Recurso da Web

Exportar e importar regras de Controle da Web

É possível exportar a lista de regras do Controle da Web para um arquivo JSON ou XML. Em seguida, você pode modificar o arquivo para, por exemplo, adicionar um grande número de endereços do mesmo tipo. É possível usar a função de exportação/importação para fazer backup da lista de regras de Controle da Web ou para migrar a lista para um servidor diferente.

Como exportar e importar uma lista de regras do Controle da Web no console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Controles de Segurança** → **Controle da Web**.
4. Para exportar a lista de regras do Controle da Web:
   a. Selecione as regras que deseja exportar. Para selecionar várias portas, use as teclas **CTRL** ou **SHIFT**.
      Se você não selecionou nenhuma regra, o Kaspersky Endpoint Security exportará todas as regras.
   b. Clique no link **Exportar**.
   c. 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.
   d. Salvar o arquivo.
      O Kaspersky Endpoint Security exporta toda a lista de regras para o arquivo XML.
5. Para importar a lista de regras do Controle da Web:
   a. Clique no link **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 Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.
6. Salvar alterações.

Como exportar e importar uma lista de regras do Controle da Web no Web Console e Cloud Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Controles de segurança** → **Controle da Web**.

5. Para exportar a lista de regras, na seção **Lista de regras**:

   a. Selecione as regras que deseja exportar.

   b. Clique no botão → **Exportar**.

      O Kaspersky Endpoint Security exporta a lista de regras para um arquivo JSON na pasta de downloads padrão.

6. Para importar a lista de regras, na seção **Lista de regras**:

   a. Clique no botão → **Importar**.

      Na janela exibida, selecione o arquivo JSON do qual deseja importar a lista de regras.

   b. Abra o arquivo.

      Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo JSON.

7. Salvar alterações.

Exportar e importar endereços de recursos da Web da regra de Controle da Web

Se tiver criado uma lista de endereços de recurso da Web em uma regra de acesso de recurso da Web, é possível exportá-la para um arquivo:

- No formato TXT no Console de Administração (MMC)
- No formato JSON no Web Console
- No formato CSV na interface do aplicativo

A seguir, será possível importar a lista deste arquivo para evitar ter de criar uma nova lista de endereços de recurso da Web manualmente ao configurar uma regra de acesso. A opção de exportar e importar a lista de endereços de recurso da Web é útil se, por exemplo, você criar regras de acesso com parâmetros semelhantes.

Também é possível exportar/importar todas as regras de Controle da Web e não apenas os endereços de recursos da Web de uma única regra.

Como exportar/importar endereços de recursos da Web da regra do Controle da Web no Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Controles de Segurança** → **Controle da Web**.

5. No bloco **Configurações do controle da web**, selecione a regra cuja lista de endereços de recursos da Web deseja exportar ou importar.

   As propriedades da regra de Controle da Web são exibidas.

6. Para exportar a lista de recursos da Web, faça o seguinte na lista de endereços:

   a. Selecione os endereços que deseja exportar.

      Se você não selecionou nenhum endereço, o Kaspersky Endpoint Security exportará todos os endereços.

   b. Clique no botão .

   c. Na janela que é aberta, insira o nome do arquivo TXT para o qual deseja exportar a lista de endereços de recursos da Web e selecione a pasta na qual deseja salvar esse arquivo.

   d. Salvar o arquivo.

      O Kaspersky Endpoint Security exporta a lista de endereços de recursos da web para um arquivo TXT.

7. Para importar a lista de recursos da web, faça o seguinte na lista de endereços:

   a. Clique no botão .

      Na janela exibida, selecione o arquivo TXT do qual deseja importar a lista de recursos da Web.

   b. Abra o arquivo.

      Se o computador já tiver uma lista de endereços, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo TXT.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como exportar / importar endereços de recursos da Web da regra do Controle da Web no Web Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Controle da Web**.

5. No bloco **Lista de regras**, selecione a regra cuja lista de endereços de recursos da Web deseja exportar ou importar.

   As propriedades da regra de Controle da Web são exibidas.

6. No bloco **Escopo** → **Sites individuais**, clique no botão **Editar**.

7. Para exportar a lista de recursos da Web, faça o seguinte na lista de endereços:

   a. Selecione os endereços que deseja exportar.

   b. Clique no botão → **Exportar**.

      O Kaspersky Endpoint Security exporta a lista de endereços de recursos da Web para um arquivo JSON na pasta de downloads padrão.

8. Para importar a lista de recursos da web, faça o seguinte na lista de endereços:

   a. Clique no botão → **Importar**.

      Na janela que é aberta, selecione o arquivo JSON do qual deseja importar a lista de endereços de recursos da Web.

   b. Abra o arquivo.

      Se o computador já tiver uma lista de endereços, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo JSON.

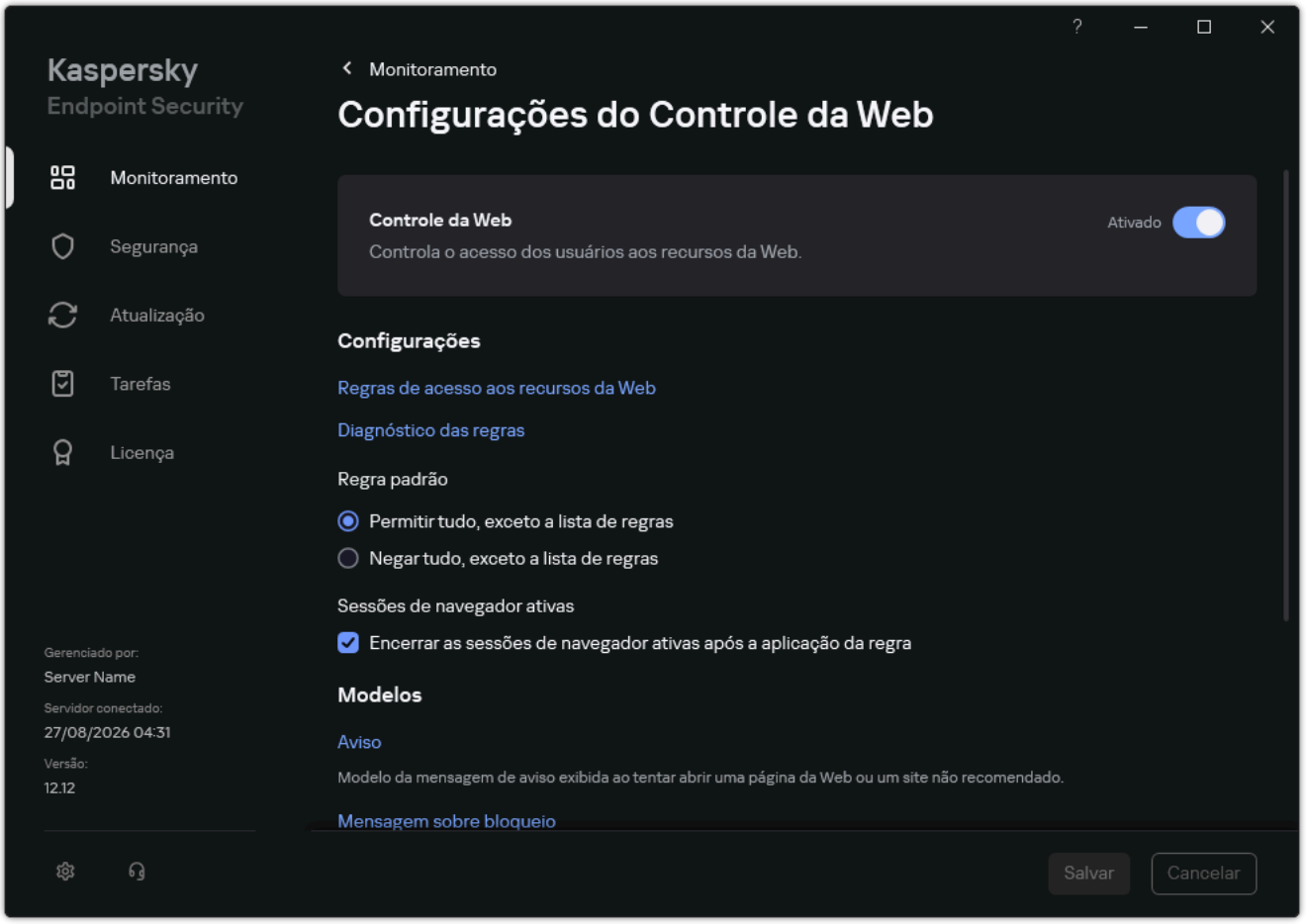
   Você pode exportar e importar grupos de sites da mesma forma.

9. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como exportar / importar endereços de recursos da Web da regra do Controle da Web na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle da Web**.



Configurações do Controle da Web

3. No bloco **Configurações**, clique no botão **Regras de acesso aos recursos da Web**.

4. Selecione a regra cuja lista de endereços de recurso da Web deseja exportar ou importar.

5. Para exportar a lista de Endereços da Web confiáveis, faça o seguinte, na seção **Endereços**:

   a. Selecione os endereços que deseja exportar.

      Se você não selecionou nenhum endereço, o Kaspersky Endpoint Security exportará todos os endereços.

   b. Clique **Exportar**.

   c. Na janela que é aberta, insira o nome do arquivo CSV para o qual deseja exportar a lista de endereços de recursos da Web e selecione a pasta na qual deseja salvar esse arquivo.

   d. Salvar o arquivo.

      O Kaspersky Endpoint Security exporta a lista de endereços de recursos da web para um arquivo CSV.

6. Para importar a lista de recursos da web, faça o seguinte, na seção **Endereços**:

   a. Clique **Importar**.

      Na janela exibida, selecione o arquivo CSV do qual deseja importar a lista de recursos da Web.

   b. Abra o arquivo.

      Se o computador já tiver uma lista de endereços, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo CSV.

7. Salvar alterações.

Monitoramento da atividade do usuário na Internet

O Kaspersky Endpoint Security permite que você registre dados em visitas a todos os sites, incluindo sites permitidos. Isso permite que você obtenha o histórico completo das visualizações do navegador. O Kaspersky Endpoint Security envia eventos de atividades do usuário para o Kaspersky Security Center, para o log local do Kaspersky Endpoint Security e para o log de eventos do Windows. Para receber eventos no Kaspersky Security Center, é necessário definir as configurações de eventos em uma política no Console de administração ou no Web Console. Você também pode configurar a transmissão de eventos de Controle da Web por e-mail e a exibição de notificações na tela no computador do usuário.

Navegadores compatíveis com a função de monitoramento: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. O monitoramento da atividade do usuário não funciona em outros navegadores.

O Kaspersky Endpoint Security cria os seguintes eventos de atividade do usuário na Internet:

- Bloquear o site (status *Crítico*).
- Abrir um site não recomendado (status *Advertência*).
- Visita a um site permitido (status *Informações*).

Antes de habilitar o monitoramento da atividade do usuário na Internet, você deve fazer o seguinte:

- Injete um script de interação de página da Web no tráfego da Web (consulte as instruções abaixo). O script permite o registro de eventos do Controle da Web.
- Para o monitoramento de tráfego HTTPS, você precisa ativar a verificação de conexões criptografadas.

Injetar um script de interação de página da Web

Como injetar um script de interação de página da Web, no tráfego da Web, pelo Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Configurações de rede**.
4. No bloco **Verificação de conexões criptografadas**, marque a caixa de seleção **Injetar script no tráfego da web para interagir com páginas da web**.
5. Salvar alterações.

Como injetar um script de interação de página da Web, no tráfego da Web, pelo Web Console e pelo Cloud Console

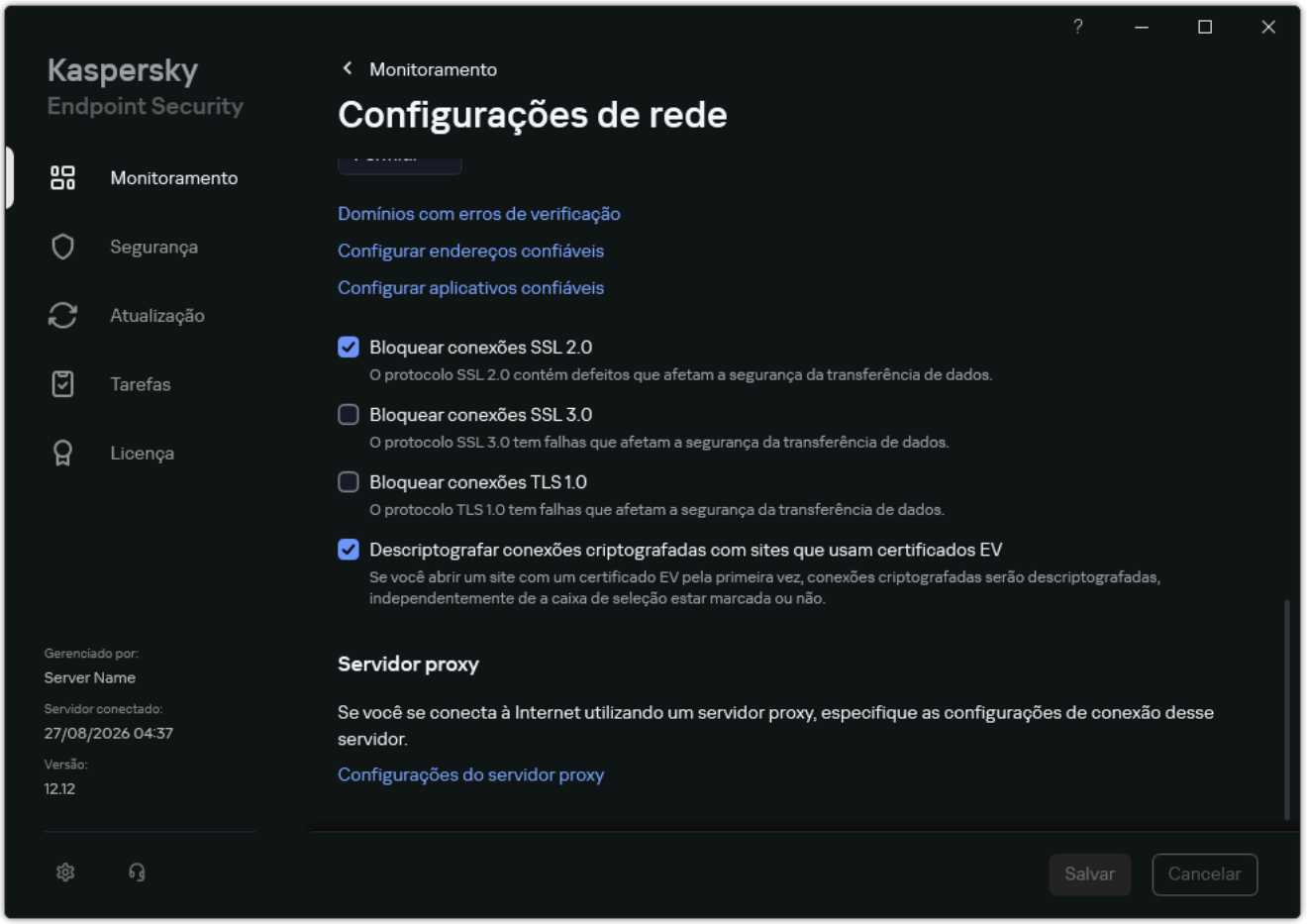
1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Na janela da política, selecione **Configurações gerais** → **Configurações de rede**.
5. Em **Monitoramento de conexões à Internet**, ative o botão de alternância **Monitoramento de conexões à Internet ATIVADO**.
6. Salvar alterações.

Como injetar um script de interação de página da Web, no tráfego da Web, pela interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações de rede**.



Configurações de aplicativo rede

3. No bloco **Processamento de tráfego**, marque a caixa de seleção **Injetar script no tráfego da Web para interagir com páginas da Web**.

4. Salvar alterações.

Como resultado, o Kaspersky Endpoint Security injetará um script de interação de página da Web no tráfego da Web. Esse script permite o registro de eventos do Controle da Web para o log de eventos do aplicativo, log de eventos do sistema operacional e relatórios.

Configuração de criação de log de eventos de Controle da Web

Para configurar o registro de eventos do Controle da Web no computador do usuário:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Interface**.

3. No bloco **Notificações**, clique no botão **Configurar notificações**.

4. Na janela exibida, selecione a seção **Controle da Web**.

   Isso abre a tabela de métodos de notificação e eventos do Controle da Web.

5. Configure o método de notificação para cada evento: **Salvar no relatório local** ou **Salvar no Log de eventos do Windows**.

   Para registrar eventos de visita a sites permitidos, você também precisa configurar o Controle da Web (consulte as instruções abaixo).

   Na tabela de eventos, você também pode ativar uma notificação na tela e uma notificação por e-mail. Para enviar notificações por e-mail, você precisa definir as configurações do servidor SMTP. Para obter mais informações sobre como enviar notificações por e-mail, consulte a Ajuda do Kaspersky Security Center.

6. Salvar alterações.

Como resultado, o Kaspersky Endpoint Security começa a registrar eventos da atividade do usuário na Internet.

O Controle da Web envia eventos de atividade do usuário ao Kaspersky Security Center da seguinte maneira:

- Se você estiver usando o Kaspersky Security Center, o Controle da Web envia eventos para todos os objetos que compõem a página da web. Por esse motivo, vários eventos podem ser criados quando uma página da Web é bloqueada. Por exemplo, ao bloquear a página da Web http://www.example.com, o Kaspersky Endpoint Security pode retransmitir eventos para os seguintes objetos: http://www.example.com, http://www.example.com/icon.ico, http://www.example.com/file.js, etc.

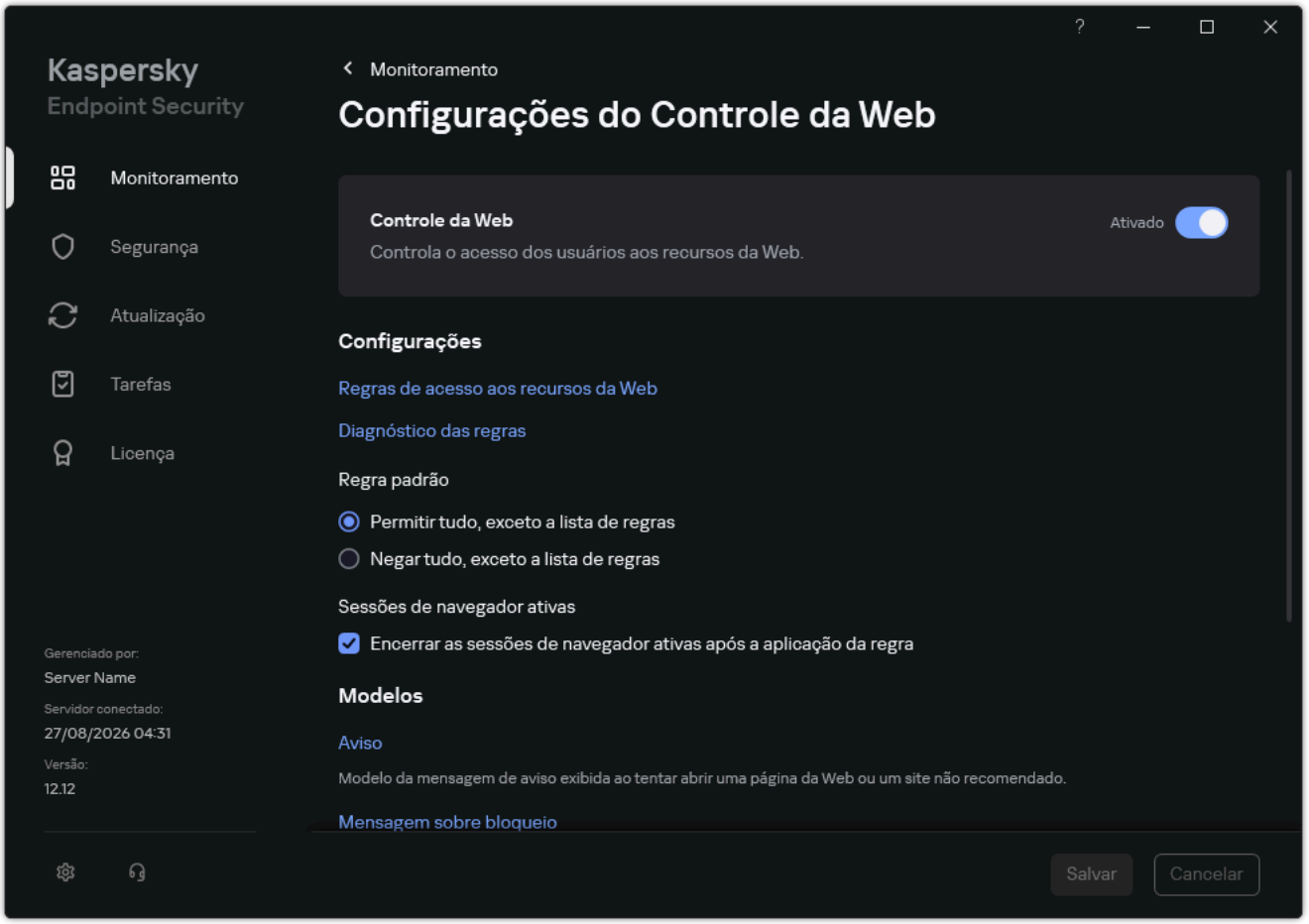
- Se você estiver usando o Kaspersky Security Center Cloud Console, o Controle da Web agrupa eventos e envia apenas o protocolo e o domínio do site. Por exemplo, se um usuário abrir os sites indesejáveis http://www.example.com/main, http://www.example.com/contact, http://www.example.com/gallery, o Kaspersky Endpoint Security enviará apenas um evento com o objeto http://www.example.com.

Eventos de criação de log ao visitar sites permitidos

Para habilitar a criação de logs de eventos ao visitar sites permitidos:

1. Na janela principal do aplicativo, clique no botão ⚙.

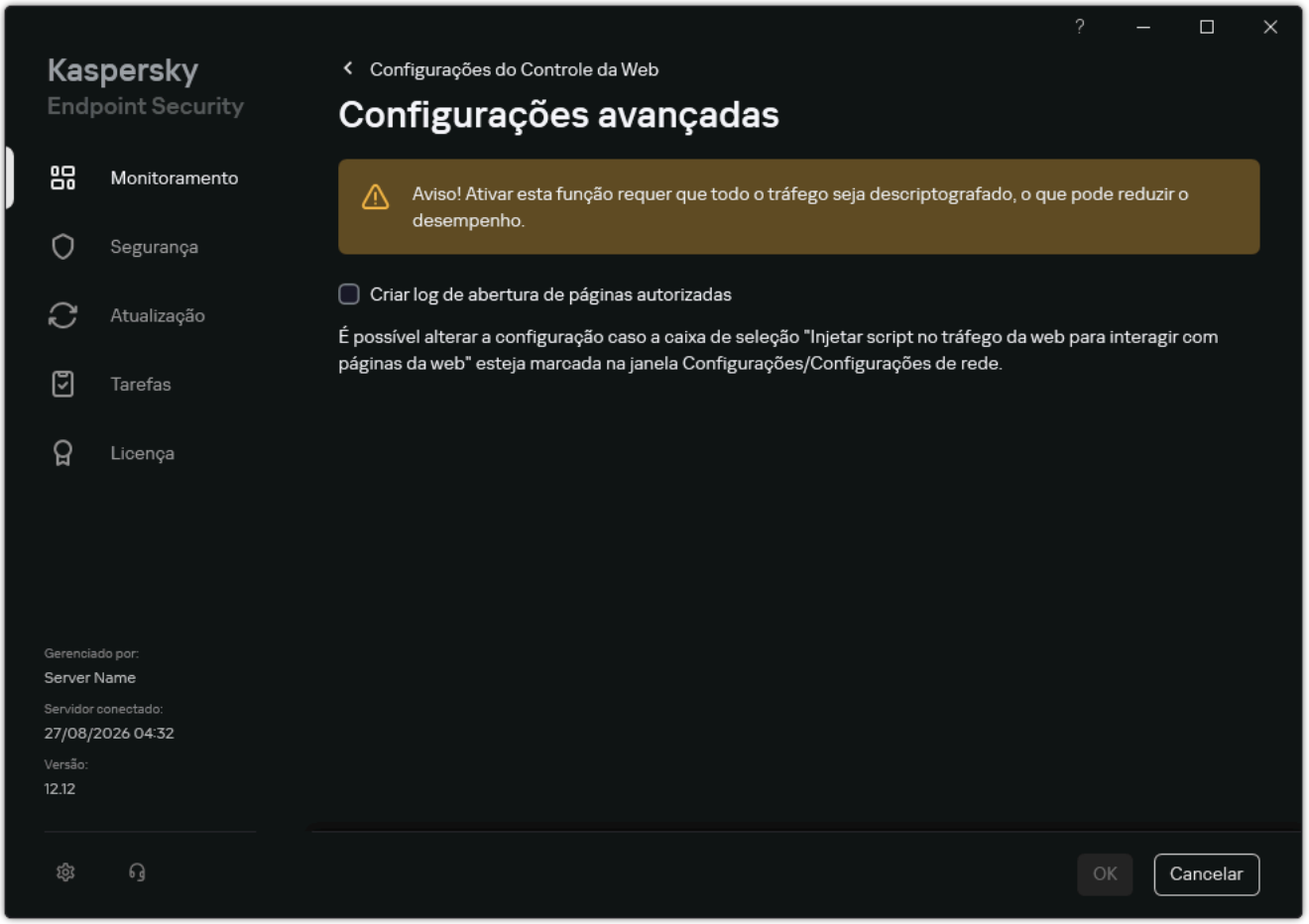
2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle da Web**.



Configurações do Controle da Web

3. No bloco **Adicional**, clique no botão **Configurações avançadas**.

4. Na janela que é aberta, marque a caixa de seleção **Criar log de abertura de páginas autorizadas**.



Configurações avançadas do Controle da Web

5. Salvar alterações.

Como resultado, você poderá visualizar o histórico completo do navegador.

Editar modelos de mensagens do Controle da Web

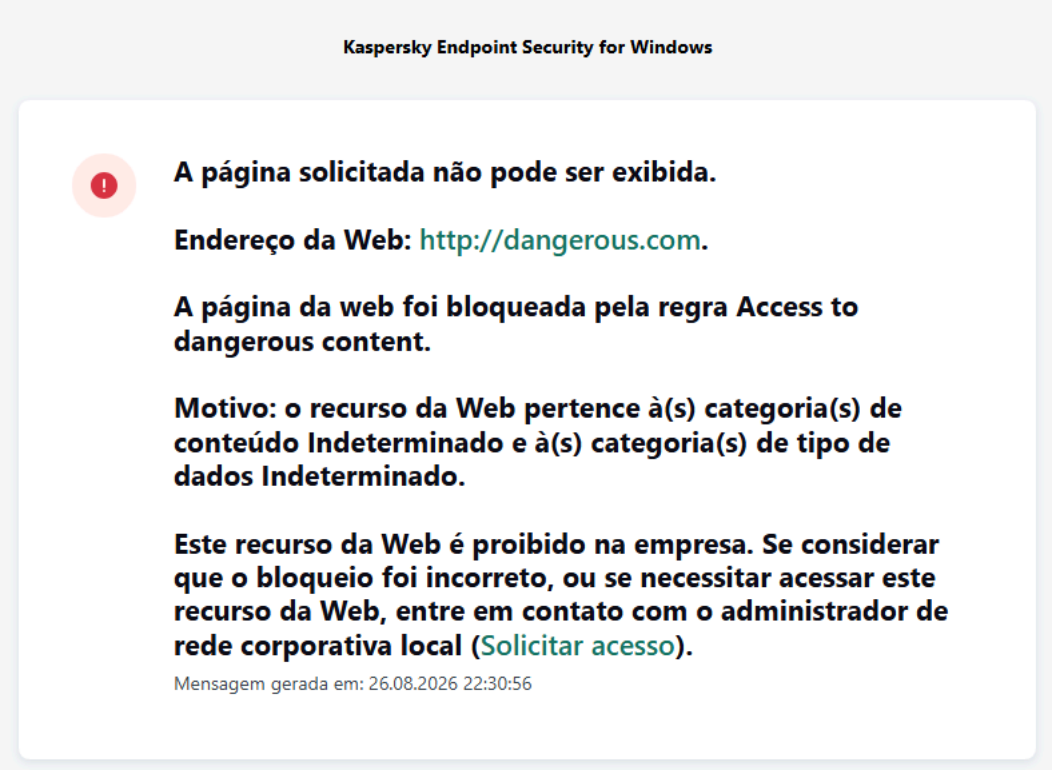
Dependendo do tipo de ação especificada nas propriedades das regras do Controle da Web, o Kaspersky Endpoint Security exibe uma das seguintes mensagens quando os usuários tentam acessar recursos da Internet (o aplicativo substitui a página HTML com a mensagem com a resposta do servidor HTTP):

- Mensagem de aviso. Esta mensagem avisa o usuário que visitar o recurso da Web não é recomendado e/ou viola a política de segurança corporativa. O Kaspersky Endpoint Security exibe uma mensagem de aviso se a opção **Avisar** for selecionada nas configurações da regra que descreve este recurso da Web.

  Se o usuário considerar que o aviso é um engano, ele pode clicar no link da mensagem de alerta para enviar uma mensagem pré-gerada ao administrador da rede corporativa local.

- Mensagem informando sobre o bloqueio de um recurso da Web. Caso a opção **Bloquear** seja selecionada nas configurações da regra que descrevem o recurso da Web, o Kaspersky Endpoint Security exibe uma mensagem de aviso informando que um recurso da Web foi bloqueado (ver figura abaixo).

Se o usuário considerar que o recurso da Web foi bloqueado por engano, ele pode clicar no link na mensagem de notificação de bloqueio de recurso da Web para enviar uma mensagem pré-gerada ao administrador da rede corporativa local.



Mensagem sobre o bloqueio de recurso da Web

São fornecidos modelos especiais para uma mensagem de aviso, a mensagem informando que um recurso da web está bloqueado e a mensagem a ser enviada ao administrador da rede local. Variáveis especiais são fornecidas para gerenciar o modelo de mensagem (por exemplo, `%USER_NAME%`). As variáveis permitem que um mesmo modelo de mensagem seja utilizado em diferentes computadores. Ao criar uma mensagem, o Kaspersky Endpoint Security obtém o valor da variável nas configurações do sistema operacional e o insere na mensagem referente ao computador, usuário e evento específicos.

Como alterar o modelo de mensagem do Controle da Web no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Controles de Segurança** → **Controle da Web**.

4. No bloco **Configurações de modelos de mensagem**, clique no botão **Modelos**.

5. Configure os modelos de mensagem do Controle da Web:

   - **Aviso**. O campo de entrada consiste em um modelo da mensagem que é exibida se uma regra para avisar sobre tentativas de acessar um recurso da Web não desejado for acionada.

   - **Mensagem sobre bloqueio**. O campo de entrada contém o modelo da mensagem que aparece se uma regra que bloqueia o acesso a um recurso da Web for acionada.

   - **Mensagem para o administrador**. O modelo da mensagem a ser enviada ao administrador de LAN caso o usuário considere que o bloqueio seja um erro. Depois que o usuário solicitar o acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio de acesso à página da Web para o administrador**. A descrição do evento contém uma mensagem ao administrador com variáveis substituídas. É possível visualizar esses eventos no console do Kaspersky Security Center com o uso da seleção de eventos predefinida **Pedidos de usuário**. Caso sua organização não tenha o Kaspersky Security Center implantado ou não haja conexão com o Servidor de Administração, o aplicativo enviará uma mensagem ao administrador para o endereço de e-mail especificado.

   Para inserir uma variável no modelo, posicione o cursor onde necessário, clique em **Variável** e selecione a opção necessária na lista.

   Você também pode restaurar o texto original do modelo clicando no botão **Por padrão**.

6. Salvar alterações.

Como alterar o modelo de mensagem do Controle da Web no Web Console e Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Controle da Web**.

5. No bloco **Modelos de mensagem**, clique no link **Mensagem sobre bloqueio de site** e configure os modelos para mensagens do Controle da Web:

   - **Aviso**. O campo de entrada consiste em um modelo da mensagem que é exibida se uma regra para avisar sobre tentativas de acessar um recurso da Web não desejado for acionada.

   - **Mensagem sobre bloqueio**. O campo de entrada contém o modelo da mensagem que aparece se uma regra que bloqueia o acesso a um recurso da Web for acionada.

   - **Mensagem para o administrador**. O modelo da mensagem a ser enviada ao administrador de LAN caso o usuário considere que o bloqueio seja um erro. Depois que o usuário solicitar o acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio de acesso à página da Web para o administrador**. A descrição do evento contém uma mensagem ao administrador com variáveis substituídas. É possível visualizar esses eventos no console do Kaspersky Security Center com o uso da seleção de eventos predefinida **Pedidos de usuário**. Caso sua organização não tenha o Kaspersky Security Center implantado ou não haja conexão com o Servidor de Administração, o aplicativo enviará uma mensagem ao administrador para o endereço de e-mail especificado.

   Para inserir uma variável no modelo, posicione o cursor onde necessário, clique em **Adicionar variável** e selecione a opção necessária na lista.

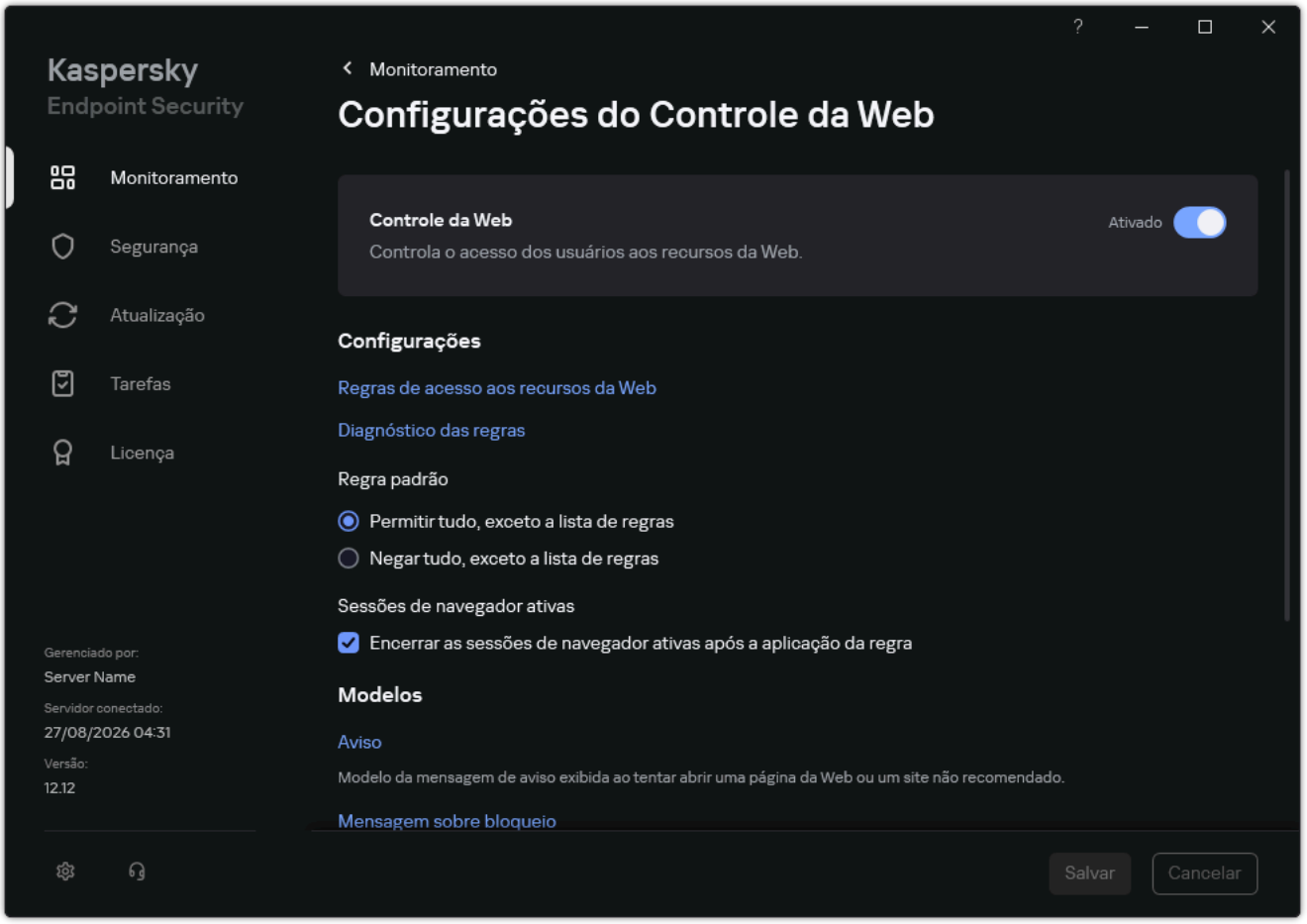
Você também pode restaurar o texto original do modelo clicando no botão **Redefinir para o padrão**.

6. Salvar alterações.

Como alterar o modelo de mensagem do Controle da Web na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle da Web**.



Configurações do Controle da Web

3. Na seção **Modelos**, configure os modelos de mensagens de Controle da Web:

- **Aviso**. O campo de entrada consiste em um modelo da mensagem que é exibida se uma regra para avisar sobre tentativas de acessar um recurso da Web não desejado for acionada.

- **Mensagem sobre bloqueio**. O campo de entrada contém o modelo da mensagem que aparece se uma regra que bloqueia o acesso a um recurso da Web for acionada.

- **Mensagem para o administrador**. O modelo da mensagem a ser enviada ao administrador de LAN caso o usuário considere que o bloqueio seja um erro. Depois que o usuário solicitar o acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio de acesso à página da Web para o administrador**. A descrição do evento contém uma mensagem ao administrador com variáveis substituídas. É possível visualizar esses eventos no console do Kaspersky Security Center com o uso da seleção de eventos predefinida **Pedidos de usuário**. Caso sua organização não tenha o Kaspersky Security Center implantado ou não haja conexão com o Servidor de Administração, o aplicativo enviará uma mensagem ao administrador para o endereço de e-mail especificado.

Para inserir uma variável no modelo, posicione o cursor onde necessário, clique em **Adicionar variável** e selecione a opção necessária na lista.

Você também pode restaurar o texto original do modelo clicando no botão **Reiniciar**.

4. Salvar alterações.

Editar máscaras de endereços de recurso da web

Usar uma *máscara de endereço de recurso da web* (também referida como "máscara de endereço") pode ser útil se precisar inserir vários endereços de recurso da web semelhantes ao criar uma regra de acesso de recurso da web. Se for algo bem planejado, uma máscara de endereço pode substituir um grande número de endereços de recurso da web.

Ao criar uma máscara de endereço, siga as seguintes regras:

1. O caractere `*` substitui qualquer sequência que contém caractere igual ou superior a zero.

   Por exemplo, se inserir a máscara de endereço `*abc*`, a regra de acesso é aplicada a todos os recursos da Web que contêm a sequência `abc`. Exemplo: `http://www.example.com/page_0-9abcdef.html`.

2. Uma sequência de caracteres `*.` (conhecida como *máscara de domínio*) permite selecionar todos os domínios de um endereço. A máscara de domínio `*.` Representa qualquer nome de domínio, subdomínio ou linha em branco.

   Exemplo: a máscara `*.example.com` representa os seguintes endereços:

   - `http://pictures.example.com`. A máscara de domínio `*.` representa `pictures.`.
   - `http://user.pictures.example.com`. A máscara de domínio `*.` representa `pictures.` e `user.`.
   - `http://example.com`. A máscara de domínio `*.` é interpretada como uma linha em branco.

3. A sequência de caracteres `www.` no início da máscara de endereço é interpretada como uma sequência `*.`.

   Exemplo: a máscara de endereço `*.example.com` é tratada como `www.example.com`. Essa máscara abrange os endereços `www2.example.com` e `www.pictures.example.com`.

4. Se uma máscara de endereço não começar com o caractere `*`, o conteúdo da máscara de endereço é equivalente ao mesmo conteúdo com o prefixo `*.`

5. Se uma máscara de endereço terminar com um caractere diferente de `/` ou `*`, o conteúdo da máscara de endereço é equivalente ao mesmo conteúdo com o sufixo `/*`.

   Exemplo: a máscara de endereço `http://www.example.com` abrange endereços como `http://www.example.com/abc`, onde `a`, `b` e `c` são quaisquer caracteres.

6. Se uma máscara de endereço terminar com o caractere `/`, o conteúdo da máscara de endereço é equivalente ao mesmo conteúdo com o sufixo `/*`.

7. A sequência de caracteres `/*` no final de uma máscara de endereço é interpretada como `/*` ou como vazia.

8. Endereços de recurso da web são verificados na máscara de endereço, considerando-se o protocolo (http ou https):

   - Se a máscara de endereço não contém nenhum protocolo de rede, esta abrange endereços com qualquer protocolo de rede.

     Exemplo: a máscara de endereço `example.com` abrange os endereços `http://` `example.com` e `https://` `example.com`.

- Se a máscara de endereço contém um protocolo de rede, esta abrange apenas endereços com o mesmo protocolo de rede da máscara de endereço.

  Exemplo: a máscara de endereço `http://*.example.com` abrange o endereço `http://www.example.com` mas não o `https://www.example.com`.

9. A máscara de endereço que está entre aspas duplas é tratada sem que sejam consideradas qualquer substituições adicionais, exceto quanto ao caractere `*` se este tiver sido incluído inicialmente na máscara de endereço. As regras 5 e 7 não se aplicam a máscaras de endereço colocadas entre aspas duplas (consulte os exemplos 14 - 18 na tabela abaixo).

10. O nome de usuário e a senha, porta de conexão, e distinção entre maiúsculas/minúsculas não são consideradas para fins de comparação com a máscara de endereço de um recurso da web.

Exemplos de como usar regras para criar máscaras de endereço

Número	Máscara de endereço	Endereço do recurso da web a verificar	O endereço é abrangido pelo endereço da máscara de endereço	Comentário
1	*.example.com	http://www.123example.com	Não	Consulte a regra 1.
2	*.example.com	http://www.123.example.com	Sim	Consulte a regra 2.
3	*example.com	http://www.123example.com	Sim	Consulte a regra 1.
4	*example.com	http://www.123.example.com	Sim	Consulte a regra 1.
5	http://www.*.example.com	http://www.123example.com	Não	Consulte a regra 1.
6	www.example.com	http://www.example.com	Sim	Consulte as regras 3, 2, 1.
7	www.example.com	https://www.example.com	Sim	Consulte as regras 3, 2, 1.
8	http://www.*.example.com	http://123.example.com	Sim	Consulte as regras 3, 4, 1.
9	www.example.com	http://www.example.com/abc	Sim	Consulte as regras 3, 5, 1.
10	example.com	http://www.example.com	Sim	Consulte as regras 3, 1.
11	http://example.com/	http://example.com/abc	Sim	Consulte a regra 6.
12	http://example.com/*	http://example.com	Sim	Consulte a regra 7.
13	http://example.com	https://example.com	Não	Consulte a regra 8.
14	"example.com"	http://www.example.com	Não	Consulte a regra 9.
15	"http://www.example.com"	http://www.example.com/abc	Não	Consulte a regra 9.
16	"*.example.com"	http://www.example.com	Sim	Consulte as regras 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Sim	Consulte as regras 1, 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Sim	Consulte as regras 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Não	A máscara de endereço contém mais informações além do endereço de um recurso da web.

Controle da Web para máquinas virtuais

O Controle da Web controla o tráfego no computador e também em uma máquina virtual implementada localmente no computador. Isso funciona sem a necessidade de instalar o aplicativo Kaspersky Endpoint Security na máquina virtual local. Isso significa que, se o usuário tentar abrir um site bloqueado por uma regra do Controle da Web em um navegador na *máquina virtual*, o aplicativo instalado no sistema operacional do *computador* host negará o acesso ao site.

O Controle da Web funciona de forma diferente em máquinas virtuais diferentes.

Oracle VM VirtualBox

O Kaspersky Endpoint Security é compatível com as regras de Controle da Web em máquinas virtuais Oracle VM VirtualBox sem limitações. O aplicativo pode controlar todo o tráfego da máquina virtual. Se um filtro por usuário estiver configurado nas regras de Controle da Web, o aplicativo funcionará corretamente porque todos os processos das máquinas virtuais serão iniciados pelo usuário local.

Estação de trabalho VMware

O Kaspersky Endpoint Security é compatível com as regras de Controle da Web em máquinas virtuais VMware Workstation, porém há limitações. O aplicativo não é compatível com regras com filtro por usuário configurado. Os processos da máquina virtual estão sendo executados com o usuário do sistema (SYSTEM). Isso torna impossível a identificação do usuário que está tentando abrir o site na máquina virtual.

Microsoft Hyper V

O Kaspersky Endpoint Security não é compatível com regras de Controle da Web em máquinas virtuais Microsoft Hyper-V.

Variáveis nos modelos de mensagem do Controle da Web

É possível usar as seguintes variáveis em modelos de mensagem do usuário ou modelos de mensagem do administrador:

- **Nome de usuário** – `%USER_NAME%`.

  Nome da conta de usuário atual no computador no qual a mensagem foi gerada, no formato `<device name>\<user alias>` (por exemplo, `DESKTOP-123\John.Smith`).

- **Endereço do recurso da Web** – `%CANONIC_REQUEST_URL%`.

  Endereço do recurso da Web bloqueado.

- **Nome da regra** – `%RULE%`.

  Nome da regra que bloqueou o recurso da Web.

- **E-mail para enviar uma mensagem** – `%COMPLAIN_EMAIL%`.

  Endereço de e-mail para comentários sobre blocos de recursos da Web. Clicar no endereço de e-mail abrirá uma janela na qual o usuário poderá escrever uma mensagem para o administrador.

- **Nome da categoria de conteúdo** – `%CONTENT_CATEGORY_LIST%`.

  Categoria de site à qual o recurso bloqueado pertence (por exemplo, *Sistemas de pagamento*).

- **Nome da categoria de tipo de dados** – `%TYPE_CATEGORY_LIST%`.

  Categoria do tipo de dados no recurso da Web bloqueado (por exemplo, *Gráficos*).

- **Link para recurso da Web solicitado** – `%CONTINUE_PAGE%`.

  Link para a página da Web solicitada (por exemplo, `http://www.example.com/pagename.html`).

- **Link para o site** – `%CONTINUE_SITE%`.

  Link para o site que contém a página da Web solicitada (por exemplo, `http://www.example.com/`).

- **Link para acessar os domínios** – `%CONTINUE_DOMAIN%`.

  Link que pode ser clicado para obter acesso a todas as páginas da Web existentes do nome de domínio. Por exemplo, caso o endereço da página da Web bloqueada seja `http://www.example.com`, a variável `%CONTINUE_DOMAIN%` será substituída pelo link `http://*.example.com`. Clicar no link permitirá o acesso a todos os endereços da Web do nome de domínio base `http://www.example.com/` inclusive os subdomínios, por exemplo, `http://start.example.com/*` ou `http://domain.domain.example.com/*`, onde o caractere `*` representa qualquer sequência de caracteres (inclusive uma string vazia).

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.

Se o Controle de dispositivos estiver ativado, o aplicativo retransmitirá as informações sobre os dispositivos conectados ao Kaspersky Security Center. É possível visualizar a lista de dispositivos conectados no Kaspersky Security Center na pasta **Avançado** → **Repositórios** → **Hardware**.

Níveis de acesso do dispositivo

O Controle de Dispositivos controla o acesso nos seguintes níveis:

- **Tipo de dispositivo**. Por exemplo, impressoras, unidades removíveis e unidades de CD/DVD.

  Você pode configurar o acesso do dispositivo da seguinte forma:

  - Permitir – ✓.
  - Bloquear – ⊘.

- Por regras (apenas impressoras e dispositivos portáteis) – .
- Depende do barramento de conexão (exceto Wi-Fi) – .
- Bloquear com exceções (somente Wi-Fi) – .

- **Barramento de conexão**. Um *barramento de conexão* é uma interface usada para conectar dispositivos ao computador (por exemplo, USB ou FireWire). Se o modo **Depende do barramento de conexão** estiver selecionado para o tipo de dispositivo, o aplicativo permitirá ou negará o acesso ao dispositivo, dependendo da interface de conexão (por exemplo, USB).

  Você pode configurar o acesso do dispositivo da seguinte forma:

  - Permitir – .
  - Bloquear – .

- **Dispositivos confiáveis**. *Dispositivos confiáveis* aqueles aos quais os usuários especificados têm acesso total a qualquer momento.

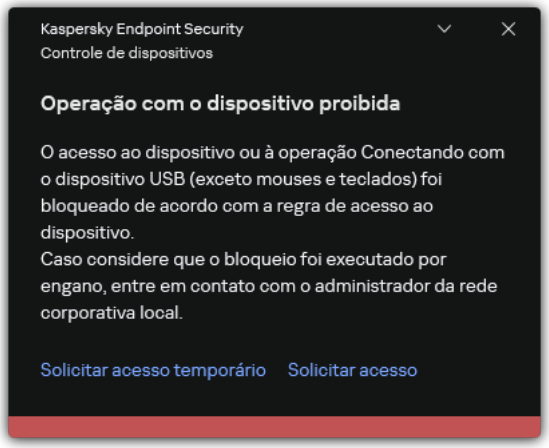
  Você pode adicionar dispositivos confiáveis com base nos seguintes dados:

  - **Dispositivos por ID**. Cada dispositivo possui um identificador exclusivo (Hardware ID ou HWID). É possível visualizar o ID nas propriedades do dispositivo usando ferramentas do sistema operacional. Exemplo de ID de dispositivo: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Adicionar dispositivos por ID é conveniente se você deseja adicionar vários dispositivos específicos.
  - **Dispositivos por modelo**. Cada dispositivo tem um Vendor ID (VID) e um Product ID (PID). É possível visualizar os IDs nas propriedades do dispositivo usando ferramentas do sistema operacional. Modelo para inserir o VID e o PID: `VID_1234&PID_5678`. Adicionar dispositivos por modelo é conveniente se você usar dispositivos de um determinado modelo em sua empresa. Dessa forma, você pode adicionar todos os dispositivos deste modelo.
  - **Dispositivos por máscara de ID**. Se você estiver usando vários dispositivos com IDs semelhantes, poderá adicionar dispositivos à lista confiável usando máscaras. O caractere `*` substitui qualquer conjunto de caracteres. O Kaspersky Endpoint Security não suporta o caractere `?` ao inserir uma máscara. Por exemplo, `WDC_C*`.
  - **Dispositivos por modelo de máscara**. Se você estiver usando vários dispositivos com VIDs ou PIDs semelhantes (por exemplo, dispositivos do mesmo fabricante), poderá adicionar dispositivos à lista confiável usando máscaras. O caractere `*` substitui qualquer conjunto de caracteres. O Kaspersky Endpoint Security não suporta o caractere `?` ao inserir uma máscara. Por exemplo, `VID_05AC&PID_*`.

O Controle de Dispositivos regula o acesso do usuário a dispositivos usando *regras de acesso*. O Controle de Dispositivos também permite salvar eventos de conexão/desconexão do dispositivo. Para salvar eventos, é necessário configurar o registro de eventos em uma política.

Se o acesso a um dispositivo depender do barramento de conexão (o status), o Kaspersky Endpoint Security não salva eventos de conexão/desconexão de dispositivos. Para permitir que o Kaspersky Endpoint Security salve eventos de conexão/desconexão de dispositivos, conceda o acesso ao tipo correspondente de dispositivo (o status) ou adicione o dispositivo à lista confiável.

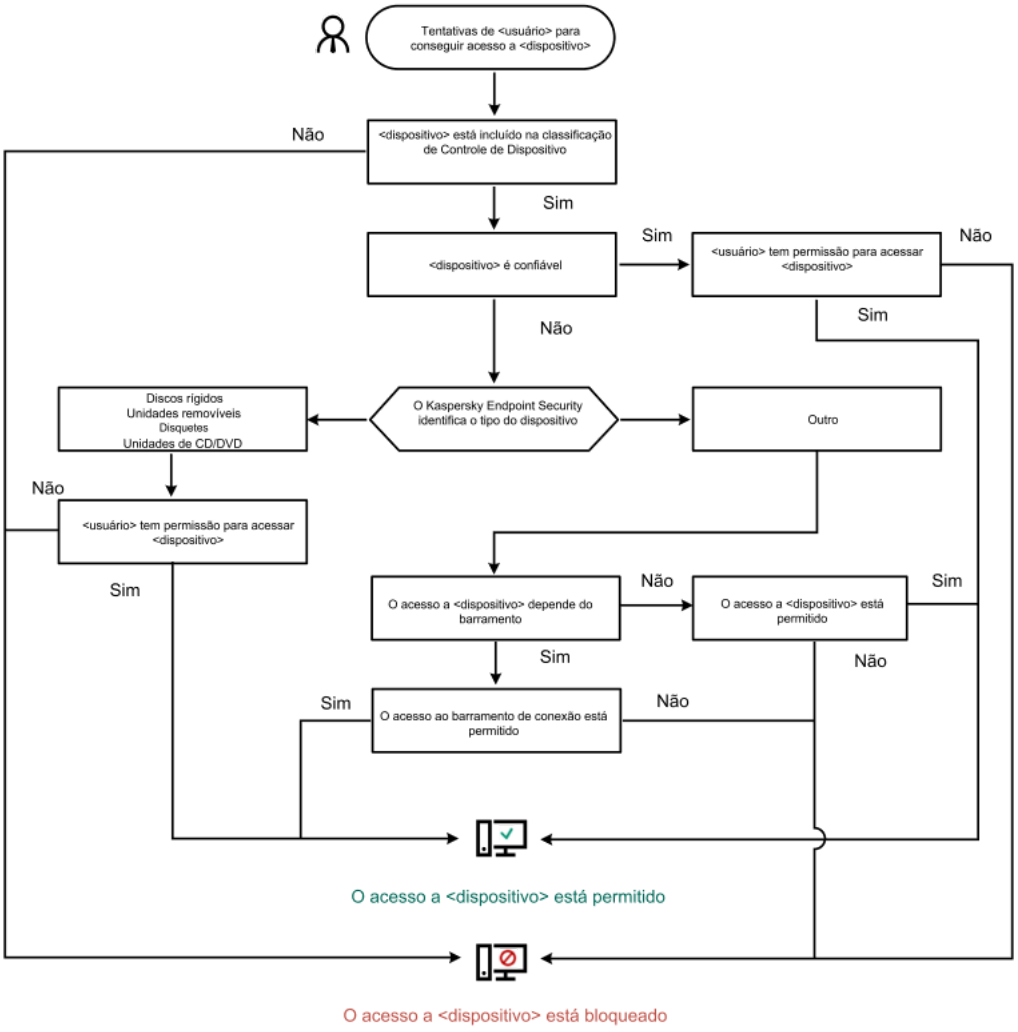
Quando um dispositivo que estiver bloqueado pelo Controle de Dispositivos for conectado ao computador, o Kaspersky Endpoint Security vai bloquear o acesso e exibir uma notificação (veja a figura abaixo).



Notificação do Controle de Dispositivos

Algoritmo de operação do Controle de Dispositivos

O Kaspersky Endpoint Security decide se permite ou não o acesso a um dispositivo quando o usuário o conecta ao computador (veja a figura a seguir).



Algoritmo de operação do Controle de Dispositivos

Se um dispositivo estiver conectado e o acesso for permitido, você poderá editar a regra de acesso e bloquear o acesso. Nesse caso, na próxima vez que alguém tentar acessar o dispositivo (como exibir a árvore de pastas ou executar operações de leitura ou gravação), o Kaspersky Endpoint Security bloqueará o acesso. O dispositivo que não está no sistema de arquivos é bloqueado somente na próxima vez que for conectado.

Se um usuário do computador com Kaspersky Endpoint Security instalado precisar solicitar acesso a um dispositivo que o usuário acredita estar bloqueado por engano, envie ao usuário as instruções de acesso a solicitação.

Sobre as regras de acesso

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. Você não pode adicionar um dispositivo que esteja fora da classificação de Controle de Dispositivos. O acesso a esses dispositivos é permitido para todos os usuários.

Regras de acesso do dispositivo

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	Controle de acesso	Agendamento para acesso a dispositivos	Atribuição de usuários e/ou grupos de usuários	Prioridade	Permissão para leitura/gravação
Discos rígidos	✓	✓	✓	✓	✓
Unidades removíveis (incluindo unidades flash USB)	✓	✓	✓	✓	✓
Disquetes	✓	✓	✓	✓	✓
Unidades de CD/DVD	✓	✓	✓	✓	✓
Dispositivos portáteis (MTP)	✓	✓	✓	✓	✓
Impressoras locais	✓	–	✓	✓	–
Impressoras de rede	✓	–	✓	✓	–
Modems	✓	–	–	–	–
Dispositivos de fita	✓	–	–	–	–
Dispositivos multifuncionais	✓	–	–	–	–
Leitores de cartões inteligentes	✓	–	–	–	–
Dispositivos do Windows CE USB ActiveSync	✓	–	–	–	–
Adaptadores de rede externos	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
Câmeras e scanners	✓	–	–	–	–

Regras de acesso para redes Wi-Fi

Uma regra de acesso à rede Wi-Fi determina se o uso das redes Wi-Fis é permitido (o status ✓) ou proibido (o status ⊘). Você pode adicionar uma *rede Wi-Fi confiável* (o status) a uma regra. O uso de uma rede Wi-Fi confiável é permitido sem limitações. Por padrão, uma regra de acesso à rede Wi-Fi permite o acesso a qualquer rede Wi-Fi.

Regras de acesso ao barramento de conexão

Caso **Depende do barramento de conexão** esteja selecionado para a regra de acesso por tipo de dispositivo, o aplicativo permitirá ou negará o acesso ao dispositivo, dependendo da interface de conexão. As regras que permitem o acesso aos barramentos são criadas por padrão para todos os barramento de conexão presentes na classificação do componente de Controle de Dispositivos.

As regras de acesso ao barramento de conexão determinam se a conexão de dispositivos é permitida (o status ✓) ou proibida (o status ⊘). A prioridade das regras de acesso por tipo de dispositivo é mais alta do que a prioridade das regras de acesso ao barramento de conexão.

> O teclado e o mouse não podem ser bloqueados usando o Controle de dispositivos. Se você proibir o acesso ao barramento de conexão USB, o usuário continuará trabalhando com um teclado e mouse conectados via USB. O componente Prevenção contra ataque BadUSB foi projetado para impedir que dispositivos USB infectados que imitam teclados se conectem ao computador.

Obter informações sobre os dispositivos instalados

O Kaspersky Security Center recebe informações sobre os dispositivos instalados dos seguintes provedores: Agente de Rede e Kaspersky Endpoint Security. As informações sobre os dispositivos instalados são necessárias para o gerenciamento de acesso e a criação de uma lista de dispositivos confiáveis.

Informações sobre o hardware do computador

Se o Agente de Rede estiver instalado em um dispositivo Windows, ele enviará as seguintes informações sobre o hardware do dispositivo ao Servidor de Administração:

- RAM
- dispositivos de armazenamento (incluindo discos rígidos)
- placa-mãe
- CPU
- adaptador de rede
- monitores
- GPU
- placa de som

O Agente de Rede fornece essas informações a cada sincronização com o Kaspersky Security Center. Você pode visualizar o hardware de um computador nas propriedades do computador (**Registro de hardware**).

Informações de hardware

O Kaspersky Endpoint Security fornece informações sobre o hardware instalado: impressoras, unidades removíveis, dispositivos portáteis (MTP) e assim por diante. Para receber informações de hardware, é necessário aplicar uma política ativa que permita a transmissão de informações sobre os dispositivos instalados (essa transmissão é ativada por padrão).

Como ativar a transmissão de dados sobre dispositivos instalados no Console de Gerenciamento (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Configurações gerais** → **Relatórios e Armazenamento**.
5. No bloco **Transferência de dados para o Servidor de Administração**, clique no botão **Configurações**.
6. Marque a caixa de seleção **Dispositivos instalados**.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar a transmissão de dados sobre dispositivos instalados no Web Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Integração KSC**.
5. No bloco **Transferência de dados para o Servidor de Administração**, clique no botão **Configurações avançadas**.
6. Marque a caixa de seleção **Sobre os dispositivos instalados**.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como resultado, você pode visualizar a lista de dispositivos instalados no console do Kaspersky Security Center (**Repositórios** → **Hardware**).

Gerenciar o acesso a dispositivos por tipo

O Controle de dispositivos permite gerenciar o acesso aos dispositivos por tipo. O tipo do dispositivo será determinado pelo sistema operacional quando o dispositivo for conectado. Você pode procurar o tipo de dispositivo pela ferramenta Gerenciador de dispositivos que está incorporada ao sistema operacional. Para gerenciar o acesso aos dispositivos, você deve 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. Você não pode adicionar um dispositivo que esteja fora da classificação de Controle de Dispositivos. O acesso a esses dispositivos é permitido para todos os usuários.

Por padrão, o Controle de dispositivos permite o acesso a todos os dispositivos para todos os usuários.

O acesso aos dispositivos pode ser configurado da seguinte forma:

- **Permitir**.

  O Kaspersky Endpoint Security concede acesso total aos dispositivos a todos os usuários.

- **Bloquear**.

  O Kaspersky Endpoint Security bloqueia conexões de dispositivos. O aplicativo permite que somente dispositivos confiáveis possam ser conectados.

- **Depende do barramento de conexão**.

  O Kaspersky Endpoint Security determina a interface de conexão dos dispositivos e restringe o acesso a eles de acordo com seu status de conexão de barramento. O aplicativo também permite conectar dispositivos confiáveis.

- **Por regras**.

  Para alguns tipos de dispositivo, é possível designar usuários individuais ou um grupo de usuários que tem permissão para utilizar os dispositivos, configurar o agendamento para o acesso aos dispositivos e as 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 ao disco do sistema seja bloqueado, o aplicativo poderá causar uma falha (BSOD) ao inicializar o sistema operacional.

Se um dispositivo não se enquadrar no esquema de classificação de Controle de dispositivos, o acesso a tal dispositivo não poderá ser restrito.

Como gerenciar o acesso a dispositivos por tipo no Console de Administração (MMC)

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

2. Na árvore do console, selecione **Políticas**.

3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

4. Na janela da política, selecione **Controles de Segurança** → **Controle de dispositivos**.

5. 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 Controle de dispositivos.

6. Configure regras de acesso para dispositivos:

   a. Selecione o modo de acesso: **Permitir**, **Bloquear**, **Depende do barramento de conexão**, **Por regras**.

      Para selecionar o modo de acesso **Por regras**, é necessário clicar duas vezes para abrir as propriedades da regra de acesso.

   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. No caso de dispositivos de armazenamento (por exemplo, mídia removível), é possível configurar permissões de acesso para usuários individuais. Você também pode configurar um agendamento para o acesso aos dispositivos e configurar as permissões de leitura e gravação.

      É possível adicionar dispositivos na lista confiável. *Dispositivos confiáveis* aqueles aos quais os usuários especificados têm acesso total a qualquer momento.

   d. Se necessário, configure as regras de impressão.

   e. Se necessário, configure as regras de acesso a dispositivos Bluetooth.

   f. Se necessário, configure as regras de conexão Wi-Fi do computador.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como gerenciar o acesso a dispositivos por tipo no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Controle de dispositivos**.

5. Em **Regras de acesso ao dispositivo**, selecione a guia **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. Configure regras de acesso para dispositivos:

   a. Selecione o modo de acesso: **Permitir**, **Bloquear**, **Dependente do barramento**, **Personalizado**.

      Se o modo de acesso estiver ausente no menu suspenso, abra as propriedades da regra de acesso clicando duas vezes no tipo de dispositivo.

   b. Caso o modo de acesso **Dependente do barramento** seja selecionado, será necessário configurar regras de acesso para as interfaces de conexão na guia **Barramentos de conexão**.

c. No caso de dispositivos de armazenamento (por exemplo, mídia removível), é possível configurar permissões de acesso para usuários individuais. Você também pode configurar um agendamento para o acesso aos dispositivos e configurar as permissões de leitura e gravação.

É possível adicionar dispositivos na lista confiável. *Dispositivos confiáveis* aqueles aos quais os usuários especificados têm acesso total a qualquer momento.

d. Se necessário, configure as regras de impressão.

e. Se necessário, configure as regras de acesso a dispositivos Bluetooth.

f. Se necessário, configure as regras de conexão Wi-Fi do computador.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como gerenciar o acesso a dispositivos na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de Segurança** → **Controle de dispositivos**.

3. No bloco **Acessar as configurações**, clique no link **Dispositivos e redes Wi-Fi**.

   A tabela lista as regras de acesso para todos os dispositivos presentes na classificação do componente Controle de Dispositivos.

4. Configure regras de acesso para dispositivos:

   a. Selecione o modo de acesso: **Permitir**, **Bloquear**, **Depende do barramento de conexão**, **Por regras**.

   Se o modo de acesso estiver ausente no menu suspenso, abra as propriedades da regra de acesso clicando duas vezes no tipo de dispositivo.

   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. No caso de dispositivos de armazenamento (por exemplo, mídia removível), é possível configurar permissões de acesso para usuários individuais. Você também pode configurar um agendamento para o acesso aos dispositivos e configurar as permissões de leitura e gravação.

   É possível adicionar dispositivos na lista confiável. *Dispositivos confiáveis* aqueles aos quais os usuários especificados têm acesso total a qualquer momento.

   d. Se necessário, configure as regras de impressão.

   e. Se necessário, configure as regras de acesso a dispositivos Bluetooth.

   f. Se necessário, configure as regras de conexão Wi-Fi do computador.

5. Salvar alterações.

Como resultado, quando um usuário tentar obter acesso a um dispositivo, o aplicativo bloqueará o acesso de acordo com as regras. O Kaspersky Endpoint Security também registra um evento correspondente. Se você quiser conceder acesso a dispositivos individuais, poderá adicionar esses dispositivos à lista de dispositivos confiáveis.

Gerenciar o acesso a dispositivos por meio de barramento de conexão

Para editar uma regra de acesso aos barramentos de conexão:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de dispositivos**.
3. No bloco **Acessar as configurações**, clique no botão **Barramentos de conexão**.

   A janela aberta mostra as regras de acesso para todos os barramentos de conexão incluídos na classificação do componente Controle de Dispositivos.
4. Selecione a regra de acesso que deseja editar.
5. Na coluna **Acesso**, selecione se deseja ou não permitir o acesso ao barramento de conexão: **Permitir** ou **Bloquear**.

   Caso tenha alterado o acesso ao barramento de conexão **Porta serial** (COM) ou **Porta paralela** (LPT), é necessário reiniciar o computador para ativar a regra de acesso.
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 para 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 nos *dispositivos de armazenamento*. Para esses dispositivos, é possível configurar permissões de gravação e leitura. O Controle de dispositivos é compatível com os seguintes tipos de *dispositivos de armazenamento*:

- Discos rígidos
- Unidades removíveis (incluindo unidades flash USB)
- Disquetes
- Unidades de CD/DVD
- Dispositivos portáteis (MTP) Os dispositivos portáteis (MTP) incluem, por exemplo, dispositivos móveis, câmeras fotográficas, reprodutores de mídia e assim por diante.

Dessa forma, você pode, por exemplo, permitir o uso de mídia removível somente para o grupo de administradores. Para outros tipos de dispositivo, é possível negar ou permitir o acesso de todos os usuários. Você também pode configurar direitos de acesso do usuário para a utilização de impressoras.

Como configurar direitos de acesso do usuário aos dados em dispositivos de armazenamento no Console de administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Controles de Segurança** → **Controle de dispositivos**.
5. 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 Controle de dispositivos.
6. Para configurar regras de acesso a dispositivos de armazenamento, clique duas vezes para abrir a lista de regras.
7. Configure a regra de acesso do dispositivo de armazenamento:

   a. No bloco **Regras de acesso**, clique no botão **Adicionar**.

      Isso abre uma janela para adicionar uma nova regra de acesso a dispositivo de armazenamento.

   b. No campo **Prioridade da regra**, defina a prioridade de *gravação 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 Endpoint Security regula o acesso ao dispositivo com base na regra de prioridade mais alta. O Kaspersky Endpoint 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 Endpoint 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**.
8. Em **Agendamentos para a regra de acesso selecionada**, configure o agendamento de acesso dos usuários ao dispositivo de armazenamento.

   Por exemplo, você pode permitir que os usuários utilizem dispositivos de armazenamento somente durante o horário de trabalho.

9. Configure as permissões de acesso dos usuários a dispositivos de armazenamento no gerenciador de arquivos (**Ler** / **Gravar**).

10. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como configurar os direitos de acesso do usuário aos dados em dispositivos de armazenamento no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Controle de dispositivos**.

5. No bloco **Regras de acesso ao dispositivo**, na tabela de regras de acesso, abra as propriedades das regras de acesso para dispositivos de armazenamento.

6. No bloco **Regras de acesso ao dispositivo**, selecione **Personalizado**.

7. Configure a regra de acesso do dispositivo de armazenamento:

   a. No bloco **Usuários e seus direitos**, clique no botão **Adicionar**.

      Isso abre uma janela para adicionar uma nova regra de acesso a dispositivo de armazenamento.

   b. No campo **Prioridade**, defina a prioridade de *gravação 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 Endpoint Security regula o acesso ao dispositivo com base na regra de prioridade mais alta. O Kaspersky Endpoint 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 Endpoint Security regula o acesso ao dispositivo com base em qualquer regra de bloqueio existente.

   c. Em **Usuário ou grupo**, 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 de acesso**, configure o agendamento de acesso dos usuários ao dispositivo de armazenamento.

      Por exemplo, você pode permitir que os usuários utilizem dispositivos de armazenamento somente durante o horário de trabalho.

e. Configure as permissões de acesso dos usuários a dispositivos de armazenamento no gerenciador de arquivos (**Ler** / **Gravar**).

f. Clique **Salvar**.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como configurar os direitos de acesso do usuário aos dados em dispositivos de armazenamento na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .

2. Na janela de configurações do aplicativo, selecione **Controles de Segurança** → **Controle de dispositivos**.

3. No bloco **Acessar as configurações**, clique no link **Dispositivos e redes Wi-Fi**.

   A tabela lista as regras de acesso para todos os dispositivos presentes na classificação do componente Controle de Dispositivos.

4. Para configurar as regras de acesso a dispositivos de armazenamento, clique com o botão direito para abrir a lista de regras.

5. Configure a regra de acesso do dispositivo de armazenamento:

   a. No bloco **Direitos de usuários**, clique no botão **Adicionar**.

      Isso abre uma janela para adicionar uma nova regra de acesso a dispositivo de armazenamento.

   b. No campo **Prioridade**, defina a prioridade de *gravação 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 Endpoint Security regula o acesso ao dispositivo com base na regra de prioridade mais alta. O Kaspersky Endpoint 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 Endpoint Security regula o acesso ao dispositivo com base em qualquer regra de bloqueio existente.

   c. Em **Usuários**, selecione usuários ou grupos de usuários. Você pode selecionar usuários no Active Directory ou 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**.

6. Em **Agendamento para acesso a dispositivos**, configure o agendamento de acesso dos usuários ao dispositivo de armazenamento.

   Por exemplo, você pode permitir que os usuários utilizem dispositivos de armazenamento somente durante o horário de trabalho.

7. Configure as permissões de acesso dos usuários a dispositivos de armazenamento no gerenciador de arquivos (**Ler** / **Gravar**).

8. Salvar alterações.

Diferenciação dos direitos de acesso do usuário a 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 do usuário nas propriedades do dispositivo confiável.

Gerenciamento do acesso a dispositivos móveis

O Kaspersky Endpoint Security permite controlar o acesso aos dados em dispositivos móveis que executam Android e iOS. Os dispositivos móveis pertencem à categoria de dispositivos portáteis (MTP). Portanto, para configurar o acesso de dados em dispositivos móveis, é necessário editar as configurações de acesso para dispositivos portáteis (MTP).

Quando um dispositivo móvel é conectado ao computador, o sistema operacional determina o tipo de dispositivo. Se o Android Debug Bridge (ADB), o iTunes ou aplicativos equivalentes estiverem instalados no computador, o sistema operacional identificará os dispositivos móveis como dispositivos ADB ou iTunes. Em todos os outros casos, o sistema operacional pode identificar o tipo de dispositivo móvel como um dispositivo portátil (MTP) para transferência de arquivos, um dispositivo PTP (câmera) para transferência de imagens ou outro dispositivo. O tipo de dispositivo depende do modelo do dispositivo móvel e do modo de conexão USB selecionado. O Kaspersky Endpoint Security permite configurar permissões de acesso individuais para os dados em dispositivos móveis em aplicativos ADB, iTunes ou gerenciador de arquivos. Em todos os outros casos, o Controle de Dispositivos permite o acesso a dispositivos móveis de acordo com as regras de acesso a dispositivos portáteis (MTP).

Acesso a dispositivos móveis

Os dispositivos móveis pertencem à categoria de dispositivos portáteis (MTP), portanto, as configurações para eles são as mesmas. É possível selecionar um dos seguintes modos de acesso a dispositivos móveis:

- **Permitir**. O Kaspersky Endpoint Security permite acesso total a dispositivos móveis. É possível abrir, criar, modificar, copiar ou excluir arquivos em dispositivos móveis usando o gerenciador de arquivos ou aplicativos ADB e iTunes. É possível também carregar a bateria do dispositivo conectando-o a uma porta USB do computador.

- **Bloquear**. O Kaspersky Endpoint Security restringe o acesso a dispositivos móveis no gerenciador de arquivos e nos aplicativos ADB e iTunes. O aplicativo permite o acesso apenas de dispositivos móveis confiáveis. É possível também carregar a bateria do dispositivo conectando-o a uma porta USB do computador.

- **Depende do barramento de conexão**. O Kaspersky Endpoint Security permite a conexão com dispositivos móveis de acordo com o status da conexão USB (**Permitir** ou **Bloquear**).

- **Por regras**. O Kaspersky Endpoint Security restringe o acesso a dispositivos móveis de acordo com as regras. Nas regras, é possível configurar direitos de acesso (ler/gravar), selecionar usuários ou um grupo de usuários que podem ter acesso a dispositivos móveis e configurar uma programação de acesso para dispositivos móveis. Também é possível restringir o acesso aos dados nos dispositivos móveis por meio dos aplicativos ADB e iTunes.

Configurar regras de acesso para dispositivos móveis

As regras de acesso para dispositivos portáteis (MTP), dispositivos ADB e dispositivos iTunes são configuradas de maneira diferente. Para dispositivos portáteis (MTP) e dispositivos ADB, é possível configurar as regras para usuários individuais ou grupos de usuários e criar uma programação para o momento de aplicação das regras. Para dispositivos iTunes, não é possível fazer isso. Só é possível permitir ou negar o acesso aos dados por meio do aplicativo iTunes para todos os usuários.

Como configurar regras de acesso de dispositivos móveis no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Controles de Segurança** → **Controle de dispositivos**.

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 **Dispositivos portáteis (MTP)**, configure o modo de acesso do dispositivo móvel: **Permitir** ✓, **Bloquear** ⊘, ou **Depende do barramento de conexão** ◔.

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**, defina a prioridade de gravação da regra. Uma regra inclui os seguintes atributos: conta do usuário, programação, permissões (leitura/gravação/acesso ADB) e prioridade.

      Uma regra tem uma prioridade específica. Se um usuário foi adicionado a vários grupos, o Kaspersky Endpoint Security regula o acesso ao dispositivo com base na regra de prioridade mais alta. O Kaspersky Endpoint 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 Endpoint 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**.

8. Em **Agendamentos para a regra de acesso selecionada**, configure uma agenda de acesso ao dispositivo móvel para os usuários.

   Não é possível configurar uma agenda de acesso separada para dispositivos ADB. É possível configurar uma agenda de acesso comum para dispositivos ADB e dispositivos portáteis (MTP).

9. Configure as permissões de acesso dos usuários a dispositivos móveis no gerenciador de arquivos (**Ler** / **Gravar**).

10. Configure o acesso aos dados em um dispositivo móvel mediante aplicativo ADB ao usar a caixa de seleção **Acesse via ADB**.

    Caso a caixa de seleção esteja desmarcada, quando o dispositivo móvel estiver conectado, o aplicativo ADB será impedido de detectar o dispositivo.

11. Em **Acessar via iTunes**, configure o acesso aos dados no dispositivo móvel por meio do aplicativo iTunes.

    O Kaspersky Endpoint Security aplica as configurações para acesso de dispositivos móveis por meio do aplicativo iTunes para todos os usuários. Não é possível configurar um agendamento de acesso para dispositivos iTunes.

12. Salvar alterações.

Como configurar as regras de acesso para dispositivos móveis no Web Console e Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Controle de dispositivos**.

5. No bloco **Regras de acesso ao dispositivo**, clique no link **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 **Dispositivos portáteis (MTP)**.

   Isso abre os direitos de acesso de dispositivos portáteis (MTP).

7. Configure o modo de acesso dos dispositivos móveis: **Permitir**, **Bloquear**, **Dependente do barramento**, ou **Personalizado**.

8. Use o botão de alternância **Acesso pelo iTunes para todos os usuários ATIVADO** e configure o acesso aos dados no dispositivo móvel por meio do aplicativo iTunes.

   O Kaspersky Endpoint Security aplica as configurações para acesso de dispositivos móveis por meio do aplicativo iTunes para todos os usuários. Não é possível configurar um agendamento de acesso para dispositivos iTunes.

9. Caso selecione o modo **Personalizado**, é necessário adicionar as regras de acesso para os dispositivos. Para isso, em **Usuários e seus direitos**, clique no botão **Adicionar** e configure a regra de acesso do dispositivo móvel:

   a. No campo **Prioridade**, defina a prioridade de gravação da regra. Uma regra inclui os seguintes atributos: conta do usuário, programação, permissões (leitura/gravação/acesso ADB) e prioridade.

      Uma regra tem uma prioridade específica. Se um usuário foi adicionado a vários grupos, o Kaspersky Endpoint Security regula o acesso ao dispositivo com base na regra de prioridade mais alta. O Kaspersky Endpoint 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 Endpoint Security regula o acesso ao dispositivo com base em qualquer regra de bloqueio existente.

   b. Em **Usuário ou grupo**, selecione usuários ou grupos de usuários para acessar os dispositivos móveis. 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.

   c. Em **Agendamento do acesso**, configure uma agenda de acesso ao dispositivo móvel para os usuários.

      > Não é possível configurar uma agenda de acesso separada para dispositivos ADB. É possível configurar uma agenda de acesso comum para dispositivos ADB e dispositivos portáteis (MTP).

   d. Configure as permissões de acesso dos usuários a dispositivos móveis no gerenciador de arquivos (**Ler** / **Gravar**).

   e. Configure o acesso aos dados em um dispositivo móvel mediante aplicativo ADB ao usar a caixa de seleção **Acesse via ADB**.

      Caso a caixa de seleção esteja desmarcada, quando o dispositivo móvel estiver conectado, o aplicativo ADB será impedido de detectar o dispositivo.

10. Salvar alterações.

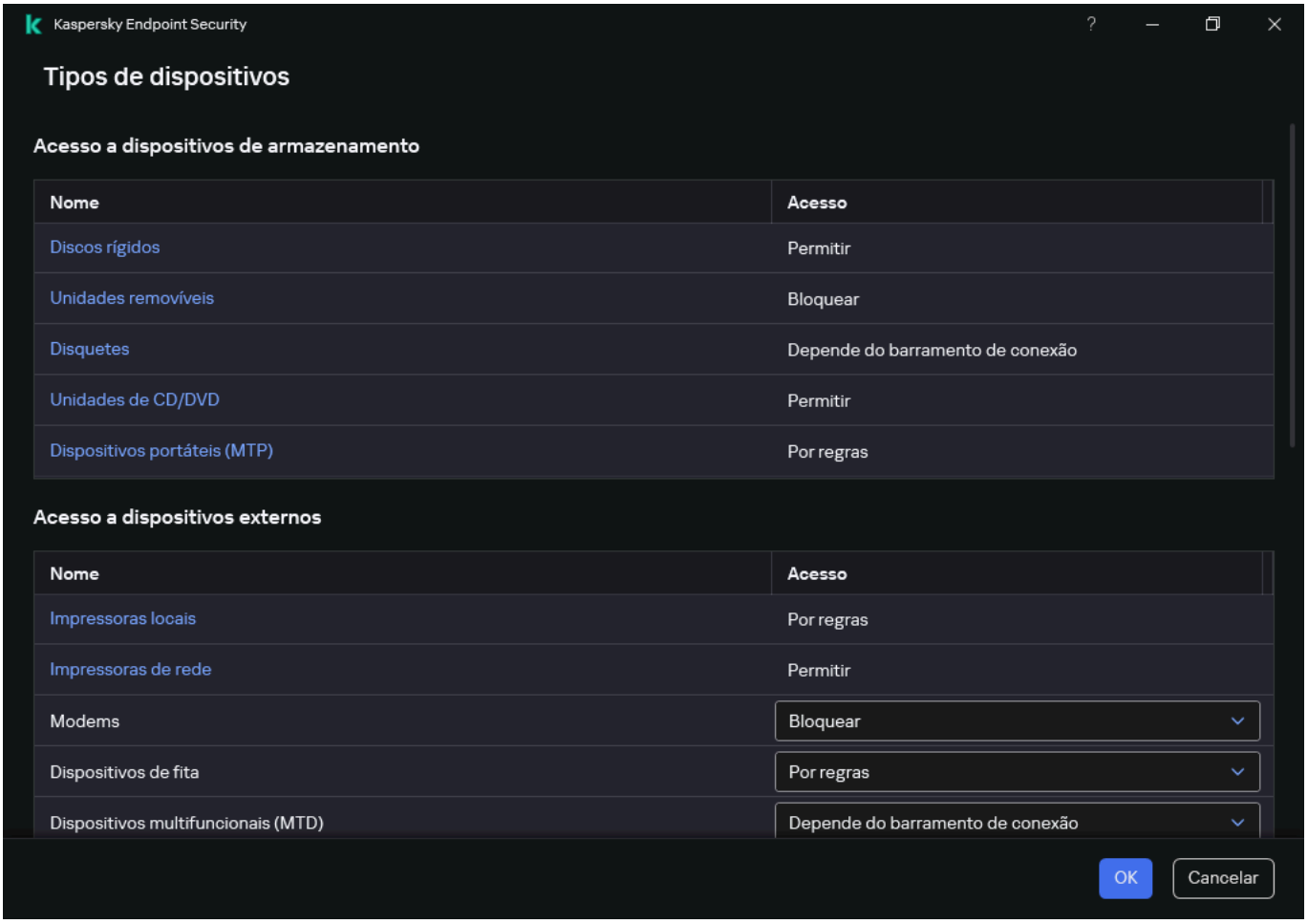
Como configurar as regras de acesso de dispositivos móveis na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de dispositivos**.

3. No bloco **Acessar as configurações**, clique no botão **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.



Tipos de dispositivos no componente Controle de Dispositivos

4. No bloco **Acesso a dispositivos de armazenamento**, clique no link **Dispositivos portáteis (MTP)**.

   Isso abrirá uma janela contendo as regras de acesso aos dispositivos portáteis (MTP).

5. Em **Acesso**, configure o modo de acesso dos dispositivos móveis: **Permitir**, **Bloquear**, **Depende do barramento de conexão**, ou **Por regras**.

6. Caso selecione o modo **Por regras**, é necessário adicionar as regras para os dispositivos:

   a. No bloco **Direitos de 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 de gravação da regra. Uma regra inclui os seguintes atributos: conta do usuário, programação, permissões (leitura/gravação/acesso ADB) e prioridade.

      Uma regra tem uma prioridade específica. Se um usuário foi adicionado a vários grupos, o Kaspersky Endpoint Security regula o acesso ao dispositivo com base na regra de prioridade mais alta. O Kaspersky Endpoint 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 Endpoint Security regula o acesso ao dispositivo com base em qualquer regra de bloqueio existente.

c. Em **Estado**, ative a regra de acesso do dispositivo móvel.

d. Embaixo de **Regras de acesso**, configure as permissões de acesso a dispositivos móveis para os usuários.

- Configure as permissões de acesso dos usuários a dispositivos móveis no gerenciador de arquivos (**Ler** / **Gravar**).

- Configure o acesso aos dados em um dispositivo móvel mediante aplicativo ADB ao usar a caixa de seleção **Acesse via ADB**.

  Caso a caixa de seleção esteja desmarcada, quando o dispositivo móvel estiver conectado, o aplicativo ADB será impedido de detectar o dispositivo.

e. Em **Usuários**, selecione usuários ou grupos de usuários para acessar os dispositivos móveis. 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.

f. Em **Agendamento para acesso a dispositivos**, configure a agenda de acesso ao dispositivo para os usuários.

> Não é possível configurar uma agenda de acesso separada para dispositivos ADB. É possível configurar uma agenda de acesso comum para dispositivos ADB e dispositivos portáteis (MTP).

g. Em **Acessar via iTunes**, configure o acesso aos dados no dispositivo móvel por meio do aplicativo iTunes.

> O Kaspersky Endpoint Security aplica as configurações para acesso de dispositivos móveis por meio do aplicativo iTunes para todos os usuários. Não é possível configurar um agendamento de acesso para dispositivos iTunes.

7. Salvar alterações.

Como resultado, o acesso do usuário a dispositivos móveis ficará restrito conforme as regras. Caso tenha proibido o acesso a dispositivos móveis nos aplicativos ADB e iTunes, ao conectar um dispositivo móvel, os aplicativos ADB e iTunes serão impedidos de detectar o dispositivo móvel.

Dispositivos móveis confiáveis

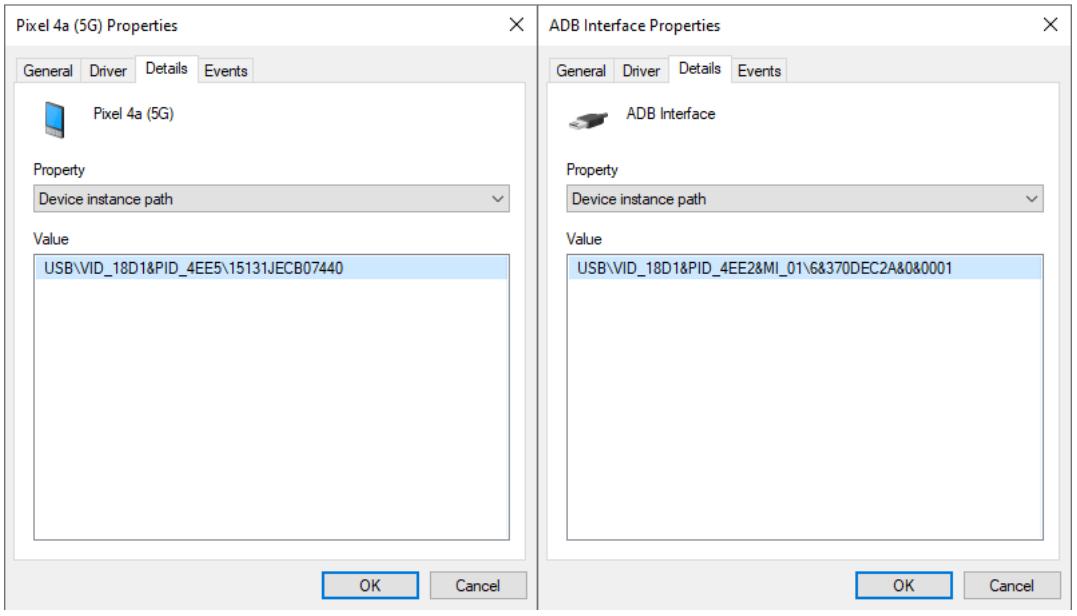
Dispositivos confiáveis aqueles aos quais os usuários especificados têm acesso total a qualquer momento.

O procedimento para adicionar dispositivo móvel confiável é exatamente o mesmo de outros tipos de dispositivos confiáveis. É possível adicionar um dispositivo móvel por ID ou modelo de dispositivo.

Para adicionar um dispositivo móvel confiável por ID, será necessário um ID exclusivo (Hardware ID – HWID). É possível encontrar o ID nas propriedades do dispositivo usando as ferramentas do sistema operacional (veja a figura abaixo). A ferramenta Gerenciador de Dispositivos permite fazer isso. IDs de dispositivos portáteis (MTP), ADB e dispositivos iTunes são diferentes, mesmo para o mesmo dispositivo móvel. O ID de um dispositivo portátil (MTP) pode ter esta aparência: `15131JECB07440`. O ID de um dispositivo ADB pode ter esta aparência: `6&370DEC2A&0&0001`. Adicionar dispositivos por ID é conveniente se você deseja adicionar vários dispositivos específicos. Também é possível usar máscaras.

Se você instalou os aplicativos ADB ou iTunes após conectar um dispositivo ao computador, o ID exclusivo do dispositivo poderá ser redefinido. Isso significa que o Kaspersky Endpoint Security identificará esse dispositivo como um novo dispositivo. Se um dispositivo é confiável, adicione-o à lista confiável novamente.

Para adicionar um dispositivo móvel confiável pelo modelo do dispositivo, serão necessários o Vendor ID (VID) e o Product ID (PID). É possível encontrar os IDs nas propriedades do dispositivo usando as ferramentas do sistema operacional (veja a figura abaixo). Modelo para inserir o VID e o PID: `VID_18D1&PID_4EE5`. Adicionar dispositivos por modelo é conveniente se você usar dispositivos de um determinado modelo em sua empresa. Dessa forma, você pode adicionar todos os dispositivos deste modelo.



ID do dispositivo no Gerenciador de Dispositivos

Gerenciando o acesso a dispositivos Bluetooth

O Kaspersky Endpoint 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 Endpoint 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 Endpoint 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 Endpoint 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 Endpoint Security restringe o acesso a dispositivos Bluetooth. É possível permitir a conexão apenas de dispositivos de entrada Bluetooth (a classe Human Interface Devices). Esses dispositivos incluem teclados, mouses, joysticks 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.

Como configurar regras de acesso a dispositivos Bluetooth no Console de Administração (MMC)

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

2. Na árvore do console, selecione **Políticas**.

3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

4. Na janela da política, selecione **Controles de Segurança** → **Controle de dispositivos**.

5. 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.

6. No menu de contexto do tipo de dispositivo **Bluetooth**, configure o modo de acesso do dispositivo Bluetooth: **Permitir** , **Bloquear** , **Permitir e não registrar** .

7. 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)**.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como configurar as regras de acesso para dispositivos Bluetooth no Web Console e Cloud Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Controle de dispositivos**.

5. No bloco **Regras de acesso ao dispositivo**, clique no link **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 **Dispositivos Bluetooth**.

   As configurações de acesso ao dispositivo Bluetooth são abertas.

7. Configurar o modo de acesso do dispositivo Bluetooth: **Permitir**, **Bloquear**, **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. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

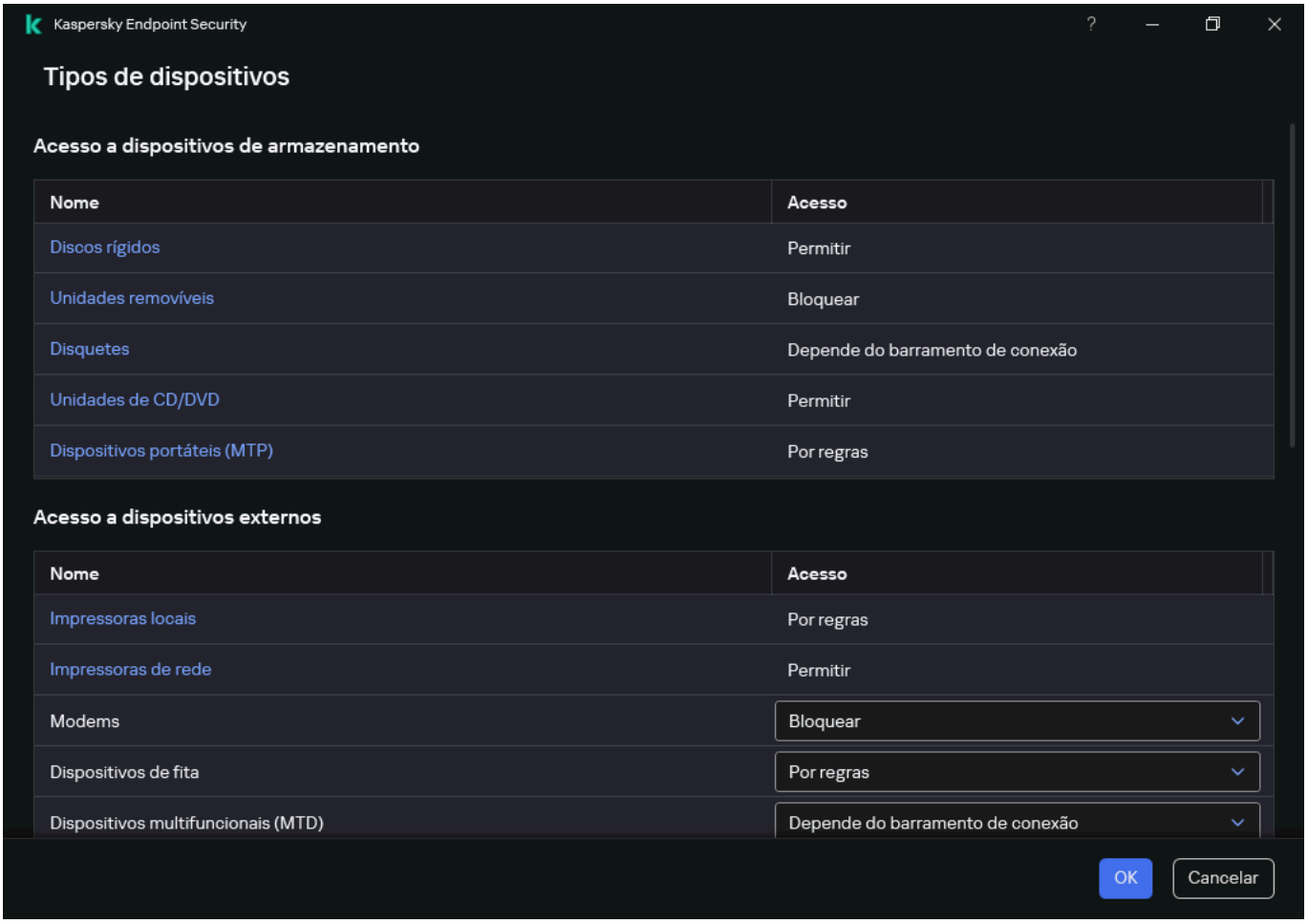
Como configurar as regras de acesso do dispositivo Bluetooth na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de dispositivos**.

3. No bloco **Acessar as configurações**, clique no botão **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.



Tipos de dispositivos no componente Controle de Dispositivos

4. No bloco **Acesso a dispositivos externos**, clique no link **Bluetooth**.

   As configurações de acesso ao dispositivo Bluetooth são abertas.

5. Em **Acesso**, configure o modo de acesso dos dispositivos Bluetooth: **Permitir**, **Bloquear**, **Permitir e não registrar**.

6. 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)**.

7. Salvar alterações.

Controle de impressão

O controle de impressões não é compatível com computadores baseados em Arm.

É possível usar o controle de impressão para configurar o acesso do usuário às impressoras locais e de rede.

Controle de impressoras locais

O Kaspersky Endpoint Security permite configurar o acesso a impressoras locais em dois níveis: *conexão* e *impressão*.

O Kaspersky Endpoint Security controla a conexão da impressora local nos seguintes barramentos: USB, porta serial (COM), porta paralela (LPT).

O Kaspersky Endpoint Security controla a conexão de impressoras locais às portas COM e LPT somente no nível do barramento. Assim, para impedir conexões de impressoras via portas COM e LPT, você precisa selecionar o modo de acesso Depende do barramento de conexão para impressoras locais e proibir conexões aos 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 Endpoint Security concede acesso total às impressoras locais para todos os usuários. Os usuários podem conectar impressoras e imprimir documentos usando os meios fornecidos pelo sistema operacional.

- **Bloquear** ⊘. O Kaspersky Endpoint Security bloqueia a conexão de impressoras locais. O aplicativo permite conectar apenas a impressoras confiáveis.

- **Depende do barramento de conexão**. O Kaspersky Endpoint Security permite a conexão às impressoras locais de acordo com o status de conexão 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 Endpoint 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 Endpoint 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 Endpoint Security concede acesso à impressão em impressoras de rede a todos os usuários.

- **Bloquear**. O Kaspersky Endpoint Security restringe o acesso a impressoras de rede para todos os usuários. O aplicativo permite o acesso apenas a impressoras confiáveis.

- **Por regras**. O Kaspersky Endpoint Security concede acesso à impressão de acordo com as regras de impressão. Nas regras, é possível selecionar usuários ou um grupo de usuários que terão ou não permissão para imprimir documentos na impressora de rede.

Adicionar regras de impressão para impressoras

Como adicionar regras de impressão no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Controles de Segurança** → **Controle de dispositivos**.

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 para tipos de dispositivos de **Impressoras locais** e **Impressoras de rede**, configure o modo de acesso para as impressoras relevantes: **Permitir**, **Bloquear**, **Permitir e não registrar** (somente para impressoras de rede) ou **Depende do barramento de conexão** (somente para impressoras locais).

6. Para configurar as regras de impressão em impressoras locais e de rede, clique duas vezes nas listas de regras para abri-las.

7. Selecione **Por regras** como o modo de acesso à impressora.

8. Selecione os usuários ou grupo de usuários para os quais deseja aplicar a regra de impressão.

   a. Clique **Adicionar**.

      Uma janela será exibida para adicionar uma nova regra de impressão.

   b. 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 Endpoint Security regula o acesso ao dispositivo com base na regra de prioridade mais alta. O Kaspersky Endpoint 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 Endpoint Security regula o acesso ao dispositivo com base em qualquer regra de bloqueio existente.

   c. Em **Ação**, configure o acesso do usuário para imprimir na impressora.

   d. 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.

   e. Clique **OK**.

9. Salvar alterações.

Como adicionar regras de impressão no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Controle de dispositivos**.

5. No bloco **Regras de acesso ao dispositivo**, clique no link **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 **Impressoras locais** ou **Impressoras de rede**.

   Isso abre as regras de acesso à impressora.

7. Configure o modo de acesso para as impressoras relevantes: **Permitir**, **Bloquear**, **Permitir e não registrar** (somente para impressoras de rede), **Dependente do barramento** (somente para impressoras locais) ou **Personalizado**.

8. Caso selecione o modo **Personalizado** será necessário adicionar as regras de impressão para impressoras locais ou de rede. Para fazer isto, clique no botão **Adicionar** na tabela de regras de impressão.

   Isso abre as configurações da nova regra de impressão.

9. 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 Endpoint Security regula o acesso ao dispositivo com base na regra de prioridade mais alta. O Kaspersky Endpoint 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 Endpoint Security regula o acesso ao dispositivo com base em qualquer regra de bloqueio existente.

10. Em **Ação**, configure o acesso do usuário para imprimir na impressora.

11. Em **Usuário ou grupo**, 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.

12. Salvar alterações.

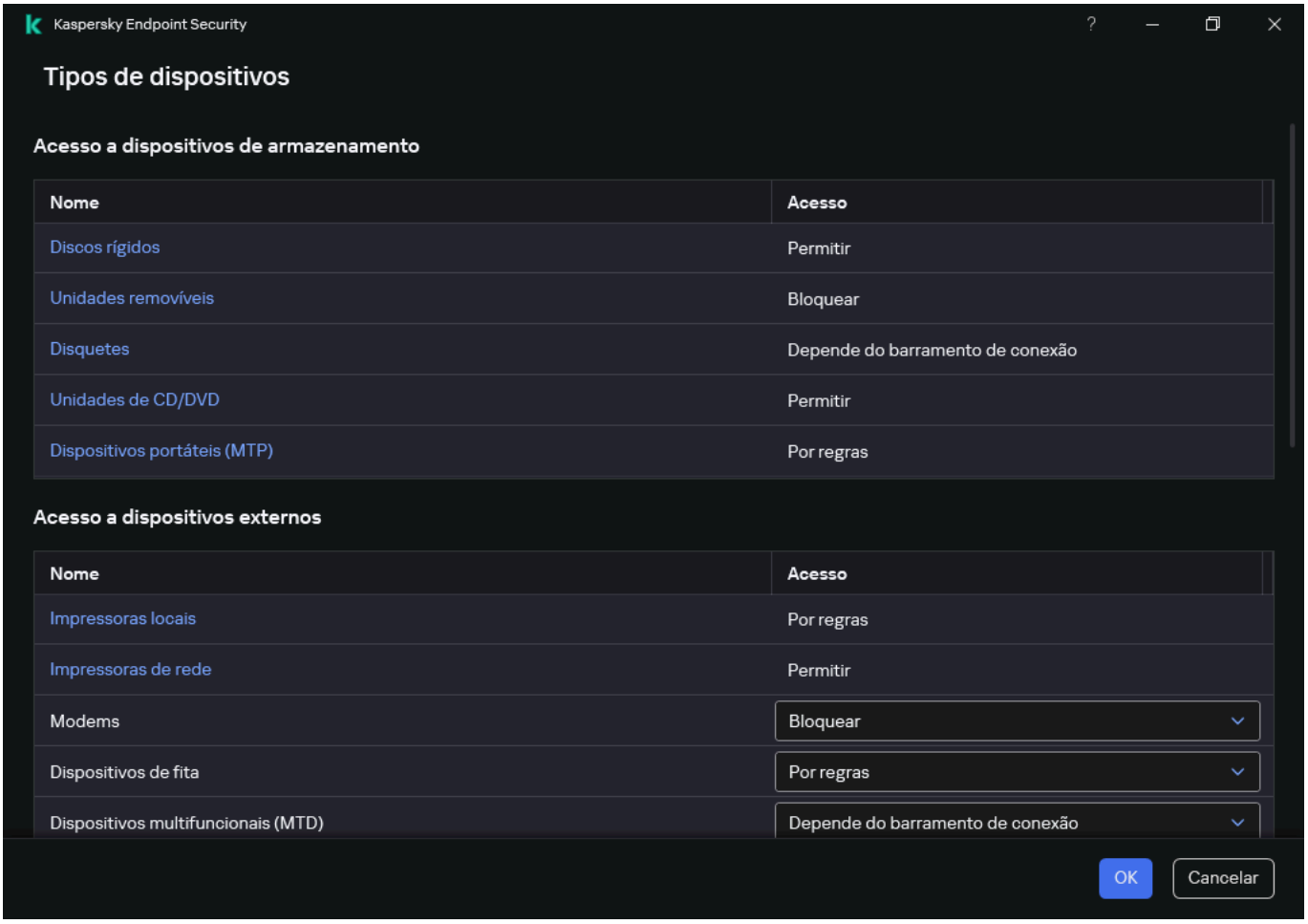
Como adicionar regras de impressão na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de dispositivos**.

3. No bloco **Acessar as configurações**, clique no botão **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.



Tipos de dispositivos no componente Controle de Dispositivos

4. Em **Acesso a dispositivos externos**, clique em **Impressoras locais** ou **Impressoras de rede**.

   Isso abre uma janela com regras de acesso à impressora.

5. Em **Acesso às impressoras locais** ou **Acesso às impressoras da rede**, configure o modo de acesso às impressoras: **Permitir**, **Bloquear**, **Permitir e não registrar** (somente para impressoras de rede), **Depende do barramento de conexão** (somente para impressoras locais) ou **Por regras**.

6. Caso selecione o modo **Por regras**, é necessário adicionar as regras de impressão para impressoras. Selecione os usuários ou grupo de usuários para os quais deseja aplicar a regra de impressão.

   a. Clique **Adicionar**.

      Uma janela será exibida para adicionar uma nova regra de impressão.

   b. Atribua uma prioridade à entrada da regra. Uma entrada de regra inclui os seguintes atributos: conta do usuário, permissões (permitir/bloquear) e prioridade.

      Uma regra tem uma prioridade específica. Se um usuário foi adicionado a vários grupos, o Kaspersky Endpoint Security regula o acesso ao dispositivo com base na regra de prioridade mais alta. O Kaspersky Endpoint 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 Endpoint Security regula o acesso ao dispositivo com base em qualquer regra de bloqueio existente.

c. Em **Ação**, configure as permissões do usuário para acessar a impressão.

d. Em **Usuários e grupos**, 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. Salvar alterações.

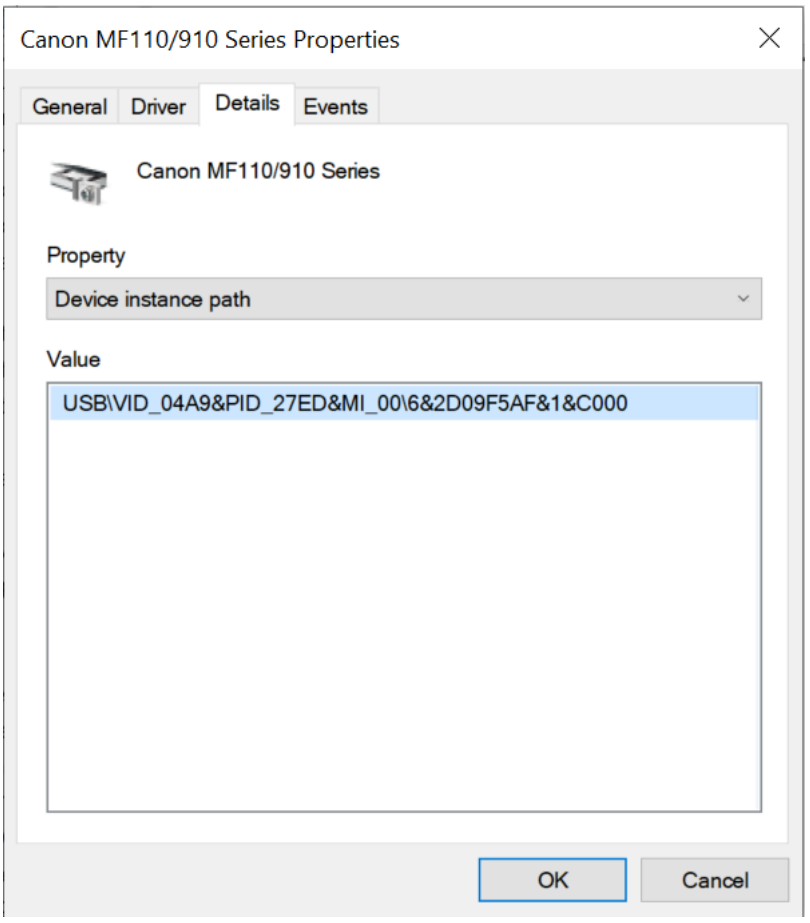
Impressoras confiáveis

Dispositivos confiáveis aqueles aos quais os usuários especificados têm acesso total a qualquer momento.

O procedimento para adicionar impressoras confiáveis é exatamente o mesmo de outros tipos de dispositivos confiáveis. É possível adicionar impressoras locais por ID ou modelo de dispositivo. É possível adicionar apenas impressoras de rede por ID de dispositivo.

Para adicionar uma impressora local confiável por ID, será necessário um ID exclusivo. (Hardware ID – HWID). É possível encontrar o ID nas propriedades do dispositivo usando as ferramentas do sistema operacional (veja a figura abaixo). A ferramenta Device Manager permite fazer isso. O ID de uma impressora local pode ter esta aparência: `6&2D09F5AF&1&C000`. Adicionar dispositivos por ID é conveniente se você deseja adicionar vários dispositivos específicos. Também é possível usar máscaras.

Para adicionar uma impressora local confiável por modelo de dispositivo, você precisará do Vendor ID (VID) e do Product ID (PID). É possível encontrar os IDs nas propriedades do dispositivo usando as ferramentas do sistema operacional (veja a figura abaixo). Modelo para inserir o VID e o PID: `VID_04A9&PID_27FD`. Adicionar dispositivos por modelo é conveniente se você usar dispositivos de um determinado modelo em sua empresa. Dessa forma, você pode adicionar todos os dispositivos deste modelo.



ID do dispositivo no Gerenciador de Dispositivos

Para adicionar uma impressora de rede confiável, é necessário ter o ID do dispositivo. Para impressoras de rede, o ID do dispositivo pode ser o nome de rede da impressora (nome da impressora compartilhada), o endereço IP ou o URL da impressora.

Controle de conexões Wi-Fi

O Controle de Dispositivos permite gerenciar a conexão Wi-Fi do computador (laptop). 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 Endpoint Security não controlará conexões com as redes Wi-Fi.

Como restringir as conexões Wi-Fi no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Controles de Segurança** → **Controle de dispositivos**.

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 para o tipo do dispositivo **Wi-Fi**, selecione a ação do Controle de Dispositivos a ser executada ao se conectar à rede Wi-Fi: **Permitir** (✓), **Bloquear** (⊘), ou **Bloquear com exceções** (▤).

6. Caso tenha selecionado a opção **Bloquear com exceções**, crie uma lista de redes Wi-Fi confiáveis:

   a. Clique duas vezes para abrir a lista de redes Wi-Fi confiáveis.

   b. No bloco **Redes Wi-Fi confiáveis**, clique no botão **Adicionar**.

   c. 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.

     > A partir do Kaspersky Endpoint Security for Windows versão 12.0, o suporte ao protocolo WPA3 passou a ser adicionado ao aplicativo. Se uma política do Kaspersky Endpoint Security versão 12.2 for aplicada em um computador, o protocolo WPA2 será selecionado nos computadores com o Kaspersky Endpoint Security versão 11.11.0 e anteriores; o WPA2/WPA3 será selecionado para as versões 12.0 a 12.1; e o WPA3 será selecionado para as versões 12.2 e posteriores.

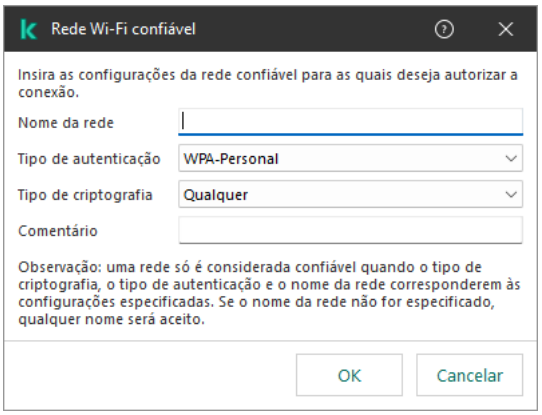
   - **Tipo de criptografia**. Tipo de criptografia usado para proteger o tráfego Wi-Fi.

   - **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.



Configurações da rede Wi-Fi confiável

Como restringir conexões Wi-Fi no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Controle de dispositivos**.

5. Em **Regras de acesso ao dispositivo**, selecione a guia **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. No bloco **Redes Wi-Fi**, clique no link **Wi-Fi**.

7. Na janela exibida, selecione a ação do Controle de dispositivos executada ao se conectar ao Wi-Fi: **Permitir**, **Bloquear**, ou **Bloquear com exclusões**.

8. Caso tenha selecionado a opção **Bloquear com exclusões**, crie uma lista de redes Wi-Fi confiáveis:

   a. Clique duas vezes para abrir a lista de redes Wi-Fi confiáveis.

   b. No bloco **Redes Wi-Fi confiáveis**, clique no botão **Adicionar**.

   c. Isso abre uma janela; nessa janela, configure a rede Wi-Fi confiável (veja a figura abaixo):

   - **Nome**. Nome ou SSID (Service Set Identifier) da rede Wi-Fi.

   - **Tipo de autenticação**. Tipo de autenticação usado ao conectar a redes Wi-Fi.

     A partir do Kaspersky Endpoint Security for Windows versão 12.0, o suporte ao protocolo WPA3 passou a ser adicionado ao aplicativo. Se uma política do Kaspersky Endpoint Security versão 12.2 for aplicada em um computador, o protocolo WPA2 será selecionado nos computadores com o Kaspersky Endpoint Security versão 11.11.0 e anteriores; o WPA2/WPA3 será selecionado para as versões 12.0 a 12.1; e o WPA3 será selecionado para as versões 12.2 e posteriores.

- **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.

Como restringir conexões Wi-Fi na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de dispositivos**.
3. No bloco **Acessar as configurações**, clique no botão **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.
4. No bloco **Acesso a redes Wi-Fi**, clique no link **Wi-Fi**.

   A janela aberta mostra as regras de acesso à rede Wi-Fi.

Configurações de acesso Wi-Fi

5. Em **Acesso**, selecione a ação do Controle de Dispositivos realizada ao conectar à rede Wi-Fi: **Permitir**, **Bloquear**, ou **Bloquear com exceções**.

6. Caso tenha selecionado a opção **Bloquear com exceções**, crie uma lista de redes Wi-Fi confiáveis:

   a. No bloco **Redes Wi-Fi confiáveis**, clique no botão **Adicionar**.

   b. 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.

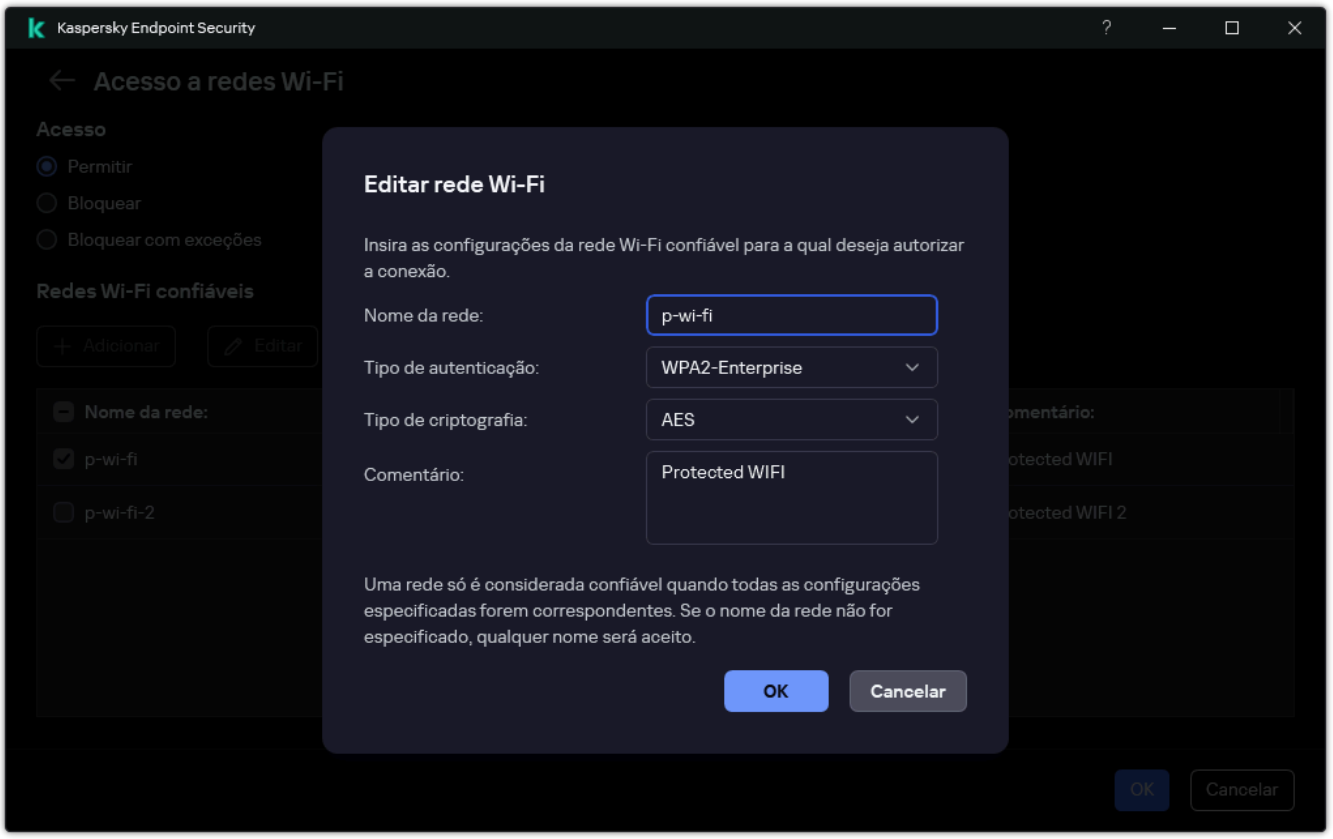
     > A partir do Kaspersky Endpoint Security for Windows versão 12.0, o suporte ao protocolo WPA3 passou a ser adicionado ao aplicativo. Se uma política do Kaspersky Endpoint Security versão 12.2 for aplicada em um computador, o protocolo WPA2 será selecionado nos computadores com o Kaspersky Endpoint Security versão 11.11.0 e anteriores; o WPA2/WPA3 será selecionado para as versões 12.0 a 12.1; e o WPA3 será selecionado para as versões 12.2 e posteriores.

   - **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.

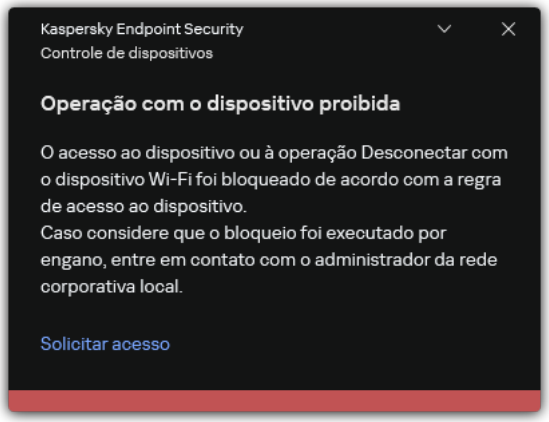
   > Uma rede Wi-Fi será considerada confiável se as suas configurações coincidirem com todas as configurações especificadas na regra.

7. Salvar alterações.



Configurações da rede Wi-Fi confiável

Assim, quando um usuário tenta se conectar a uma rede Wi-Fi não listada como confiável, o aplicativo bloqueia a conexão e exibe uma notificação (veja a figura abaixo).



Notificação do Controle de Dispositivos

Monitorar o uso de unidades removíveis

O monitoramento do uso de unidades removíveis inclui:

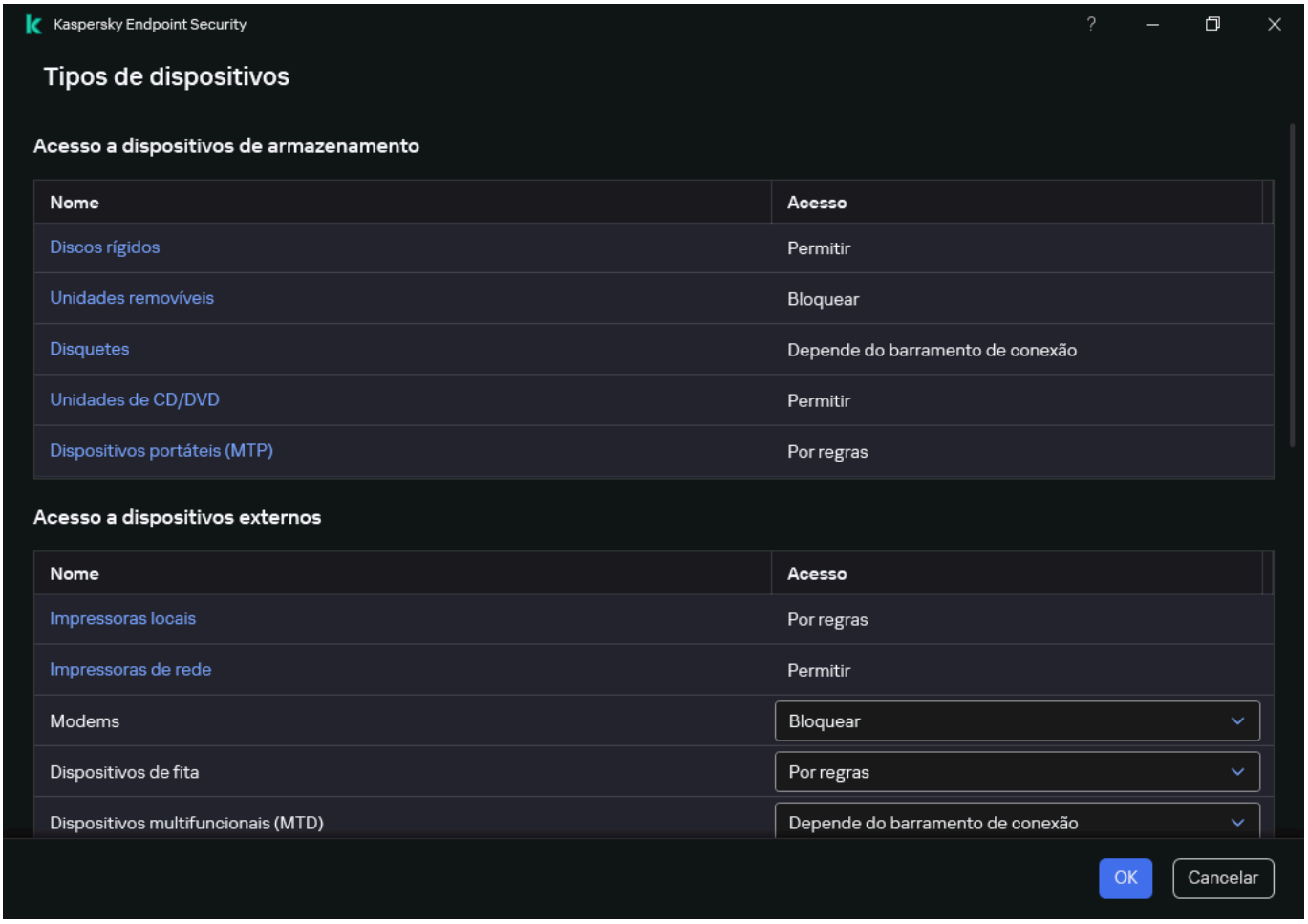
- Monitoramento das operações em arquivos em unidades removíveis.
- Monitoramento da conexão e desconexão de unidades removíveis confiáveis.

  O Kaspersky Endpoint 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 *Mensagem informativa*.

Para habilitar o monitoramento do uso da unidade removível:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de dispositivos**.
3. No bloco **Acessar as configurações**, clique no botão **Dispositivos e redes Wi-Fi**.

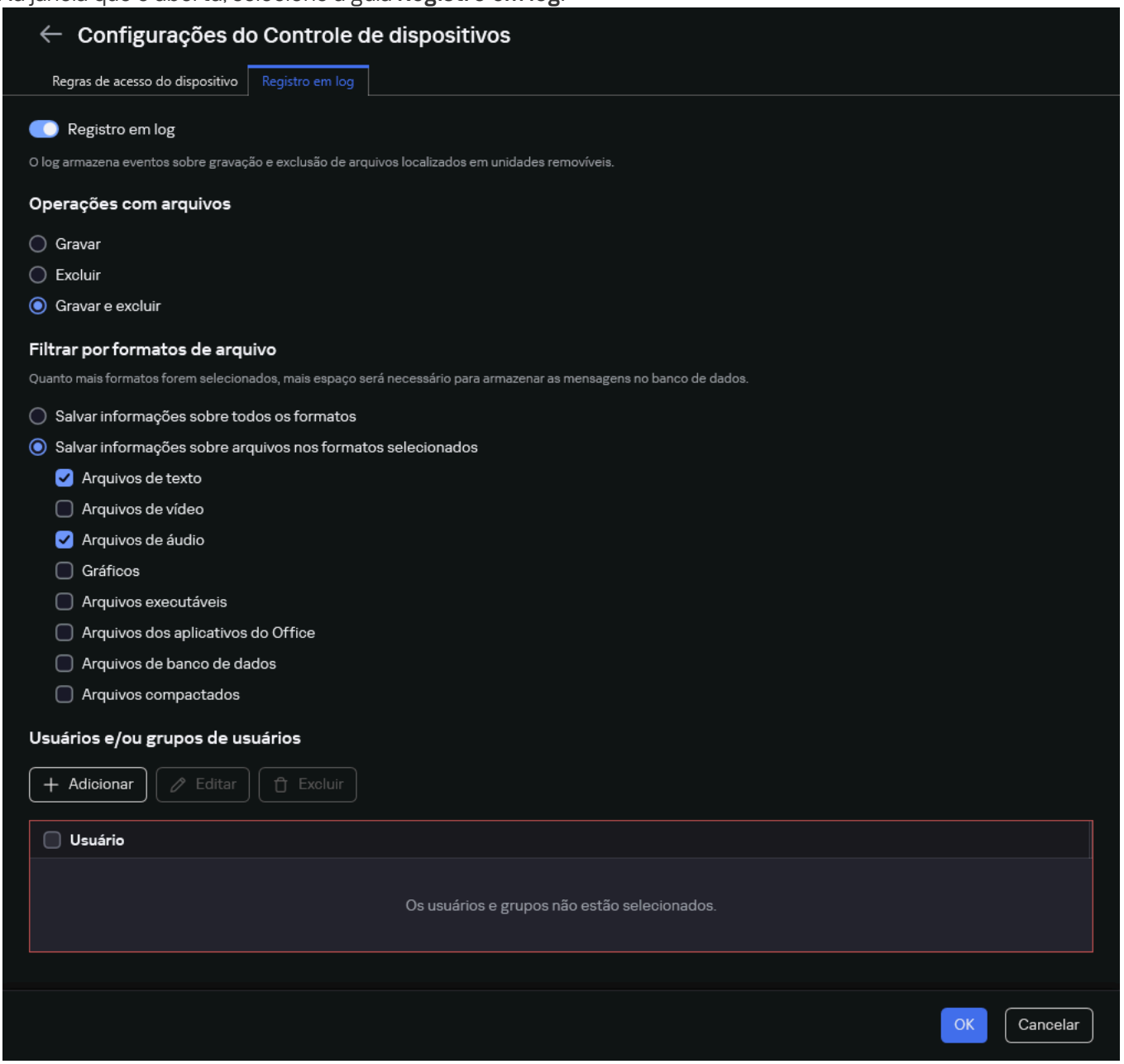
A janela aberta exibe as regras de acesso para todos os dispositivos incluídos na classificação do componente de Controle de Dispositivos.



Tipos de dispositivos no componente Controle de Dispositivos

4. No bloco **Acesso a dispositivos de armazenamento**, selecione **Unidades removíveis**.

5. Na janela que é aberta, selecione a guia **Registro em log**.



As configurações de monitoramento de uso de unidade removível

6. Ative o botão de alternância **Registro em log**.

7. Na seção **Operações com arquivos**, selecione as operações que deseja monitorar: **Gravar**, **Excluir**.

8. Na seção **Filtrar por formatos de arquivo**, selecione os formatos de arquivos cujas operações associadas devem ser registradas pelo Controle de Dispositivos.

9. Selecione os usuários ou grupo de usuários cujo uso de unidades removíveis você deseja monitorar.

10. Salvar alterações.

Como resultado, quando os usuários gravam em arquivos localizados em unidades removíveis ou excluem arquivos de unidades removíveis, o Kaspersky Endpoint Security salva as informações sobre tais operações no log de eventos e envia os eventos para o Kaspersky Security Center. Você pode exibir eventos associados com arquivos em unidades removíveis no Console de Administração do Kaspersky Security Center na área de trabalho do nó **Servidor de Administração** na guia **Eventos**. Para que os eventos sejam exibidos no log de eventos do Kaspersky Endpoint Security local, é necessário marcar a caixa de seleção **Operação com arquivo realizada** nas configurações de notificações para o componente Controle de Dispositivos.

Alterar a duração do armazenamento em cache

O componente Controle de Dispositivos registra eventos relacionados aos dispositivos monitorados, como conexão e desconexão de um dispositivo, leitura de um arquivo de um dispositivo, gravação de um arquivo em um dispositivo e outros eventos. O Controle de Dispositivos permite ou bloqueia a ação de acordo com as configurações do Kaspersky Endpoint Security.

O Controle de Dispositivos salva informações sobre eventos por um período específico de tempo denominado *período de armazenamento em cache*. Se as informações sobre um evento forem armazenadas em cache e este evento for repetido, não há necessidade de notificar o Kaspersky Endpoint Security sobre isso ou de pedir novamente para conceder acesso à ação correspondente, como conectar um dispositivo. Isso torna mais conveniente trabalhar com um dispositivo.

Um evento é considerado um evento duplicado se todas as configurações de evento a seguir corresponderem ao registro no cache:

- ID do dispositivo
- SID da conta do usuário tentando acessar
- Categoria do dispositivo
- Ação realizada com o dispositivo
- Permissão do aplicativo para esta ação: permitido ou negado
- Caminho para o processo usado para realizar a ação
- Arquivo que está sendo acessado

Antes de alterar o período de armazenamento em cache, desative a Autodefesa do Kaspersky Endpoint Security. Depois de alterar o período de armazenamento em cache, ative a Autodefesa.

Para alterar o período de armazenamento em cache:

1. Abra o editor de registro no computador.
2. No editor de registro, vá para a seguinte seção:
   - Para sistemas operacionais de 64 bits:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES.14.2\environment`
   - Para sistemas operacionais de 32 bits:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\environment]`
3. Abra `DeviceControlEventsCachePeriod` para edição.
4. Defina o número de minutos que o Controle de Dispositivos deve salvar informações sobre um evento antes que essas informações sejam excluídas.

Ações com 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.

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 5000 dispositivos confiáveis, pois isso pode causar instabilidade no sistema.

O Kaspersky Endpoint Security permite adicionar um dispositivo à lista confiável das seguintes maneiras:

- Se o Kaspersky Security Center não estiver implantado na sua organização, você poderá conectar o dispositivo ao computador e adicioná-lo à lista de confiáveis nas configurações do aplicativo. Para distribuir a lista de dispositivos confiáveis para todos os computadores da sua organização, você pode ativar a mesclagem de listas de dispositivos confiáveis em uma política ou usar o procedimento de exportação/importação.

- Se o Kaspersky Security Center estiver implantado em sua organização, você poderá detectar todos os dispositivos conectados remotamente e criar uma lista de dispositivos confiáveis na política. A lista de dispositivos confiáveis estará disponível em todos os computadores aos quais a diretiva é aplicada.

O Kaspersky Endpoint Security permite controlar o uso de dispositivos confiáveis (conexão e desconexão). É possível ativar o login de eventos configurações de notificação para o componente de Controle de Dispositivos. Os eventos têm o nível de gravidade *Mensagens informativas*.

Adicionar um dispositivo à lista de confiáveis

O Kaspersky Security Center recebe informações sobre os dispositivos se o Kaspersky Endpoint Security estiver instalado nos computadores, o Controle de Dispositivos estiver ativado e a transmissão de dados do dispositivo estiver ativada. Não é possível adicionar um dispositivo à lista confiável, a menos que as informações sobre esse dispositivo estejam disponíveis no Kaspersky Security Center.

Por padrão, quando um dispositivo é adicionado à lista de dispositivos confiáveis, o acesso a este é concedido a todos os usuários (ao grupo Todos os usuários).

Você pode adicionar um dispositivo à lista confiável de acordo com os seguintes dados:

- **Dispositivos por ID**. Cada dispositivo possui um identificador exclusivo (Hardware ID ou HWID). É possível visualizar o ID nas propriedades do dispositivo usando ferramentas do sistema operacional. Exemplo de ID de dispositivo: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Adicionar dispositivos por ID é conveniente se você deseja adicionar vários dispositivos específicos.

- **Dispositivos por modelo**. Cada dispositivo tem um Vendor ID (VID) e um Product ID (PID). É possível visualizar os IDs nas propriedades do dispositivo usando ferramentas do sistema operacional. Modelo para inserir o VID e o PID: `VID_1234&PID_5678`. Adicionar dispositivos por modelo é conveniente se você usar dispositivos de um determinado modelo em sua empresa. Dessa forma, você pode adicionar todos os dispositivos deste modelo.

- **Dispositivos por máscara de ID**. Se você estiver usando vários dispositivos com IDs semelhantes, poderá adicionar dispositivos à lista confiável usando máscaras. O caractere `*` substitui qualquer conjunto de caracteres. O Kaspersky Endpoint Security não suporta o caractere `?` ao inserir uma máscara. Por exemplo, `WDC_C*`.

- **Dispositivos por modelo de máscara**. Se você estiver usando vários dispositivos com VIDs ou PIDs semelhantes (por exemplo, dispositivos do mesmo fabricante), poderá adicionar dispositivos à lista confiável usando máscaras. O caractere `*` substitui qualquer conjunto de caracteres. O Kaspersky Endpoint Security não suporta o caractere `?` ao inserir uma máscara. Por exemplo, `VID_05AC&PID_*`.

Como adicionar um dispositivo à lista confiável no Console de Administração (MMC)

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

2. Na árvore do console, selecione **Políticas**.

3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

4. Na janela da política, selecione **Controles de Segurança** → **Controle de dispositivos**.

5. Na parte direita da janela, selecione a guia **Dispositivos confiáveis**.

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.

8. Para filtrar dispositivos, selecione um tipo de dispositivo na lista suspensa **Tipo do dispositivo** (por exemplo, **Unidades removíveis**).

   O Kaspersky Endpoint Security não é compatível com a adição de dispositivos do tipo **Disquetes** na lista de dispositivos confiáveis.

9. No campo **Nome / Modelo**, insira o ID do dispositivo, modelo (VID e PID) ou máscara, dependendo do método de adição selecionado.

   A adição de dispositivos por máscara do modelo (VID e PID) funciona da seguinte forma: se você inserir uma máscara de modelo que não corresponda a nenhum modelo, a Kaspersky Endpoint Security verifica se o ID do dispositivo (HWID) corresponde à máscara. O Kaspersky Endpoint Security verifica apenas a parte da ID do dispositivo que determina o fabricante e o tipo do dispositivo (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Se a máscara do modelo correspondente a esta parte do ID do dispositivo, os dispositivos que corresponderem à máscara serão adicionados à lista de dispositivos confiáveis no computador. Ao mesmo tempo, a lista de dispositivos no Kaspersky Security Center permanece vazia quando você clica no botão **Efetuar upgrade**. Para exibir a lista de dispositivos corretamente, você pode adicionar dispositivos por máscara de identificação do dispositivo.

10. Para filtrar dispositivos, no campo **Computador**, digite o nome do computador ou uma máscara para o nome do computador ao qual o dispositivo está conectado.

    O caractere `*` substitui qualquer conjunto de caracteres. O caractere `?` substitui qualquer caractere único.

11. Clique **Efetuar upgrade**.

    A tabela exibe uma lista de dispositivos que atendem aos critérios de filtragem definidos.

12. Marque as caixas de seleção próximas aos nomes dos dispositivos que deseja adicionar à lista de dispositivos confiáveis.

13. No campo **Comentário**, insira uma descrição do motivo da adição de dispositivos à lista confiável.

14. Clique no botão **Selecionar**, à direita do campo **Permitido a usuários e/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.

    Por padrão, o acesso a dispositivos confiáveis é permitido para o grupo Todos.

15. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como adicionar um dispositivo à lista confiável na Web Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Ir para a seção **Zona Confiável**.

5. Na janela aberta, clique no link **Dispositivos**.

   Essa ação abre uma janela que contém uma lista de dispositivos confiáveis.

6. Na parte direita da janela, selecione a guia **Dispositivos confiáveis**.

7. 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.

8. Clique **Adicionar**.

   Essa ação abre o formulário para adicionar um dispositivo confiável.

9. Em **Usuário ou grupo**, selecione os usuários aos quais você deseja permitir o acesso a dispositivos confiáveis.

   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.

   Por padrão, o acesso a dispositivos confiáveis é permitido para o grupo Todos.

10. Para filtrar dispositivos, selecione um tipo de dispositivo na lista suspensa **Tipo do dispositivo** (por exemplo, **Unidades removíveis**).

    O Kaspersky Endpoint Security não é compatível com a adição de dispositivos do tipo **Disquetes** na lista de dispositivos confiáveis.

11. Se você não souber o ID exato ou o modelo do dispositivo, marque a caixa de seleção **Usar máscara**.

12. Selecione como deseja adicionar o dispositivo: por ID do dispositivo ou por modelo (VID e PID).

    A adição de dispositivos por máscara do modelo (VID e PID) funciona da seguinte forma: se você inserir uma máscara de modelo que não corresponda a nenhum modelo, a Kaspersky Endpoint Security verifica se o ID do dispositivo (HWID) corresponde à máscara. O Kaspersky Endpoint Security verifica apenas a parte da ID do dispositivo que determina o fabricante e o tipo do dispositivo (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Se a máscara do modelo correspondente a esta parte do ID do dispositivo, os dispositivos que corresponderem à máscara serão adicionados à lista de dispositivos confiáveis no computador. Ao mesmo tempo, a lista vazia de dispositivos será exibida no Kaspersky Security Center. Para exibir a lista de dispositivos corretamente, você pode adicionar dispositivos por máscara de identificação do dispositivo.

13. Para filtrar dispositivos, no campo **Pesquisar dispositivos confiáveis**, digite o nome do computador ou uma máscara para o nome do computador ao qual o dispositivo está conectado.

    O caractere `*` substitui qualquer conjunto de caracteres. O caractere `?` substitui qualquer caractere único.

    A tabela exibe uma lista de dispositivos que atendem aos critérios de filtragem definidos.

14. Marque as caixas de seleção próximas aos nomes dos dispositivos que deseja adicionar à lista de dispositivos confiáveis.

15. No campo **Comentário**, insira uma descrição do motivo da adição de dispositivos à lista confiável.

16. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como adicionar um dispositivo à lista confiável a partir da interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de dispositivos**.
3. No bloco **Acessar as configurações**, clique no botão **Dispositivos confiáveis**.

   A lista de dispositivos confiáveis é aberta.
4. Clique **Selecionar**.

   Abrirá a lista de dispositivos conectados. A lista de dispositivos depende do valor que é selecionado na lista suspensa **Exibir dispositivos conectados**.
5. Na lista de dispositivos, selecione o dispositivo que deseja adicionar à lista confiável.

   > O Kaspersky Endpoint Security não é compatível com a adição de dispositivos do tipo **Disquetes** na lista de dispositivos confiáveis.
6. No campo **Comentário**, você pode fornecer qualquer informação relevante sobre o dispositivo confiável.
7. Selecione os usuários ou grupos de usuários para os quais deseja permitir o acesso aos dispositivos confiáveis.

   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.
8. Salvar alterações.

Quando um dispositivo está conectado, o Kaspersky Endpoint Security verifica a lista de dispositivos confiáveis para um usuário autorizado. Se o dispositivo for confiável, o Kaspersky Endpoint Security permitirá acesso ao dispositivo com todas as permissões, mesmo se o acesso ao tipo de dispositivo ou barramento de conexão for negado. Se o dispositivo não for confiável e o acesso for negado, você poderá solicitar acesso ao dispositivo bloqueado.

Exportação e importação da lista de dispositivos confiáveis

Para distribuir a lista de dispositivos confiáveis para todos os computadores da organização, você pode usar o procedimento de exportação/importação.

Por exemplo, se você precisar distribuir uma lista de unidades removíveis confiáveis, faça o seguinte:

1. Conecte as unidades removíveis em seqüência ao seu computador.
2. Nas configurações do Kaspersky Endpoint Security, adicione as unidades removíveis à lista confiável. Se necessário, configure as permissões de acesso do usuário. Por exemplo, permita que apenas administradores acessem as unidades removíveis.
3. Exporte a lista de dispositivos confiáveis nas configurações do Kaspersky Endpoint Security (consulte as instruções abaixo).

4. Distribua o arquivo da lista de dispositivos confiáveis para outros computadores em sua organização. Por exemplo, coloque o arquivo em uma pasta compartilhada.

5. Importe a lista de dispositivos confiáveis nas configurações do Kaspersky Endpoint Security em outros computadores da organização (consulte as instruções abaixo).

Para importar ou exportar a lista de dispositivos confiáveis:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de dispositivos**.

3. No bloco **Acessar as configurações**, clique no botão **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 **Exportar**.

   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 Endpoint Security exporta toda a lista de dispositivos confiáveis para o arquivo XML.

5. Para importar a lista de dispositivos confiáveis:

   a. Selecione a ação desejada na lista suspensa **Importar**: **Importar e adicionar aos existentes** ou **Importar e substituir existentes**.

   b. Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de dispositivos confiáveis.

   c. Abra o arquivo.

6. Salvar alterações.

Quando um dispositivo está conectado, o Kaspersky Endpoint Security verifica a lista de dispositivos confiáveis para um usuário autorizado. Se o dispositivo for confiável, o Kaspersky Endpoint Security permitirá acesso ao dispositivo com todas as permissões, mesmo se o acesso ao tipo de dispositivo ou barramento de conexão for negado.

Obter acesso a um dispositivo bloqueado

Ao configurar o Controle de Dispositivos, você pode bloquear acidentalmente o acesso a um dispositivo necessário para o trabalho.

Se o Kaspersky Security Center não estiver implantado em sua organização, você poderá fornecer acesso a um dispositivo nas configurações do Kaspersky Endpoint Security. Por exemplo, você pode adicionar o dispositivo à lista confiável ou desabilitar o Controle de Dispositivos temporariamente.

Se o Kaspersky Security Center estiver implantado em sua organização e uma política tiver sido aplicada a computadores, você poderá fornecer acesso a um dispositivo no Console de Administração.

Modo online para conceder acesso

Só é possível conceder acesso a um dispositivo bloqueado no modo on-line se o Kaspersky Security Center estiver implantado na organização e uma política tiver sido aplicada ao computador. O computador deve ter a capacidade de estabelecer uma conexão com o Servidor de Administração.

A concessão de acesso no modo online consiste das seguintes etapas:

1. O usuário envia ao administrador uma mensagem contendo uma solicitação de acesso.
2. O administrador recebe uma mensagem com a solicitação no console do Kaspersky Security Center.

   O console do Kaspersky Security Center tem uma seleção de eventos predefinida *Pedidos de usuário* para o fácil rastreamento de mensagens de usuários.
3. O administrador adiciona o dispositivo à lista confiável.

   Você pode adicionar um dispositivo confiável em uma política para o grupo de administração ou nas configurações locais do aplicativo para um computador individual.
4. O administrador atualiza as configurações do Kaspersky Endpoint Security no computador do usuário.

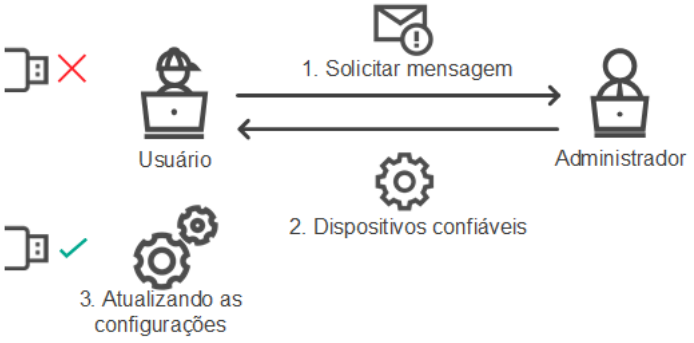


Diagrama esquemático para permitir acesso a um dispositivo no modo online

Modo offline para conceder acesso

Só é possível conceder acesso a um dispositivo bloqueado no modo offline se o Kaspersky Security Center estiver implantado na organização e uma política tiver sido aplicada ao computador. Nas configurações de política, na seção **Controle de dispositivos**, a caixa de seleção **Permitir solicitações de acesso temporário** deve estar selecionada.

Se você precisar conceder acesso temporário a um dispositivo bloqueado, mas não puder adicionar o dispositivo à lista confiável, você pode conceder acesso ao dispositivo no modo offline. Dessa forma, você pode conceder acesso a um dispositivo bloqueado mesmo se o computador não tiver acesso à rede ou se o computador estiver fora da rede corporativa.

A concessão de acesso no modo offline consiste das seguintes etapas:

1. O usuário cria um arquivo de solicitação de acesso e o envia ao administrador.
2. O administrador cria uma chave de acesso a partir do arquivo de solicitação de acesso e a envia ao usuário.
3. O usuário ativa a chave de acesso.

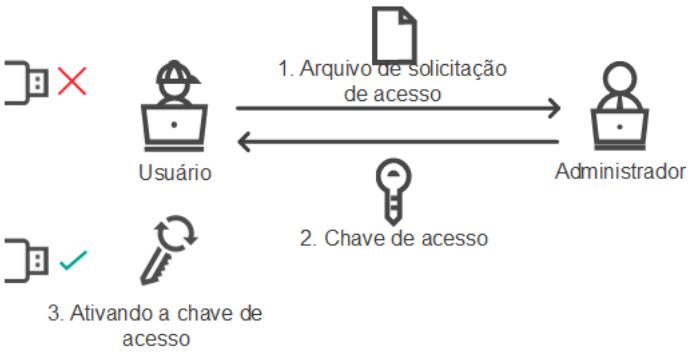


Diagrama esquemático para permitir acesso a um dispositivo no modo offline

Modo online para conceder acesso

Só é possível conceder acesso a um dispositivo bloqueado no modo on-line se o Kaspersky Security Center estiver implantado na organização e uma política tiver sido aplicada ao computador. O computador deve ter a capacidade de estabelecer uma conexão com o Servidor de Administração.

Um usuário solicita acesso a um dispositivo bloqueado da seguinte forma:

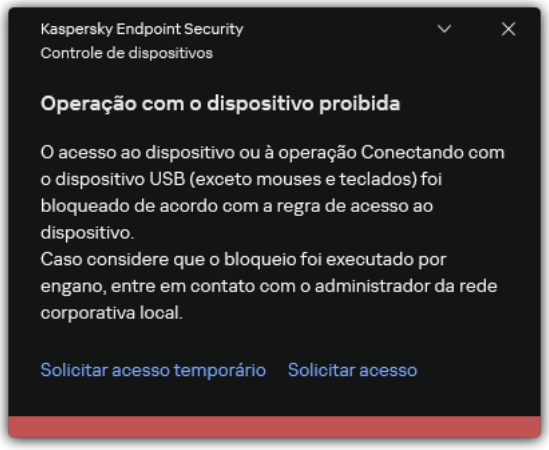
1. Conecte o dispositivo ao computador.

   O Kaspersky Endpoint Security exibirá uma notificação informando que o acesso ao dispositivo está bloqueado (consulte a figura abaixo).

2. Clique no link **Solicitar acesso**.

   Uma janela com uma mensagem para o administrador é aberta. Esta mensagem contém informações sobre o dispositivo bloqueado.

3. Clique **Enviar**.



Notificação do Controle de Dispositivos

Em seguida, o administrador no console do Kaspersky Security Center recebe o evento *Mensagem de bloqueio de acesso ao dispositivo para o administrador*. O evento inclui o nome de usuário, o nome do computador, os detalhes do dispositivo a que o usuário está tentando obter acesso e outras informações. É possível configurar como o administrador é notificado sobre esses eventos e, por exemplo, selecionar notificações por e-mail. O console do Kaspersky Security Center tem uma seleção de eventos predefinida *Pedidos de usuário* para o fácil rastreamento de mensagens de usuários.

Para permitir o acesso, é necessário adicionar o dispositivo na lista confiável. Após atualizar as configurações do Kaspersky Endpoint Security no computador, o usuário pode obter acesso ao dispositivo.

Modo offline para conceder acesso

Só é possível conceder acesso a um dispositivo bloqueado no modo offline se o Kaspersky Security Center estiver implantado na organização e uma política tiver sido aplicada ao computador. Nas configurações de política, na seção **Controle de dispositivos**, a caixa de seleção **Permitir solicitações de acesso temporário** deve estar selecionada.

Um usuário solicita acesso a um dispositivo bloqueado da seguinte forma:

1. Conecte o dispositivo ao computador.

   O Kaspersky Endpoint Security exibirá uma notificação informando que o acesso ao dispositivo está bloqueado (consulte a figura abaixo).

2. Clique no link **Solicitar acesso temporário**.

   Uma janela com uma lista de dispositivos conectados será aberta.

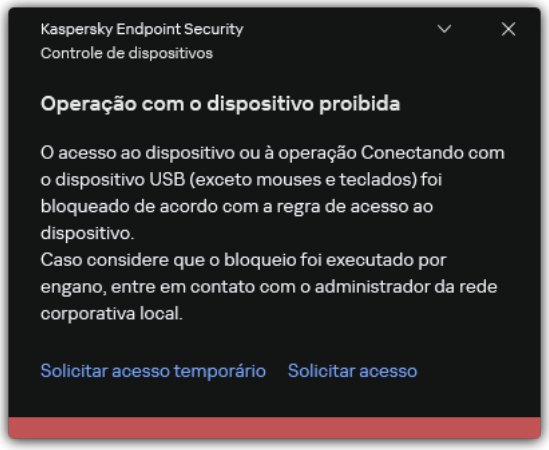
3. A partir da lista de dispositivos conectados, selecione o dispositivo que você deseja acessar.

4. Clique **Gerar arquivo de solicitação de acesso**.

5. No campo **Duração do acesso**, especifique o intervalo de tempo em que você deseja ter acesso ao dispositivo.

6. Salve o arquivo na memória do computador.

   Como resultado, será feito o download de um arquivo de solicitação de acesso com a extensão *.akey para a memória do computador. Use qualquer método disponível para enviar o arquivo de solicitação de acesso ao dispositivo ao administrador de rede local corporativa.



Notificação do Controle de Dispositivos

Como o administrador pode criar uma chave de acesso para o dispositivo bloqueado no Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração a que o computador cliente em questão pertence.
3. No espaço de trabalho, selecione a guia **Dispositivos**.
4. Na lista de computadores clientes, selecione o computador do usuário que precisa de permissão temporária de acesso ao dispositivo bloqueado.
5. No menu de contexto do computador, selecione o item **Conceder acesso no modo off-line**.
6. Uma janela será aberta; nessa janela, selecione a guia **Controle de dispositivos**.
7. Clique no botão **Procurar** e faça o download do arquivo de solicitação de acesso recebido do usuário.

   Você verá informações sobre o dispositivo bloqueado ao qual o usuário solicitou acesso.
8. Se necessário, altere o valor de configuração da **Duração do acesso**.

   Por padrão, a configuração **Duração do acesso** assume o valor indicado pelo usuário ao criar o arquivo de solicitação de acesso.
9. Especifique o valor para a configuração **Ativado por**.

   Essa configuração define o período durante o qual o usuário pode ativar o acesso para o dispositivo bloqueado com uma chave de acesso fornecida.
10. Salve o arquivo de chave de acesso na memória do computador.

Como o administrador pode criar uma chave de acesso para o dispositivo bloqueado no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Ativos (dispositivos)**.
2. Na lista de computadores clientes, selecione o computador do usuário que precisa de permissão temporária de acesso ao dispositivo bloqueado.
3. Clique no botão de reticências (**...**) acima da lista de computadores e, então, no botão **Permitir acesso ao dispositivo em modo offline**.
4. Na janela exibida, selecione a seção **Controle de dispositivos**.
5. Clique no botão **Visão Geral** e faça o download do arquivo de solicitação de acesso recebido do usuário.

   Você verá informações sobre o dispositivo bloqueado ao qual o usuário solicitou acesso.
6. Se necessário, altere o valor de configuração da **Duração do acesso (horas)**.

   Por padrão, a configuração **Duração do acesso (horas)** assume o valor indicado pelo usuário ao criar o arquivo de solicitação de acesso.

7. Especifique o período de tempo durante o qual a chave de acesso pode ser ativada no dispositivo.

   Essa configuração define o período durante o qual o usuário pode ativar o acesso para o dispositivo bloqueado com uma chave de acesso fornecida.

8. Salve o arquivo de chave de acesso na memória do computador.

Como resultado, será feito o download da chave de acesso ao dispositivo bloqueado para a memória do computador. Um arquivo de chave de acesso tem a extensão *.acode. Use qualquer método disponível para enviar a chave de acesso do dispositivo bloqueado ao usuário.

O usuário ativa a chave de acesso da seguinte maneira:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de dispositivos**.

3. No bloco **Solicitação de acesso**, clique no botão **Solicitar acesso ao dispositivo**.

4. Na janela que é aberta, clique no botão **Ativar chave de acesso**.

5. Na janela que é aberta, selecione o arquivo com a chave de acesso do dispositivo recebida do administrador da rede local corporativa.

   Isso abre uma janela contendo informações sobre a provisão de acesso.

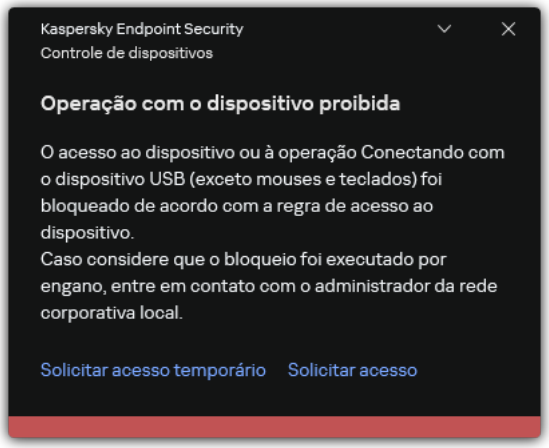
6. Clique **OK**.

Como resultado, o usuário recebe acesso ao dispositivo pelo período definido pelo administrador. O usuário recebe o conjunto completo de direitos para acessar o dispositivo (leitura e gravação). Quando a chave expirar, o acesso ao dispositivo será bloqueado. Se o usuário necessitar de acesso permanente ao dispositivo, adicione-o à lista confiável.

Editar os modelos de mensagens do Controle de Dispositivo

Quando o usuário tenta obter acesso a um dispositivo bloqueado, o Kaspersky Endpoint Security exibe uma mensagem informando que o acesso ao dispositivo está bloqueado ou que a execução com o conteúdo do dispositivo não é permitida. Os especialistas da Kaspersky fornecem um modelo de mensagem ao usuário que descreve os motivos pelos quais o acesso ao dispositivo foi bloqueado (veja a figura abaixo).

Variáveis especiais são fornecidas para gerenciar o modelo de mensagem (por exemplo, `%USER_NAME%`). As variáveis permitem que um mesmo modelo de mensagem seja utilizado em diferentes computadores. Ao criar uma mensagem, o Kaspersky Endpoint Security obtém o valor da variável nas configurações do sistema operacional e o insere na mensagem referente ao computador, usuário e evento específicos.



Notificação do Controle de Dispositivos

Se o usuário acredita que o acesso ao dispositivo foi erroneamente bloqueado ou que uma operação com o conteúdo do dispositivo foi proibida por engano, o usuário pode enviar uma mensagem ao administrador de rede corporativa local clicando no link na mensagem exibida sobre a ação bloqueada. Para isso, o usuário deve clicar nos botões **Solicitar acesso** ou **Solicitar acesso temporário** e enviar uma mensagem ao administrador descrevendo a situação. Também é possível preparar um modelo da mensagem para o administrador ao adicionar nele os dados que podem informar sua decisão quanto à permissão ou bloqueio do acesso ao dispositivo. Depois que o usuário solicitar o acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio de acesso ao dispositivo para o administrador**. A descrição do evento contém uma mensagem ao administrador com variáveis substituídas. É possível visualizar esses eventos no console do Kaspersky Security Center com o uso da seleção de eventos predefinida **Pedidos de usuário**. Caso sua organização não tenha o Kaspersky Security Center implantado ou não haja conexão com o Servidor de Administração, o aplicativo enviará uma mensagem ao administrador para o endereço de e-mail especificado.

Como alterar os modelos de mensagem do Controle de Dispositivos no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Controles de Segurança** → **Controle de dispositivos**.

4. No bloco **Configurações de modelos de mensagem**, clique no botão **Modelos**.

5. Uma janela é aberta; nela, configure os modelos do Controle de Aplicativos:

   - **Mensagem sobre bloqueio**. Modelo da mensagem que é exibida quando um usuário tenta acessar um dispositivo bloqueado. Essa mensagem também é exibida quando um usuário tenta executar uma operação no conteúdo do dispositivo que foi bloqueado para esse usuário.

   - **Mensagem para o administrador**. Um modelo da mensagem que é enviada ao administrador da rede local quando o usuário acredita que o acesso ao dispositivo está bloqueado ou uma operação com o conteúdo do dispositivo é proibida por engano.

   Para inserir uma variável no modelo, posicione o cursor onde necessário, clique em **Variável** e selecione a opção necessária na lista.

Você também pode restaurar o texto do modelo padrão.

6. Salvar alterações.

Como alterar os modelos de mensagem do Controle de Dispositivos no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Controle de dispositivos**.

5. No bloco **Modelos de mensagem**, configure modelos para mensagens de Controle de Aplicativos:

   - **Mensagem para o usuário**. Modelo da mensagem que é exibida quando um usuário tenta acessar um dispositivo bloqueado. Essa mensagem também é exibida quando um usuário tenta executar uma operação no conteúdo do dispositivo que foi bloqueado para esse usuário.

   - **Mensagem para o administrador**. Um modelo da mensagem que é enviada ao administrador da rede local quando o usuário acredita que o acesso ao dispositivo está bloqueado ou uma operação com o conteúdo do dispositivo é proibida por engano.

   Para inserir uma variável no modelo, posicione o cursor onde necessário, clique em **Adicionar variável** e selecione a opção necessária na lista.

   Você também pode restaurar o texto do modelo padrão.

6. Salvar alterações.

Como alterar os modelos de mensagem do Controle de Dispositivos na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de aplicativos**.

3. No bloco **Modelos de mensagem**, configure modelos para mensagens de Controle de Aplicativos:

   - **Mensagem sobre bloqueio**. Modelo da mensagem que é exibida quando um usuário tenta acessar um dispositivo bloqueado. Essa mensagem também é exibida quando um usuário tenta executar uma operação no conteúdo do dispositivo que foi bloqueado para esse usuário.

   - **Mensagem para o administrador**. Um modelo da mensagem que é enviada ao administrador da rede local quando o usuário acredita que o acesso ao dispositivo está bloqueado ou uma operação com o conteúdo do dispositivo é proibida por engano.

   Para inserir uma variável no modelo, posicione o cursor onde necessário, clique em **Adicionar variável** e selecione a opção necessária na lista.

   Você também pode restaurar o texto do modelo padrão.

4. Salvar alterações.

Antibridging

O antibridging inibe a criação de pontes de rede, impedindo o estabelecimento simultâneo de várias conexões de rede para um computador. Isso permite que você proteja uma rede corporativa de ataques a redes não protegidas e não autorizadas.

O antibridging regula o estabelecimento de conexões de rede usando *regras de conexão*.

As regras de conexão são criadas para os seguintes tipos predefinidos de dispositivos:

- Adaptadores de rede;
- Adaptadores de Wi-Fi;
- Modems.

Se uma regra de conexão for ativada, o Kaspersky Endpoint Security:

- Bloqueia a conexão ativa ao estabelecer uma nova conexão caso o tipo de dispositivo especificado na regra seja usado para ambas as conexões;
- Bloqueia as conexões estabelecidas usando os tipos de dispositivos nos quais regras de baixa prioridade são usadas.

Ativar o antibridging

O Antibridging é desativado por padrão.

Para ativar o Antibridging:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de dispositivos**.
3. No bloco **Acessar as configurações**, clique no botão **Antibridging**.
4. Use o botão de alternância **Ativar Antibridging** para ativar ou desativar esse recurso.
5. Salvar alterações.

Depois que o Antibridging é ativado, o Kaspersky Endpoint Security bloqueia conexões já estabelecidas, de acordo com as regras de conexão.

Mudar o status de uma regra de conexão

Para alterar o status de uma regra de conexão:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de dispositivos**.
3. No bloco **Acessar as configurações**, clique no botão **Antibridging**.
4. Na seção **Regras para dispositivos**, selecione a regra cujo status você deseja alterar.
5. Use os botões de alternância na coluna **Controle** para ativar ou desativar a regra.
6. Salvar alterações.

Alterar a prioridade de uma regra de conexão

Para alterar a prioridade de uma regra de conexão:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de dispositivos**.
3. No bloco **Acessar as configurações**, clique no botão **Antibridging**.
4. Na seção **Regras para dispositivos**, selecione a regra cuja prioridade você deseja alterar.
5. Use os botões **Acima**/**Abaixo** para definir a prioridade da regra de conexão.

   Quanto mais alta uma regra estiver na tabela de regras, maior será sua prioridade. O AntiBridging bloqueia todas as conexões, exceto uma conexão estabelecida usando o tipo do dispositivo para o qual a regra de prioridade mais alta é usada.
6. Salvar alterações.

Controle Adaptativo de Anomalias

O componente estará disponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para computadores pessoais. O componente estará indisponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para servidores.

O componente de Controle Adaptativo de Anomalias monitora e bloqueia ações suspeitas que não são típicas dos computadores em uma rede empresarial. O Controle Adaptativo de Anomalias usa um conjunto de regras para rastrear comportamentos incomuns (por exemplo, a regra *Inicialização do Microsoft PowerShell pelo aplicativo Office*). As regras são criadas pelos especialistas da Kaspersky com base em cenários típicos de atividade maliciosa. Você pode configurar como o Controle Adaptativo de Anomalias manipula cada regra e, por exemplo, permitir a execução de scripts do PowerShell que automatizam determinadas tarefas de fluxo de trabalho. Kaspersky Endpoint Security atualiza o conjunto de regras junto com os bancos de dados do aplicativo. As atualizações para os conjuntos de regras devem ser confirmadas manualmente.

Configurações de Controle Adaptativo de Anomalias

A configuração do controle Adaptativo de Anomalias adaptável consiste nas seguintes etapas:

1. Treinamento do Controle Adaptativo de Anomalias.

   Depois de ativar o Controle Adaptativo de Anomalias, suas regras funcionam *modo de treinamento*. Durante o treinamento, o Controle Adaptativo de Anomalias monitora o acionamento de regras e envia os eventos do Kaspersky Security Center. Cada regra tem sua própria duração do modo de treinamento. A duração do modo de treinamento é definida pelos especialistas da Kaspersky. Normalmente, o modo de treinamento é ativado por duas semanas.

   Se uma regra não foi acionada durante o treinamento, o Controle Adaptativo de Anomalias considerará as ações associadas a essa regra como incomuns. O Kaspersky Endpoint Security irá bloquear todas as ações associadas a essa regra.

   Caso uma regra tenha sido acionada durante o treinamento, o Kaspersky Endpoint Security registra os eventos no relatório de acionamento da regra e no repositório do **Acionadores de regra no estado de Treinamento inteligente**.

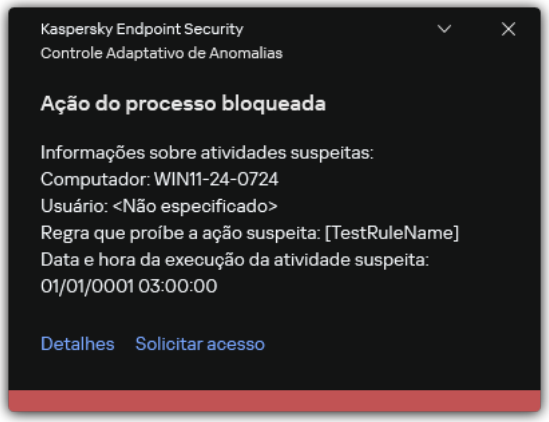
2. Analisando o relatório de acionamento de regras.

   O administrador analisa o relatório de acionamento de regra ou o conteúdo do repositório **Acionadores de regra no estado de Treinamento inteligente**. Em seguida, o administrador pode selecionar o comportamento do Controle Adaptativo de Anomalias quando a regra for acionada: bloquear ou permitir. O administrador também pode continuar a monitorar como a regra funciona e estender a duração do modo de treinamento. Se o administrador não realizar nenhuma ação, o aplicativo também continuará a funcionar no modo de treinamento. O período do modo de treinamento é reiniciado.

O Controle Adaptativo de Anomalias é configurado em tempo real por meio dos seguintes canais:

- O Controle Adaptativo de Anomalias inicia automaticamente o bloqueio das ações associadas às regras que nunca foram acionadas no modo de treinamento.
- O Kaspersky Endpoint Security adiciona novas regras ou remove as obsoletas.
- O administrador configura a operação do Controle Adaptativo de Anomalias após revisar o relatório de acionamento de regras e o conteúdo do repositório **Acionadores de regra no estado de Treinamento inteligente**. Recomendamos verificar o relatório sobre o acionamento de regras e o conteúdo do armazenamento **Acionadores de regra no estado de Treinamento inteligente**.

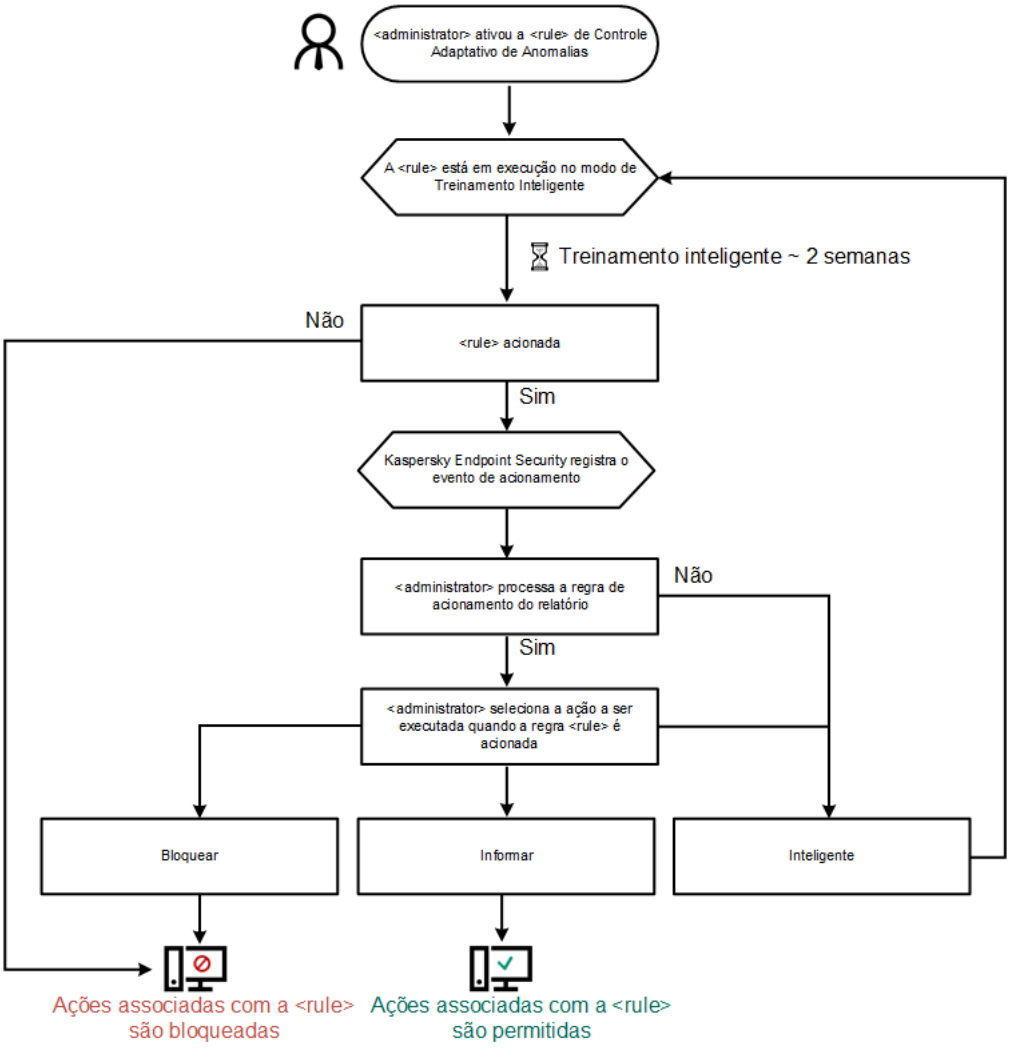
Quando um aplicativo malicioso tenta executar uma ação, o Kaspersky Endpoint Security bloqueia a ação e exibe uma notificação (veja a figura abaixo).



Notificações do Controle Adaptativo de Anomalias

Algoritmo operacional do Controle Adaptativo de Anomalias

O Kaspersky Endpoint Security decide se permite ou bloqueia uma ação associada a uma regra com base no algoritmo a seguir (veja a figura abaixo).



Algoritmo operacional do Controle Adaptativo de Anomalias

Treinamento do Controle Adaptativo de Anomalias

O Controle Adaptativo de Anomalias inclui um conjunto de regras (padrões de comportamento). Depois de ativar o Controle Adaptativo de Anomalias, suas regras funcionam *modo de treinamento*. Durante o treinamento, o Controle Adaptativo de Anomalias monitora o acionamento de regras e envia os eventos do Kaspersky Security Center. O Controle Adaptativo de Anomalias não bloqueia a atividade do aplicativo no computador, apenas informa o administrador. Também é possível fazer a seleção manual da ação que será executada quando uma regra de Controle Adaptativo de Anomalias for acionada.

Como exibir a lista de regras do Controle Adaptativo de Anomalias no Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Controles de segurança** → **Controle Adaptativo de Anomalias**.
5. Marque a caixa de seleção **Controle Adaptativo de Anomalias**.
6. Em **Configurações das regras do Controle Adaptativo de Anomalias**, consulte a lista de regras.

   Por padrão, todas as regras funcionam no modo **Inteligente**.
7. Se necessário, confirme a atualização da regra do Controle Adaptativo de Anomalias.
8. Se necessário, selecione uma ação quando uma regra do Controle Adaptativo de Anomalias for acionada:
   - **Bloquear**. Se esta ação for selecionada, quando uma Regra de Controle Adaptativo de Anomalias for acionada, o Kaspersky Endpoint Security bloqueará a atividade coberta pela regra e registrará uma entrada contendo as informações sobre a atividade.
   - **Informar**. Se esta ação for selecionada, quando uma Regra de Controle Adaptativo de Anomalias for acionada, o Kaspersky Endpoint Security permitirá a atividade coberta pela regra e registrará uma entrada contendo as informações sobre a atividade.
9. Se necessário, desative as regras que não deseje usar.
10. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como exibir as regras do Controle Adaptativo de Anomalias no Web Console e no Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Controles de segurança** → **Controle Adaptativo de Anomalias**.
5. Ative o botão de alternância **Controle Adaptativo de Anomalias ATIVADO**.

6. Em **Regras**, consulte a lista de regras.

   Por padrão, todas as regras funcionam no modo **Inteligente**.

7. Se necessário, confirme a atualização da regra do Controle Adaptativo de Anomalias.

8. Se necessário, selecione uma ação quando uma regra do Controle Adaptativo de Anomalias for acionada:

   - **Bloquear**. Se esta ação for selecionada, quando uma Regra de Controle Adaptativo de Anomalias for acionada, o Kaspersky Endpoint Security bloqueará a atividade coberta pela regra e registrará uma entrada contendo as informações sobre a atividade.

   - **Informar**. Se esta ação for selecionada, quando uma Regra de Controle Adaptativo de Anomalias for acionada, o Kaspersky Endpoint Security permitirá a atividade coberta pela regra e registrará uma entrada contendo as informações sobre a atividade.

9. Se necessário, desative as regras que não deseje usar.

10. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como exibir a lista de regras do Controle Adaptativo de Anomalias na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle Adaptativo de Anomalias**.

3. Ative o botão de alternância **Controle Adaptativo de Anomalias**.

4. No bloco **Regras**, clique no link **Editar regras**.

   A lista de regra de controle adaptativo de anomalias é aberta. Por padrão, todas as regras funcionam no modo **Inteligente**.

5. Se necessário, confirme a atualização da regra do Controle Adaptativo de Anomalias.

6. Se necessário, selecione uma ação quando uma regra do Controle Adaptativo de Anomalias for acionada:

   - **Bloquear**. Se esta ação for selecionada, quando uma Regra de Controle Adaptativo de Anomalias for acionada, o Kaspersky Endpoint Security bloqueará a atividade coberta pela regra e registrará uma entrada contendo as informações sobre a atividade.

   - **Informar**. Se esta ação for selecionada, quando uma Regra de Controle Adaptativo de Anomalias for acionada, o Kaspersky Endpoint Security permitirá a atividade coberta pela regra e registrará uma entrada contendo as informações sobre a atividade.

7. Se necessário, desative as regras que não deseje usar.

8. Salvar alterações.

Cada regra tem sua própria duração do modo de treinamento. A duração do modo de treinamento é definida pelos especialistas da Kaspersky. Normalmente, o modo de treinamento é ativado por duas semanas.

Se uma regra não for acionada nenhuma vez durante o treinamento, o Controle Adaptativo de Anomalias considera esse comportamento atípico e altera o status da regra para **Bloqueio inteligente**. No futuro, o aplicativo bloqueará qualquer atividade que corresponda a essa regra.

Se uma regra for acionada durante o treinamento, será necessário fazer a configuração manual da ação que o aplicativo deve aplicar à atividade detectada que corresponde a essa regra. Se não for selecionada uma ação para quando a regra é acionada, o Controle Adaptativo de Anomalias continuará no modo de treinamento.

Ativar e desativar uma regra de Controle Adaptativo de Anomalias

Para ativar ou desativar uma regra de Controle Adaptativo de Anomalias:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle Adaptativo de Anomalias**.
3. No bloco **Regras**, clique no botão **Editar regras**.

   A lista de regra de controle adaptativo de anomalias é aberta.
4. Na tabela, selecione um conjunto de regras (por exemplo, *Atividade de aplicativos do Office*) e expanda o conjunto.
5. Selecione uma regra (por exemplo, *Inicialização do Microsoft PowerShell pelo aplicativo Office*).
6. Use o botão de alternância na coluna **Estado** para ativar ou desativar a regra de controle adaptativo de anomalias.
7. Salvar alterações.

Modificar a ação executada quando uma regra de Controle Adaptativo de Anomalias é acionada

Para modificar a ação executada quando uma regra de Controle Adaptativo de Anomalias é acionada:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle Adaptativo de Anomalias**.
3. No bloco **Regras**, clique no botão **Editar regras**.

   A lista de regra de controle adaptativo de anomalias é aberta.
4. Selecione uma regra na tabela.
5. Clique **Editar**.

   A janela de propriedades da regra de controle adaptativo de anomalias é aberta.

6. No bloco **Ação**, escolha uma das seguintes opções:

   - **Inteligente**. Caso esta opção seja selecionada, a regra de Controle Adaptativo de Anomalias funcionará no estado de Treinamento inteligente durante um período de tempo definido pelos especialistas da Kaspersky. Nesse modo, quando uma regra de Controle Adaptativo de Anomalias for acionada, o Kaspersky Endpoint Security permite a atividade definida pela regra e registra uma entrada no armazenamento **Acionadores de regra no estado de Treinamento inteligente** do Servidor de Administração do Kaspersky Security Center. Quando o período para trabalhar no estado de Treinamento inteligente acaba, o Kaspersky Endpoint Security bloqueia a atividade contemplada por uma regra de controle adaptativo de anomalia e registra em evento uma entrada contendo informações sobre a atividade.

   - **Bloquear**. Se esta ação for selecionada, quando uma Regra de Controle Adaptativo de Anomalias for acionada, o Kaspersky Endpoint Security bloqueará a atividade coberta pela regra e registrará uma entrada contendo as informações sobre a atividade.

   - **Informar**. Se esta ação for selecionada, quando uma Regra de Controle Adaptativo de Anomalias for acionada, o Kaspersky Endpoint Security permitirá a atividade coberta pela regra e registrará uma entrada contendo as informações sobre a atividade.

7. Salvar alterações.

Criar uma exclusão para uma regra de Controle Adaptativo de Anomalias

> Você não pode criar mais de 1.000 exclusões da Regra de Controle Adaptativo de Anomalias. Não é recomendado criar mais de 200 exclusões. Para reduzir o número de exclusões usadas, recomenda-se usar máscaras nas configurações de exclusões.

Uma exclusão para regra de Controle Adaptativo de Anomalias inclui uma descrição dos objetos de origem e destino. O *objeto de origem* é aquele que executa as ações. O *objeto de destino* é aquele em que as ações estão sendo executadas. Por exemplo, você abriu um arquivo nomeado `file.xlsx`. Como resultado, um arquivo da biblioteca com a extensão DLL é carregado na memória do computador. Essa biblioteca é utilizada por um navegador (nome do arquivo executável `browser.exe`). Nesse exemplo, `file.xlsx` é o objeto de origem, Excel é o processo de origem, `browser.exe` é o arquivo de destino e Navegador é o processo de destino.

Para criar uma exclusão para uma regra de Controle Adaptativo de Anomalias:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle Adaptativo de Anomalias**.

3. No bloco **Regras**, clique no botão **Editar regras**.

   A lista de regra de controle adaptativo de anomalias é aberta.

4. Selecione uma regra na tabela.

5. Clique **Editar**.

   A janela de propriedades da regra de controle adaptativo de anomalias é aberta.

6. No bloco **Exclusões**, clique no botão **Adicionar**.

   A janela de propriedades de exclusão é exibida.

7. Selecione o usuário para o qual deseja configurar uma exclusão.

   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 Controle Adaptativo de Anomalias não é compatível com exclusões para grupo de usuários. Caso um grupo de usuário seja selecionado, o Kaspersky Endpoint Security não aplica a exclusão.

8. No campo **Descrição**, insira uma descrição da exclusão.

9. Definir as configurações do objeto de origem ou processo de origem iniciado pelo objeto:

   - **Processo de origem**. Caminho ou máscara do caminho até o arquivo ou a pasta que contém os arquivos (por exemplo, `C:\Dir\File.exe` ou `Dir\*.exe`).

   - **Hash do processo de origem**. Hash SHA256 do arquivo.

   - **Objeto de origem**. Caminho ou máscara do caminho até o arquivo ou a pasta que contém os arquivos (por exemplo, `C:\Dir\File.exe` ou `Dir\*.exe`). Por exemplo, o caminho do arquivo `document.docm`, que usa um script ou macro para iniciar os processos de destino.

     Você também pode especificar outros objetos a serem excluídos, como um endereço web, macro, comando na linha de comando, caminho de registro ou outros. Especifique o objeto de acordo com o seguinte modelo: `object://<object>`, em que `<object>` é o nome do objeto, por exemplo, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. Você também pode usar máscaras, por exemplo, `object://*C:\Windows\temp\*`.

   - **Hash do objeto de origem**. Hash SHA256 do arquivo.

   A regra de Controle Adaptativo de Anomalias não é aplicada a ações executadas pelo objeto ou a processos iniciados pelo objeto.

10. Especifique as configurações do objeto de destino ou processos de destino iniciados no objeto.

    - **Processo de destino**. Caminho ou máscara do caminho até o arquivo ou a pasta que contém os arquivos (por exemplo, `C:\Dir\File.exe` ou `Dir\*.exe`).

    - **Hash do processo de destino**. Hash SHA256 do arquivo.

    - **Objeto de destino**. O comando para iniciar o processo de destino. Especifique o comando usando o seguinte padrão `object://<command>`, por exemplo, `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`. Você também pode usar máscaras, por exemplo, `object://*C:\Windows\temp\*`.

    - **Hash do objeto de destino**. Hash SHA256 do arquivo.

    A regra de Controle Adaptativo de Anomalias não é aplicada a ações executadas no objeto ou nos processos iniciados no objeto.

11. Salvar alterações.

Exportar e importar exclusões para regras de controle adaptativo de anomalias

Para exportar ou importar a lista de exclusões para regras selecionadas:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle Adaptativo de Anomalias**.
3. No bloco **Regras**, clique no botão **Editar regras**.

   A lista de regra de controle adaptativo de anomalias é aberta.
4. Para exportar a lista de regras:

   a. Selecione as regras cujas exceções deseja exportar.

   b. Clique **Exportar**.

   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. Confirme que deseja exportar apenas as exclusões selecionadas ou exportar toda a lista de exclusões.

   e. Salvar o arquivo.
5. Para importar a lista de exclusões:

   a. Clique **Importar**.

   b. Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de exclusões.

   c. Abra o arquivo.

   Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.
6. Salvar alterações.

Aplicar atualizações das regras de Controle Adaptativo de Anomalias

As novas regras do Controle Adaptativo de Anomalias podem ser adicionadas à tabela de regras, e as regras existentes do Controle Adaptativo de Anomalias podem ser excluídas da tabela de regras quando os bancos de dados de antivírus forem atualizados. O Kaspersky Endpoint Security distingue as regras do Controle Adaptativo de Anomalias que devem ser excluídas ou adicionadas à tabela, se uma atualização dessas regras não tiver sido aplicada.

Até que a atualização seja aplicada, o Kaspersky Endpoint Security exibirá as regras de Controle Adaptativo de Anomalias definidas para serem excluídas pela atualização na tabela de regras e atribuirá o status *Desativado* a elas. Não é possível alterar as configurações dessas regras.

Para aplicar atualizações das regras do Controle Adaptativo de Anomalias:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle Adaptativo de Anomalias**.
3. No bloco **Regras**, clique no botão **Editar regras**.

   A lista de regra de controle adaptativo de anomalias é aberta.
4. Na janela que é aberta, clique no botão **Aprovar atualizações**.

   O botão **Aprovar atualizações** está disponível quando uma atualização das regras do Controle Adaptativo de Anomalias está disponível.
5. Salvar alterações.

Editar modelos de mensagem de Controle Adaptativo de Anomalias

Quando um usuário tenta fazer uma ação, bloqueada pelas regras de Controle Adaptativo de Anomalias, o Kaspersky Endpoint Security exibe uma mensagem de que as ações potencialmente perigosas estão bloqueadas. Caso o usuário considere que uma ação foi bloqueada por engano, ele poderá utilizar o link no texto da mensagem para enviar uma mensagem ao administrador da rede corporativa local.

Modelos especiais estão disponíveis para mensagens ao administrador referentes ao bloqueio de ações potencialmente perigosas. Variáveis especiais são fornecidas para gerenciar o modelo de mensagem (por exemplo, `%USER_NAME%`). As variáveis permitem que um mesmo modelo de mensagem seja utilizado em diferentes computadores. Ao criar uma mensagem, o Kaspersky Endpoint Security obtém o valor da variável nas configurações do sistema operacional e o insere na mensagem referente ao computador, usuário e evento específicos.

Para editar um modelo de mensagem:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle Adaptativo de Anomalias**.

3. Na seção **Modelos**, configure os modelos para mensagens de Controle Adaptativo de Anomalias:

   - **Mensagem sobre bloqueio**. Modelo da mensagem exibida a um usuário quando uma regra do Controle Adaptativo de Anomalias que bloqueia uma ação atípica é acionada.

   - **Mensagem para o administrador**. Modelo da mensagem que pode ser enviada por um usuário ao administrador da rede corporativa local se o usuário considerar o bloqueio como um erro. Depois que o usuário solicitar o acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio de atividade do aplicativo para o administrador**. A descrição do evento contém uma mensagem ao administrador com variáveis substituídas. É possível visualizar esses eventos no console do Kaspersky Security Center com o uso da seleção de eventos predefinida **Pedidos de usuário**. Caso sua organização não tenha o Kaspersky Security Center implantado ou não haja conexão com o Servidor de Administração, o aplicativo enviará uma mensagem ao administrador para o endereço de e-mail especificado.

   Para inserir uma variável no modelo, posicione o cursor onde necessário, clique em **Adicionar variável** e selecione a opção necessária na lista.

   Você também pode restaurar o texto original do modelo clicando no botão **Reiniciar**.

4. Salvar alterações.

Monitorando as operações do Controle Adaptativo de Anomalias

O Controle Adaptativo de Anomalias inclui várias ferramentas de monitoramento. O objetivo principal do monitoramento do Controle Adaptativo de Anomalias é configurar o componente durante o treinamento.

Relatórios do Controle Adaptativo de Anomalias

O Controle Adaptativo de Anomalias utiliza os seguintes relatórios:

- **Relatório sobre o estado das regras de Controle Adaptativo de Anomalias**. O relatório contém informações sobre o status das regras de Controle Adaptativo de Anomalias (*Desativado*, *Treinamento inteligente*, *Bloqueio inteligente*, *Notificar*, *Bloquear*). Esse relatório permite analisar o nível de treinamento do Controle Adaptativo de Anomalias e avaliar o número de regras cujo modo foi alterado de *Treinamento inteligente* para operação normal (por exemplo, *Bloqueio inteligente*).

- **Relatório sobre regras de Controle Adaptativo de Anomalias acionadas**. O relatório contém informações sobre acionadores de regras. O relatório também mostra o modo de acionamento da regra: *Bloquear* (incluindo *Bloqueio inteligente*) ou *Notificar*. Esse relatório permite avaliar a atividade do Controle Adaptativo de Anomalias nos computadores dos usuários.

Como exibir os relatórios do Controle Adaptativo de Anomalias no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Controles de Segurança** → **Controle Adaptativo de Anomalias**.
4. Realize uma das seguintes ações:
   - Caso queira visualizar o relatório sobre o estado das regras do Controle Adaptativo de Anomalias, clique em **Relatório sobre o estado das regras de Controle Adaptativo de Anomalias**.
   - Caso queira visualizar o relatório sobre regras de Controle Adaptativo de Anomalias acionadas, clique em **Relatório sobre regras de Controle Adaptativo de Anomalias acionadas**.
5. O processo de geração do relatório é iniciado.

O relatório é exibido em uma nova janela.

Como exibir relatórios do Controle Adaptativo de Anomalias no Web Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Controles de segurança** → **Controle Adaptativo de Anomalias**.
5. No bloco **Regras**, execute uma das seguintes ações:
   - Caso queira visualizar o relatório sobre o estado das regras de Controle Adaptativo de Anomalias, selecione **Visualizar relatório** → **Estado das regras**.
   - Caso queira visualizar o relatório sobre regras de Controle Adaptativo de Anomalias acionadas, clique em **Visualizar relatório** → **Detecções**.
6. O processo de geração do relatório é iniciado.

O relatório é exibido em uma nova janela.

Para gerar relatórios no console do Kaspersky Security Center, você deve ativar a transferência de dados para o Servidor de Administração. A transferência de dados é ativada por padrão.

Como ativar a transferência de dados do Controle Adaptativo de Anomalias para o Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Relatórios e Armazenamento**.
4. No bloco **Transferência de dados para o Servidor de Administração**, clique no botão **Configurações**.

5. Selecione as seguintes opções:

   - **Relatório sobre o estado das regras de Controle Adaptativo de Anomalias**.
   - **Relatório sobre regras de Controle Adaptativo de Anomalias acionadas**.

6. Salvar alterações.

Como ativar a transferência de dados para o Controle Adaptativo de Anomalias no Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Integração KSC**.
5. Em **Transferência de dados para o Servidor de Administração**, selecione as seguintes opções:

   - **Relatório sobre o estado das regras de Controle Adaptativo de Anomalias**.
   - **Relatório sobre regras de Controle Adaptativo de Anomalias acionadas**.

6. Salvar alterações.

Armazenamento Acionadores de regra no estado de Treinamento inteligente

No modo de treinamento, o Controle Adaptativo de Anomalias envia informações sobre as regras acionadas para um armazenamento separado, **Acionadores de regra no estado de Treinamento inteligente**. As informações sobre as regras acionadas são representadas no armazenamento como uma lista de eventos. Para ajustar o Controle Adaptativo de Anomalias, você pode confirmar o comportamento atípico no computador ou adicionar uma exclusão da regra.

Eventos do Controle Adaptativo de Anomalias

O Controle Adaptativo de Anomalias registra eventos de acionamento da regra nos modos *Bloquear* (incluindo *Bloqueio inteligente*) e *Notificar*. Os seguintes eventos são fornecidos para esta finalidade:

Ação do processo bloqueada

Ação do processo ignorada

Os eventos contêm informações sobre a atividade suspeita, incluindo somas de verificação de arquivos, os usuários envolvidos, o tempo de acionamento da regra e o nome do computador. Depois de analisar o evento, você poderá adicionar exclusões da regra imediatamente se achar que a atividade é legítima.

Controle de aplicativos

O Controle de aplicativos gerencia a inicialização de aplicativos nos computadores dos usuários. Isso permite que você implemente uma política de segurança corporativa ao usar aplicativos. O Controle de aplicativos também reduz o risco de infecção do computador, restringindo o acesso aos aplicativos.

A configuração do Controle de aplicativos consiste nas seguintes etapas:

1. Criar categorias de aplicativos.

   O administrador cria categorias de aplicativos que o administrador deseja gerenciar. As categorias de aplicativos destinam-se a todos os computadores da rede corporativa, independentemente dos grupos de administração. Para criar uma categoria, você pode usar os seguintes critérios: Categoria KL (por exemplo, *Navegadores* ou outra categoria), hash de arquivo, fornecedor do aplicativo e outros critérios.

2. Criar regras de Controle de aplicativos.

   O administrador cria regras de Controle de aplicativos na política para o grupo de administração. A regra inclui as categorias de aplicativos e o status de inicialização dos aplicativos dessas categorias: bloqueados ou permitidos. O administrador pode criar muitas regras. Um aplicativo pode corresponder aos critérios de várias regras. A prioridade da regra de bloqueio é mais alta do que a de permissão. O Kaspersky Endpoint Security verifica se um aplicativo corresponde a uma regra sempre que for iniciado. O Kaspersky Endpoint Security compara sequencialmente o aplicativo com todas as regras de Controle de Aplicativos.

3. Selecionar o modo de Controle de aplicativos.

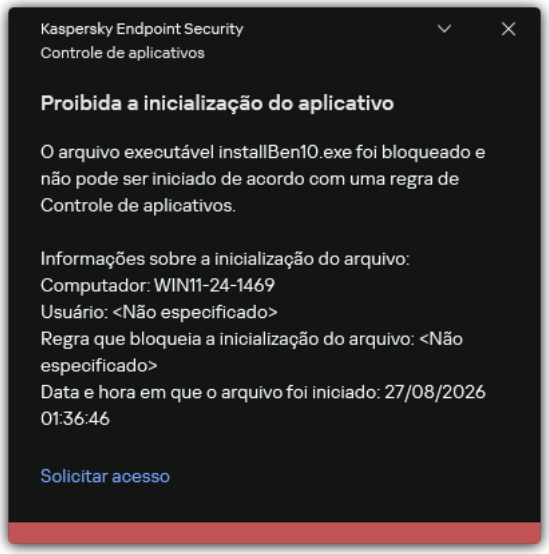
   O administrador escolhe o modo para trabalhar com aplicativos que não estão incluídos em nenhuma das regras: (Lista de bloqueio e de permissão de aplicativos).

Quando um usuário tenta iniciar um aplicativo proibido, o Kaspersky Endpoint Security impede o início do aplicativo e exibe uma notificação (veja a figura abaixo).

Um *modo de teste* é fornecido para verificar a configuração do Controle de aplicativos. Nesse modo, o Kaspersky Endpoint Security faz o seguinte:

- Permite a inicialização de aplicativos, inclusive os proibidos.
- Mostra uma notificação sobre a inicialização de um aplicativo proibido e adiciona informações ao relatório no computador do usuário.

- Envia dados sobre a inicialização de aplicativos proibidos ao Kaspersky Security Center.



Notificações do Controle de aplicativos

Modos de operação do Controle de aplicativos

O componente Controle de aplicativos opera em dois modos:

- **Lista de bloqueio**. Nesse modo, o Controle de aplicativos permite que os usuários iniciem todos os aplicativos, exceto os que são proibidos nas regras de Controle de aplicativos.

  Esse modo de Controle de aplicativos é ativado por padrão.

- **Lista de permissão**. Nesse modo, o Controle de aplicativos impede que os usuários iniciem aplicativos, exceto os que são permitidos e não proibidos nas regras de Controle de aplicativos.

  Se as regras de permissão do Controle de aplicativos estiverem totalmente configuradas, o componente bloqueará a inicialização de todos os novos aplicativos que não foram verificados pelo administrador da LAN, enquanto permite a operação do sistema operacional e dos aplicativos confiáveis nos quais os usuários confiam no trabalho.

  Você pode ler as recomendações sobre a configuração de regras de Controle de aplicativos no modo de lista de permissão.

O Controle de aplicativos pode ser configurado para operar nesses modos, usando a interface local do Kaspersky Endpoint Security e usando o Kaspersky Security Center.

No entanto, o Kaspersky Security Center oferece ferramentas que não estão disponíveis na interface local do Kaspersky Endpoint Security, como as ferramentas necessárias para as seguintes tarefas:

- Criar categorias de aplicativos.

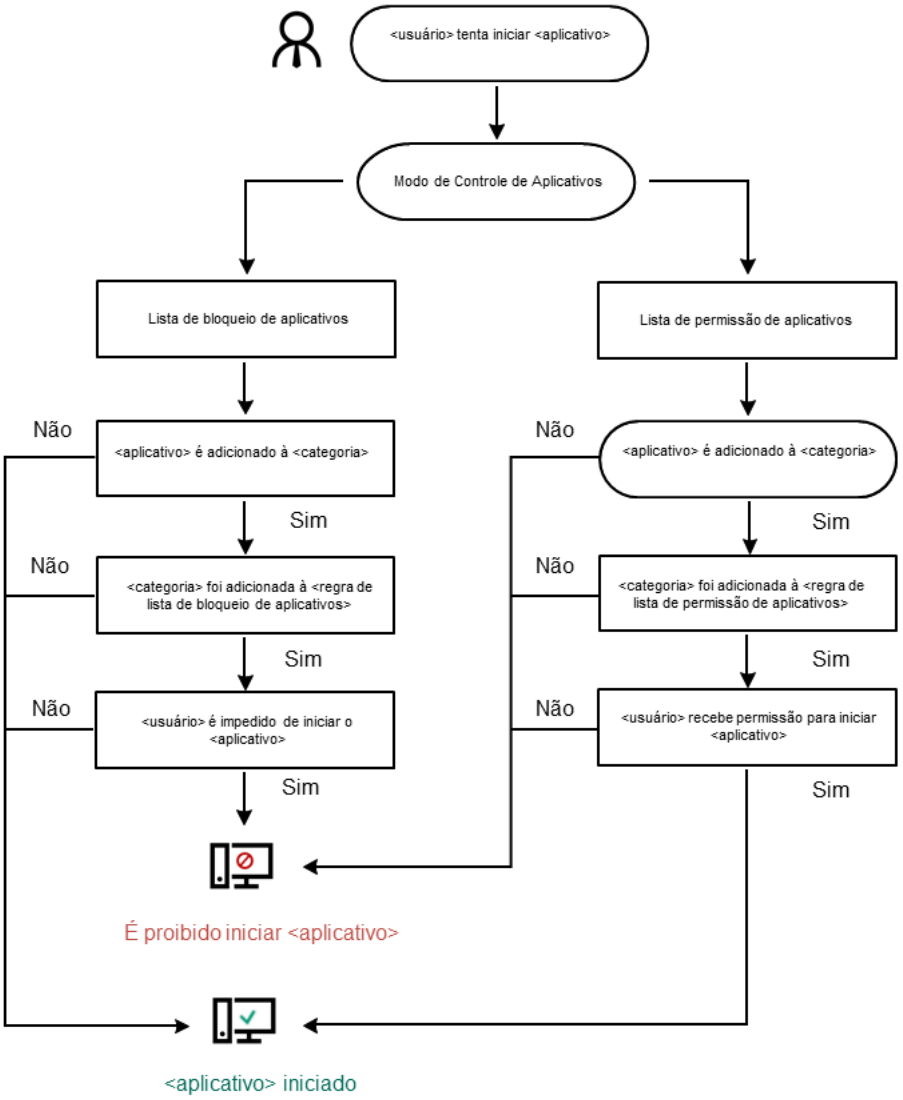
  As regras de Controle de aplicativos criadas no console de administração do Kaspersky Security Center são baseadas nas categorias de aplicativos personalizadas e não nas condições de inclusão e exclusão, como é o caso da interface local do Kaspersky Endpoint Security.

- Receber informações sobre os aplicativos que estão instalados nos computadores da rede local corporativa.

É por isso que é recomendável usar o Kaspersky Security Center para configurar a operação do componente Controle de aplicativos.

Algoritmo de operação do controle de aplicativos

O Kaspersky Endpoint Security usa um algoritmo para tomar uma decisão sobre iniciar um aplicativo (veja a figura abaixo).



Algoritmo de operação do controle de aplicativos

Limitações de funcionalidade do Controle de Aplicativos

A operação do componente Controle de Aplicativos é limitada nos seguintes casos:

- Quando a versão do aplicativo é atualizada, não há suporte para a importação de configurações do componente Controle de Aplicativos.

- Se não houver conexão com os servidores da KSN, o Kaspersky Endpoint Security recebe informações sobre a reputação dos aplicativos e os seus módulos somente dos bancos de dados locais.

  A lista de aplicativos que o Kaspersky Endpoint Security designa como categoria KL **Outro software\Aplicativos, confiável de acordo com a reputação no KSN** pode ser diferente caso a conexão com os servidores da KSN esteja disponível ou não.

- No banco de dados de Kaspersky Security Center, informações de 150.000 arquivos processados podem ser armazenadas. Uma vez que este número de registros for alcançado, os novos arquivos não serão processados. Para retomar operações de inventário, você deve excluir os arquivos que foram anteriormente inventariados no banco de dados do Kaspersky Security Center do computador no qual o Kaspersky Endpoint Security está instalado.

- O componente não controla a inicialização de scripts a menos que o script seja enviado ao interpretador via a linha de comando.

  Se a inicialização de um interpretador for permitida por regras de Controle de Aplicativos, o componente não bloqueará um script iniciado neste interpretador.

  Se pelo menos um dos scripts especificados na linha de comando do interpretador for impedido de iniciar pelas Regras de controle de aplicativos, o componente bloqueará todos os scripts, especificados na linha de comando do interpretador.

- O componente não controla os scripts de inicialização dos interpretadores que não são suportador por Kaspersky Endpoint Security.

  O Kaspersky Endpoint Security suporta os seguintes interpretadores:

  - Java
  - PowerShell

  Os seguintes tipos de interpretadores são suportados:

  - %ComSpec%
  - %SystemRoot%\system32\regedit.exe
  - %SystemRoot%\regedit.exe
  - %SystemRoot%\system32\regedt32.exe

- %SystemRoot%\system32\cscript.exe
- %SystemRoot%\system32\wscript.exe
- %SystemRoot%\system32\msiexec.exe
- %SystemRoot%\system32\mshta.exe
- %SystemRoot%\system32\rundll32.exe
- %SystemRoot%\system32\wwahost.exe
- %SystemRoot%\syswow64\cmd.exe
- %SystemRoot%\syswow64\regedit.exe
- %SystemRoot%\syswow64\regedt32.exe
- %SystemRoot%\syswow64\cscript.exe
- %SystemRoot%\syswow64\wscript.exe
- %SystemRoot%\syswow64\msiexec.exe
- %SystemRoot%\syswow64\mshta.exe
- %SystemRoot%\syswow64\rundll32.exe
- %SystemRoot%\syswow64\wwahost.exe

Obter informações sobre aplicativos instalados

Para criar regras ideais de Controle de Aplicativos, recomenda-se primeiro obter uma ideia dos aplicativos que são usados nos computadores na rede local corporativa. Para fazer isto, você pode obter as seguintes informações:

- Fornecedores, versões e localizações de aplicativos usados na rede corporativa.
- Frequência das atualizações do aplicativo.
- As políticas de uso de aplicativo adotadas na empresa (pode ser políticas de segurança ou políticas administrativas).
- Localização do armazenamento dos pacotes de distribuição do aplicativo.

Exibir informações do aplicativo

As informações sobre os aplicativos instalados são fornecidas pelo Agente de Rede do Kaspersky Security Center. As informações sobre os aplicativos instalados ficam disponíveis no console do Kaspersky Security Center, dentro da pasta **Registro de aplicativos**. O Agente de Rede atualiza as informações em cada sincronização com o Kaspersky Security Center. Para obter detalhes das informações enviadas pelo Agente de Rede, consulte a Ajuda do Kaspersky Security Center.

Para abrir a janela de propriedades do aplicativo na pasta Registro de Aplicativos:

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do Console de Administração, selecione **Avançado** → **Gerenciamento de aplicativos** → **Registro de aplicativos**.
3. Selecione um aplicativo.
4. No menu de contexto do aplicativo, selecione **Propriedades**.

Exibir informações sobre arquivos executáveis

É possível reduzir a carga no banco de dados ao consultar informações sobre arquivos executáveis. Para conseguir isso, recomendamos executar a tarefa *Inventário* em vários computadores de referência que tenham seu conjunto padrão de software instalado.

As informações sobre arquivos executáveis são fornecidas pelo Kaspersky Endpoint Security. Para receber informações sobre o hardware, é necessário aplicar uma política ativa que permita a transmissão de informações sobre os aplicativos instalados (essa transmissão é ativada por padrão).

Como ativar o envio de informações do aplicativo no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Relatórios e Armazenamento**.
4. No bloco **Transferência de dados para o Servidor de Administração**, clique no botão **Configurações**.
5. Marque a caixa de seleção **Aplicativos iniciados**.
6. Salvar alterações.

Como ativar o envio das informações do aplicativo no Web Console e Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Integração KSC**.
5. No bloco **Transferência de dados para o Servidor de Administração**, clique no botão **Configurações avançadas**.

6. Na janela que é aberta, marque a caixa de seleção **Sobre os aplicativos iniciados**.

7. Salvar alterações.

É possível obter uma lista de arquivos executáveis usando a tarefa *Inventário* do Kaspersky Endpoint Security. É possível visualizar a lista de arquivos executáveis no console do Kaspersky Security Center, dentro da pasta **Arquivos executáveis**.

Antes de executar a tarefa *Inventário*, assegure-se de que o banco de dados atenda às recomendações do Kaspersky Security Center. Para obter detalhes sobre as limitações do banco de dados, consulte a ajuda do Kaspersky Security Center.

Como executar a tarefa de Inventário no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **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

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Inventário**.

Etapa 2. Escopo do inventário

Crie uma lista de pastas nas quais deseja que o Kaspersky Endpoint Security procure arquivos executáveis. Defina as configurações de inventário (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. Seleção da conta para executar a tarefa

Selecione uma conta para executar a tarefa de *Inventário*. Por padrão, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de usuário local. Se o escopo do inventário incluir unidades de rede ou outros objetos com acesso restrito, selecione uma conta de usuário com os direitos de acesso suficientes.

Etapa 5. Configurar um agendamento de início de tarefa

Configure o agendamento da tarefa, por exemplo, manualmente.

Etapa 6. Definir o nome da tarefa

Insira um nome para a tarefa, por exemplo, *Inventário de linha de base*.

Etapa 7. Concluir a criação da tarefa

Conclua o 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 resultado, uma pesquisa de arquivos executáveis é realizada nos computadores dos usuários de acordo com o agendamento configurado.

Como executar uma tarefa de Inventário no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Inventário**.

   c. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Inventário de linha de base*.

   d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Vá para a próxima etapa.

5. Selecione uma conta para executar a tarefa. Por padrão, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de usuário local.

6. Conclua o assistente.

   Uma nova tarefa será exibida na lista de tarefas.

7. Para configurar a tarefa, acesse as propriedades dela (consulte a tabela abaixo).

8. Marque a caixa de seleção ao lado da tarefa.

9. Clique **Iniciar**.

   Você pode monitorar o status da tarefa e o número de dispositivos nos quais a tarefa foi concluída com êxito ou concluída com um erro. Como resultado, os arquivos executáveis serão pesquisados nos computadores do usuário de acordo com o agendamento especificado.

Para abrir a janela de propriedades de um arquivo executável na pasta Arquivos executáveis:

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

2. Na árvore do Console de Administração, selecione **Avançado** → **Gerenciamento de aplicativos** → **Arquivos executáveis**.

3. Selecionar um arquivo executável.

4. No menu de contexto do arquivo executável, selecione **Propriedades**.

Para visualizar informações gerais sobre o aplicativo e os respectivos arquivos executáveis, e a lista de computadores em que o aplicativo está instalado, abra a janela propriedades do aplicativo que está selecionada na pasta **Registro de aplicativos** ou na pasta **Arquivos executáveis**.

Atualização das informações sobre aplicativos instalados e arquivos executáveis

A operação do componente Controle de Aplicativos com o banco de dados de arquivos executáveis foi otimizada no Kaspersky Endpoint Security. O Kaspersky Endpoint Security atualiza automaticamente o banco de dados após o arquivo ser excluído do computador. Isso permite manter o banco de dados atualizado, além de economizar os recursos do Kaspersky Security Center. Para manter o banco de dados dos aplicativos instalados atualizado, o envio de informações do aplicativo ao Servidor de Administração deve estar ativado (ativado por padrão).

Configurações de inventário

Parâmetro	Descrição
Escopos do inventário	Lista de objetos que formarão o escopo do inventário.
Inventário de módulos de DLL	O Kaspersky Endpoint Security procura módulos DLL no escopo do inventário e envia informações ao Kaspersky Security Center. Ativar o inventário de módulos DLL aumenta significativamente o tempo necessário para se concluir a tarefa de Inventário e o tamanho do banco de dados.
Inventário de arquivos script	O Kaspersky Endpoint Security procura scripts no escopo do inventário e envia as informações ao Kaspersky Security Center. Ativar o inventário de arquivos script aumenta significativamente o tempo necessário para se concluir a tarefa de Inventário e o tamanho do banco de dados.

Parâmetro	Descrição
Executar apenas quando o computador estiver ocioso	Início adiado da tarefa quando os recursos do computador estão ocupados. O Kaspersky Endpoint Security inicia a tarefa de verificação se o computador estiver bloqueado ou se a proteção de tela estiver ativada. Caso interrompa a execução da tarefa, por exemplo, desbloqueando o computador, o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que foi interrompido. Essa opção de programação permite conservar os recursos do computador quando ele está sendo utilizado.
Verificar apenas arquivos novos e modificados	Verifica apenas os arquivos novos e aqueles que foram modificados desde a última vez em que foram verificados. Isso ajuda a reduzir a duração de uma verificação. Esse modo se aplica a arquivos simples e compostos.
Ignorar arquivo verificado por mais de (seg) N seg	Limitação do tempo de execução da tarefa. Depois do tempo especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está marcada como concluída. Na próxima vez que o Kaspersky Endpoint Security executar a tarefa, ela será executada desde o início e dentro do cronograma.
Verificar arquivos compactados	Verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros arquivos compactados. O aplicativo verifica os arquivos por extensão e formato. Ao verificar os arquivos, o aplicativo executa uma descompactação recursiva. Isso permite detectar ameaças em arquivos multinível (arquivo dentro de arquivo).
Verificar pacotes de distribuição	Verificação de pacotes de distribuição de aplicativos de terceiros.
Não descompactar arquivos compostos grandes	Se esta caixa de seleção for marcada, o aplicativo não verificará arquivos compostos se o tamanho deles exceder o valor especificado. Se esta caixa de seleção estiver desmarcada, o aplicativo verificará os arquivos compostos de todos os tamanhos. O aplicativo verifica arquivos grandes extraídos de arquivos compactados independentemente de a caixa de seleção estar selecionada ou não.

Como ativar o modo Aplicativos bloqueados

No modo *Aplicativos bloqueados*, o Controle de aplicativos permite que os usuários iniciem todos os aplicativos, exceto os que são proibidos nas regras do Controle de aplicativos. Ou seja, se nenhuma regra de negação existir, o Controle de aplicativos permite que o aplicativo seja iniciado. Esse modo de Controle de aplicativos é ativado por padrão.

Antes de ativar o modo *Aplicativos bloqueados*, recomendamos testar as regras do Controle de aplicativos. Para isso, ative o modo de teste.

Como ativar o modo de Aplicativos bloqueados no Console de administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Controles de Segurança** → **Controle de aplicativos**.
5. Marque a caixa de seleção **Controle de aplicativos**.
6. No bloco **Configurações do controle de aplicativos**, use a lista suspensa **Modo de controle** para selecionar **Lista de bloqueio**.

7. Na lista suspensa **Ação**, selecione a ação para o Controle de aplicativos:

- **Testar regras**. O Controle de aplicativos não bloqueia aplicativos que estão impedidos de serem executados pelas regras, mas gera eventos sobre a execução de aplicativos que, de outra forma, seriam bloqueados.

- **Aplicar regras**. O Controle de aplicativos bloqueia os aplicativos bloqueados e gera os eventos correspondentes.

8. Selecione o status das regras do Controle de aplicativos:

- **Ativado**. Este status significa que a regra é usada quando o componente Controle de Aplicativos está em execução.

- **Desativado**. Este status significa que a regra é ignorada quando o componente Controle de Aplicativos está em execução.

- **Testar**. Esse status significa que Kaspersky Endpoint Security sempre permite a inicialização de aplicativos aos quais a regra aplica mas registra informações sobre a inicialização de tais aplicativos no relatório.

Se necessário, adicione novas regras de Controle de aplicativos.

9. Defina as configurações avançadas do Controle de aplicativos:

- **Monitorar o carregamento de módulos DLL (aumenta significativamente a carga no sistema)**. Se a caixa de seleção for marcada, o Kaspersky Endpoint Security controlará o carregamento de módulos DLL quando os usuários tentarem iniciar aplicativos. As informações sobre o módulo DLL e o aplicativo que carregou este módulo DLL são registradas no relatório.

  Ao ativar o controle sobre o carregamento de módulos DLL e drivers, certifique-se de que uma das regras a seguir seja ativada nas configurações do Controle de Aplicativos: a regra **Golden Image** padrão ou outra regra que contenha a categoria KL de "**Golden Image\Certificados confiáveis**" e garanta que os módulos DLL e drivers confiáveis sejam carregados antes da inicialização do Kaspersky Endpoint Security. A ativação do controle de carregamento de módulos DLL e drivers quando a regra **Golden Image** é desativada pode causar instabilidade no sistema operacional.

  O Kaspersky Endpoint Security monitora somente os módulos DLL e drivers carregados desde que a caixa de seleção foi marcada. Depois de marcar a caixa de seleção, é recomendável reiniciar o computador para garantir que o aplicativo monitore todos os módulos DLL e drivers, incluindo aqueles carregados antes do Kaspersky Endpoint Security iniciar.

- **Usar verificação rigorosa de assinatura digital**. É possível selecionar um certificado como uma condição de acionamento para uma regra de Controle de Aplicativos. Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security aplicará regras somente a aplicativos assinados com certificados do armazenamento de certificados do sistema confiável. Os aplicativos assinados com esses certificados também são considerados confiáveis pelos componentes de proteção, por exemplo, a tarefa *Verificação de malware*. No entanto, caso um certificado de outro armazenamento seja especificado em uma regra de controle de aplicativos, o Kaspersky Endpoint Security não aplicará tal regra.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security aplicará regras a aplicativos assinados por um certificado do Trusted Root Certificate Store do Windows. Esses aplicativos não fazem parte da zona confiável. Os componentes de proteção monitoram a atividade desses aplicativos.

- **Mensagem sobre bloqueio**. Modelo da mensagem que é exibida quando uma regra de Controle de Aplicativos que impede a inicialização de um aplicativo é acionada.

- **Mensagem para o administrador**. Modelo da mensagem que um usuário pode enviar ao administrador da rede local corporativa, se o usuário acreditar que um aplicativo foi bloqueado por engano.

10. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como definir o modo Aplicativos bloqueados no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Controle de aplicativos**.

5. Ative o botão de alternância **Controle de aplicativos ATIVADO**.

6. No bloco **Modo de operação**, selecione **Bloquear tudo, exceto a lista de regras**.

7. No bloco **Ação**, selecione a ação para o Controle de aplicativos:

   - **Informar**. O Controle de aplicativos não bloqueia aplicativos que estão impedidos de serem executados pelas regras, mas gera eventos sobre a execução de aplicativos que, de outra forma, seriam bloqueados.

   - **Aplicar regras**. O Controle de aplicativos bloqueia os aplicativos bloqueados e gera os eventos correspondentes.

8. Selecione o status das regras do Controle de aplicativos:

   - **Ativado**. Este status significa que a regra é usada quando o componente Controle de Aplicativos está em execução.

   - **Desativado**. Este status significa que a regra é ignorada quando o componente Controle de Aplicativos está em execução.

   - **Modo de teste**. Esse status significa que Kaspersky Endpoint Security sempre permite a inicialização de aplicativos aos quais a regra aplica mas registra informações sobre a inicialização de tais aplicativos no relatório.

   Se necessário, adicione novas regras de Controle de aplicativos.

9. Defina as configurações avançadas do Controle de aplicativos:

   - **Monitorar o carregamento de módulos DLL**. Se a caixa de seleção for marcada, o Kaspersky Endpoint Security controlará o carregamento de módulos DLL quando os usuários tentarem iniciar aplicativos. As informações sobre o módulo DLL e o aplicativo que carregou este módulo DLL são registradas no relatório.

Ao ativar o controle sobre o carregamento de módulos DLL e drivers, certifique-se de que uma das regras a seguir seja ativada nas configurações do Controle de Aplicativos: a regra **Golden Image** padrão ou outra regra que contenha a categoria KL de "**Golden Image\Certificados confiáveis**" e garanta que os módulos DLL e drivers confiáveis sejam carregados antes da inicialização do Kaspersky Endpoint Security. A ativação do controle de carregamento de módulos DLL e drivers quando a regra **Golden Image** é desativada pode causar instabilidade no sistema operacional.

O Kaspersky Endpoint Security monitora somente os módulos DLL e drivers carregados desde que a caixa de seleção foi marcada. Depois de marcar a caixa de seleção, é recomendável reiniciar o computador para garantir que o aplicativo monitore todos os módulos DLL e drivers, incluindo aqueles carregados antes do Kaspersky Endpoint Security iniciar.

- **Usar verificação rigorosa de assinatura digital**. É possível selecionar um certificado como uma condição de acionamento para uma regra de Controle de Aplicativos. Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security aplicará regras somente a aplicativos assinados com certificados do armazenamento de certificados do sistema confiável. Os aplicativos assinados com esses certificados também são considerados confiáveis pelos componentes de proteção, por exemplo, a tarefa *Verificação de malware*. No entanto, caso um certificado de outro armazenamento seja especificado em uma regra de controle de aplicativos, o Kaspersky Endpoint Security não aplicará tal regra.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security aplicará regras a aplicativos assinados por um certificado do Trusted Root Certificate Store do Windows. Esses aplicativos não fazem parte da zona confiável. Os componentes de proteção monitoram a atividade desses aplicativos.

- **Mensagem para o usuário**. Modelo da mensagem que é exibida quando uma regra de Controle de Aplicativos que impede a inicialização de um aplicativo é acionada.

- **Mensagem para o administrador**. Modelo da mensagem que um usuário pode enviar ao administrador da rede local corporativa, se o usuário acreditar que um aplicativo foi bloqueado por engano.

10. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar o modo Aplicativos bloqueados na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de aplicativos**.

3. Ative o botão de alternância **Controle de aplicativos**.

4. No bloco **Modo Controle de Inicialização de Aplicativos**, selecione **Lista de bloqueio. Todos os aplicativos, exceto os na lista de regras, são permitidos**.

5. No bloco **Ação bloqueada por regras durante inicialização de aplicativos**, selecione a ação para o Controle de aplicativos:

   - **Informar (modo de teste) e registrar eventos em relatório**. O Controle de aplicativos não bloqueia aplicativos que estão impedidos de serem executados pelas regras, mas gera eventos sobre a execução de aplicativos que, de outra forma, seriam bloqueados.

   - **Bloquear**. O Controle de aplicativos bloqueia os aplicativos bloqueados e gera os eventos correspondentes.

6. Selecione o status das regras do Controle de aplicativos:

- **Ativado**. Este status significa que a regra é usada quando o componente Controle de Aplicativos está em execução.
- **Desativado**. Este status significa que a regra é ignorada quando o componente Controle de Aplicativos está em execução.
- **Modo de teste**. Esse status significa que Kaspersky Endpoint Security sempre permite a inicialização de aplicativos aos quais a regra aplica mas registra informações sobre a inicialização de tais aplicativos no relatório.

Se necessário, adicione novas regras de Controle de aplicativos.

7. Defina as configurações avançadas do Controle de aplicativos:

- **Monitorar o carregamento de módulos DLL**. Se a caixa de seleção for marcada, o Kaspersky Endpoint Security controlará o carregamento de módulos DLL quando os usuários tentarem iniciar aplicativos. As informações sobre o módulo DLL e o aplicativo que carregou este módulo DLL são registradas no relatório.

  Ao ativar o controle sobre o carregamento de módulos DLL e drivers, certifique-se de que uma das regras a seguir seja ativada nas configurações do Controle de Aplicativos: a regra **Golden Image** padrão ou outra regra que contenha a categoria KL de "**Golden Image\Certificados confiáveis**" e garanta que os módulos DLL e drivers confiáveis sejam carregados antes da inicialização do Kaspersky Endpoint Security. A ativação do controle de carregamento de módulos DLL e drivers quando a regra **Golden Image** é desativada pode causar instabilidade no sistema operacional.

  O Kaspersky Endpoint Security monitora somente os módulos DLL e drivers carregados desde que a caixa de seleção foi marcada. Depois de marcar a caixa de seleção, é recomendável reiniciar o computador para garantir que o aplicativo monitore todos os módulos DLL e drivers, incluindo aqueles carregados antes do Kaspersky Endpoint Security iniciar.

- **Usar verificação rigorosa de assinatura digital**. É possível selecionar um certificado como uma condição de acionamento para uma regra de Controle de Aplicativos. Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security aplicará regras somente a aplicativos assinados com certificados do armazenamento de certificados do sistema confiável. Os aplicativos assinados com esses certificados também são considerados confiáveis pelos componentes de proteção, por exemplo, a tarefa *Verificação de malware*. No entanto, caso um certificado de outro armazenamento seja especificado em uma regra de controle de aplicativos, o Kaspersky Endpoint Security não aplicará tal regra.

  Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security aplicará regras a aplicativos assinados por um certificado do Trusted Root Certificate Store do Windows. Esses aplicativos não fazem parte da zona confiável. Os componentes de proteção monitoram a atividade desses aplicativos.

- **Modelos de mensagens sobre o bloqueio de aplicativo**. Modelo da mensagem que é exibida quando uma regra de Controle de Aplicativos que impede a inicialização de um aplicativo é acionada.
- **Texto do modelo de mensagem exibido quando um aplicativo tem a inicialização bloqueada**. Modelo da mensagem que um usuário pode enviar ao administrador da rede local corporativa, se o usuário acreditar que um aplicativo foi bloqueado por engano.

8. Salvar alterações.

Como resultado, o Controle de aplicativos bloqueia os aplicativos bloqueados. O Kaspersky Endpoint Security também gera eventos de *Proibida a inicialização do aplicativo*. É possível usar esses eventos para gerar o relatório *Relatório de aplicativos proibidos* no console do Kaspersky Security Center. No resumo do relatório, é possível visualizar a lista de aplicativos e computadores em que a regra de Controle de aplicativos foi acionada.

Controle de aplicativos com base em um computador de linha de base

É possível usar um computador de linha de base para criar uma imagem com o conjunto de aplicativos necessários. Essa imagem pode então ser utilizada para implementar o sistema operacional e os aplicativos em outros computadores. Nem sempre é possível manter a imagem atualizada. O Controle de aplicativos permite manter uma lista de aplicativos permitidos com base em um computador de linha de base. O Controle de aplicativos determina automaticamente que aplicativos serão instalados no computador de linha de base e atualiza a categoria. Dessa forma, os computadores recebem uma lista atualizada de aplicativos permitidos.

A configuração do Controle de aplicativos com base num computador de linha de base envolve as seguintes etapas:

1. Criar uma categoria de atualização automática. Ao criar a nova categoria, selecione a **Categoria que inclui arquivos executáveis de uma pasta específica** e defina o computador de linha de base.

   Como criar uma categoria cuja atualização seja automática no Console de Administração (MMC)

   1. Abra o Console de Administração do Kaspersky Security Center.
   2. Na árvore do Console de Administração, selecione **Avançado** → **Gerenciamento de aplicativos** → **Categorias de aplicativos**.
   3. Clique no botão **Nova categoria** no espaço de trabalho.

      Isso inicia o assistente de criação de categoria de aplicativos.
   4. Siga as instruções do assistente de criação de categoria de aplicativos.

   Etapa 1. Selecionar o tipo de categoria

   Selecione a **Categoria que inclui arquivos executáveis de dispositivos selecionados** como o tipo de categoria.

   Etapa 2. Inserir um nome de categoria de usuário

   Nesta etapa, especifique um nome para a categoria de aplicativos.

Etapa 3. Configurações

> Esta etapa estará disponível se você selecionou o tipo de categoria **Categoria que inclui arquivos executáveis dos dispositivos selecionados**.

Nesta etapa, clique no botão **Adicionar** e especifique os computadores cujos arquivos executáveis serão adicionados à categoria de aplicativos pelo Kaspersky Security Center. Todos os arquivos executáveis dos computadores especificados apresentados na pasta **Arquivos executáveis** serão adicionados à categoria do aplicativo pelo Kaspersky Security Center.

Nesta etapa, você também pode definir as seguintes configurações:

- Algoritmo para cálculo da função hash. Para selecionar um algoritmo, você deve marcar pelo menos uma das seguintes caixas de seleção:
  - **Calcular o SHA256 para arquivos nessa categoria (compatível com o Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versões posteriores)**.
  - **Calcular o MD5 para os arquivos nesta categoria (compatível com versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.
- A caixa de seleção **Sincronizar dados com o repositório do Servidor de Administração**. Marque esta caixa de seleção se quiser que o Kaspersky Security Center limpe periodicamente a categoria de aplicativos e adicione a ela todos os arquivos executáveis dos computadores especificados apresentados na pasta **Arquivos executáveis**.

  Caso a caixa de seleção **Sincronizar dados com o repositório do Servidor de Administração** esteja desmarcada, o Kaspersky Security Center não fará nenhuma modificação em uma categoria de aplicativos depois que ela for criada.

Etapa 4. Filtrar

Nesta etapa, configure um filtro de arquivos.

Você pode especificar o tipo de arquivo que deseja usar para criar a categoria de aplicativos.

- **Todos os arquivos**. A categoria corresponderá a todos os arquivos. Esta opção está selecionada por padrão.
- **Somente arquivos fora das categorias de aplicativos**. A categoria corresponderá somente a arquivos fora das categorias de aplicativos.

É possível especificar pastas de computadores selecionados que contenham arquivos que você deseja usar para criar a categoria de aplicativos.

- **Todas as pastas**. A categoria corresponderá a todas as pastas. Esta opção está selecionada por padrão.
- **Pasta especificada**. A categoria corresponderá somente à pasta especificada. Ao selecionar essa opção, é necessário especificar o caminho da pasta.

Etapa 5. Criar uma categoria personalizada

Conclua o assistente.

Como criar uma categoria em que a adição de conteúdo seja automática no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **Operações** → **Aplicativos de terceiros** → **Categorias de aplicativos**.

   A lista de categorias de aplicativos é aberta.

2. Clique **Adicionar**.

   Isso inicia o assistente de criação de categoria de aplicativos.

3. Defina as configurações gerais da categoria de aplicativos:

   - Nome da categoria.
   - Método de criação da categoria. Selecione a **Categoria que inclui arquivos executáveis de dispositivos selecionados** como o tipo de categoria.

   Vá para a próxima etapa.

4. Defina as configurações avançadas da categoria de aplicativos:

   - Especifique os computadores a partir dos quais o Kaspersky Security Center adicionará arquivos executáveis à categoria de aplicativos. Todos os arquivos executáveis dos computadores especificados apresentados na pasta **Arquivos executáveis** serão adicionados à categoria do aplicativo pelo Kaspersky Security Center.
   - Selecione um algoritmo para o cálculo da função hash.
   - Configure um intervalo para sincronizar dados com o armazenamento do Servidor de Administração.
   - Configure um filtro de arquivos.

5. Conclua o assistente.

Ao criar uma categoria cuja atualização seja automática, pode ser conveniente subdividir os arquivos em várias categorias. Por exemplo, arquivos do sistema operacional e arquivos da pasta Program Files. Para fazer isso, use um filtro nas configurações da categoria e selecione pastas individuais.

2. Selecionar o modo de Controle de aplicativos. É necessário impedir a execução de todos os aplicativos que não são explicitamente permitidos. Para isso, selecione o modo *Aplicativos bloqueados*.

3. Criar regra de Controle de aplicativos. Nas configurações da regra, selecione a categoria à qual os arquivos executáveis do computador de linha de base pertencem.

   Como configurar o Controle de aplicativos usando um computador de linha de base no Console de Administração (MMC)

   1. Abra o Console de Administração do Kaspersky Security Center.
   2. Na árvore do console, selecione **Políticas**.

3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

4. Na janela da política, selecione **Controles de Segurança** → **Controle de aplicativos**.

5. Marque a caixa de seleção **Controle de aplicativos**.

6. No bloco **Configurações do controle de aplicativos**, use a lista suspensa **Modo de controle** para selecionar **Lista de bloqueio**.

7. Na lista suspensa **Ação**, selecione a ação para o Controle de aplicativos:

   - **Testar regras**. O Controle de aplicativos não bloqueia aplicativos que estão impedidos de serem executados pelas regras, mas gera eventos sobre a execução de aplicativos que, de outra forma, seriam bloqueados.

   - **Aplicar regras**. O Controle de aplicativos bloqueia os aplicativos bloqueados e gera os eventos correspondentes.

8. Na lista de regras do Controle de aplicativos, clique no botão **Adicionar**.

   Isso iniciará o assistente para adicionar uma regra do Controle de aplicativos.

9. Na lista suspensa **Categoria**, selecione uma categoria cuja atualização seja automática com base no computador de linha de base.

10. Selecione os usuários ou grupo de usuários para os quais deseja aplicar a regra de Controle de aplicativos.

11. Defina as configurações avançadas da regra de Controle de aplicativos:

    - **Negar para outros usuários**. O aplicativo impede a inicialização de aplicativos que pertencem à categoria selecionada para todos os usuários que não estejam na lista.

    - **Atualizadores confiáveis**. O Kaspersky Endpoint Security considera os aplicativos incluídos na categoria selecionada como atualizadores confiáveis com permissão para criar outros arquivos executáveis que, por sua vez, terão permissão para serem executados.

12. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como configurar o Controle de aplicativos usando um computador de linha de base no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Controle de aplicativos**.

5. Ative o botão de alternância **Controle de aplicativos ATIVADO**.

6. No bloco **Modo de operação**, selecione **Bloquear tudo, exceto a lista de regras**.

7. No bloco **Ação**, selecione a ação para o Controle de aplicativos:

   - **Informar**. O Controle de aplicativos não bloqueia aplicativos que estão impedidos de serem executados pelas regras, mas gera eventos sobre a execução de aplicativos que, de outra forma, seriam bloqueados.

   - **Aplicar regras**. O Controle de aplicativos bloqueia os aplicativos bloqueados e gera os eventos correspondentes.

8. Na lista de regras do Controle de aplicativos, clique no botão **Adicionar**.

   Isso iniciará o assistente para adicionar uma regra do Controle de aplicativos.

9. Em **Categorias/Aplicativos**, selecione uma categoria cuja atualização seja automática com base no computador de linha de base.

10. Selecione os usuários ou grupo de usuários para os quais deseja aplicar a regra de Controle de aplicativos.

11. Defina as configurações avançadas da regra de Controle de aplicativos:

    - **Usuários**. O aplicativo impede a inicialização de aplicativos que pertencem à categoria selecionada para todos os usuários que não estejam na lista.

    - **Atualizadores confiáveis**. O Kaspersky Endpoint Security considera os aplicativos incluídos na categoria selecionada como atualizadores confiáveis com permissão para criar outros arquivos executáveis que, por sua vez, terão permissão para serem executados.

12. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como configurar o Controle de aplicativos usando um computador de linha de base na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .

2. Na janela de configurações do aplicativo, selecione **Controles de Segurança** → **Controle de aplicativos**.

3. Ative o botão de alternância **Controle de aplicativos**.

4. No bloco **Modo Controle de Inicialização de Aplicativos**, selecione **Lista de bloqueio. Todos os aplicativos, exceto os na lista de regras, são permitidos**.

5. No bloco **Ação bloqueada por regras durante inicialização de aplicativos**, selecione a ação para o Controle de aplicativos:

   - **Informar (modo de teste) e registrar eventos em relatório**. O Controle de aplicativos não bloqueia aplicativos que estão impedidos de serem executados pelas regras, mas gera eventos sobre a execução de aplicativos que, de outra forma, seriam bloqueados.

   - **Bloquear**. O Controle de aplicativos bloqueia os aplicativos bloqueados e gera os eventos correspondentes.

6. Na lista de regras do Controle de aplicativos, clique no botão **Adicionar**.

   Isso iniciará o assistente para adicionar uma regra do Controle de aplicativos.

7. Em **Categoria**, selecione uma categoria cuja atualização seja automática com base no computador de linha de base.

8. Selecione os usuários ou grupo de usuários para os quais deseja aplicar a regra de Controle de aplicativos.

9. Defina as configurações avançadas da regra de Controle de aplicativos:

   - **Negar para outros usuários**. O aplicativo impede a inicialização de aplicativos que pertencem à categoria selecionada para todos os usuários que não estejam na lista.

   - **Atualizadores confiáveis**. O Kaspersky Endpoint Security considera os aplicativos incluídos na categoria selecionada como atualizadores confiáveis com permissão para criar outros arquivos executáveis que, por sua vez, terão permissão para serem executados.

10. Salvar alterações.

Gerenciar regras de Controle de Aplicativos

O Kaspersky Endpoint Security controla a inicialização de aplicativos por usuários através de regras. Uma regra de Controle de Aplicativos especifica as condições de acionamento e a ação realizada pelo Controle de Aplicativos quando a regra é acionada (permitindo ou bloqueando a inicialização do aplicativo pelos usuários).

Condições de acionamento da regra

Uma condição de acionamento de regra tem a seguinte correlação: "tipo de condição - critério da condição - valor da condição". Com base nas condições de acionamento de regra, o Kaspersky Endpoint Security aplica (ou não aplica) uma regra a um aplicativo.

Os seguintes tipos de condições são usados nas regras:

- *Condições de inclusão*. O Kaspersky Endpoint Security aplica a regra ao aplicativo se o aplicativo corresponder a pelo menos uma das condições de inclusão.

- *Condições de exclusão*. O Kaspersky Endpoint Security não aplica a regra ao aplicativo se o aplicativo corresponder a pelo menos uma das condições de exclusão e não corresponder a nenhuma das condições de inclusão.

Condições de acionamento da regra são criadas usando critérios. Os critérios a seguir são usados para criar regras no Kaspersky Endpoint Security:

- Caminho para a pasta que contém o arquivo executável do aplicativo ou caminho para o arquivo executável do aplicativo.

- Metadados: nome do arquivo executável do aplicativo, versão do arquivo executável do aplicativo, versão do aplicativo e fornecedor do aplicativo.

- Hash do arquivo executável de um aplicativo.

- Certificado: emissor, assunto, impressão digital.

- Inclusão do aplicativo na KL category.

- Localização do arquivo executável do aplicativo em uma unidade removível.

O valor do critério deve ser especificado para cada critério usado na condição. Se os parâmetros do aplicativo a serem iniciados corresponderem aos valores dos critérios especificados em condições de inclusão, a regra será acionada. Nesse caso, o Controle de Aplicativos realiza a ação especificada na regra. Se os parâmetros de aplicativo coincidirem com os valores de critérios especificados na condição de exclusão, o Controle de Aplicativos não controlará a inicialização do aplicativo.

Caso tenha selecionado um certificado como uma condição de acionamento de regras, será necessário garantir que esse certificado seja adicionado ao armazenamento confiável do sistema no computador e verificar as configurações de uso do armazenamento confiável do sistema no aplicativo.

As decisões tomadas pelo componente Controle de Aplicativos quando uma regra é acionada

Quando uma regra é acionada, o Controle de Aplicativos permite que os usuários (ou grupos de usuários) iniciem aplicativos ou bloqueia a inicialização de acordo com a regra. Você pode selecionar usuários individuais ou grupos de usuários que podem ou não iniciar aplicativos que acionam uma regra.

Se uma regra que não especifica quais usuários têm permissão para iniciar aplicativos que satisfaçam à regra, ela é denominada regra de *bloqueio*.

A regra que não especifica nenhum usuário que não tem permissão para iniciar aplicativos que correspondem à regra, ela é chamada de regra de *permissão*.

A prioridade da regra de bloqueio é mais alta do que a de permissão. Por exemplo, se uma regra de permissão do Controle de Aplicativos tiver sido atribuída a um grupo de usuários, enquanto a regra de bloqueio do Controle de Aplicativos foi atribuída a um usuário neste grupo de usuários, esse usuário será impedido de iniciar o aplicativo.

Status operacional de uma regra

As Regra de Controle de Aplicativos podem ter um dos seguintes status operacionais:

- **Ativado**. Este status significa que a regra é usada quando o componente Controle de Aplicativos está em execução.
- **Desativado**. Este status significa que a regra é ignorada quando o componente Controle de Aplicativos está em execução.
- **Modo de teste**. Este status significa que o Kaspersky Endpoint Security permite a inicialização de aplicativos aos quais as regras se aplicam, mas registra informações sobre a inicialização de tais aplicativos no relatório.

Adicionar uma condição de acionamento para a regra de Controle de Aplicativos

Para criar regras de Controle de Aplicativos com maior conveniência, crie categorias de aplicativos.

É recomendável criar a categoria "Aplicativos de trabalho" que abrange o conjunto de aplicativos padrão que é usado pela empresa. Se diferentes grupo de usuários usam conjuntos de aplicativos diversos, é possível criar uma categoria de aplicativos separada para cada grupo de usuários.

Para criar uma categoria de aplicativo no Console de Administração:

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

2. Na árvore do Console de Administração, selecione **Avançado** → **Gerenciamento de aplicativos** → **Categorias de aplicativos**.

3. Clique no botão **Nova categoria** no espaço de trabalho.

   O assistente de criação de categoria de usuário é iniciado.

4. Siga as instruções do assistente de criação de nova categoria.

Etapa 1. Selecionar o tipo de categoria

Nesta etapa, selecione um dos seguintes tipos de categorias de aplicativos:

- Categoria com conteúdo adicionado manualmente. Os dados dos arquivos executáveis são adicionados manualmente à categoria Caso tenha selecionado esse tipo de categoria, nas etapas *Configurando condições para inclusão de aplicativos em categorias* e *Configurando condições para excluir aplicativos de categorias* será possível definir os critérios pelos quais os arquivos executáveis serão incluídos na categoria.

- Categoria que inclui arquivos executáveis dos dispositivos selecionados. Esses arquivos executáveis são processados automaticamente e suas métricas são adicionadas à categoria Caso tenha selecionado esse tipo de categoria, na etapa *Configurações* será possível especificar um computador cujos arquivos executáveis serão incluídos automaticamente na categoria.

- Categoria que inclui arquivos executáveis de uma pasta específica. Os arquivos executáveis de aplicativos copiados para a pasta especificada são processados automaticamente e suas métricas são adicionadas à categoria Caso tenha selecionado esse tipo de categoria, na etapa *Pasta do repositório* será possível especificar uma pasta a partir da qual os arquivos executáveis serão incluídos automaticamente na categoria.

Ao criar uma categoria com conteúdo adicionado automaticamente, o Kaspersky Security Center executa o inventário de arquivos com os seguintes formatos: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX e SCR.

Etapa 2. Inserir um nome de categoria de usuário

Nesta etapa, especifique um nome para a categoria de aplicativos.

Etapa 3. Configurar as condições de inclusão de aplicativos em uma categoria

Ao adicionar um grande número de condições às regras de Controle de Aplicativos (por exemplo, hashes de arquivos), o consumo de recursos do computador aumenta. Quando o número total de condições atinge 50 mil, podem ocorrer problemas de desempenho. Para otimizar o desempenho, recomenda-se revisar e reduzir o número de condições.

Esta etapa estará disponível se você selecionou o tipo de categoria **Categoria com conteúdo adicionado manualmente**.

Nesta etapa, na lista suspensa **Adicionar**, selecione as condições para incluir aplicativos na categoria:

- **Da lista de arquivos executáveis**. Adicione aplicativos a partir da lista de arquivos executáveis no dispositivo cliente à categoria personalizada.
- **Das propriedades do arquivo**. Especifique dados detalhados de arquivos executáveis como condição para adicionar aplicativos à categoria personalizada.
- **Metadados a partir de arquivos na pasta**. Selecione uma pasta no dispositivo cliente que contenha arquivos executáveis. O Kaspersky Security Center indicará os metadados desses arquivos executáveis como uma condição para adicionar aplicativos à categoria personalizada.
- **Checksums dos arquivos na pasta**. Selecione uma pasta no dispositivo cliente que contenha arquivos executáveis. O Kaspersky Security Center indicará os hashes desses arquivos executáveis como uma condição para adicionar aplicativos à categoria personalizada.
- **Certificados para arquivos da pasta**. Selecione uma pasta no dispositivo de cliente que contém arquivos executáveis assinados com certificados. O Kaspersky Security Center indicará os certificados desses arquivos executáveis como uma condição para adicionar aplicativos à categoria personalizada.

  Não é recomendável usar condições cujas propriedades não têm o parâmetro **Impressão digital do certificado** especificado.

- **Metadados dos arquivos do instalador MSI**. Selecione o pacote MSI. O Kaspersky Security Center indicará os metadados de arquivos executáveis compactados neste pacote de instalação MSI como uma condição para adicionar aplicativos à categoria personalizada.
- **Checksums dos arquivos do instalador MSI do aplicativo**. Selecione o pacote MSI. O Kaspersky Security Center indicará os hashes de arquivos executáveis compactados neste pacote de instalação MSI como condição para adicionar aplicativos à categoria personalizada.
- **Da categoria KL**. Especifique uma categoria KL como condição para adicionar aplicativos à categoria personalizada. A *Categoria KL* é uma lista de aplicativos que têm atributos de tema compartilhados. A lista é mantida pelos especialistas da Kaspersky. Por exemplo, a categoria KL conhecida como *Aplicativos de escritório* inclui aplicativos do pacote Microsoft Office, Adobe Acrobat e outras.

  Selecione todas as categorias KL para gerar uma lista estendida de aplicativos confiáveis.

- **Especificar caminho para o aplicativo (máscaras aceitas)**. Selecione uma pasta no dispositivo cliente. O Kaspersky Security Center adicionará arquivos executáveis dessa pasta à categoria personalizada.
- **Selecionar certificado do repositório**. Selecione os certificados que foram usados para assinar os arquivos executáveis como uma condição para adicionar aplicativos à categoria personalizada.

  Não é recomendável usar condições cujas propriedades não têm o parâmetro **Impressão digital do certificado** especificado.

É possível escolher o armazenamento de certificados. Por padrão, o Controle de aplicativos aplica regras somente para aplicativos assinados com um certificado do armazenamento de certificados do sistema confiável. Ele é ativado pela caixa de seleção **Usar verificação rigorosa de assinatura digital**.

- **Tipo de unidade**. Especifique o tipo de dispositivo de armazenamento (todos os discos rígidos e unidades removíveis ou apenas unidades removíveis) como condição para adicionar aplicativos à categoria personalizada.

Etapa 4. Configurar as condições de exclusão de aplicativos de uma categoria

Esta etapa estará disponível se você selecionou o tipo de categoria **Categoria com conteúdo adicionado manualmente**.

Os Aplicativos especificados nesta etapa serão excluídos da categoria mesmo se tiverem sido especificados na etapa "Configurar as condições de inclusão de aplicativos a uma categoria".

Nesta etapa, na lista suspensa **Adicionar**, selecione uma das seguintes condições para excluir aplicativos da categoria:

- **Da lista de arquivos executáveis**. Adicione aplicativos a partir da lista de arquivos executáveis no dispositivo cliente à categoria personalizada.
- **Das propriedades do arquivo**. Especifique dados detalhados de arquivos executáveis como condição para adicionar aplicativos à categoria personalizada.
- **Metadados a partir de arquivos na pasta**. Selecione uma pasta no dispositivo cliente que contenha arquivos executáveis. O Kaspersky Security Center indicará os metadados desses arquivos executáveis como uma condição para adicionar aplicativos à categoria personalizada.
- **Checksums dos arquivos na pasta**. Selecione uma pasta no dispositivo cliente que contenha arquivos executáveis. O Kaspersky Security Center indicará os hashes desses arquivos executáveis como uma condição para adicionar aplicativos à categoria personalizada.
- **Certificados para arquivos da pasta**. Selecione uma pasta no dispositivo de cliente que contém arquivos executáveis assinados com certificados. O Kaspersky Security Center indicará os certificados desses arquivos executáveis como uma condição para adicionar aplicativos à categoria personalizada.
- **Metadados dos arquivos do instalador MSI**. Selecione o pacote MSI. O Kaspersky Security Center indicará os metadados de arquivos executáveis compactados neste pacote de instalação MSI como uma condição para adicionar aplicativos à categoria personalizada.
- **Checksums dos arquivos do instalador MSI do aplicativo**. Selecione o pacote MSI. O Kaspersky Security Center indicará os hashes de arquivos executáveis compactados neste pacote de instalação MSI como condição para adicionar aplicativos à categoria personalizada.
- **Da categoria KL**. Especifique uma categoria KL como condição para adicionar aplicativos à categoria personalizada. A *Categoria KL* é uma lista de aplicativos que têm atributos de tema compartilhados. A lista é mantida pelos especialistas da Kaspersky. Por exemplo, a categoria KL conhecida como *Aplicativos de escritório* inclui aplicativos do pacote Microsoft Office, Adobe Acrobat e outras.

  Selecione todas as categorias KL para gerar uma lista estendida de aplicativos confiáveis.

- **Especificar caminho para o aplicativo (máscaras aceitas)**. Selecione uma pasta no dispositivo cliente. O Kaspersky Security Center adicionará arquivos executáveis dessa pasta à categoria personalizada.

- **Selecionar certificado do repositório**. Selecione os certificados que foram usados para assinar os arquivos executáveis como uma condição para adicionar aplicativos à categoria personalizada.

- **Tipo de unidade**. Especifique o tipo de dispositivo de armazenamento (todos os discos rígidos e unidades removíveis ou apenas unidades removíveis) como condição para adicionar aplicativos à categoria personalizada.

Etapa 5. Configurações

Esta etapa estará disponível se você selecionou o tipo de categoria **Categoria que inclui arquivos executáveis dos dispositivos selecionados**.

Nesta etapa, clique no botão **Adicionar** e especifique os computadores cujos arquivos executáveis serão adicionados à categoria de aplicativos pelo Kaspersky Security Center. Todos os arquivos executáveis dos computadores especificados apresentados na pasta **Arquivos executáveis** serão adicionados à categoria do aplicativo pelo Kaspersky Security Center.

Nesta etapa, você também pode definir as seguintes configurações:

- Algoritmo para cálculo da função hash. Para selecionar um algoritmo, você deve marcar pelo menos uma das seguintes caixas de seleção:

  - **Calcular o SHA256 para arquivos nessa categoria (compatível com o Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versões posteriores)**.

  - **Calcular o MD5 para os arquivos nesta categoria (compatível com versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

- A caixa de seleção **Sincronizar dados com o repositório do Servidor de Administração**. Marque esta caixa de seleção se quiser que o Kaspersky Security Center limpe periodicamente a categoria de aplicativos e adicione a ela todos os arquivos executáveis dos computadores especificados apresentados na pasta **Arquivos executáveis**.

  Caso a caixa de seleção **Sincronizar dados com o repositório do Servidor de Administração** esteja desmarcada, o Kaspersky Security Center não fará nenhuma modificação em uma categoria de aplicativos depois que ela for criada.

Etapa 6. Pasta de repositório

Esta etapa estará disponível se você selecionou o tipo de categoria **Categoria que inclui arquivos executáveis de uma pasta específica**.

Nesta etapa, especifique a pasta na qual o Kaspersky Security Center buscará arquivos executáveis para adicionar aplicativos automaticamente à categoria de aplicativos.

Nesta etapa, você também pode definir as seguintes configurações:

- A caixa de seleção **Incluir bibliotecas de link dinâmico (DLL) nessa categoria**. Marque esta caixa de seleção se desejar que as bibliotecas de vínculo dinâmico (arquivos DLL) sejam incluídas na categoria do aplicativo.

  A inclusão de arquivos DLL na categoria do aplicativo pode reduzir o desempenho do Kaspersky Security Center.

- A caixa de seleção **Incluir dados de script nesta categoria**. Marque esta caixa de seleção se desejar que os scripts sejam incluídos na categoria de aplicativo.

  Incluir scripts na categoria do aplicativo pode reduzir o desempenho do Kaspersky Security Center.

- Algoritmo para cálculo da função hash. Para selecionar um algoritmo, você deve marcar pelo menos uma das seguintes caixas de seleção:

  - **Calcular o SHA256 para arquivos nessa categoria (compatível com o Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versões posteriores)**.

  - **Calcular o MD5 para os arquivos nesta categoria (compatível com versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

- A caixa de seleção **Forçar verificação da pasta para procurar alterações**. Marque essa caixa de seleção se quiser que o Kaspersky Security Center procure periodicamente arquivos executáveis na pasta usada para adicionar automaticamente à categoria de aplicativos.

  Se a caixa de seleção **Forçar verificação da pasta para procurar alterações** for desmarcada, o Kaspersky Security Center só buscará arquivos executáveis na pasta usada para adicionar automaticamente à categoria de aplicativos caso tenham sido feitas alterações na pasta e arquivos tenham sido adicionados a ela ou excluídos dela.

- O campo **Intervalo de verificação (1 a 168 horas)**. Neste campo, você pode especificar o intervalo de tempo (em horas) após o qual o Kaspersky Security Center procurará arquivos executáveis na pasta usada para adicionar automaticamente à categoria de aplicativos.

  O campo estará disponível se a caixa de seleção **Forçar verificação da pasta para procurar alterações** estiver marcada.

Etapa 7. Criar uma categoria personalizada

Conclua o assistente.

Para adicionar uma nova condição de acionamento a uma regra de Controle de Aplicativos pela interface do aplicativo:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de aplicativos**.

3. Clique nos botões **Aplicativos bloqueados** ou **Aplicativos permitidos**.

   A lista de regras de Controle de Aplicativos é aberta.

4. Selecione a regra para a qual você deseja configurar uma condição de acionamento.

   A janela de propriedades de Regra de Controle de Aplicativos é aberta.

5. Selecione a guia **Condições: N** ou a guia **Exclusões: N** e clique no botão **Adicionar**.

6. Selecione as condições de acionamento para a regra de Controle de Aplicativos:

   - **Condições das propriedades dos aplicativos iniciados**. Na lista de aplicativos em execução, você pode selecionar os aplicativos aos quais a regra de Controle de Aplicativos será aplicada. O Kaspersky Endpoint Security também lista os aplicativos que estavam em execução anteriormente no computador. Você precisa selecionar o critério que deseja usar para criar uma ou várias condições de acionamento de regra: **Hash do arquivo**, **Certificado**, **Categoria KL**, **Metadados** ou **Caminho para arquivo ou pasta**.

   - **Condições "Categoria KL"**. A *Categoria KL* é uma lista de aplicativos que têm atributos de tema compartilhados. A lista é mantida pelos especialistas da Kaspersky. Por exemplo, a categoria KL de "aplicativos do Office" inclui todos os aplicativos do pacote Microsoft Office, Adobe® Acrobat® e outros.

   - **Condição personalizada**. Você pode selecionar o arquivo do aplicativo e selecionar uma das condições de acionamento da regra: **Hash do arquivo**, **Certificado**, **Metadados** ou **Caminho para arquivo ou pasta**.

   - **Condição por unidade de arquivo (unidade removível)**. A regra de Controle de Aplicativos é aplicada apenas a arquivos executados em uma unidade removível.

   - **Condições das propriedades dos arquivos na pasta especificada**. A regra de Controle de Aplicativos é aplicada apenas a arquivos na pasta especificada. Você também pode incluir ou excluir arquivos de subpastas. Você precisa selecionar o critério que deseja usar para criar uma ou várias condições de acionamento de regra: **Hash do arquivo**, **Certificado**, **Categoria KL**, **Metadados** ou **Caminho para arquivo ou pasta**.

7. Salvar alterações.

Ao adicionar condições, leve em consideração as seguintes considerações especiais para o Controle de Aplicativos:

- O Kaspersky Endpoint Security é compatível com os caracteres `*` e `?` para inserção de uma máscara nos metadados: **Nome do arquivo**, **nome do aplicativo**, **fornecedor**.

- O Kaspersky Endpoint Security não tem suporte para um hash de arquivo MD5 e não controla a inicialização de aplicativos baseados em hash MD5. Um hash SHA256 é usado como uma condição de acionamento da regra.

- Não se recomenda usar somente os critérios do **Emissor** e **Entidade do certificado** como condições de acionamento de regra. O uso desses critérios é inseguro.

- Se você estiver usando um link simbólico **Caminho para arquivo ou pasta**, é aconselhado a resolver o link simbólico para a operação correta da regra de Controle de Aplicativos. Para isso, clique no botão **Resolver link simbólico**.

Adicionar arquivos executáveis da pasta de Arquivos executáveis à categoria de aplicativos

Na pasta **Arquivos executáveis**, é exibida a lista de arquivos executáveis detectados nos computadores. O Kaspersky Endpoint Security gera uma lista de arquivos executáveis depois de executar a Tarefa de inventário.

Para adicionar arquivos executáveis da pasta Arquivos executáveis na categoria de aplicativos:

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

2. Na árvore do Console de Administração, selecione **Avançado** → **Gerenciamento de aplicativos** → **Arquivos executáveis**.

3. Na área de trabalho, selecione o arquivo executável que você quer adicionar à categoria de aplicativos.

4. Clique com o botão direito para abrir o menu de contexto dos arquivos executáveis selecionados e selecione **Adicionar à categoria**.

5. Na janela que é aberta, faça o seguinte:

   - Na parte superior da janela, escolha uma das seguintes opções:

     - **Adicionar a uma nova categoria de aplicativos**. Escolha essa opção se quiser criar uma nova categoria de aplicativos e adicionar arquivos executáveis a ela.

     - **Adicionar a uma categoria de aplicativos existente**. Escolha essa opção se quiser selecionar uma categoria de aplicativos existente e adicionar arquivos executáveis a ela.

   - No bloco **Tipo de regra**, escolha uma das seguintes opções:

     - **Regras para adicionar às inclusões**. Selecione essa opção se quiser criar uma condição que adiciona arquivos executáveis à categoria de aplicativos.

     - **Regras para adicionar às exclusões**. Selecione essa opção se quiser criar uma condição que exclui arquivos executáveis da categoria de aplicativos.

   - No bloco **Parâmetro usado como condição**, selecione uma das seguintes opções:

     - **Detalhes do certificado (ou hashes SHA256 para arquivos sem um certificado)**.

     - **Detalhes do certificado (arquivos sem um certificado serão ignorados)**.

     - **Somente SHA256 (arquivos sem hash serão ignorados)**.

     - **Somente MD5 (modo descontinuado, somente para a versão Kaspersky Endpoint Security 10 Service Pack 1)**.

6. Salvar alterações.

Adicionar arquivos executáveis relacionados a eventos à categoria de aplicativos

Para adicionar arquivos executáveis relacionados a eventos do Controle de Aplicativos à categoria de aplicativos:

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

2. No nó **Servidor de Administração** da árvore do Console de Administração, selecione a guia **Eventos**.

3. Escolha uma seleção de eventos relacionados à operação do componente Controle de Aplicativos (Exibir os eventos resultantes da operação do componente Controle de Aplicativos, Exibir os eventos resultantes da operação de teste do componente Controle de Aplicativos) na lista suspensa **Seleções de eventos**.

4. Clique no botão **Executar seleção**.

5. Selecione os eventos cujos arquivos executáveis associados você quer adicionar à categoria de aplicativos.

6. Clique com o botão direito para abrir o menu de contexto dos eventos selecionados e selecionar **Adicionar à categoria**.

7. Na janela que é aberta, defina as configurações da categoria do aplicativo:

   - Na parte superior da janela, escolha uma das seguintes opções:

     - **Adicionar a uma nova categoria de aplicativos**. Escolha essa opção se quiser criar uma nova categoria de aplicativos e adicionar arquivos executáveis a ela.

     - **Adicionar a uma categoria de aplicativos existente**. Escolha essa opção se quiser selecionar uma categoria de aplicativos existente e adicionar arquivos executáveis a ela.

   - No bloco **Tipo de regra**, escolha uma das seguintes opções:

     - **Regras para adicionar às inclusões**. Selecione essa opção se quiser criar uma condição que adiciona arquivos executáveis à categoria de aplicativos.

     - **Regras para adicionar às exclusões**. Selecione essa opção se quiser criar uma condição que exclui arquivos executáveis da categoria de aplicativos.

   - No bloco **Parâmetro usado como condição**, selecione uma das seguintes opções:

     - **Detalhes do certificado (ou hashes SHA-256 para arquivos sem certificado)**.

     - **Detalhes do certificado (arquivos sem um certificado serão ignorados)**.

     - **Somente SHA-256 (arquivos sem hash serão ignorados)**.

     - **Somente MD5 (modo descontinuado, somente para a versão Kaspersky Endpoint Security 10 Service Pack 1)**.

8. Salvar alterações.

Adicionar uma regra de Controle de aplicativos

Para adicionar uma regra de Controle de Aplicativos usando o Kaspersky Security Center:

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Controles de Segurança** → **Controle de aplicativos**.

   Na parte direita da janela, as configurações do componente Controle de Aplicativos serão exibidas.

4. Clique **Adicionar**.

   A janela **Regra de Controle de aplicativos** é aberta.

5. Realize uma das seguintes ações:

   - Se você quiser criar uma nova categoria:

     a. Clique **Criar uma categoria**.

     O assistente de criação de categoria de usuário é iniciado.

     b. Siga as instruções do assistente de criação de nova categoria.

     c. Na lista suspensa **Categoria**, selecione a categoria do aplicativo criada.

   - Se você quiser editar uma categoria existente:

     a. Na lista suspensa **Categoria**, selecione a categoria do aplicativo criada que você deseja editar.

     b. Clique **Propriedades**.

     c. Modifique as configurações da categoria do aplicativo selecionada.

     d. Salvar alterações.

     e. Na lista suspensa **Categoria**, selecione a categoria de aplicativo criada com base na qual você deseja criar uma regra.

6. Na tabela **Usuários e seus direitos**, clique no botão **Adicionar**.

   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. Na tabela **Usuários e seus direitos**, proceda da seguinte maneira:

   - Para permitir que usuários e/ou grupos de usuários iniciem aplicativos que pertencem à categoria selecionada, marque as caixas de seleção **Permitir** nas linhas relevantes.

   - Para impedir que usuários e/ou grupos de usuários iniciem aplicativos que pertencem à categoria selecionada, marque as caixas de seleção **Bloquear** nas linhas relevantes.

8. Marque a caixa de seleção **Negar para outros usuários** se desejar que todos os usuários que não aparecem na coluna **Usuário ou grupo** e que não fazem parte do grupo de usuários especificados na coluna **Usuário ou grupo** sejam impedidos de iniciarem aplicativos que pertencem à categoria selecionada.

9. Para que o Kaspersky Endpoint Security considere aplicativos que correspondam às condições de acionamento da regra como atualizadores confiáveis com permissão para serem executados subsequentemente, marque a caixa de seleção **Atualizadores confiáveis**.

   Quando as configurações do Kaspersky Endpoint Security são migradas, a lista de arquivos executáveis criados por atualizadores confiáveis é migrada também.

10. Salvar alterações.

Para adicionar uma regra de Controle de Aplicativos:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de aplicativos**.

3. Clique nos botões **Aplicativos bloqueados** ou **Aplicativos permitidos**.

   A lista de regras de Controle de Aplicativos é aberta.

4. Clique **Adicionar**.

   A janela de configurações Regra de Controle de Aplicativos é aberta.

5. Na guia **Configurações gerais**, defina as configurações principais da regra:

   a. No campo **Nome da regra**, insira ou edite o nome da regra.

   b. No campo **Descrição**, insira uma descrição da regra.

   c. Na tabela **Usuários e seus direitos**, clique no botão **Adicionar**.

      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.

      A regra aplica-se a todos os usuários por padrão.

      > Se não houver usuário especificado na tabela, a regra não poderá ser salva.

   d. Na tabela **Usuários e seus direitos**, use a alternância para definir o direito dos usuários de iniciar os aplicativos.

   e. Marque a caixa de seleção **Negar para outros usuários** caso queira que o aplicativo evite a execução de aplicativos que satisfaçam as condições de acionamento de regras para todos os usuários que não estejam listados na tabela **Usuários e seus direitos** e não sejam membros de grupos de usuários listados na tabela **Usuários e seus direitos**.

      > Se a caixa de seleção **Negar para outros usuários** for desmarcada, o Kaspersky Endpoint Security não controlará a inicialização de aplicativos por usuários que não são especificados na tabela **Usuários e seus direitos** e que não pertencem aos grupos de usuários especificados na tabela **Usuários e seus direitos**.

   f. Marque a caixa de seleção **Atualizadores confiáveis** se desejar que o Kaspersky Endpoint 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 Endpoint 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.

6. Na guia **Condições: N**, crie ou edite a lista de condições de inclusão para disparar a regra.

7. Na guia **Exclusões: N**, crie ou edite a lista de condições de exclusão para disparar a regra.

   Quando as configurações do Kaspersky Endpoint Security são migradas, a lista de arquivos executáveis criados por atualizadores confiáveis é migrada também.

8. Salvar alterações.

Alterar o status de uma regra de Controle de aplicativos usando o Kaspersky Security Center

Para alterar o status de uma regra de Controle de Aplicativos no Console de Administração:

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Controles de Segurança** → **Controle de aplicativos**.

   Na parte direita da janela, as configurações do componente Controle de Aplicativos serão exibidas.

4. Na coluna **Status**, clique com o botão esquerdo para abrir o menu de contexto e selecionar um dos seguintes itens:

   - **Ativado**. Este status significa que a regra é usada quando o componente Controle de Aplicativos está em execução.

   - **Desativado**. Este status significa que a regra é ignorada quando o componente Controle de Aplicativos está em execução.

   - **Testar**. Esse status significa que Kaspersky Endpoint Security sempre permite a inicialização de aplicativos aos quais a regra aplica mas registra informações sobre a inicialização de tais aplicativos no relatório.

5. Salvar alterações.

Para alterar o status de uma regra de Controle de aplicativos na interface do aplicativo:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de aplicativos**.

3. Clique nos botões **Aplicativos bloqueados** ou **Aplicativos permitidos**.

   A lista de regras de Controle de Aplicativos é aberta.

4. Na coluna **Status**, abra o menu de contexto e selecione um dos seguintes itens:

   - **Ativado**. Este status significa que a regra é usada quando o componente Controle de Aplicativos está em execução.

   - **Desativado**. Este status significa que a regra é ignorada quando o componente Controle de Aplicativos está em execução.

   - **Modo de teste**. Este status significa que o Kaspersky Endpoint Security sempre permite a inicialização de aplicativos aos quais esta regra aplica, mas registra as informações sobre a inicialização de tais aplicativos no relatório.

5. Salvar alterações.

Exportar e importar regras de Controle de Aplicativos

Você pode exportar a lista de regras de Controle de Aplicativos para um arquivo XML. Você pode usar a função de exportação/importação para fazer backup da lista de regras de Controle de Aplicativos ou para migrar a lista para um servidor diferente.

Ao exportar e importar regras de Controle de Aplicativos, tenha em mente as seguintes considerações:

- O Kaspersky Endpoint Security exporta a lista de regras apenas para o modo de Controle de Aplicativos ativo. Em outras palavras, se o Controle de Aplicativos estiver operando no modo de lista de bloqueio, o Kaspersky Endpoint Security exportará regras apenas para esse modo. Para exportar a lista de regras para o modo de lista de permissão, é necessário mudar para esse modo e executar a operação de exportação novamente.

- O Kaspersky Endpoint Security usa categorias de aplicativos para que as regras de Controle de Aplicativos funcionem. Ao migrar a lista de regras de Controle de Aplicativos para um servidor diferente, também é necessário migrar a lista de categorias de aplicativos. Para mais detalhes sobre a exportação e importação de categorias de aplicativos, consulte a Ajuda do Kaspersky Security Center.

Como exportar e importar uma lista de regras de Controle de Aplicativos no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Controles de Segurança** → **Controle de aplicativos**.

4. Para exportar a lista de Regras de Controle de Aplicativos:

   a. Selecione as regras que deseja exportar. Para selecionar várias portas, use as teclas **CTRL** ou **SHIFT**.

      Se você não selecionou nenhuma regra, o Kaspersky Endpoint Security exportará todas as regras.

   b. Clique no link **Exportar**.

   c. 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.

   d. Salvar o arquivo.

      O Kaspersky Endpoint Security exporta toda a lista de regras para o arquivo XML.

5. Para importar uma lista de regras de Controle de Aplicativos:

   a. Clique no link **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 Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

6. Salvar alterações.

Como exportar e importar uma lista de Regras de Controle de Aplicativos no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Controle de aplicativos**.

5. Em **Modo de operação**, selecione uma lista de regras: lista de bloqueio ou lista de permissão de aplicativos.

6. Para exportar a lista de regras:

   a. Selecione as regras que deseja exportar.

   b. Clique no botão → **Exportar**.

      O Kaspersky Endpoint Security exporta a lista de regras para um arquivo JSON na pasta de downloads padrão.

7. Para importar a lista de regras:

   a. Clique no botão → **Importar**.

      Na janela exibida, selecione o arquivo JSON do qual deseja importar a lista de regras.

   b. Abra o arquivo.

      Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo JSON.

8. Salvar alterações.

Exibir eventos resultantes da operação do componente Controle de Aplicativos

Para exibir eventos resultantes da operação do componente Controle de Aplicativos recebido pelo Kaspersky Security Center:

1. Abra o Console de Administração do Kaspersky Security Center.
2. No nó **Servidor de Administração** da árvore do Console de Administração, selecione a guia **Eventos**.
3. Clique no botão **Criar a seleção**.
4. Na janela exibida, selecione a seção **Eventos**.
5. Clique no botão **Limpar tudo**.
6. Na tabla **Eventos**, marque as caixas de seleção **Proibida a inicialização do aplicativo**.
7. Salvar alterações.
8. Na lista suspensa **Seleções de eventos**, marque a seleção criada.
9. Clique no botão **Executar seleção**.

Visualização do relatório sobre aplicativos bloqueados

Para exibir o relatório sobre aplicativos bloqueados:

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 **Outro** → **Relatório de aplicativos proibidos**.

   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.

Testar as regras de Controle de Aplicativos

Para garantir que as regras de Controle de aplicativos não bloqueiem os aplicativos necessários para o trabalho, é recomendável ativar o teste de regras de Controle de aplicativos e analisar sua operação após a criação de novas regras. Quando o teste das regras de Controle de Aplicativos está ativado, o Kaspersky Endpoint Security não bloqueia aplicativos cuja inicialização é proibida pelo Controle de Aplicativos, mas, em vez disso, envia notificações sobre sua inicialização para o Servidor de Administração.

Uma análise da operação das regras de Controle de aplicativos requer uma revisão dos eventos gerados do Controle de aplicativos que são informados ao Kaspersky Security Center. Se o modo de teste não resultar em evento de inicialização bloqueado para todos os aplicativos necessários para o trabalho do usuário do computador, isso significa que as regras corretas foram criadas. Caso contrário, é aconselhável atualizar as configurações das regras que você criou, criar regras adicionais ou excluir as regras existentes.

Por padrão, o Kaspersky Endpoint Security permite a inicialização de todos os aplicativos, exceto os aplicativos proibidos pelas regras.

Habilitando e desabilitando o teste de regra de Controle de Aplicativos

Para ativar ou desativar o teste das regras de Controle de Aplicativos no Kaspersky Security Center:

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Controles de Segurança** → **Controle de aplicativos**.

   Na parte direita da janela, as configurações do componente Controle de Aplicativos serão exibidas.

4. Na lista suspensa **Modo de controle**, selecione um dos seguintes itens:

   - **Lista de bloqueio**. Caso esta opção seja selecionada, o Controle de aplicativos permitirá a todos os usuários iniciar qualquer aplicativo, exceto nos casos quando os aplicativos satisfazem as condições de regras de bloqueio do Controle de aplicativos.

   - **Lista de permissão**. Caso esta opção seja selecionada, o Controle de aplicativos impedirá todos os usuários de iniciar qualquer aplicativo, exceto nos casos quando os aplicativos satisfazem as condições de regras de permissão do Controle de aplicativos.

5. Realize uma das seguintes ações:

   - Se você quiser ativar o modo de teste das regras de Controle de Aplicativos, selecione a opção **Testar regras** na lista suspensa **Ação**.

   - Caso queira ativar o Controle de Aplicativos para gerenciar a inicialização de aplicativos nos computadores dos usuários, na lista suspensa, selecione **Aplicar regras**.

6. Salvar alterações.

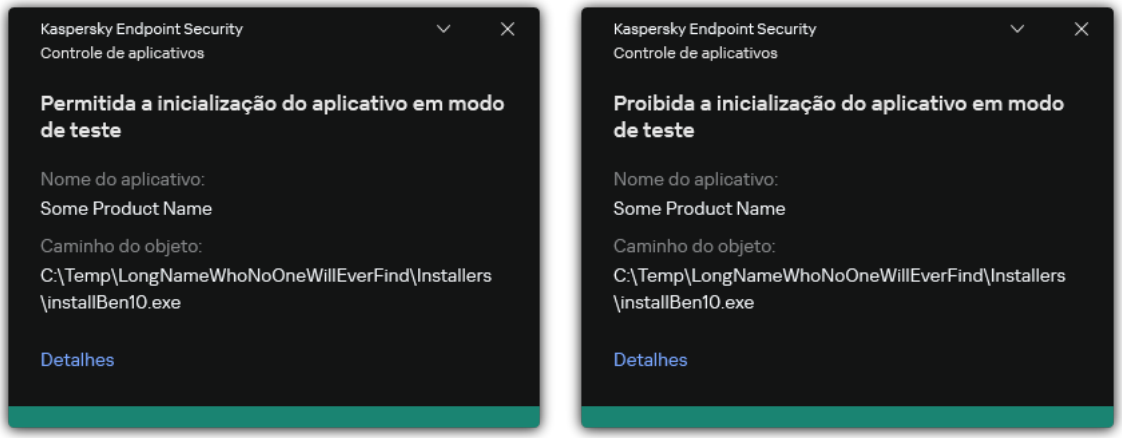
Para ativar o teste de regras de Controle de Aplicativos ou para selecionar uma ação de bloqueio para o Controle de Aplicativos:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de aplicativos**.
3. Clique nos botões **Aplicativos bloqueados** ou **Aplicativos permitidos**.

   A lista de regras de Controle de Aplicativos é aberta.
4. Na coluna **Status** selecione **Modo de teste**.

   Este status significa que o Kaspersky Endpoint Security sempre permite a inicialização de aplicativos aos quais esta regra aplica, mas registra as informações sobre a inicialização de tais aplicativos no relatório.
5. Salvar alterações.

O Kaspersky Endpoint Security não bloqueará aplicativos cuja inicialização é proibida pelo componente Controle de Aplicativos, mas enviará notificações sobre sua inicialização ao Servidor de Administração. Também é possível configurar a exibição de notificações sobre o teste de regras no computador do usuário (veja a figura abaixo).



Notificações do Controle de aplicativos no modo de teste

Exibir o relatório de aplicativos bloqueados no modo de teste:

Para exibir o relatório de aplicativos bloqueados no modo de teste:

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 **Outro** → **Relatório sobre aplicativos proibidos no modo de teste**.

   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.

Exibir eventos resultantes da operação de teste do componente Controle de Aplicativos

Para exibir eventos de testes do Controle de Aplicativos recebidos pelo Kaspersky Security Center:

1. Abra o Console de Administração do Kaspersky Security Center.
2. No nó **Servidor de Administração** da árvore do Console de Administração, selecione a guia **Eventos**.
3. Clique no botão **Criar a seleção**.
4. Na janela exibida, selecione a seção **Eventos**.
5. Clique no botão **Limpar tudo**.
6. Na tabla **Eventos**, marque as caixas de seleção **Proibida a inicialização do aplicativo em modo de teste** e **Permitida a inicialização do aplicativo em modo de teste**.
7. Salvar alterações.
8. Na lista suspensa **Seleções de eventos**, marque a seleção criada.
9. Clique no botão **Executar seleção**.

Monitoramento de atividades do aplicativo

O componente estará disponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para computadores pessoais. O componente estará indisponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para servidores.

O *Monitoramento de atividades do aplicativo* é uma ferramenta desenvolvida para exibir informações sobre a atividade de aplicativos no computador de um usuário em tempo real.

A utilização do Monitoramento de atividades do aplicativo requer a instalação dos componentes Controle de Aplicativos e Prevenção de Intrusão do Host. Caso esses componentes não estejam instalados, a seção Monitoramento de atividades do aplicativo na janela principal do aplicativo estará escondida.

Para iniciar o Monitoramento de atividades de aplicativos:

Na janela principal do aplicativo, na seção **Monitoramento**, clique no bloco **Monitoramento de atividades do aplicativo**.

Nessa janela, informações sobre a atividade de aplicativos no computador do usuário são apresentadas em três guias:

- A guia **Todos os aplicativos** exibe informações sobre todos os aplicativos instalados no computador.
- A guia **Em execução** exibe informações sobre o consumo de recursos do computador por cada aplicativo em tempo real. Dessa guia, também é possível prosseguir para as configurações de permissões para um aplicativo específico.
- A guia **Executar ao iniciar** exibe a lista de aplicativos iniciados junto com o sistema operacional.

Caso queira ocultar as informações de atividade do aplicativo no computador de um usuário, é possível restringir o acesso do usuário à ferramenta Monitoramento de atividades do aplicativo.

Como ocultar o monitoramento de atividades do aplicativo na interface do aplicativo usando o console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Interface**.
4. Use a caixa de seleção **Ocultar a seção Monitoramento de atividades do aplicativo** para conceder ou revogar o acesso à ferramenta.
5. Salvar alterações.

Como ocultar o monitoramento de atividades do aplicativo na interface do aplicativo usando o Web Console e Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Interação com o usuário**.
5. Use a caixa de seleção **Ocultar a seção Monitoramento de atividades do aplicativo** para conceder ou revogar o acesso à ferramenta.
6. Salvar alterações.

Regras para criar máscaras de nome para arquivos ou pastas

Uma *máscara de nome de arquivo ou pasta* é uma representação do nome de uma pasta ou do nome e extensão de um arquivo usando caracteres comuns.

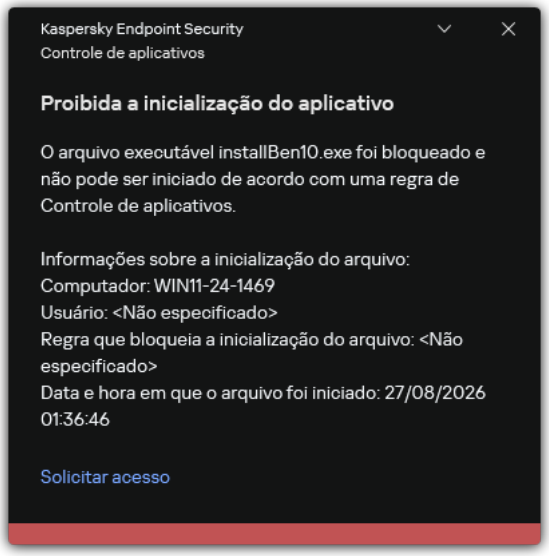
Você pode usar os seguintes caracteres comuns para criar uma máscara de nome de arquivo ou pasta:

- O caractere `*` (asterisco), que assume o lugar de qualquer outro conjunto de caracteres (inclusive um conjunto vazio). Por exemplo, a máscara `C:\*.txt` incluirá todos os caminhos para os arquivos com a extensão `txt` localizados em qualquer pasta na unidade (C:).

- `?` (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.

Editar modelos de mensagem de Controle de Aplicativos

Quando um usuário tenta iniciar um aplicativo que é bloqueado por uma regra de Controle de Aplicativos, o Kaspersky Endpoint Security exibe uma mensagem informando que o aplicativo está bloqueado. Os especialistas da Kaspersky fornecem um modelo de mensagem ao usuário que descreve os motivos pelos quais o aplicativo foi bloqueado (veja a figura abaixo). Variáveis especiais são fornecidas para gerenciar o modelo de mensagem (por exemplo, `%USER_NAME%`). As variáveis permitem que um mesmo modelo de mensagem seja utilizado em diferentes computadores. Ao criar uma mensagem, o Kaspersky Endpoint Security obtém o valor da variável nas configurações do sistema operacional e o insere na mensagem referente ao computador, usuário e evento específicos.



Notificações do Controle de aplicativos

Caso o usuário considere que o aplicativo foi bloqueado por engano, o usuário pode utilizar o link no texto da mensagem para enviar uma mensagem ao administrador da rede corporativa local. Para isso, o usuário deve clicar no botão **Solicitar acesso** e enviar uma mensagem ao administrador descrevendo a situação. Também é possível preparar um modelo da mensagem para o administrador, adicionando os dados que podem informar sua decisão quanto à permissão ou bloqueio do acesso ao aplicativo. Depois que o usuário solicitar o acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio de inicialização do aplicativo para o administrador**. A descrição do evento contém uma mensagem ao administrador com variáveis substituídas. É possível visualizar esses eventos no console do Kaspersky Security Center com o uso da seleção de eventos predefinida **Pedidos de usuário**. Caso sua organização não tenha o Kaspersky Security Center implantado ou não haja conexão com o Servidor de Administração, o aplicativo enviará uma mensagem ao administrador para o endereço de e-mail especificado.

Como editar o modelo de mensagem do Controle de Aplicativos no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Controles de Segurança** → **Controle de aplicativos**.

4. No bloco **Configurações de modelos de mensagem**, clique no botão **Modelos**.

5. Uma janela é aberta; nela, configure os modelos do Controle de Aplicativos:

   - **Mensagem sobre bloqueio**. Modelo da mensagem que é exibida quando uma regra de Controle de Aplicativos que impede a inicialização de um aplicativo é acionada.

     Não é possível configurar modelos de mensagem para o Controle de Aplicativos no modo de teste. O Controle de Aplicativos no modo de teste exibe notificações predefinidas.

   - **Mensagem para o administrador**. Modelo da mensagem que um usuário pode enviar ao administrador da rede local corporativa, se o usuário acreditar que um aplicativo foi bloqueado por engano.

   Para inserir uma variável no modelo, posicione o cursor onde necessário, clique em **Variável** e selecione a opção necessária na lista.

   Você também pode restaurar o texto original do modelo clicando no botão **Por padrão**.

6. Salvar alterações.

Como editar o modelo de mensagem do Controle de Aplicativos no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Controle de aplicativos**.

5. No bloco **Modelos de mensagem**, clique no link **Mensagens sobre bloqueio de inicialização do aplicativo** e configure modelos para mensagens do Controle de aplicativos:

   - **Mensagem para o usuário**. Modelo da mensagem que é exibida quando uma regra de Controle de Aplicativos que impede a inicialização de um aplicativo é acionada.

     Não é possível configurar modelos de mensagem para o Controle de Aplicativos no modo de teste. O Controle de Aplicativos no modo de teste exibe notificações predefinidas.

   - **Mensagem para o administrador**. Modelo da mensagem que um usuário pode enviar ao administrador da rede local corporativa, se o usuário acreditar que um aplicativo foi bloqueado por engano.

   Para inserir uma variável no modelo, posicione o cursor onde necessário, clique em **Adicionar variável** e selecione a opção necessária na lista.

   Você também pode restaurar o texto original do modelo clicando no botão **Redefinir para o padrão**.

6. Salvar alterações.

Como editar o modelo de mensagem do Controle de Aplicativos na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Controle de aplicativos**.

3. No bloco **Modelos de mensagens sobre o bloqueio de aplicativo**, configure modelos para mensagens de Controle de Aplicativos:

   - **Mensagem sobre bloqueio**. Modelo da mensagem que é exibida quando uma regra de Controle de Aplicativos que impede a inicialização de um aplicativo é acionada.

     Não é possível configurar modelos de mensagem para o Controle de Aplicativos no modo de teste. O Controle de Aplicativos no modo de teste exibe notificações predefinidas.

   - **Mensagem para o administrador**. Modelo da mensagem que um usuário pode enviar ao administrador da rede local corporativa, se o usuário acreditar que um aplicativo foi bloqueado por engano.

   Para inserir uma variável no modelo, posicione o cursor onde necessário, clique em **Adicionar variável** e selecione a opção necessária na lista.

   Você também pode restaurar o texto original do modelo clicando no botão **Reiniciar**.

4. Salvar alterações.

Variáveis nos modelos de mensagem do Controle de Aplicativos

É possível usar as seguintes variáveis em modelos de mensagem do usuário ou modelos de mensagem do administrador:

- **Nome da regra que foi acionada** – `%RULE%`.

  Nome da regra que bloqueou a execução de um arquivo.

- **Data atual** – `%DATE%`.

  Data na qual a execução do arquivo foi bloqueada, no formato DD.MM.AAAA.

- **Hora atual** – `%TIME%`.

  Hora na qual a execução do arquivo foi bloqueada no formato HH:MM.

- **Nome de usuário** – `%USER_NAME%`.

  Nome da conta de usuário atual no computador no qual a execução do arquivo foi bloqueada, no formato `<device name>\<user alias>` (por exemplo, `DESKTOP-123\John.Smith`).

- **Nome do computador** – `%COMPUTER_NAME%`.

  Nome do computador no qual a execução do arquivo foi bloqueada.

- **Nome do arquivo executável** – `%FILE_NAME%`.

  Nome do arquivo executável de um aplicativo bloqueado.

- **Categoria KL do arquivo executável** – `%KL_CAT%`.

  Categoria KL à qual o aplicativo bloqueado pertence (por exemplo, *Navegadores* ou outra categoria).

- **Caminho para o arquivo executável** – `%FILE_PATH%`.

  Caminho completo para o arquivo executável do aplicativo bloqueado.

- **Versão do arquivo executável** – `%FILE_VERSION%`.

  Versão do arquivo executável de um aplicativo bloqueado.

- **Nome original do arquivo executável** – `%ORIGINAL_FILE_NAME%`.

  Nome original do arquivo executável do aplicativo bloqueado. O nome do arquivo foi especificado nas propriedades do arquivo executável do aplicativo.

- **Fornecedor** – `%FILE_PUBLISHER%`.

  Fornecedor do aplicativo bloqueado.

- **Nome do aplicativo** – `%FILE_PRODUCT_NAME%`.

  Nome do aplicativo bloqueado.

- **Versão do aplicativo** – `%PRODUCT_VERSION%`.

  Versão do aplicativo bloqueado.

- **Hash do arquivo executável** – `%FILE_HASH%`.

  Hash do arquivo executável de um aplicativo bloqueado.

- **Emissor de certificado** – `%CERT_ISSUER%`.

  Emissor do certificado com o qual o arquivo executável foi assinado.

- **Entidade do certificado** – `%CERT_SUBJECT%`.

  Assunto do certificado com o qual o arquivo executável foi assinado.

- **Impressão digital do certificado** – `%CERT_THUMBPRINT%`.

  Impressão digital do certificado com a qual o arquivo executável foi assinado.

Práticas recomendadas para realizar um inventário de arquivos executáveis

A tarefa *Inventário* obtém informações sobre arquivos executáveis (por exemplo, EXE, BAT e CMD), módulos DLL e scripts (PowerShell, JS e outros). Essas informações são necessárias para configurar categorias do Controle de Aplicativos e permissões de aplicativos para o componente Prevenção de Intrusão do Host. A tarefa *Inventário* deve ser executada periodicamente para manter as informações atualizadas. A tarefa *Inventário*, assim como a tarefa *Verificação de malware*, consome muitos recursos. Portanto, recomendamos configurar a tarefa para ser executada à noite ou nos fins de semana.

Etapas do inventário de arquivos executáveis

1. Selecione o grupo de computadores de referência nos quais o conjunto típico de software está instalado. Recomendamos usar o menor número possível de computadores no procedimento de inventário de arquivos executáveis. Quanto menos tarefas *Inventário*, menor será a carga no Servidor de Administração do Kaspersky Security Center.

2. Mova os computadores de referência para um grupo de administração separado no console do Kaspersky Security Center. Você pode nomear o grupo, por exemplo, *Computadores de referência*.

3. Crie uma tarefa *Inventário* para o grupo de administração *Computadores de referência*. Recomendamos manter as configurações padrão da tarefa.

Exemplo de inventário de arquivos executáveis em uma organização

Por exemplo, sua organização tem 100 computadores que executam o Windows 11 25H2. Todos os computadores têm a mesma versão e localização do sistema operacional. O conjunto de atualizações instaladas nos computadores também é o mesmo.

Em uma organização como essa, não é necessário executar a tarefa *Inventário* em todos os computadores. A maioria dos arquivos executáveis nesses computadores é idêntica. É suficiente criar uma tarefa para um computador de referência. Você pode criar tarefas *Inventário* adicionais para computadores cuja configuração seja diferente da configuração de referência.

Melhores práticas para implementar uma lista de aplicativos permitidos

Ao planejar a implementação de uma lista de aplicativos permitidos, é recomendável executar as seguintes ações:

1. Forme os seguintes tipos de grupos:

   - Grupos de usuário. Os grupos de usuários para quem você deve permitir o uso de vários conjuntos de aplicativos.

   - Grupos de administração. Um ou vários grupos de computadores aos quais o Kaspersky Security Center aplicará a lista de aplicativos permitidos. É necessário criar vários grupos de computadores se diferentes configurações de lista de permissão forem usadas para esses grupos.

2. Crie uma lista de aplicativos com permissão para inicializar.

   Antes de criar uma lista, é aconselhável fazer o seguinte:

   a. Executar a tarefa de inventário.

      Informações sobre criação, reconfiguração e inicialização de uma tarefa de inventário estão disponíveis na seção Gerenciamento de tarefas.

   b. Exiba a lista de arquivos executáveis.

Configurar o modo Lista de permissão para aplicativos

Ao configurar o modo lista de permissão, é recomendável executar as seguintes ações:

1. Criar categorias de aplicativos contendo os aplicativos com permissão de iniciar.

   Selecione um dos seguintes métodos para criar categorias de aplicativos:

   - **Categoria com conteúdo adicionado manualmente**. Adicione manualmente a essa categoria usando as seguintes condições:

     - Metadados do arquivo. O Kaspersky Security Center adiciona todos os arquivos executáveis acompanhados pelos metadados especificados à categoria de aplicativos.

     - Código de hash do arquivo. O Kaspersky Security Center adiciona todos os arquivos executáveis com o hash especificado à categoria de aplicativos.

       O uso dessa condição exclui a capacidade de instalar automaticamente as atualizações porque versões diferentes dos arquivos terão um hash diferente.

     - Certificado de arquivo. O Kaspersky Security Center adiciona todos os arquivos executáveis assinados com o certificado especificado à categoria de aplicativos.

     - Categoria KL. O Kaspersky Security Center adiciona todos os aplicativos na categoria KL especificada à categoria de aplicativos.

- Pasta do aplicativo. O Kaspersky Security Center adiciona todos os arquivos executáveis dessa pasta à categoria personalizada.

  O uso da condição da **Pasta do aplicativo** pode não ser seguro, porque qualquer aplicativo da pasta especificada poderá ser iniciado. É recomendável aplicar regras que usem as categorias de aplicativos com a condição da **Pasta do aplicativo** apenas para usuários cuja instalação automática de atualizações deve ser permitida.

- **Categoria que inclui arquivos executáveis de uma pasta específica**. É possível especificar uma pasta da qual os arquivos executáveis serão automaticamente atribuídos à categoria de aplicativos criada.

- **Categoria que inclui arquivos executáveis dos dispositivos selecionados**. É possível especificar um computador ao qual todos os arquivos executáveis serão atribuídos automaticamente à categoria de aplicativos criada.

  Ao utilizar esse método para criar categorias de aplicativos, o Kaspersky Security Center recebe as informações sobre os aplicativos no computador a partir de uma pasta de **Arquivos executáveis**.

2. Selecione o modo Lista de permissão para o componente Controle de Aplicativos.

3. Crie regras de Controle de Aplicativos usando as categorias de aplicativos criadas.

   A regra de **Golden Image** e regra de **Atualizadores confiáveis** são inicialmente definidas para o modo de Lista de permissão. Essas regras de Controle de Aplicativos correspondem às categorias KL. A categoria KL *Golden Image* inclui programas que asseguram a operação normal do sistema operacional. A categoria KL *Atualizadores confiáveis* inclui atualizadores para os fornecedores de software mais respeitáveis. Você não é possível excluir essas regras. As configurações dessas regras não podem ser editadas. Por padrão, a regra **Golden Image** é ativada e a regra **Atualizadores confiáveis** é desativada. Todos os usuários podem iniciar aplicativos que combinam com as condições de acionamento dessas regras.

4. Determine os aplicativos para os quais a instalação automática das atualizações deve ser permitida.

   Você pode permitir a instalação automática de atualizações em uma das seguintes formas:

   - Especifique uma lista estendida de aplicativos permitidos, permitindo a inicialização de todos os aplicativos pertencentes a qualquer categoria KL.

   - Especifique uma lista extensa de aplicativos permitidos permitindo a inicialização de todos os aplicativos assinados com certificados.

     Para permitir a inicialização de todos os aplicativos assinados com certificados, crie uma categoria com uma condição baseada em certificado que use apenas o parâmetro **Assunto** com o valor `*`.

   - Para a regra de Controle de Aplicativos, selecione o parâmetro **Atualizadores confiáveis**. Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security considerará os aplicativos incluídos na regra como Atualizadores confiáveis. O Kaspersky Endpoint Security permite a inicialização de aplicativos que foram instalados ou atualizados por aplicativos incluídos na regra, desde que nenhuma regra de bloqueio seja aplicada a esses aplicativos.

     Quando as configurações do Kaspersky Endpoint Security são migradas, a lista de arquivos executáveis criados por atualizadores confiáveis é migrada também.

- Crie uma pasta e coloque nela os arquivos executáveisdos aplicativos para os quais você deseja permitir a instalação automática de atualizações. Em seguida, crie uma categoria de aplicativos com a condição da **Pasta do aplicativo** e especifique o caminho para essa pasta. Depois, crie uma regra de permissão e selecione essa categoria.

  O uso da condição da **Pasta do aplicativo** pode não ser seguro, porque qualquer aplicativo da pasta especificada poderá ser iniciado. É recomendável aplicar regras que usem as categorias de aplicativos com a condição da **Pasta do aplicativo** apenas para usuários cuja instalação automática de atualizações deve ser permitida.

Teste do modo Lista de permissão

Para garantir que as regras de Controle de aplicativos não bloqueiem os aplicativos necessários para o trabalho, é recomendável ativar o teste de regras de Controle de aplicativos e analisar sua operação após a criação de novas regras. Quando o teste está ativado, o Kaspersky Endpoint Security não bloqueia aplicativos cuja inicialização é proibida pelas regras do Controle de Aplicativos, mas, em vez disso, envia notificações sobre sua inicialização para o Servidor de Administração.

Ao testar o modo lista de permissão, é recomendável executar as seguintes ações:

1. Determinar o período de teste (nos limites de vários dias a dois meses).
2. Ative o teste de regras de Controle de Aplicativos.
3. Examine os eventos resultantes do teste da operação do Controle de Aplicativos e os relatórios sobre aplicativos bloqueados no modo de teste para analisar os resultados do teste.
4. Com base nos resultados da análise, altere as configurações do modo lista de permissão.

   Em particular, com base nos resultados do teste, você pode adicionar arquivos executáveis relacionados a eventos a uma categoria de aplicativo.

Suporte para o modo Lista de permissão

Depois de selecionar uma ação de bloqueio para o Controle de Aplicativos, é recomendável continuar a dar suporte ao modo lista de permissão executando as seguintes ações:

- Examine os eventos resultantes da operação de Controle de Aplicativos e relatórios sobre execuções bloqueadas para analisar a eficácia do Controle de Aplicativos.
- Analise solicitações de usuários para acessar aplicativos.
- Analise arquivos executáveis desconhecidos verificando sua reputação no Kaspersky Security Network.
- Antes de instalar as atualizações para o sistema operacional ou para o software, instale essas atualizações em um grupo de testes de computadores para verificar como elas serão processadas pelas regras de Controle de Aplicativos.
- Adicione os aplicativos necessários às categorias usadas nas regras do Controle de Aplicativos.

Monitoramento de Portas de rede

Durante a operação do Kaspersky Endpoint Security, os componentes Controle da Web, Proteção Contra Ameaças ao Correio, Proteção Contra Ameaças da Web, Detecção de Comportamento e Prevenção de Exploits monitoram os fluxos de dados transmitidos por protocolos específicos e que passam por portas TCP e UDP abertas e específicas no computador do usuário. Por exemplo, o componente Proteção Contra Ameaças ao Correio analisa as informações transmitidas via SMTP, enquanto o componente Proteção Contra Ameaças da Web analisa as informações transmitidas via HTTP e FTP.

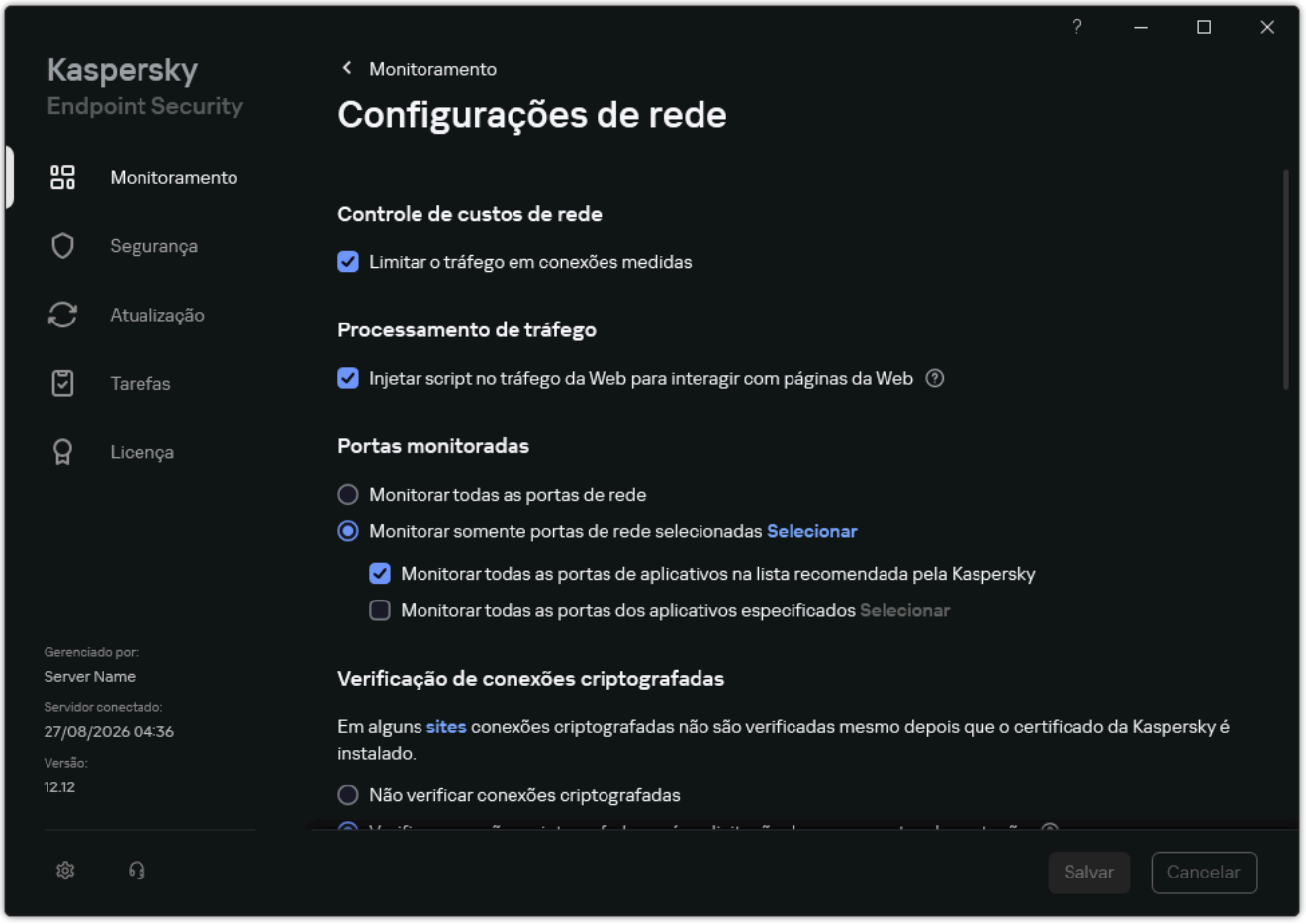
O Kaspersky Endpoint Security divide as portas TCP e UDP do computador do usuário em vários grupos, de acordo com a probabilidade de comprometimento. Algumas portas de rede são reservadas para serviços vulneráveis. É aconselhável monitorar essas portas com mais cuidado, porque elas têm uma probabilidade maior de serem atingidas por um ataque de rede. Se você usar serviços não padrão que dependem de portas de rede não padrão, estas portas de rede também poderão ser alvo de um computador atacante. É possível especificar uma lista de portas de rede e uma lista de aplicativos que exigem acesso de rede. Essas portas e aplicativos recebem atenção especial dos componentes Proteção Contra Ameaças ao Correio e Proteção Contra Ameaças da Web durante o monitoramento do tráfego de rede.

Para ajudar a garantir a segurança do computador, os componentes Detecção de Comportamento e Prevenção de Exploits também monitoram fluxos de dados que passam pelas portas de rede. Os componentes fazem o monitoramento contínuo do tráfego de rede em busca de processos individuais que possam representar ameaças.

Ativar o monitoramento de todas as portas de rede

Para ativar o monitoramento de todas as portas de rede:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações de rede**.



Configurações de monitoramento de portas de rede

3. No bloco **Portas monitoradas**, selecione **Monitorar todas as portas de rede**.
4. Salvar alterações.

Criar uma lista de portas de rede monitoradas

Para criar uma lista de portas de rede monitoradas:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações de rede**.
3. No bloco **Portas monitoradas**, selecione **Monitorar somente portas de rede selecionadas**.

4. Clique **Selecionar**.

   Abrirá uma lista de portas de rede que são geralmente usadas para a transmissão de e-mail e tráfego de rede. Esta lista de portas de rede está incluída no pacote do Kaspersky Endpoint Security.

5. Use o botão de alternância na coluna **Status** para habilitar ou desabilitar o monitoramento da porta de rede.

6. Se a porta de rede não for exibida na lista de portas de rede, adicione-a da seguinte forma:

   a. Clique **Adicionar**.

   b. Na janela que é aberta, digite o número da porta de rede e uma breve descrição.

   c. Defina o status **Ativo** ou **Inativo** para o monitoramento de portas de rede.

7. Salvar alterações.

Quando o protocolo FTP é executado em modo passivo, a conexão pode ser estabelecida através de uma porta de rede aleatória que não é adicionada à lista de portas monitoradas. Para proteger essas conexões, ative o monitoramento de todas as portas de rede ou configure o controle das portas de rede para aplicativos que estabelecem conexões FTP.

Criar uma lista de aplicativos para todas as portas de rede que são monitoradas

Você pode criar uma lista de aplicativos para os quais todas as portas de rede são monitoradas pelo Kaspersky Endpoint Security.

É recomendável incluir aplicativos que recebem ou transmitem dados via FTP na lista de aplicativos para os quais todas as portas de rede são monitoradas.

Para criar uma lista de aplicativos para os quais todas as portas de rede são monitoradas:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações de rede**.

3. No bloco **Portas monitoradas**, selecione **Monitorar somente portas de rede selecionadas**.

4. Marque a caixa de seleção **Monitorar todas as portas de aplicativos na lista recomendada pela Kaspersky**.

   Se esta caixa de seleção for marcada, o Kaspersky Endpoint Security monitorará todas as portas dos seguintes aplicativos:

   - Adobe Acrobat Reader.
   - Apple Application Support.
   - Google Chrome.
   - Microsoft Edge.

- Mozilla Firefox.
- Internet Explorer.
- Java.
- mIRC.
- Opera.
- Pidgin.
- Safari.
- Mail.ru Agent.
- Yandex Browser.

5. Marque a caixa de seleção **Monitorar todas as portas dos aplicativos especificados**.
6. Clique **Selecionar**.

   Aparecerá uma lista de aplicativos para os quais as portas de rede são monitoradas pelo Kaspersky Endpoint Security.

7. Use o botão de alternância na coluna **Status** para habilitar ou desabilitar o monitoramento da porta de rede.
8. Se um aplicativo não estiver incluído na lista, adicione-o desta forma:

   a. Clique **Adicionar**.

   b. Na janela que se abre, digite o caminho para o arquivo executável do aplicativo e uma breve descrição.

   c. Defina o status **Ativo** ou **Inativo** para o monitoramento de portas de rede.

9. Salvar alterações.

Exportar e importar listas de portas monitoradas

O Kaspersky Endpoint Security usa as seguintes listas para monitorar as portas de rede: lista de portas de rede e lista de aplicativos cujas portas são monitoradas pelo Kaspersky Endpoint Security. Você pode exportar listas de portas monitoradas para um arquivo XML. Em seguida, você pode modificar o arquivo para, por exemplo, adicionar um grande número de portas com a mesma descrição. Você também pode usar a função de exportação/importação para fazer backup das listas de portas monitoradas ou para migrar as listas para um servidor diferente.

Como exportar e importar listas de portas monitoradas no Console de Administração (MMC)

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Configurações de rede**.

5. Para exportar a lista de portas de rede:

   a. No bloco **Portas monitoradas**, selecione **Monitorar somente as portas de rede selecionadas**.

   b. Clique no link **selecionados N portas**.

      A janela **Portas de rede** é aberta. A janela **Portas de rede** exibe uma lista de portas de rede que são geralmente usadas para a transmissão de e-mail e tráfego de rede. Esta lista de portas de rede está incluída no pacote do Kaspersky Endpoint Security.

   c. Na lista de portas de rede, selecione as portas que deseja exportar.

   d. Clique **Exportar**.

   e. Na janela que é aberta, insira o nome do arquivo XML para o qual deseja exportar a lista de portas de rede e selecione a pasta na qual deseja salvar esse arquivo.

   f. Salvar o arquivo.

      O Kaspersky Endpoint Security exporta toda a lista de portas de rede para o arquivo XML.

6. Para exportar a lista de aplicativos cujas portas são monitoradas pelo Kaspersky Endpoint Security:

   a. No bloco **Portas monitoradas**, marque a caixa de seleção **Monitorar todas as portas dos aplicativos especificados**.

   b. Clique no link **selecionados N aplicativos**.

   c. Na lista de aplicativos, selecione os aplicativos que deseja exportar.

   d. Clique **Exportar**.

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

   f. Salvar o arquivo.

      O Kaspersky Endpoint Security exporta toda a lista de aplicativos para o arquivo XML.

7. Para importar a lista de portas de rede:

   a. Na lista de portas de rede, clique no botão **Importar**.

      Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de portas de rede.

   b. Abra o arquivo.

      Se o computador já tiver uma lista de portas de rede, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

8. Para importar uma lista de aplicativos cujas portas são monitoradas pelo Kaspersky Endpoint Security:

   a. Na lista de aplicativos, clique no botão **Importar**.

      Na janela que é aberta, selecione o arquivo XML do qual deseja importar a lista de aplicativos.

b. Abra o arquivo.

Se o computador já tiver uma lista de aplicativos, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

9. Salvar alterações.

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Configurações gerais** → **Configurações de rede**.

4. No bloco **Portas monitoradas**, selecione **Monitorar somente as portas de rede selecionadas**.

5. Clique **Configurações**.

A janela **Portas de rede** é aberta. A janela **Portas de rede** exibe uma lista de portas de rede que são geralmente usadas para a transmissão de e-mail e tráfego de rede. Esta lista de portas de rede está incluída no pacote do Kaspersky Endpoint Security.

6. Para exportar a lista de portas de rede:

a. Na lista de portas de rede, selecione as portas que deseja exportar. Para selecionar várias portas, use as teclas **CTRL** ou **SHIFT**.

Se você não selecionou nenhuma porta, o Kaspersky Endpoint Security exportará todas as portas.

b. Clique **Exportar**.

c. Na janela que é aberta, insira o nome do arquivo XML para o qual deseja exportar a lista de portas de rede e selecione a pasta na qual deseja salvar esse arquivo.

d. Salvar o arquivo.

O Kaspersky Endpoint Security exporta toda a lista de portas de rede para o arquivo XML.

7. Para exportar a lista de aplicativos cujas portas são monitoradas pelo Kaspersky Endpoint Security:

a. Marque a caixa de seleção **Monitorar todas as portas dos aplicativos especificados**.

b. Na lista de aplicativos, selecione os aplicativos que deseja exportar. Para selecionar várias portas, use as teclas **CTRL** ou **SHIFT**.

Se você não selecionou nenhum aplicativo, o Kaspersky Endpoint Security exportará todos os aplicativos.

c. Clique **Exportar**.

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

e. Salvar o arquivo.

O Kaspersky Endpoint Security exporta toda a lista de aplicativos para o arquivo XML.

8. Para importar a lista de portas de rede:

a. Na lista de portas de rede, clique no botão **Importar**.

Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de portas de rede.

b. Abra o arquivo.

Se o computador já tiver uma lista de portas de rede, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

9. Para importar uma lista de aplicativos cujas portas são monitoradas pelo Kaspersky Endpoint Security:

a. Na lista de aplicativos, clique no botão **Importar**.

Na janela que é aberta, selecione o arquivo XML do qual deseja importar a lista de aplicativos.

b. Abra o arquivo.

Se o computador já tiver uma lista de aplicativos, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

10. Salvar alterações.

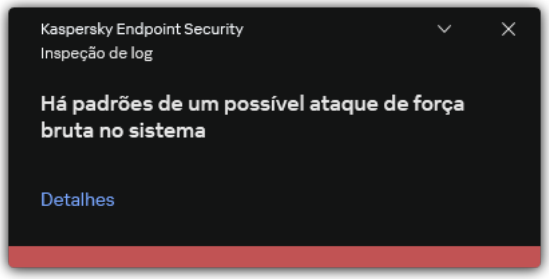
Inspeção do Log

O componente estará disponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para servidores. O componente estará indisponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para estações de trabalho.

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 Endpoint 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* (veja a figura abaixo).

Caso queira usar a Inspeção de Log, certifique-se de que as configurações de segurança da política de auditoria estejam definidas e que o sistema esteja registrando os eventos relevantes (para mais informações, consulte o site de suporte técnico da Microsoft.).



Notificação de Inspeção de Log

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 regras predefinidas no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Controles de Segurança** → **Inspeção de log**.
4. Certifique-se de que a caixa de seleção **Inspeção de log** esteja marcada.
5. No bloco **Regras predefinidas**, clique no botão **Configurações**.
6. 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**.
7. 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**.

8. 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. No bloco **Detecção de logon na rede**, especifique o início e o fim do intervalo de tempo.

      O Kaspersky Endpoint 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 Endpoint Security não monitora as tentativas de logon desses usuários e computadores.

   d. Clique em **OK**.

9. Salvar alterações.

Como configurar as regras predefinidas no Web Console e Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Inspeção de log**.

5. Certifique-se de que o botão de alternância **Inspeção de Log ATIVADA** esteja ligado.

6. No bloco **Regras predefinidas**, ative ou desative as regras predefinidas usando os 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**.

   a. **Alterações suspeitas detectadas no grupo de administradores integrado privilegiado**.

7. Caso seja necessário, configure a regra **Há padrões de um possível ataque de força bruta no sistema**:

   a. Clique em **Configurações** sob a 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 **OK**.

8. Se tiver selecionado a regra **Há uma atividade atípica detectada durante a sessão de logon na rede**, será preciso definir suas configurações:

   a. Clique em **Configurações** sob a regra.

   b. No bloco **Detecção de logon na rede**, especifique o início e o fim do intervalo de tempo.

      O Kaspersky Endpoint 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. No bloco **Exclusões**, adicione 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 Endpoint Security não monitora as tentativas de logon desses usuários e computadores.

   d. Clique **OK**.

9. Salvar alterações.

Como configurar regras predefinidas na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Inspeção de log**.

3. Certifique-se de que o botão de alternância **Inspeção de log** esteja ligado.

4. No bloco **Regras predefinidas**, clique no botão **Configurar**.

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**.

a. **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 em **Configurações** sob a 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.

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 em **Configurações** sob a regra.

   b. No bloco **Detecção de logon de rede**, especifique o início e o fim do intervalo de tempo.

      O Kaspersky Endpoint 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. No bloco **Exclusões**, adicione 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 Endpoint Security não monitora as tentativas de logon desses usuários e computadores.

8. Salvar alterações.

Como resultado, quando a regra é acionada, o Kaspersky Endpoint Security cria um *Evento crítico*.

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 três regras criadas pelos especialistas da Kaspersky.

Como adicionar uma regra personalizada no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Controles de Segurança** → **Inspeção de log**.
4. Certifique-se de que a caixa de seleção **Inspeção de log** esteja marcada.
5. No bloco **Regras personalizadas**, clique no botão **Configurações**.
6. Na janela aberta, marque as caixas de seleção ao lado das regras personalizadas que deseja ativar.
7. Se necessário, clique em **Adicionar** para criar suas próprias regras personalizadas.
8. 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.
9. Salvar alterações.

Como adicionar uma regra personalizada no Web Console e no Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Controles de segurança** → **Inspeção de log**.
5. Certifique-se de que o botão de alternância **Inspeção de Log ATIVADA** esteja ligado.
6. No bloco **Regras personalizadas**, selecione as regras personalizadas que deseja ativar.
7. Se necessário, clique em **Adicionar** para criar suas próprias regras personalizadas.
8. Uma janela será aberta; nessa janela, configure a regra personalizada:
   - **Nome da regra**.
   - **Nome de log personalizado**. Logs de eventos do Windows. Os seguintes logs estão disponíveis: *Application*, *Security*, *System*.

- **Origem**. 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.

9. Salvar alterações.

Como adicionar uma regra personalizada na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Inspeção de log**.

3. Certifique-se de que o botão de alternância **Inspeção de log** esteja ligado.

4. No bloco **Regras personalizadas**, clique no botão **Configurar**.

5. Na janela aberta, marque as caixas de seleção ao lado das regras personalizadas que deseja ativar.

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*).

   - **Identificador 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 é acionada, o Kaspersky Endpoint Security cria um evento *Crítico*.

Monitor de integridade do sistema

O componente estará disponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para servidores. O componente estará indisponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para estações de trabalho.

A partir da versão 12.6 o Kaspersky Endpoint Security for Windows inclui o componente do monitor de integridade do sistema em vez do componente do 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 Endpoint 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 *Verificação de integridade do sistema*, 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.

Migração das configurações do Monitor de integridade de arquivos

Ao atualizar o Kaspersky Endpoint Security para a versão 12.6, as configurações do monitor de integridade de arquivos são migradas automaticamente. Como parte da migração, o aplicativo move as regras de monitoramento para o monitor de integridade do sistema. As regras do monitor de integridade de arquivos são migradas para o monitor de integridade do sistema quando a migração do KSWS para o KES for feita.

> Para garantir a operação correta do monitor de integridade do sistema, o aplicativo Kaspersky Endpoint Security e o plug-in de gerenciamento devem ser atualizados para a versão 12.6. Caso tenha uma versão anterior do plug-in de gerenciamento instalado, não será possível configurar o monitor de integridade do sistema porque o plug-in de gerenciamento não tem a seção **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 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.

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 monitor de integridade do sistema não monitora as alterações nos arquivos nas pastas compartilhadas do servidor. O monitor de integridade do sistema só pode ser usado localmente.

O Kaspersky Endpoint 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` (disponível apenas no Monitor de integridade do sistema em tempo real)

- `HKEY_CURRENT_USER` (disponível apenas no Monitor de integridade do sistema em tempo real)

> A tarefa *Verificação 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.

Modos do monitor de integridade do sistema em tempo real

Para garantir que as regras do monitor de integridade do sistema não bloqueiem nenhuma ação com recursos críticos para o funcionamento do sistema operacional ou outros serviços, recomendamos ativar o modo de teste e analisar como o componente afeta o sistema. Com o modo de teste ativado, o Kaspersky Endpoint Security não bloqueia a atividade do usuário proibida pelas regras, em vez disso, gera eventos *Aviso* ⚠.

O componente monitor de integridade do sistema em tempo real tem dois modos:

- Bloquear

  Neste modo, o monitor de integridade do sistema rastreia as alterações no sistema e executa uma ação de acordo com as regras: **Permitir** ou **Bloquear**. O monitor de integridade do sistema também gera um evento correspondente e altera o status do dispositivo no console do Kaspersky Security Center.

- Informar

  Neste modo, o monitor de integridade do sistema permite executar ações com arquivos e chaves do registro do escopo de monitoramento. Se a ação com os arquivos ou o registro for proibida, o aplicativo gerará um evento: *A operação proibida foi permitida no modo de teste*. Para analisar como as regras afetam o sistema, basta consultar os relatórios.

Ativação do monitoramento da integridade do sistema em tempo real

Como ativar o monitor de integridade do sistema em tempo real no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Controles de Segurança** → **Monitor de integridade do sistema**.
4. Marque a caixa de seleção **Monitor de integridade do sistema**.
5. Em **Modo de operação para regras de bloqueio**, selecione um modo para o monitor de integridade do sistema em tempo real:
   - **Bloquear**. Neste modo, o monitor de integridade do sistema bloqueia as ações com arquivos e chaves do registro do escopo de monitoramento e gera um evento correspondente.
   - **Informar**. Neste modo, o monitor de integridade do sistema permite executar ações com arquivos e chaves do registro do escopo de monitoramento e gera um evento correspondente.
6. No bloco **Monitor de integridade do sistema em tempo real**, marque a caixa de seleção **Monitor de integridade do sistema em tempo real**.
7. 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 do dispositivo externo: *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.

8. Configure o monitoramento de arquivos e registros:

   a. Marque a caixa de seleção **Monitorar os arquivos e o registro**.

   b. Clique **Configurações**.

      Isso abre a lista de regras do monitor de integridade do sistema.

   c. Clique **Adicionar**.

      Também é possível importar as regras de outra fonte.

   d. Configure a regra do monitor de integridade do sistema (consulte a tabela abaixo).

9. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar o monitor de integridade do sistema em tempo real no Web Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Monitor de integridade do sistema**.

5. Ative o botão de alternância **Monitor de integridade do sistema** ATIVADO.

6. Selecione a guia **Windows**.

7. Em **Monitor de integridade do sistema em tempo real**, selecione um modo para o monitor de integridade do sistema em tempo real:

   - **Aplicar regras**. Neste modo, o monitor de integridade do sistema bloqueia as ações com arquivos e chaves do registro do escopo de monitoramento e gera um evento correspondente.

   - **Testar regras (informar)**. Neste modo, o monitor de integridade do sistema permite executar ações com arquivos e chaves do registro do escopo de monitoramento e gera um evento correspondente.

8. Configure o monitoramento de arquivos e registros:

   a. Marque a caixa de seleção **Monitorar os arquivos e o registro**.

   b. Clique **Regras**.

      Isso abre a lista de regras do monitor de integridade do sistema.

   c. Clique **Adicionar**.

      Também é possível importar as regras de outra fonte.

   d. Configure a regra do monitor de integridade do sistema (consulte a tabela abaixo).

9. 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 do dispositivo externo: *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.

10. Para aplicar a política aos computadores, feche os ícones de cadeado 🔒 e salve as alterações.

Como ativar o monitor de integridade do sistema em tempo real na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Monitor de integridade do sistema**.

3. Ativar o botão de alternância **Monitor de integridade do sistema**.

4. Em **Modo de operação para regras de bloqueio**, selecione um modo para o monitor de integridade do sistema em tempo real:

   - **Bloquear**. Neste modo, o monitor de integridade do sistema bloqueia as ações com arquivos e chaves do registro do escopo de monitoramento e gera um evento correspondente.

   - **Informar**. Neste modo, o monitor de integridade do sistema permite executar ações com arquivos e chaves do registro do escopo de monitoramento e gera um evento correspondente.

5. No bloco **Monitor de integridade do sistema em tempo real**, marque a caixa de seleção **Monitor de integridade do sistema em tempo real**.

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 do dispositivo externo: *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.

7. Configure o monitoramento de arquivos e registros:

   a. Marque a caixa de seleção **Monitorar os arquivos e o registro**.

   b. Clique **Configurar**.

      Isso abre a lista de regras do monitor de integridade do sistema.

   c. Clique **Adicionar**.

      Também é possível importar as regras de outra fonte.

8. Configure a regra do monitor de integridade do sistema (consulte a tabela abaixo).

9. Salvar alterações.

Configurações da regra do monitor de integridade do sistema em tempo real

Parâmetro	Descrição
Nome da regra	Nome da regra do monitor de integridade do sistema em tempo real
Operações com os arquivos e registro	• **Permitir**. O monitor de integridade do sistema permite executar ações com arquivos e chaves do registro do escopo de monitoramento. • **Bloquear**. O comportamento do monitor de integridade do sistema depende do modo selecionado. Caso o *modo de proteção do sistema* seja selecionado, o monitor de integridade do sistema bloqueia as ações com os arquivos e chaves de registro do escopo de monitoramento, gera um evento correspondente e altera o status do dispositivo no console do Kaspersky Security Center. Caso o *modo de teste* seja selecionado, o monitor de integridade do sistema permite executar ações com os arquivos e chaves do registro do escopo de monitoramento.
Nível de gravidade do evento	O Kaspersky Endpoint 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 de evento: *Informativo*, *Aviso*, *Crítico*.

Escopo de monitoramento	• **Arquivo**. Lista de arquivos e pastas monitorados pelo componente. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.
	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.
	  • `?` (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**. Lista de chaves de registro e valores monitorados pelo componente. O Kaspersky Endpoint Security tem suporte aos caracteres `*` e `?` ao inserir uma máscara.

Exclusões	• **Arquivo**. Lista de exclusões do escopo de monitoramento. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara. Por exemplo, `C:\Folder\Application\*.log`. As entradas de exclusão têm uma prioridade mais alta do que as entradas de escopo de monitoramento.
	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.
	  • `?` (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**. Lista de exclusões do escopo de monitoramento. O Kaspersky Endpoint Security tem suporte aos caracteres `*` e `?` ao inserir uma máscara. As entradas de exclusão têm uma prioridade mais alta do que as entradas de 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 Endpoint 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. A Kaspersky recomenda usar contas de usuário locais somente em casos especiais quando não for possível usar contas de usuário de domínio.

Parâmetro	Descrição
Marcadores de operação de arquivo / Operações monitoradas	Marcadores que caracterizam a ação com os arquivos ou chaves de registro que serão monitorados pelo aplicativo.
Hashing	Cálculo de um hash do arquivo na modificação. O Kaspersky Endpoint Security adiciona informações sobre o hash do arquivo quando um evento é gerado.

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 *Verificação de integridade do sistema*, o aplicativo compara o estado atual dos objetos incluídos no escopo de monitoramento com seu estado de *linha de base*. Em contraste com o monitor de integridade do sistema em tempo real, a tarefa *Verificação de integridade do sistema* ajuda a limitar o número de eventos e permite gerar um relatório geral de alterações no sistema operacional.

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. É possível configurar as regras para serem compartilhadas pelo monitor de integridade do sistema em tempo real e a tarefa *Verificação de integridade do sistema* ou criar regras separadas para a tarefa. Para criar uma linha de base, o Kaspersky Endpoint Security aplica o escopo de monitoramento da tarefa *Verificação de integridade do sistema* para a tarefa *Atualização da linha de base*.

Criação e atualização de uma linha de base

A tarefa *Verificação de integridade do sistema* precisa de uma linha de base para funcionar. A *linha de base* é um estado registrado de objetos no sistema que o aplicativo usa como referência ao comparar com o estado atual. Caso o estado atual do sistema seja diferente do estado do sistema registrado na linha de base, o Kaspersky Endpoint Security gerará o evento correspondente. É possível criar ou atualizar uma linha de base com o uso da tarefa *Atualização da linha de base*.

É possível atualizar a linha de base nos seguintes modos:

- Atualização completa.

  O aplicativo atualiza todos os objetos no escopo de monitoramento.

- Atualização incremental.

  O aplicativo detecta e atualiza apenas os objetos modificados ou novos.

Como criar ou atualizar uma linha de base no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **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

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Atualização da linha de base**.

Etapa 2. Seleção do modo de atualização da linha de base

Seleção do modo de atualização da linha de base:

- **Atualização completa**. O aplicativo atualiza todos os objetos no escopo de monitoramento.
- **Atualização incremental**. O aplicativo detecta e atualiza apenas os objetos modificados ou novos.

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. Definir o nome da tarefa

Digite o nome da tarefa, por exemplo *linha de base 2024*.

Etapa 5. Concluir a criação da tarefa

Conclua o 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 criar ou atualizar uma linha de base no Web Console

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Atualização da linha de base**.

   c. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Linha de base 2024*.

   d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Vá para a próxima etapa.

5. Selecione uma conta para executar a tarefa. Por padrão, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de usuário local.

6. Conclua o assistente.

   Uma nova tarefa será exibida na lista de tarefas.

7. Clique na Nova Tarefa.

   A janela de propriedades da tarefa é exibida.

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

9. Seleção do modo de atualização da linha de base:

   - **Atualização completa**. O aplicativo atualiza todos os objetos no escopo de monitoramento.

   - **Atualização incremental**. O aplicativo detecta e atualiza apenas os objetos modificados ou novos.

10. Salvar alterações.

11. Marque a caixa de seleção ao lado da tarefa.

12. Clique **Iniciar**.

Configuração do escopo de monitoramento para a tarefa Verificação de integridade do sistema

Por padrão, o escopo de monitoramento da tarefa *Verificação de integridade do sistema* é igual ao escopo de monitoramento do monitor de integridade do sistema em tempo real. 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 Verificação de integridade do sistema no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Controles de Segurança** → **Monitor de integridade do sistema**.

4. Marque a caixa de seleção **Monitor de integridade do sistema**.

5. Em **Verificação de integridade do sistema**, selecione o modo de configuração da tarefa: **Configurações personalizadas**.

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 do dispositivo externo: *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 *Verificação de integridade do sistema*, o aplicativo não monitora a desconexão dos dispositivos externos.

7. Configure o monitoramento de arquivos e registros:

   a. Marque a caixa de seleção **Monitorar os arquivos e o registro**.

   b. Clique **Configurações**.

      Isso abre a lista de regras do monitor de integridade do sistema.

   c. Clique **Adicionar**.

      Também é possível importar as regras de outra fonte.

   d. Configure a regra do monitor de integridade do sistema (consulte a tabela abaixo).

8. Salvar alterações.

Como configurar um escopo de monitoramento diferente para a tarefa Verificação de integridade do sistema no Web Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Monitor de integridade do sistema**.

5. Selecione a guia **Windows**.

6. Ative o botão de alternância **Monitor de integridade do sistema ATIVADO**.

7. Em **Verificação de integridade do sistema**, selecione o modo de configuração da tarefa: **Configurações personalizadas**.

8. 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 do dispositivo externo: *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 *Verificação de integridade do sistema*, o aplicativo não monitora a desconexão dos dispositivos externos.

9. Configure o monitoramento de arquivos e registros:

   a. Marque a caixa de seleção **Monitorar os arquivos e o registro**.

   b. Clique **Regras**.

      Isso abre a lista de regras do monitor de integridade do sistema.

   c. Clique **Adicionar**.

      Também é possível importar as regras de outra fonte.

   d. Configure a regra do monitor de integridade do sistema (consulte a tabela abaixo).

10. Salvar alterações.

Como configurar um escopo de monitoramento diferente para a tarefa Verificação de integridade do sistema na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Controles de segurança** → **Monitor de integridade do sistema**.

3. Ativar o botão de alternância **Monitor de integridade do sistema**.

4. Em **Verificação de integridade do sistema**, selecione o modo de configuração da tarefa: **Configurações personalizadas**.

5. 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 do dispositivo externo: *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 *Verificação de integridade do sistema*, o aplicativo não monitora a desconexão dos dispositivos externos.

6. Configure o monitoramento de arquivos e registros:

   a. Marque a caixa de seleção **Monitorar os arquivos e o registro**.

   b. Clique **Configurar**.

      Isso abre a lista de regras do monitor de integridade do sistema.

   c. Clique **Adicionar**.

      Também é possível importar as regras de outra fonte.

   d. Configure a regra do monitor de integridade do sistema (consulte a tabela abaixo).

7. Salvar alterações.

Configurações de uma regra de tarefa Verificação de integridade do sistema

Parâmetro	Descrição
Nome da regra	Nome da regra de tarefa *Verificação de integridade do sistema*.
Nível de gravidade do evento	O Kaspersky Endpoint 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 de evento: *Informativo*, *Aviso*, *Crítico*.

Escopo de monitoramento	• **Arquivo**. Lista de arquivos e pastas monitorados pelo componente. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.
	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.
	  • `?` (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**. Lista de chaves de registro e valores monitorados pelo componente. O Kaspersky Endpoint Security tem suporte aos caracteres `*` e `?` ao inserir uma máscara.

Exclusões	• **Arquivo**. Lista de exclusões do escopo de monitoramento. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara. Por exemplo, `C:\Folder\Application\*.log`. As entradas de exclusão têm uma prioridade mais alta do que as entradas de escopo de monitoramento.
	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.
	  • `?` (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**. Lista de exclusões do escopo de monitoramento. O Kaspersky Endpoint Security tem suporte aos caracteres `*` e `?` ao inserir uma máscara. As entradas de exclusão têm uma prioridade mais alta do que as entradas de escopo de monitoramento.

Execução da tarefa de Verificação de integridade do sistema

A tarefa *Verificação de integridade do sistema* 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 *Verificação de integridade do sistema* nos seguintes modos:

- Verificação rápida.

  Ao verificar as possíveis alterações de arquivos, os aplicativos verificam somente os atributos do arquivo. O aplicativo não verifica o conteúdo dos arquivos.

- Verificação Completa.

  Ao verificar as possíveis alterações de arquivos, os aplicativos verificam todos seus atributos e conteúdo.

O modo em que a tarefa é executada não afeta a verificação do registro ou dos dispositivos externos.

Como executar a tarefa de Verificação de integridade do sistema no Console de Administração (MMC)

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

2. Na árvore do console, selecione **Tarefas**.

   A lista de tarefas é aberta.

3. Clique **Nova tarefa**.

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

4. Selecione **Kaspersky Endpoint Security** → **Monitor de integridade do sistema de linha de base**. Selecione um modo monitor de integridade do sistema:

   - **Verificação completa**. Nesse modo, o aplicativo verifica todos os atributos e hashes dos arquivos.

   - **Verificação rápida**. Nesse modo, o aplicativo verifica somente os atributos dos arquivos.

5. 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.

   - Especifique a seleção de dispositivos para os quais 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.

6. Selecione uma conta para executar a tarefa. Por padrão, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de usuário local.

7. Configure um agendamento para iniciar uma tarefa, por exemplo, manualmente ou em um dia da semana específico.

8. Insira um nome para a tarefa.

9. Conclua o 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 uma tarefa de Verificação de integridade do sistema no Web Console

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Verificação de integridade do sistema**.

   c. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Verificação semanal de integridade do sistema*.

   d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Vá para a próxima etapa.

5. Selecione uma conta para executar a tarefa. Por padrão, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de usuário local.

6. Conclua o assistente.

   Uma nova tarefa será exibida na lista de tarefas.

7. Clique na Nova Tarefa.

   A janela de propriedades da tarefa é exibida.

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

9. Selecione um modo verificação de integridade do sistema:

   - **Verificação rápida**. O aplicativo verifica somente os atributos do arquivo. O aplicativo não verifica o conteúdo dos arquivos.

   - **Verificação completa**. O aplicativo verifica todos os atributos dos arquivos e seu conteúdo.

10. Salvar alterações.

11. Marque a caixa de seleção ao lado da tarefa.

12. Clique **Iniciar**.

Para que a tarefa *Verificação de integridade do sistema* seja concluída com êxito, o escopo de monitoramento da tarefa *Verificação de integridade do sistema* deve corresponder completamente à linha de base. Caso o escopo de monitoramento seja diferente, a tarefa será concluída com um erro. Para sincronizar os escopos de monitoramento, execute a tarefa *Atualização da linha de base* com um novo escopo de monitoramento.

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 (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Controles de Segurança** → **Monitor de integridade do sistema**.
4. Para exportar ou importar as regras do *monitor de integridade do sistema em tempo real*:
   a. No bloco **Monitor de integridade do sistema em tempo real**, clique no botão **Configurações**.
   b. Para exportar uma lista de regras do monitor de integridade do sistema em tempo real:
      1. Selecione as regras que deseja exportar. Para selecionar várias portas, use as teclas **`CTRL`** ou **`SHIFT`**.

         Se você não selecionou nenhuma regra, o Kaspersky Endpoint Security exportará todas as regras.
      2. Clique no link **Exportar**.
      3. 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.
      4. Salvar o arquivo.

         O Kaspersky Endpoint Security exporta toda a lista de regras para o arquivo XML.
   c. Para importar uma lista de regras do monitor de integridade do sistema em tempo real:
      1. Clique no link **Importar**.

         Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de regras.
      2. Abra o arquivo.

         Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

5. Para exportar ou importar as regras de *verificação de integridade do sistema*:

   a. No bloco **Verificação de integridade do sistema**, selecione **Configurações personalizadas**.

   b. Clique **Configurações**.

   c. Para exportar a lista de regras de verificação de integridade do sistema:

      1. Selecione as regras que deseja exportar. Para selecionar várias portas, use as teclas **CTRL** ou **SHIFT**.

         Se você não selecionou nenhuma regra, o Kaspersky Endpoint Security exportará todas as regras.

      2. Clique no link **Exportar**.

      3. 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.

      4. Salvar o arquivo.

      O Kaspersky Endpoint Security exporta toda a lista de regras para o arquivo XML.

   d. Para importar uma lista de regras de verificação de integridade do sistema:

      1. Clique no link **Importar**.

         Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de regras.

      2. Abra o arquivo.

      Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

6. Salvar alterações.

Como exportar e importar uma lista de regras do Monitor de integridade do sistema no Web Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Controles de segurança** → **Monitor de integridade do sistema**.

5. Selecione a guia **Windows**.

6. Para exportar ou importar as regras do *monitor de integridade do sistema em tempo real*:

   a. No bloco **Monitor de integridade do sistema em tempo real**, clique no link **Regras**.

   b. Para exportar uma lista de regras do monitor de integridade do sistema em tempo real:

      1. Selecione as regras que deseja exportar.

      2. Clique no botão → **Exportar**.

         O Kaspersky Endpoint Security exporta a lista de regras para um arquivo JSON na pasta de downloads padrão.

   c. Para importar uma lista de regras do monitor de integridade do sistema em tempo real:

      1. Clique no botão → **Importar**.

         Na janela exibida, selecione o arquivo JSON do qual deseja importar a lista de endereços confiáveis.

      2. Abra o arquivo.

         Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo JSON.

7. Para exportar ou importar as regras de *verificação de integridade do sistema*:

   a. No bloco **Verificação de integridade do sistema sob demanda**, selecione **Configurações personalizadas**.

   b. Clique no link **Regras**.

   c. Para exportar a lista de regras de verificação de integridade do sistema:

      1. Selecione as regras que deseja exportar.

      2. Clique no botão → **Exportar**.

         O Kaspersky Endpoint Security exporta a lista de regras para um arquivo JSON na pasta de downloads padrão.

   d. Para importar uma lista de regras de verificação de integridade do sistema:

      1. Clique no botão → **Importar**.

         Na janela exibida, selecione o arquivo JSON do qual deseja importar a lista de endereços confiáveis.

      2. Abra o arquivo.

         Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo JSON.

8. 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 Endpoint Security gera os seguintes relatórios sobre o componente:

- Na interface do aplicativo:
  - O relatório monitor de integridade do sistema
  - O relatório de verificação de integridade do sistema
  - O relatório de 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

  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 (MMC)

  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 Web Console

1. Na janela principal do Web Console, selecione **Monitoramento** → **Relatórios**.

2. Clique **Adicionar**.

   O Assistente de novo modelo de relatório é iniciado.

3. Em **Tipo de 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.

Redefinição do status de integridade do sistema

Os computadores no console do Kaspersky Security Center têm um dos seguintes status: *OK*, *Advertência*, ou *Crítico*. Caso o monitor de integridade do sistema detecte a modificação de arquivos ou chaves de registro no escopo de monitoramento, o status do computador será alterado para *Advertência* ou *Crítico*. O status atribuído pelo monitor de integridade do sistema é chamado de *status de integridade do sistema*. É possível redefinir o status de integridade do sistema, por exemplo, se a análise convencer de que a modificação detectada de objetos não afeta a segurança do computador.

Como redefinir o status de integridade do sistema no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **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

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Redefinição do status de integridade do sistema**.

Etapa 2. 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 3. Configurar um agendamento de início de tarefa

Configure o agendamento da tarefa, por exemplo, manualmente.

Etapa 4. Definir o nome da tarefa

Insira o nome da tarefa, por exemplo, *Redefinição do status depois da modificação do escopo de monitoramento*.

Etapa 5. Concluir a criação da tarefa

Conclua o 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 redefinir o status de integridade do sistema no Web Console

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Redefinição do status de integridade do sistema**.

   c. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Redefinição do status após a modificação do escopo de monitoramento*.

   d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Vá para a próxima etapa.

5. Selecione uma conta para executar a tarefa. Por padrão, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de usuário local.

6. Conclua o assistente.

   Uma nova tarefa será exibida na lista de tarefas.

7. Marque a caixa de seleção ao lado da tarefa.

8. Clique **Iniciar**.

Então, caso o status do computador seja alterado para *Advertência* ou *Crítico* devido aos eventos do monitor de integridade do sistema, o status do computador será redefinido para *OK*. Caso o status do computador também tenha sido alterado devido a outros eventos, o status do computador permanecerá inalterado.

Cloud Discovery

O Cloud Discovery gerencia o acesso do usuário aos serviços na nuvem. Os serviços na nuvem incluem, por exemplo, o Microsoft Teams, o Salesforce e o Microsoft Office 365. Os serviços em nuvem são agrupados em categorias, por exemplo, *Compartilhamento de arquivos*, *Aplicativos de mensagens*, *E-mail*. Os especialistas da Kaspersky atualizam regularmente as categorias do Cloud Discovery e os serviços na nuvem classificados nelas. O Kaspersky Endpoint Security atualiza o conjunto de categorias e os serviços na nuvem com os bancos de dados do aplicativo. Isso significa que o Cloud Discovery não usa a Kaspersky Security Network para categorizar os serviços na nuvem.

O Cloud Discovery oferece a seguinte funcionalidade:

- Monitoramento do uso do serviço na nuvem
- Bloqueio do acesso do usuário a serviços na nuvem

Requisitos do sistema

O Cloud Discovery está disponível caso as seguintes condições sejam satisfeitas:

- O aplicativo está instalado em um computador que executa Windows para estações de trabalho.

  O componente não está disponível para servidores.

- Kaspersky Security Center versão 15.1 ou posterior.

  O componente não está disponível no Console de Administração (MMC). Você pode configurar o Cloud Discovery no Kaspersky Security Center Web Console e no Kaspersky Security Center Cloud Console.

- Licença do Kaspersky Next.

Ative a funcionalidade do aplicativo que o componente Cloud Discovery requer:

1. **Verificar conexões criptografadas**. Isso é necessário para o monitoramento de tráfego HTTPS. É possível gerenciar essa funcionalidade na seção **Configurações de rede**.

2. **Injetar script no tráfego da Web para interagir com páginas da Web**. O script permite o registro de eventos do Cloud Discovery. O script também fornece o bloqueio completo do acesso aos serviços na nuvem. Sem o script, o aplicativo bloqueia o acesso somente por domínios de serviço na nuvem. É possível gerenciar essa funcionalidade na seção **Configurações de rede**.

Também é possível ativar a funcionalidade **Criar log de abertura de páginas autorizadas**. A funcionalidade inclui o agrupamento de eventos quando o usuário visita páginas da Web que pertencem ao mesmo domínio. Dessa forma, quando o usuário utiliza um serviço na nuvem, o Cloud Discovery registra somente um evento em vez de múltiplos eventos para cada página da Web. É possível gerenciar essa funcionalidade na seção **Controle da Web**.

Monitoramento de serviços na nuvem

Quando um usuário começa a usar um serviço na nuvem, o Kaspersky Endpoint Security registra o evento e cria uma entrada no relatório. O Cloud Discovery controla o uso do serviço na nuvem no navegador, assim como em aplicativos correspondentes. O Cloud Discovery controla o uso de serviços na nuvem por HTTP e HTTPS.

Como ativar o monitoramento de serviços na nuvem no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Comunicação e Proteção na Web** → **Cloud Discovery**.

5. Ative o botão de alternância **Cloud Discovery ATIVADO**.

6. Salvar alterações.

Como resultado, o aplicativo encaminha as informações sobre os serviços na nuvem em uso ao Kaspersky Security Center. É possível visualizar as informações de uso de serviços na nuvem nos relatórios. Caso necessário, é possível bloquear o acesso aos serviços na nuvem.

Bloqueio do acesso a serviços na nuvem

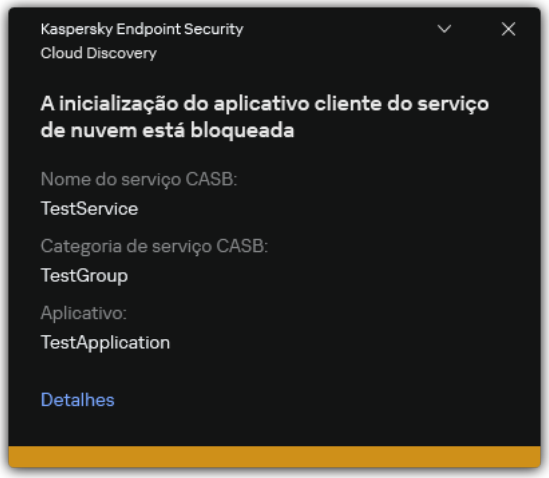
O bloqueio do acesso aos serviços na nuvem está disponível somente para as licenças Kaspersky Next EDR Optimum e XDR Expert. Este recurso não está disponível para a licença do Kaspersky Next EDR Foundations. Consulte a comparação das funcionalidades do aplicativo, dependendo do tipo de licença do Kaspersky Next na Ajuda do Kaspersky Next.

O administrador pode restringir o acesso do usuário a categorias do Cloud Discovery ou a serviços na nuvem individuais. Desse modo, o administrador pode permitir apenas serviços na nuvem seguros e evitar o vazamento de dados. *Informações de nível de risco* são exibidas para cada serviço na nuvem no Cloud Discovery. O nível de risco ajuda a detectar serviços que não atendam aos requisitos de segurança da organização.

O nível de risco é uma estimativa e não implica qualquer declaração sobre a qualidade do serviço na nuvem ou de seu fornecedor. O nível de risco é simplesmente uma recomendação dos especialistas da Kaspersky.

Os níveis de risco dos serviços na nuvem são exibidos na seção **Cloud Discovery** da política, na lista de todos os serviços na nuvem controlados.

Outros componentes do Kaspersky Endpoint Security fornecem proteção contra ameaças e rastreamento de atividade suspeita do usuário durante o uso de serviços na nuvem.



Notificação do Cloud Discovery

O Cloud Discovery não bloqueia aplicativos na nuvem que foram iniciados antes do Kaspersky Endpoint Security.

Como bloquear o acesso aos serviços na nuvem no Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Comunicação e Proteção na Web** → **Cloud Discovery**.
5. Ative o botão de alternância **Cloud Discovery ATIVADO**.

   Uma lista de todos os serviços na nuvem será exibida. Os serviços em nuvem são agrupados em categorias, por exemplo, *Compartilhamento de arquivos*, *Aplicativos de mensagens*, *E-mail*. Os especialistas da Kaspersky atualizam regularmente as categorias do Cloud Discovery e os serviços na nuvem classificados nelas. O Kaspersky Endpoint Security atualiza o conjunto de categorias e os serviços na nuvem com os bancos de dados do aplicativo.

6. Use o botão de alternância na coluna **Acesso** para configurar o acesso aos serviços na nuvem.

7. Salvar alterações.

Como resultado, o aplicativo controla o uso do serviço na nuvem no navegador, assim como em aplicativos correspondentes.

Zona confiável

Uma *zona confiável* é uma lista de objetos e aplicativos configuradas pelo administrador de sistema que o Kaspersky Endpoint 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 Endpoint 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.

Iniciando com o Kaspersky Endpoint Security 12.5 for Windows, você pode adicionar telemetria EDR à zona confiável. Isso permite otimizar os dados que o aplicativo envia para o servidor de coleta de telemetria da solução Kaspersky Anti Targeted Attack Platform (EDR).

A partir do Kaspersky Endpoint Security 12.6 for Windows, as exclusões de verificação e aplicativos confiáveis são adicionadas na zona confiável. As exclusões predefinidas de verificação e aplicativos confiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, Microsoft Exchange e System Center Configuration Manager. Isso significa que não será necessário configurar manualmente uma zona confiável para o aplicativo nos servidores.

A partir do Kaspersky Endpoint Security 12.8 for Windows, é possível instalar o aplicativo no modo Light Agent para proteger ambientes virtuais. Exclusões de verificação e aplicativos confiáveis predefinidos podem ajudar a configurar rapidamente o Kaspersky Endpoint Security em ambientes virtuais Citrix e VMware.

Criar uma exclusão de verificação

Uma *exclusão de verificação* é um conjunto de condições que devem ser atendidas para que o Kaspersky Endpoint Security não verifique um determinado objeto em busca de vírus e outras ameaças. As exclusões de verificação tornam possível usar em segurança software legítimo que pode ser explorado por criminosos para danificar o computador ou os dados do usuário. Esses aplicativos não têm necessariamente uma finalidade maliciosa, mas podem ser explorados por hackers. Para obter informações detalhadas sobre aplicativos legítimos que invasores podem usar para comprometer o computador ou os dados do usuário, acesse o site da Enciclopédia da Kaspersky.

Estes aplicativos poderão ser bloqueados pelo Kaspersky Endpoint Security. Para impedir que eles sejam bloqueados, você pode configurar exclusões de verificação para os aplicativos em uso. Para fazer isso, adicione o nome ou o nome da máscara que está listada na Enciclopédia de TI da Kaspersky à zona confiável. Por exemplo, você costuma usar o aplicativo Radmin para a administração remota de computadores. O Kaspersky Endpoint Security considera esta atividade como suspeita e poderá bloqueá-la. Para evitar que o aplicativo seja bloqueado, crie uma exclusão de verificação com o nome ou máscara de nome listado na Enciclopédia de TI da Kaspersky.

Se um aplicativo que reúne informações e as envia para serem processadas for instalado no seu computador, o Kaspersky Endpoint Security pode classificar este aplicativo como malware. Para evitar isto, você pode excluir o aplicativo da verificação configurando o Kaspersky Endpoint Security como descrito neste documento.

Exclusões de verificação são usadas pelos seguintes componentes e tarefas do aplicativo que são configurados pelo administrador do sistema:

- Detecção de Comportamento.
- Prevenção de Exploits.
- Prevenção de Intrusão do Host.
- Proteção Contra Ameaças ao Arquivo.
- Proteção Contra Ameaças da Web.
- Proteção Contra Ameaças ao Correio.
- Tarefa de *Verificação de malware*

O Kaspersky Endpoint Security não verifica um objeto se a unidade ou a pasta que contém este objeto estiver incluída no escopo da verificação no início de uma das tarefas de verificação. Contudo, a exclusão de verificação não é aplicada na execução da tarefa de Verificação Personalizada deste objeto.

Como criar uma exclusão de verificação no Console de administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Configurações gerais** → **Exclusões e tipos de objetos**.
5. No bloco **Exclusões de verificação e aplicativos confiáveis** → **Exclusões de verificação**, clique no botão **Configurações**.

   Aparecerá uma janela com uma lista de exclusões.
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 Endpoint Security ocultará a lista consolidada de exclusões de verificação na interface do usuário do aplicativo.

8. Clique em **Adicionar** e selecione uma ação:

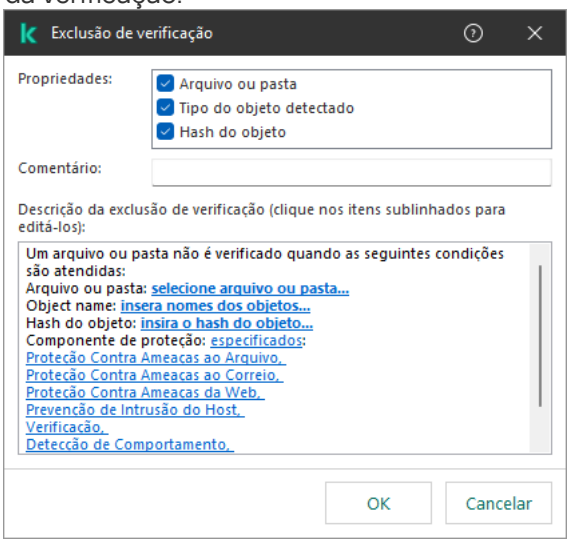
- **Categoria**. É possível agrupar as exclusões de verificação em categorias separadas. Para criar uma nova categoria, insira o seu nome e adicione pelo menos uma exclusão de verificação para ela.

- **Nova exclusão**. O Kaspersky Endpoint Security adiciona uma nova exclusão de verificação à raiz da lista.

- **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Endpoint Security nos servidores SQL, Microsoft Exchange e System Center Configuration Manager, o aplicativo inclui as *exclusões de verificação predefinidas*. Também foram adicionadas exclusões de verificação predefinidas para dar suporte à configuração do aplicativo em ambientes virtuais Citrix e VMware. É necessário selecionar as exclusões predefinidas de verificação dependendo da finalidade do servidor protegido.

- **Nova exclusão para a categoria selecionada**. Para adicionar uma nova exclusão de verificação a uma categoria específica, selecione uma categoria.

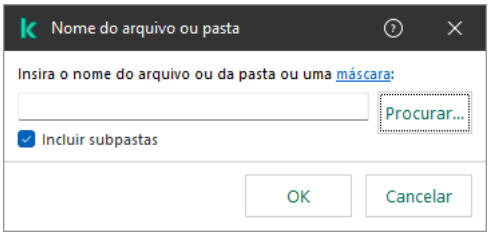
9. Para excluir um Arquivo ou pasta da verificação:



Configurações de exclusão

a. No bloco **Propriedades**, marque a caixa de seleção **Arquivo ou pasta**.

b. Clique no link no bloco abaixo para abrir a janela **Nome do arquivo ou pasta**.



Selecionar arquivo ou pasta

a. Insira o nome do arquivo ou da pasta ou a máscara do nome do arquivo ou da pasta, ou selecione o arquivo ou a pasta na árvore da pasta clicando em **Procurar**.

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.

- `?` (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\`.

O Kaspersky Endpoint Security é compatível com variáveis de ambiente

É possível excluir pastas de rede. Para fazer isso, insira o caminho para a pasta de rede manualmente (por exemplo, `\\Network Share\*`).

> O Kaspersky Endpoint Security não é compatível com a variável de ambiente `%userprofile%` ao gerar uma lista de exclusões por meio do 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.

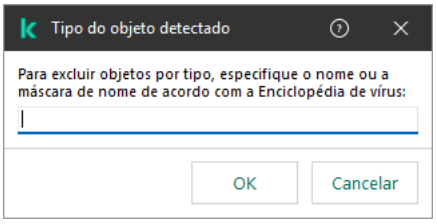
b. Caso seja necessário, desative a funcionalidade **Incluir subpastas**. Se esta funcionalidade estiver ativada, o aplicativo não verificará arquivos em nenhuma das subpastas. Se esta funcionalidade estiver desativada, o aplicativo excluirá somente a pasta selecionada do escopo da verificação. Esta opção está ativada por padrão.

c. Salvar alterações.

10. Para excluir objetos com um nome específico da verificação:

    a. No bloco **Propriedades**, marque a caixa de seleção **Tipo do objeto detectado**.

    b. Clique no link no bloco abaixo para abrir a janela **Tipo do objeto detectado**.



Selecionar objeto

    a. Digite o nome do objeto de acordo com a classificação da Enciclopédia da Kaspersky (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 Endpoint Security exclui os objetos `Client-IRC`, `Client-P2P` e `Client-SMTP` das verificações.

    b. Salvar alterações.

11. Se você deseja excluir um arquivo individual das verificações:

    a. No bloco **Propriedades**, marque a caixa de seleção **Hash do objeto**.

    b. Clique no link no bloco abaixo para abrir a janela **Hash do objeto**.

Selecionar arquivo

    a. Insira o hash do arquivo ou selecione o arquivo clicando no botão **Procurar**.

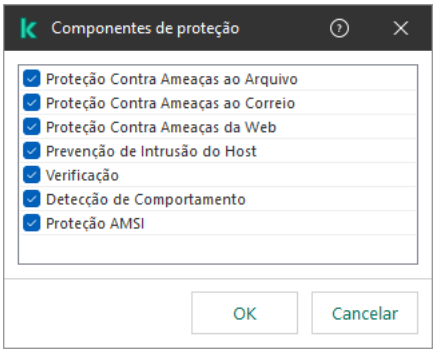
    Se o arquivo for modificado, o hash do arquivo também será modificado. Se isso acontecer, o arquivo modificado não será adicionado às exclusões.

    b. Salvar alterações.

12. Se necessário, no campo **Comentário**, insira uma breve observação sobre a exclusão de verificação que está sendo criada.

13. Especifique os componentes do Kaspersky Endpoint Security que devem usar a exclusão de verificação:

    a. Clique no link no bloco abaixo para abrir a janela **Componentes de proteção**.



Selecionar componentes de proteção

    a. Selecione as caixas em frente dos componentes aos quais a exclusão de verificação deve ser aplicada.

    Se os componentes forem especificados nas configurações da exclusão de verificação, essa exclusão será aplicada apenas durante a verificação feita por esses componentes do Kaspersky Endpoint Security.

    Se os componentes não forem especificados nas configurações da exclusão de verificação, esta exclusão será aplicada durante a verificação feita por todos os componentes do Kaspersky Endpoint Security.

14. Clique **OK**.

    A nova exclusão será adicionada à lista. É possível desativar a exclusão a qualquer momento usando a caixa de seleção ao lado do objeto.

15. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como criar uma exclusão de verificação no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Ir para a seção **Zona Confiável**.

5. Na janela aberta, clique no link **Exclusões de Verificação de malware**.

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 Endpoint 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 Endpoint Security adiciona uma nova exclusão de verificação à raiz da lista.

   - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Endpoint Security nos servidores SQL, Microsoft Exchange e System Center Configuration Manager, o aplicativo inclui as *exclusões de verificação predefinidas*. Também foram adicionadas exclusões de verificação predefinidas para dar suporte à configuração do aplicativo em ambientes virtuais Citrix e VMware. É necessário selecionar as exclusões predefinidas de verificação dependendo da finalidade do servidor protegido.

   Para adicionar uma nova exclusão de verificação a uma categoria, marque a caixa de seleção ao lado dela e selecione a opção **Nova exclusão**.

9. Selecione como deseja adicionar a exclusão: **Caminho para o arquivo ou pasta**, **Tipo de objeto** ou **Hash do objeto**.

10. Para excluir um arquivo ou pasta da verificação, insira o caminho manualmente. O Kaspersky Endpoint 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.

    - `?` (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\`.

      É possível excluir pastas de rede. Para fazer isso, insira o caminho para a pasta de rede manualmente (por exemplo, `\\Network Share\*`).

11. Se você deseja excluir um tipo específico de objeto das verificações, no campo **Tipo de objeto**, digite o nome do tipo de objeto de acordo com a classificação da Enciclopédia Kaspersky (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 Endpoint Security exclui os objetos `Client-IRC`, `Client-P2P` e `Client-SMTP` das verificações.

12. Se você deseja excluir um arquivo individual das verificações, insira o hash do arquivo no campo **Hash do objeto**.

    Se o arquivo for modificado, o hash do arquivo também será modificado. Se isso acontecer, o arquivo modificado não será adicionado às exclusões.

13. Na seção **Aplicar exclusão a**, selecione os componentes aos quais deseja que a exclusão de verificação se aplique.

14. Se necessário, no campo **Comentário**, insira uma breve observação sobre a exclusão de verificação que está sendo criada.

15. Clique em **OK**.

    A nova exclusão será adicionada à lista. Você pode usar o botão de alternância para interromper uma exclusão a qualquer momento.

16. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

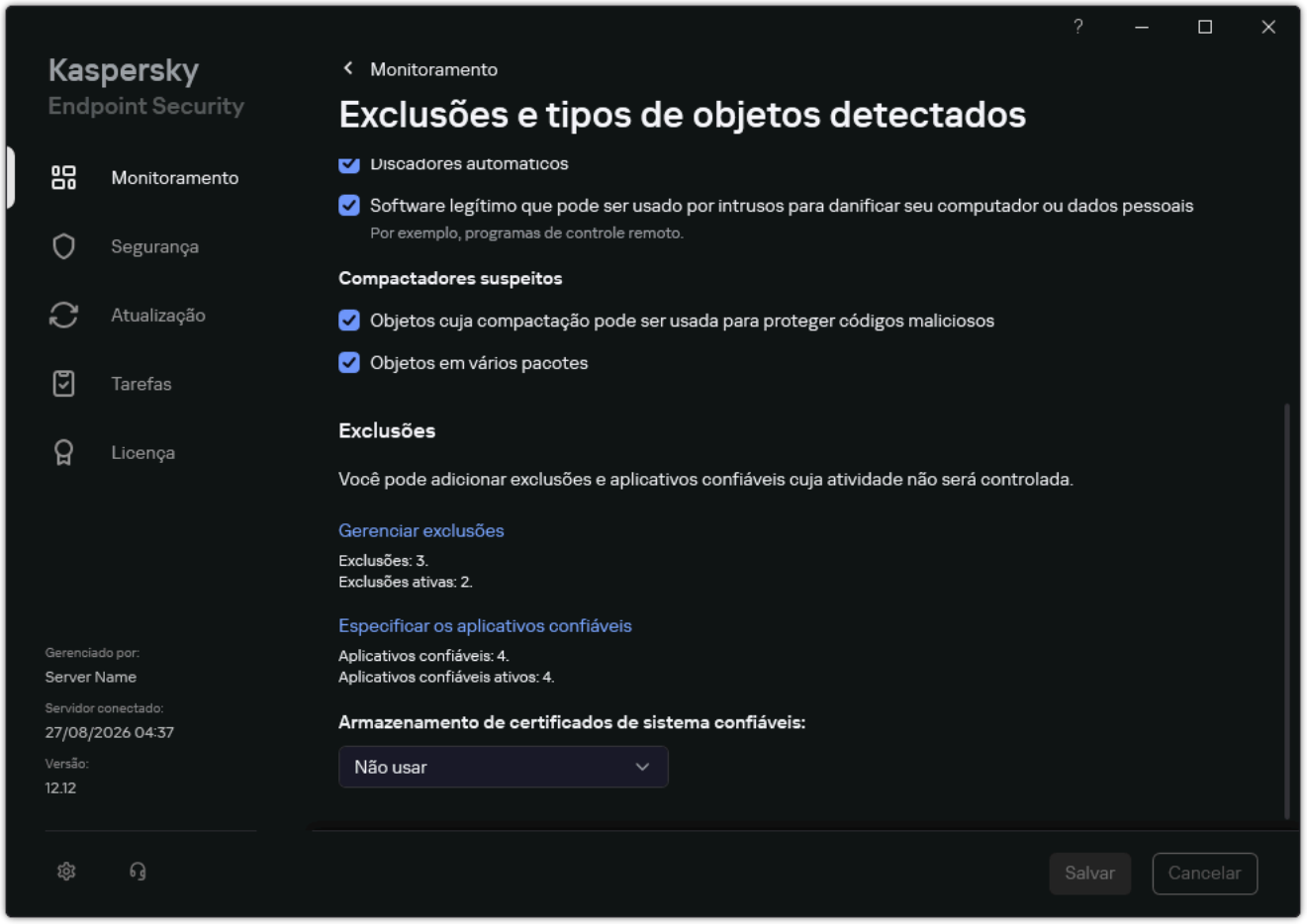
Como criar uma exclusão de verificação na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Exclusões e tipos de objetos detectados**.

3. No bloco **Exclusões**, clique no link **Gerenciar exclusões**.

O Kaspersky Endpoint Security oculta a lista de exclusões de verificação na interface do usuário do aplicativo caso a configuração de exclusões de verificação seja bloqueada pelo administrador no console (símbolo de "cadeado fechado") e as exclusões de verificação local sejam proibidas (a caixa de seleção **Permitir o uso de exclusões locais** estará desmarcada).



Configurações de exclusões

4. 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 Endpoint Security adiciona uma nova exclusão de verificação à raiz da lista.

   - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Endpoint Security nos servidores SQL, Microsoft Exchange e System Center Configuration Manager, o aplicativo inclui as *exclusões de verificação predefinidas*. Também foram adicionadas exclusões de verificação predefinidas para dar suporte à configuração do aplicativo em ambientes virtuais Citrix e VMware. É necessário selecionar as exclusões predefinidas de verificação dependendo da finalidade do servidor protegido.

   Para adicionar uma nova exclusão de verificação a uma categoria, marque a caixa de seleção ao lado dela e selecione a opção **Nova exclusão**.

5. Se você deseja excluir um arquivo ou pasta das verificações, selecione o arquivo ou pasta clicando no botão **Procurar**.

   Também é possível inserir o caminho manualmente. O Kaspersky Endpoint 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.

   - `?` (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\`.

     É possível excluir pastas de rede. Para fazer isso, insira o caminho para a pasta de rede manualmente (por exemplo, `\\Network Share\*`).

6. Se você deseja excluir um tipo específico de objeto das verificações, no campo **Tipo do objeto detectado**, digite o nome do tipo de objeto de acordo com a classificação da Enciclopédia Kaspersky (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 Endpoint Security exclui os objetos `Client-IRC`, `Client-P2P` e `Client-SMTP` das verificações.

7. Se você deseja excluir um arquivo individual das verificações, insira o hash do arquivo no campo **Hash do objeto**.

   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 **Componentes de proteção**, selecione os componentes aos quais deseja que a exclusão de verificação se aplique.

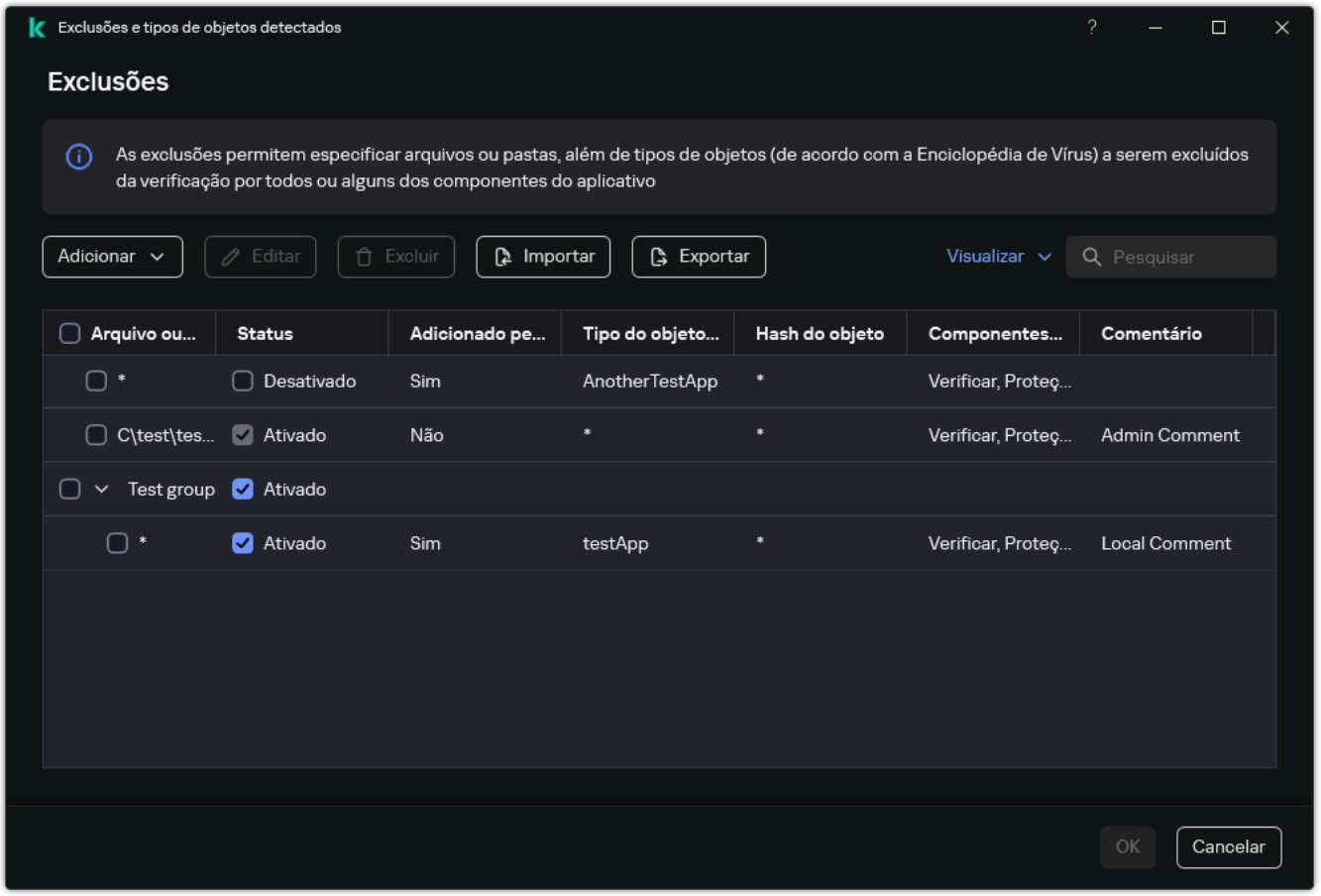
9. Se necessário, no campo **Comentário**, insira uma breve observação sobre a exclusão de verificação que está sendo criada.

10. Selecione o status **Ativo** para a exclusão.

11. Clique **Adicionar**.

    A nova exclusão será adicionada à lista. É possível desativar a exclusão a qualquer momento usando a caixa de seleção na coluna **Status**.

12. Salvar alterações.



Lista de exclusões

Exemplos de máscara de caminho:

Recomendamos especificar os caminhos relativos em vez de caminhos absolutos. Isso permite excluir não apenas os objetos do sistema de arquivos, mas também os objetos sem arquivos. Por exemplo, `*\Program Files (x86)\Folder\Subfolder`.

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 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 "test" localizados na pasta `C:\dir\`, mas não nas subpastas de `C:\dir\`.
- A máscara `C:\dir\*\test` incluirá todos os caminhos para arquivos nomeados "test" 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 nomeadas "dir", mas não nas subpastas dessas pastas.
- A máscara `dir\*` incluirá todos os caminhos para arquivos nas pastas nomeadas "dir", mas não nas subpastas dessas pastas.
- A máscara `dir\` incluirá todos os caminhos para arquivos nas pastas nomeadas "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 "test" em pastas nomeadas "dir", mas não nas subpastas dessas pastas.

Criação de uma exclusão por tipo de objetos detectados

O Kaspersky Endpoint Security classifica os objetos detectados da seguinte forma:

- **Vírus e worms**

  Subcategoria: Vírus e worms (Viruses_and_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 *Overwriting* gravam seu código sobre o código do arquivo que é infectado e apagam, assim, o conteúdo do arquivo. O arquivo infectado deixa de funcionar e não pode ser restaurado. Os vírus *Parasitic* modificam os arquivos para deixá-los total ou parcialmente funcionais. *Companion* não modifica arquivos, mas, em vez disso, cria arquivos duplicados. 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 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 por meio de Internet Relay Chats, ou seja, 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.
Net-Worm	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 (exploração) 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.

Tipo	Name	Descrição
P2P-Worm	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 (incluindo ransomware)**

  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.
Trojan	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.

Tipo	Name	Descrição
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 Trojan-Dropper 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 a ele 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.
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.

Tipo	Name	Descrição
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
Constructor	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	Explorações	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, uma exploração pode gravar ou ler arquivos ou solicitar páginas da Web "infectadas". Explorações 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. Uma exploração 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. Uma exploração incorporada 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 explorações. Nuker exploits são pacotes de rede que desativam os computadores.
FileCryptor	Criptografadores	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.

Tipo	Name	Descrição
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 legítimo que pode ser usado por intrusos para danificar 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
Cliente-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.
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.
Cliente-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 Endpoint 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 multicompactados.

  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 Endpoint Security verifica arquivos compactados.

Por padrão, o Kaspersky Endpoint Security detecta todos os tipos de objetos. Recomendamos deixar a detecção de todos os tipos de objetos ativada para melhorar a segurança do computador. Caso esteja usando utilitários internos que o aplicativo detecta como maliciosos, adicione-os em uma lista de exclusão, mas não desative a detecção de todo o tipo de objetos.

Como selecionar tipos de objetos detectados no Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Configurações gerais** → **Exclusões e tipos de objetos**.
5. No bloco **Tipos de objetos detectados**, clique no botão **Configurações**.
6. Na janela aberta, marque as caixas de seleção do lado oposto aos tipos de objetos que deseja detectar com o Kaspersky Endpoint Security.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como selecionar os tipos de objetos detectáveis no Web Console e no Cloud Console

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

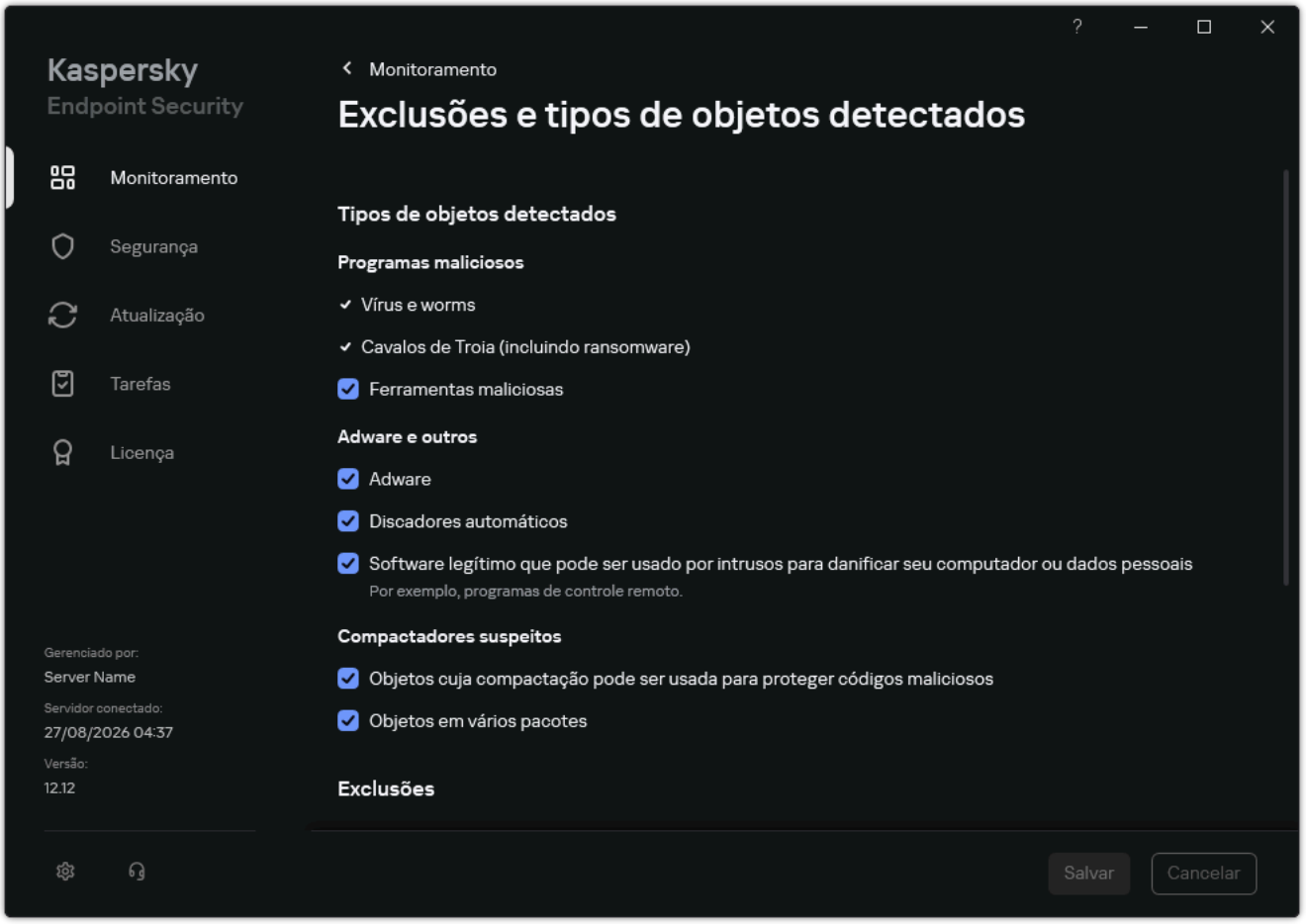
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Configurações de detecção**.
5. No bloco **Detecção de outros tipos de objetos**, marque as caixas de seleção do lado oposto aos tipos de objetos que deseja detectar com o Kaspersky Endpoint Security.
6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como selecionar os tipos de objetos detectáveis na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .
2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Exclusões e tipos de objetos detectados**.

3. No bloco **Tipos de objetos detectados**, marque as caixas de seleção do lado oposto aos tipos de objetos que deseja detectar com o Kaspersky Endpoint Security.

4. Salvar alterações.



Tipos de objetos detectáveis

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 Endpoint Security. Por padrão, o Kaspersky Endpoint Security monitora todos os objetos que são abertos, executados ou salvos por qualquer processo do aplicativo e controla a atividade de todos os aplicativos e tráfego de rede criada por eles. Depois que um aplicativo é adicionado à lista de aplicativos confiáveis, o Kaspersky Endpoint Security para de monitorar a atividade do aplicativo.

A diferença entre exclusões de verificação e aplicativos confiáveis é que, para as exclusões, o Kaspersky Endpoint 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 Endpoint Security detectará o arquivo e eliminará a ameaça. Se a pasta for adicionada às exclusões, o Kaspersky Endpoint 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 Endpoint Security podem ser consideradas seguras por vários aplicativos. Por exemplo, a interceptação de dados digitados no teclado é um processo de rotina dos programas que alternam automaticamente o layout do teclado (como o Punto Switcher). Para considerar as especificidades desses aplicativos e desativar o monitoramento de suas atividades, é recomendável adicioná-los à lista de aplicativos confiáveis.

Os aplicativos confiáveis ajudam a evitar problemas de compatibilidade entre o Kaspersky Endpoint Security e outros aplicativos (por exemplo, o problema de verificação dupla do tráfego de rede de um computador de terceiros pelo Kaspersky Endpoint 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 Endpoint Security por meio das exclusões de verificação.

Como adicionar um aplicativo à lista confiável no console de administração (MMC)

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

2. Na árvore do console, selecione **Políticas**.

3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

4. Na janela da política, selecione **Configurações gerais** → **Exclusões e tipos de objetos**.

5. No bloco **Exclusões de verificação e aplicativos confiáveis** → **Aplicativos confiáveis**, clique no botão **Configurações**.

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

6. 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.

7. Marque a caixa de seleção **Permitir o uso 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 Endpoint Security ocultará a lista consolidada de aplicativos confiáveis na interface do usuário do aplicativo.

8. 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 Endpoint Security adiciona um novo aplicativo confiável à raiz da lista.

- **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Endpoint Security nos servidores SQL, Microsoft Exchange e System Center Configuration Manager, o aplicativo inclui *aplicativos confiáveis predefinidos*. Também foram adicionados aplicativos confiáveis predefinidos para dar suporte à configuração do aplicativo em ambientes virtuais Citrix e VMware. É necessário selecionar aplicativos confiáveis predefinidos dependendo da finalidade do servidor protegido.

- **Nova exclusão para a categoria selecionada**. Para adicionar um novo aplicativo confiável a uma categoria específica, selecione uma categoria.

9. Selecione os critérios de confiança:

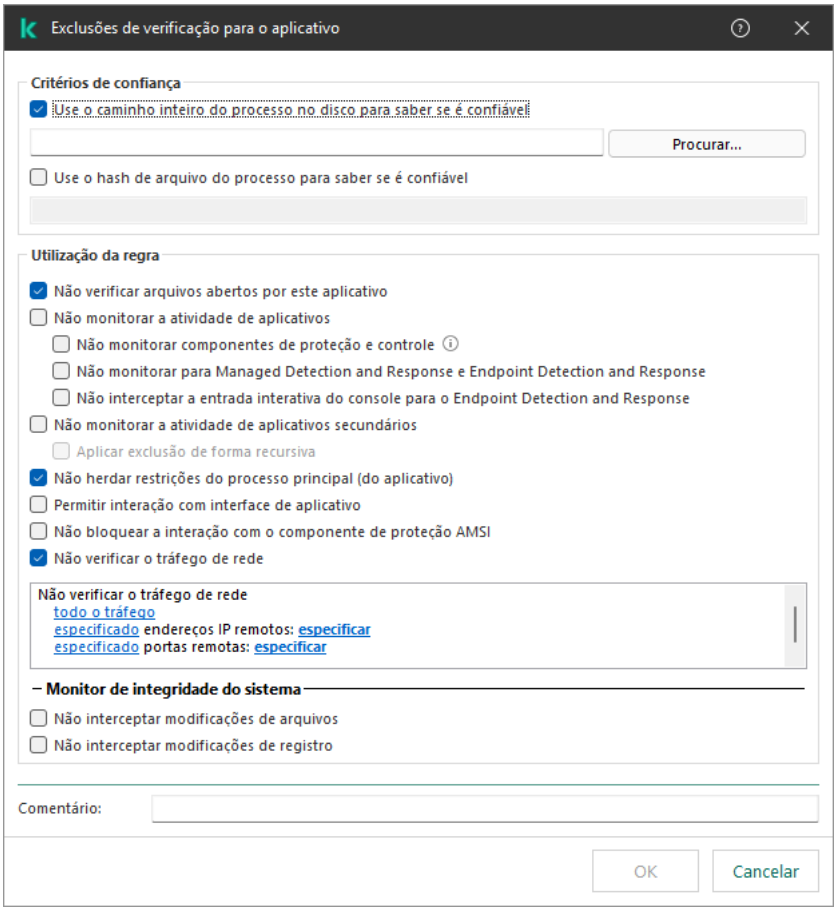
- **Use o caminho inteiro do processo no disco para saber se é confiável**. Insira o caminho para o arquivo executável do aplicativo confiável.

  O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.

  O Kaspersky Endpoint Security trata o nome do arquivo de um aplicativo confiável com a diferenciação de maiúsculas e minúsculas. Caso o nome do arquivo inserido tenha a diferenciação de maiúsculas e minúsculas errada, o Kaspersky Endpoint Security não reconhecerá o aplicativo confiável.

- **Use o hash de arquivo do processo para saber se é confiável**.

O Kaspersky Endpoint 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.



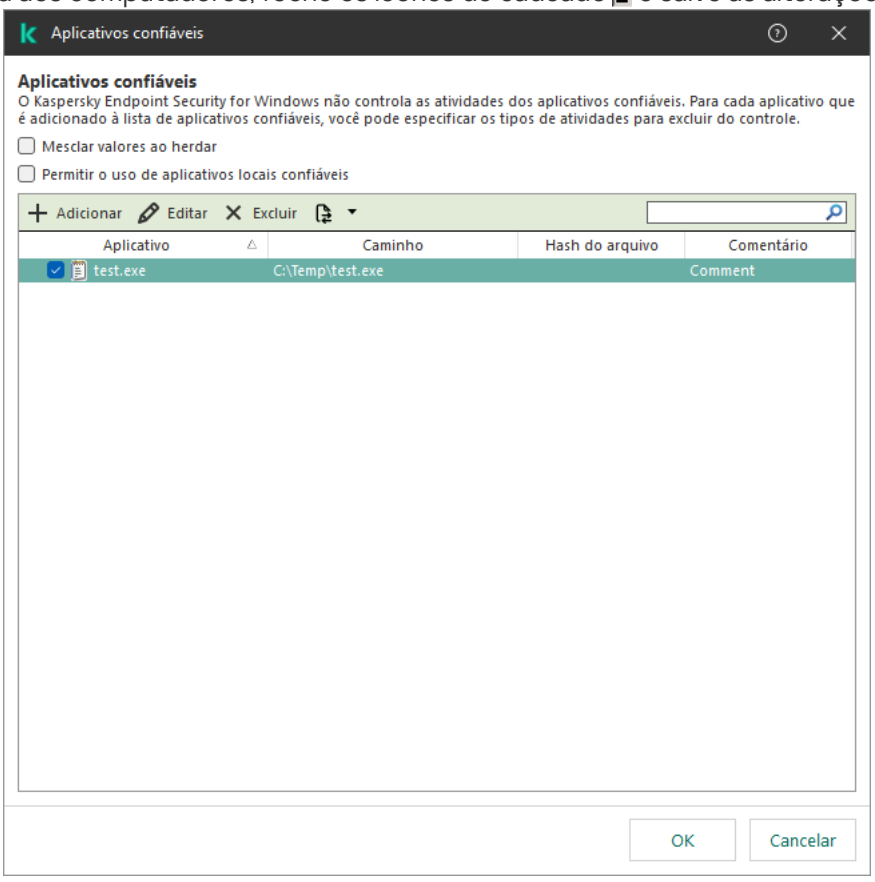
Configurações do aplicativo confiável

10. Defina as configurações avançadas para o aplicativo confiável (consulte a tabela abaixo).

11. 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.

12. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.



Lista de aplicativos confiáveis

Como adicionar um aplicativo na lista confiável no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Ir para a seção **Zona Confiável**.

5. Na janela aberta, clique no link **Aplicativos**.

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

6. 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.

7. Marque a caixa de seleção **Permitir o uso de exclusões locais** 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 Endpoint Security ocultará a lista consolidada de aplicativos confiáveis na interface do usuário do aplicativo.

8. 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 Endpoint Security adiciona um novo aplicativo confiável à raiz da lista.

   - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Endpoint Security nos servidores SQL, Microsoft Exchange e System Center Configuration Manager, o aplicativo inclui *aplicativos confiáveis predefinidos*. Também foram adicionados aplicativos confiáveis predefinidos para dar suporte à configuração do aplicativo em ambientes virtuais Citrix e VMware. É necessário selecionar aplicativos confiáveis predefinidos dependendo da finalidade do servidor protegido.

   Para adicionar um novo aplicativo confiável a uma categoria específica, marque a caixa de seleção ao lado dessa categoria e selecione a opção **Nova exclusão**.

9. Selecione os critérios de confiança:

   - **Caminho para o arquivo ou pasta**. Insira o caminho para o arquivo executável do aplicativo confiável.

     O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.

     O Kaspersky Endpoint Security trata o nome do arquivo de um aplicativo confiável com a diferenciação de maiúsculas e minúsculas. Caso o nome do arquivo inserido tenha a diferenciação de maiúsculas e minúsculas errada, o Kaspersky Endpoint Security não reconhecerá o aplicativo confiável.

   - **Hash do aplicativo**.

   > O Kaspersky Endpoint 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.

10. Defina as configurações avançadas para o aplicativo confiável (consulte a tabela abaixo).

11. 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 **Status**.

12. Para aplicar a política aos computadores, feche os ícones de cadeado 🔒 e salve as alterações.

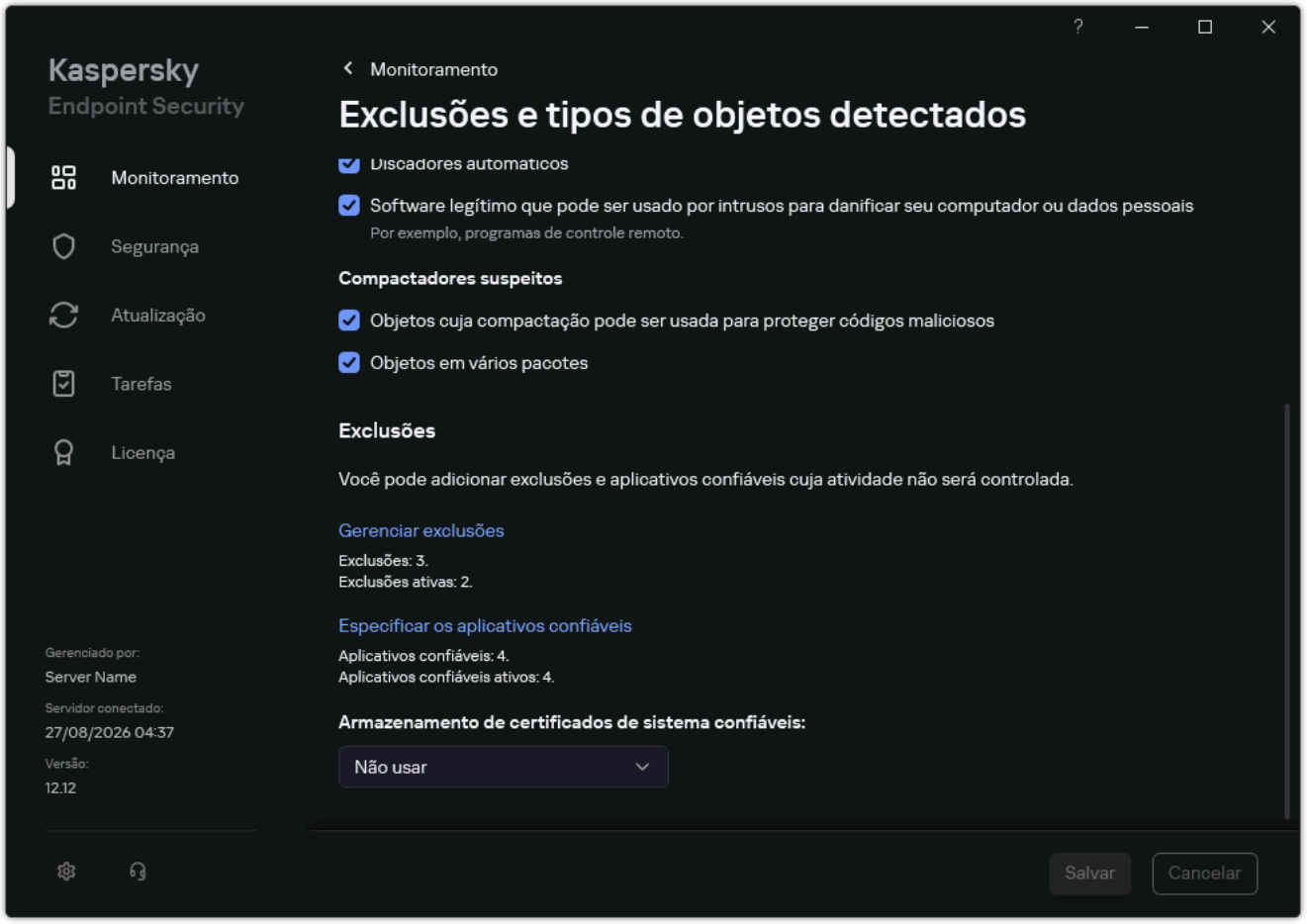
Como adicionar um aplicativo à lista confiável a partir da interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Exclusões e tipos de objetos detectados**.

3. No bloco **Exclusões**, clique no link **Especificar os aplicativos confiáveis**.

> O Kaspersky Endpoint Security oculta a lista consolidada de aplicativos confiáveis na interface do usuário do aplicativo caso a configuração de aplicativos confiáveis seja bloqueada pelo administrador no console (símbolo de "cadeado fechado") e os aplicativos confiáveis locais sejam proibidos (a caixa de seleção **Permitir o uso de aplicativos locais confiáveis** estará desmarcada).



Configurações de exclusões

4. 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 Endpoint Security adiciona um novo aplicativo confiável à raiz da lista.

   - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Endpoint Security nos servidores SQL, Microsoft Exchange e System Center Configuration Manager, o aplicativo inclui *aplicativos confiáveis predefinidos*. Também foram adicionados aplicativos confiáveis predefinidos para dar suporte à configuração do aplicativo em ambientes virtuais Citrix e VMware. É necessário selecionar aplicativos confiáveis predefinidos dependendo da finalidade do servidor protegido.

Para adicionar um novo aplicativo confiável a uma categoria específica, marque a caixa de seleção ao lado dessa categoria e selecione a opção **Nova exclusão**.

5. Selecione os critérios de confiança:

   - **Use o caminho inteiro do processo no disco para saber se é confiável**. Insira o caminho para o arquivo executável do aplicativo confiável.

     O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.

     O Kaspersky Endpoint Security trata o nome do arquivo de um aplicativo confiável com a diferenciação de maiúsculas e minúsculas. Caso o nome do arquivo inserido tenha a diferenciação de maiúsculas e minúsculas errada, o Kaspersky Endpoint Security não reconhecerá o aplicativo confiável.

   - **Use o hash de arquivo do processo para saber se é confiável**.

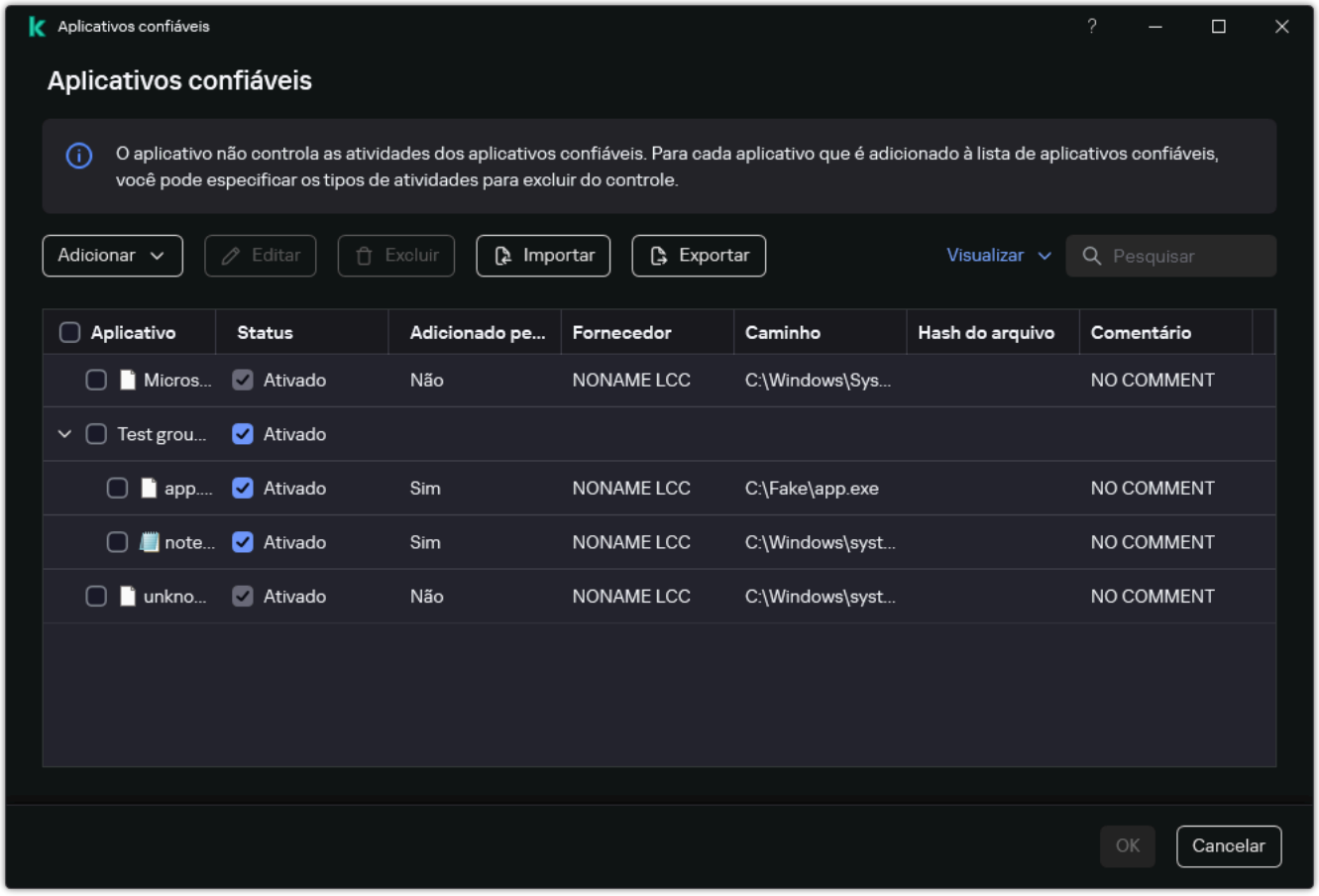
   O Kaspersky Endpoint Security é compatível com variáveis de ambiente e converte o caminho para a interface local do aplicativo. Em outras palavras, se o caminho do arquivo `%userprofile%\Documents\File.exe` for inserido, um registro `C:\Users\Fred123\Documents\File.exe` é adicionado na interface local do aplicativo para o usuário Fred123. Consequentemente, o Kaspersky Endpoint 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. 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 **Status**.

8. Salvar alterações.



Lista de aplicativos confiáveis

Configurações do aplicativo confiável

Parâmetro	Descrição
Não verificar arquivos abertos por este aplicativo	Todos os arquivos abertos pelo aplicativo são excluídos das verificações pelo Kaspersky Endpoint Security. Por exemplo, se você estiver usando aplicativos para fazer backup de arquivos, este recurso ajuda a reduzir o consumo de recursos pelo Kaspersky Endpoint Security.
Não monitorar a atividade do aplicativo	O Kaspersky Endpoint Security não monitorará os arquivos do aplicativo e a atividade de rede no sistema operacional. Você pode configurar o monitoramento da atividade dos aplicativos para diferentes componentes do Kaspersky Endpoint Security: • **Não monitorar componentes de proteção e controle**. A atividade do aplicativo é monitorada pelos seguintes componentes: Detecção de Comportamento, Prevenção de Exploit, Prevenção de Intrusão do Host, Mecanismo de Remediação e Firewall. • **Não monitorar para Managed Detection and Response e Endpoint Detection and Response**. A atividade do aplicativo é monitorada pelo MDR Agent integrado e pelo EDR (KATA) Agent integrado. • **Não interceptar a entrada interativa do console para o Endpoint Detection and Response**. O Kaspersky Endpoint Security não envia dados de telemetria sobre o gerenciamento do aplicativo no console. Os dados de telemetria são usados pela Kaspersky Anti Targeted Attack Platform (EDR).
Não monitorar a atividade de aplicativos secundários	O Kaspersky Endpoint 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 Endpoint Security a um processo filho. O processo pai é iniciado por um aplicativo para o qual os direitos do aplicativo (Prevenção de Intrusão do Host) e as Regras de rede de aplicativos (Firewall) são configurados.
Não monitorar a atividade de aplicativos secundários	O Kaspersky Endpoint 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.
Permitir interação com interface de aplicativo	A Autodefesa do Kaspersky Endpoint 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 Endpoint Security pela interface do Kaspersky Endpoint Security.
Não bloquear a interação com o componente de proteção AMSI	O Kaspersky Endpoint Security não monitorará as solicitações de aplicativos confiáveis para objetos a serem verificados pelo componente de Proteção AMSI.

Parâmetro	Descrição
Não verificar o tráfego de rede	O tráfego de rede iniciado pelo aplicativo será excluído das verificações pelo Kaspersky Endpoint Security. Você pode excluir todo o tráfego ou apenas o tráfego criptografado das verificações. Você também pode excluir endereços IP individuais e números de porta das verificações. O Kaspersky Endpoint Security versão 14.0 ou anterior não é compatível com a exclusão do tráfego de rede se um hash for especificado para um aplicativo confiável em vez de um caminho.
Não interceptar modificações de arquivos *(disponível apenas no console do Kaspersky Security Center)*	O Kaspersky Endpoint Security não monitora as alterações nos arquivos do escopo de monitoramento Monitor de integridade do sistema. O aplicativo aplica a exclusão a todos os modos do Monitor de integridade do sistema: Monitor de integridade do sistema em tempo real e Verificação de integridade do sistema sob demanda.
Não interceptar modificações de registro *(disponível apenas no console do Kaspersky Security Center)*	O Kaspersky Endpoint Security não monitora as alterações nas chaves de registro pelo escopo de monitoramento do Monitor de integridade do sistema. O aplicativo aplica a exclusão a todos os modos do Monitor de integridade do sistema: Monitor de integridade do sistema em tempo real e Verificação de integridade do sistema sob demanda.
Comentário	Se necessário, você pode fornecer um breve comentário sobre o aplicativo confiável. Os comentários ajudam a simplificar as pesquisas e a classificação de aplicativos confiáveis.
Status	Status do aplicativo confiável: • O status **Ativo** significa que o aplicativo está na zona confiável. • O status **Inativo** significa que o aplicativo foi excluído da zona confiável.

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 o uso de aplicativos locais confiáveis** na seção **Exclusões** 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 na interface do usuário 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 Endpoint Security oculta as listas de exclusões de verificação e aplicativos confiáveis na interface do usuário do aplicativo caso a configuração da zona confiável seja bloqueada pelo administrador no console (símbolo de "cadeado fechado") e as exclusões de verificação local e aplicativos confiáveis sejam proibidos.

Como adicionar um aplicativo na lista confiável no Console de Administração (MMC)

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

2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertencem os respectivos computadores clientes.

3. No espaço de trabalho, selecione a guia **Dispositivos**.

4. Clique duas vezes para abrir a janela de propriedades do computador.

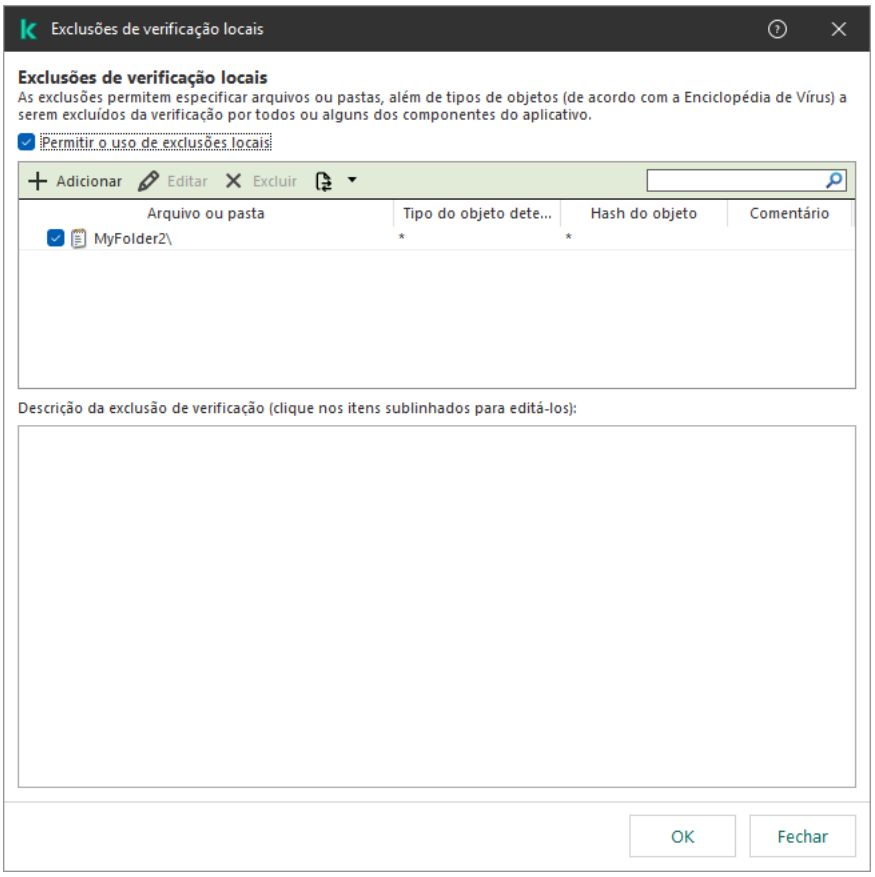
5. Na janela de propriedades do computador, selecione a seção **Aplicativos**.

6. Na lista de aplicativos da Kaspersky instalados no computador, selecione **Kaspersky Endpoint Security for Windows (14.2)** e clique duas vezes para abrir as propriedades do aplicativo.

7. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Exclusões e tipos de objetos**.

8. No bloco **Exclusões de verificação e aplicativos confiáveis** → **Exclusões de verificação locais**, clique no botão **Configurações**.

   Aparecerá uma janela com uma lista de exclusões locais.



Configurações da zona confiável

9. Faça uma lista de exclusões de verificação locais.

   As regras para criar exclusões de verificação locais são iguais às exclusões gerais. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.

10. No bloco **Exclusões de verificação e aplicativos confiáveis** → **Aplicativos locais confiáveis**, clique no botão **Configurações**.

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

11. 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 Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.

12. Salvar alterações.

Como adicionar um objeto à zona confiável local no Kaspersky Security Center Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Ativos (dispositivos)**.
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 Endpoint Security for Windows**.

   Isso abre as configurações locais do aplicativo.
5. Selecione a guia **Configurações do aplicativo**.
6. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Exclusões e tipos de objetos detectados**.
7. No bloco **Exclusões de verificação e aplicativos confiáveis**, clique no link **Exclusões de verificação locais**.
8. Faça uma lista de exclusões de verificação locais.

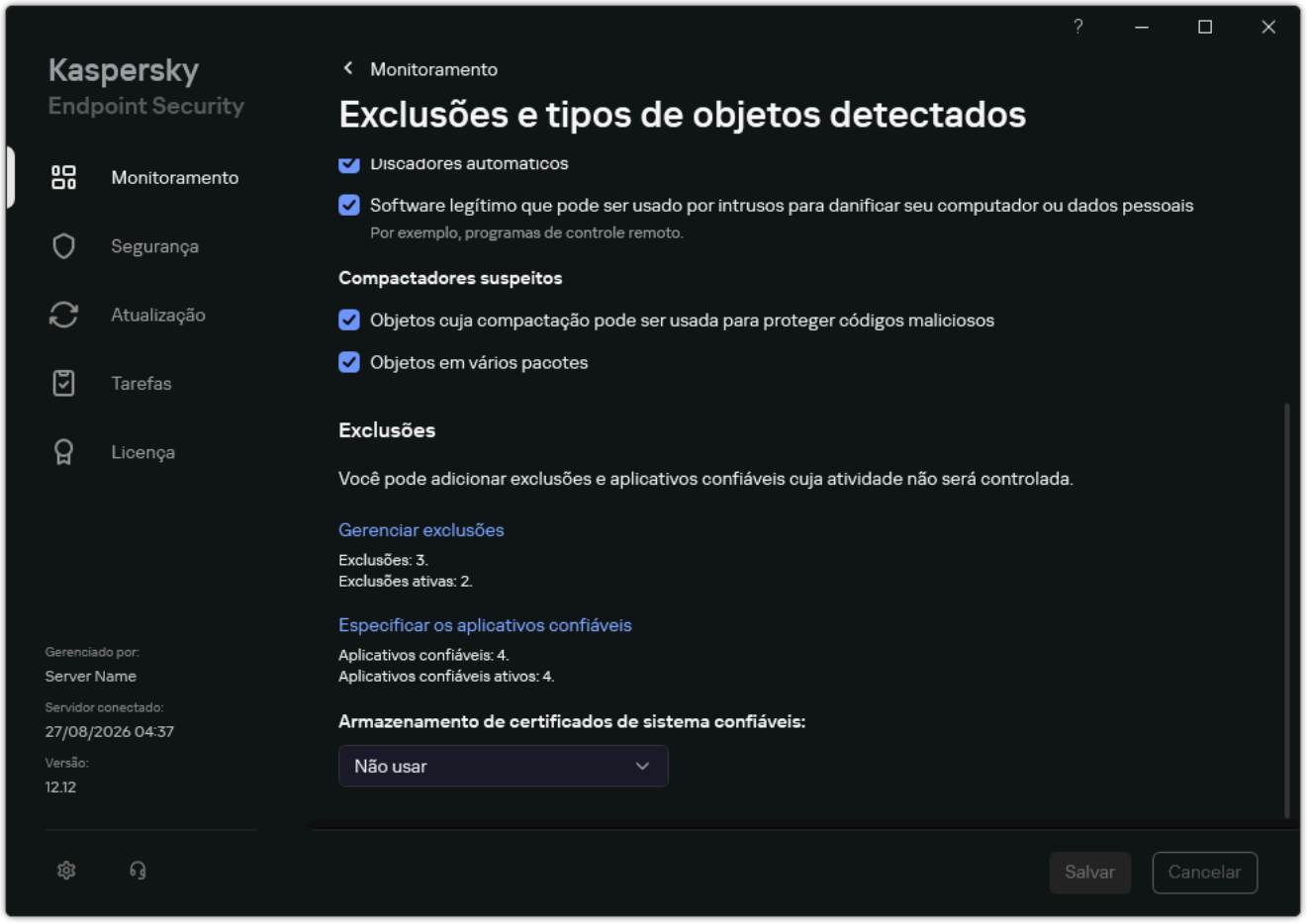
   As regras para criar exclusões locais são iguais às regras para criar exclusões gerais. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.
9. No bloco **Exclusões de verificação e aplicativos confiáveis**, clique no link **Aplicativos locais confiáveis**.
10. 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 Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.
11. Salvar alterações.

Como criar uma exclusão de verificação local na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Exclusões e tipos de objetos detectados**.
3. No bloco **Exclusões**, clique no link **Gerenciar exclusões**.

O Kaspersky Endpoint Security oculta a lista de exclusões de verificação na interface do usuário do aplicativo caso a configuração de exclusões de verificação seja bloqueada pelo administrador no console (símbolo de "cadeado fechado") e as exclusões de verificação local sejam proibidas (a caixa de seleção **Permitir o uso de exclusões locais** estará desmarcada).



Configurações de exclusões

4. 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 Endpoint Security adiciona uma nova exclusão de verificação à raiz da lista.

   - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Endpoint Security nos servidores SQL, Microsoft Exchange e System Center Configuration Manager, o aplicativo inclui as *exclusões de verificação predefinidas*. Também foram adicionadas exclusões de verificação predefinidas para dar suporte à configuração do aplicativo em ambientes virtuais Citrix e VMware. É necessário selecionar as exclusões predefinidas de verificação dependendo da finalidade do servidor protegido.

   Para adicionar uma nova exclusão de verificação a uma categoria, marque a caixa de seleção ao lado dela e selecione a opção **Nova exclusão**.

5. Se você deseja excluir um arquivo ou pasta das verificações, selecione o arquivo ou pasta clicando no botão **Procurar**.

Também é possível inserir o caminho manualmente. O Kaspersky Endpoint 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.

- `?` (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\`.

  É possível excluir pastas de rede. Para fazer isso, insira o caminho para a pasta de rede manualmente (por exemplo, `\\Network Share\*`).

6. Se você deseja excluir um tipo específico de objeto das verificações, no campo **Tipo do objeto detectado**, digite o nome do tipo de objeto de acordo com a classificação da Enciclopédia Kaspersky (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 Endpoint Security exclui os objetos `Client-IRC`, `Client-P2P` e `Client-SMTP` das verificações.

7. Se você deseja excluir um arquivo individual das verificações, insira o hash do arquivo no campo **Hash do objeto**.

   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 **Componentes de proteção**, selecione os componentes aos quais deseja que a exclusão de verificação se aplique.

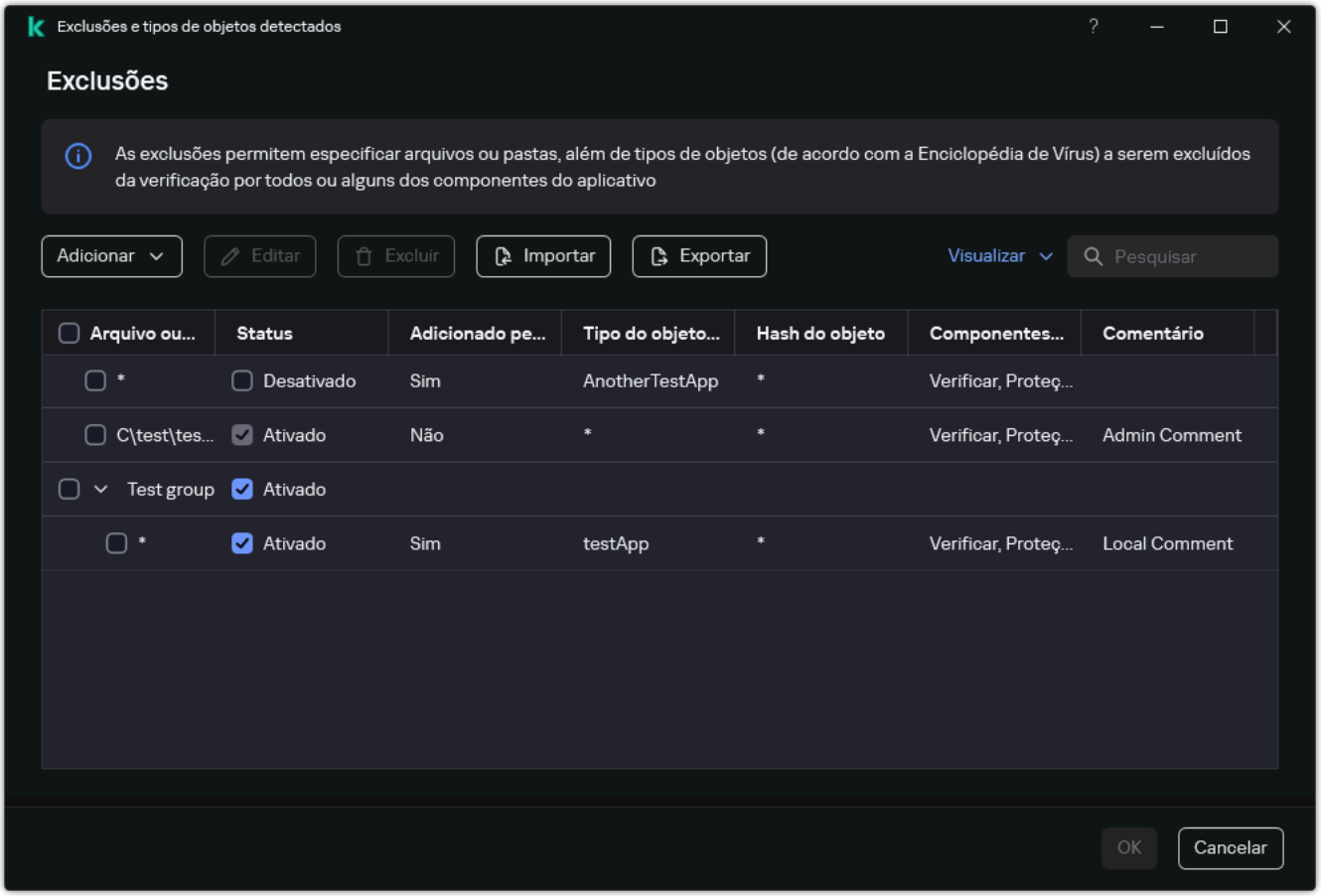
9. Se necessário, no campo **Comentário**, insira uma breve observação sobre a exclusão de verificação que está sendo criada.

10. Selecione o status **Ativo** para a exclusão.

11. Clique **Adicionar**.

    A nova exclusão será adicionada à lista. É possível desativar a exclusão a qualquer momento usando a caixa de seleção na coluna **Status**.

12. Salvar alterações.



Lista de exclusões

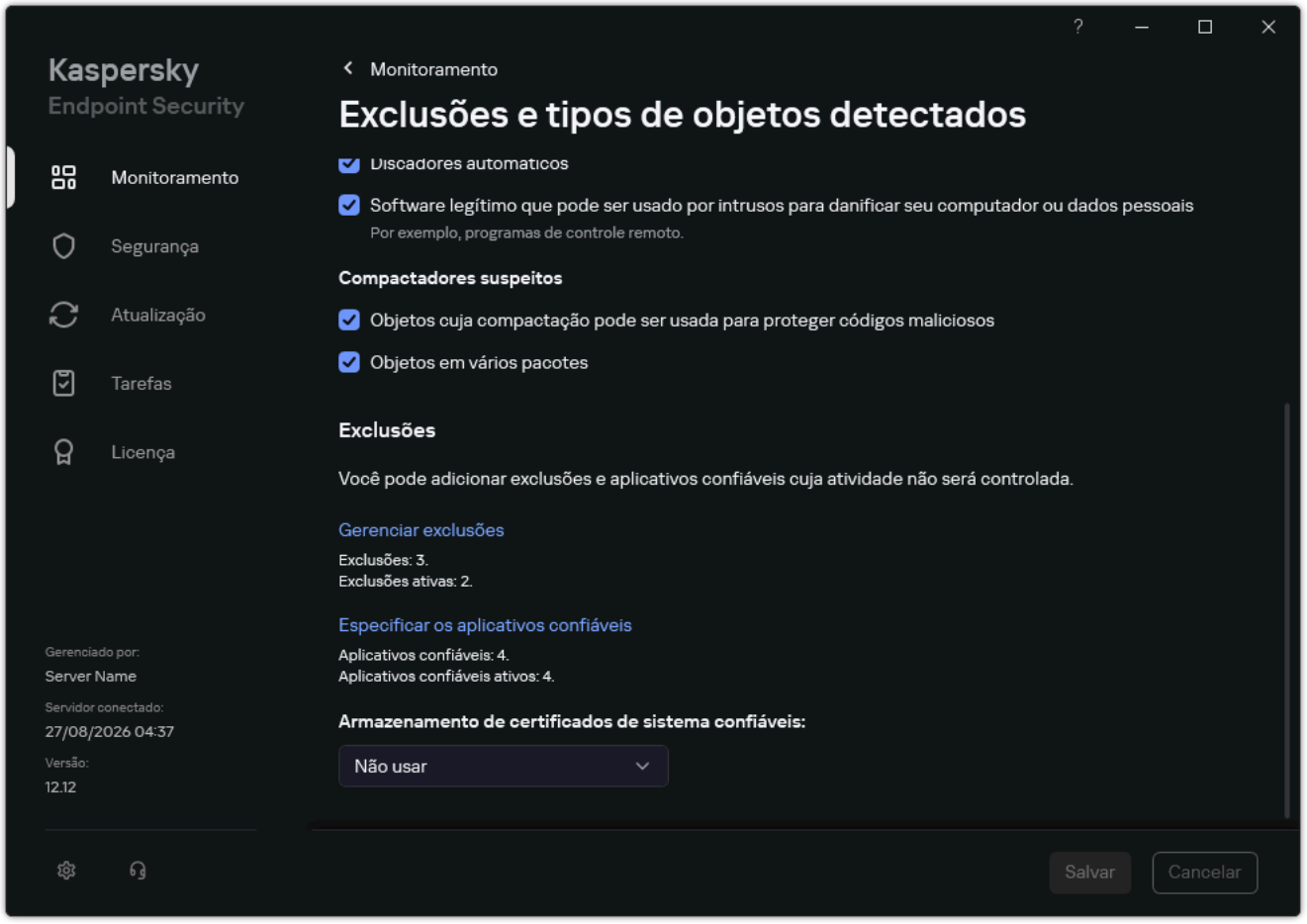
Como adicionar um aplicativo na lista de aplicativos locais confiáveis na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Exclusões e tipos de objetos detectados**.

3. No bloco **Exclusões**, clique no link **Especificar os aplicativos confiáveis**.

O Kaspersky Endpoint Security oculta a lista consolidada de aplicativos confiáveis na interface do usuário do aplicativo caso a configuração de aplicativos confiáveis seja bloqueada pelo administrador no console (símbolo de "cadeado fechado") e os aplicativos confiáveis locais sejam proibidos (a caixa de seleção **Permitir o uso de aplicativos locais confiáveis** estará desmarcada).



Configurações de exclusões

4. 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 Endpoint Security adiciona um novo aplicativo confiável à raiz da lista.

- **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Endpoint Security nos servidores SQL, Microsoft Exchange e System Center Configuration Manager, o aplicativo inclui *aplicativos confiáveis predefinidos*. Também foram adicionados aplicativos confiáveis predefinidos para dar suporte à configuração do aplicativo em ambientes virtuais Citrix e VMware. É necessário selecionar aplicativos confiáveis predefinidos dependendo da finalidade do servidor protegido.

Para adicionar um novo aplicativo confiável a uma categoria específica, marque a caixa de seleção ao lado dessa categoria e selecione a opção **Nova exclusão**.

5. Selecione os critérios de confiança:

- **Use o caminho inteiro do processo no disco para saber se é confiável**. Insira o caminho para o arquivo executável do aplicativo confiável.

  O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.

O Kaspersky Endpoint Security trata o nome do arquivo de um aplicativo confiável com a diferenciação de maiúsculas e minúsculas. Caso o nome do arquivo inserido tenha a diferenciação de maiúsculas e minúsculas errada, o Kaspersky Endpoint Security não reconhecerá o aplicativo confiável.

- **Use o hash de arquivo do processo para saber se é confiável**.

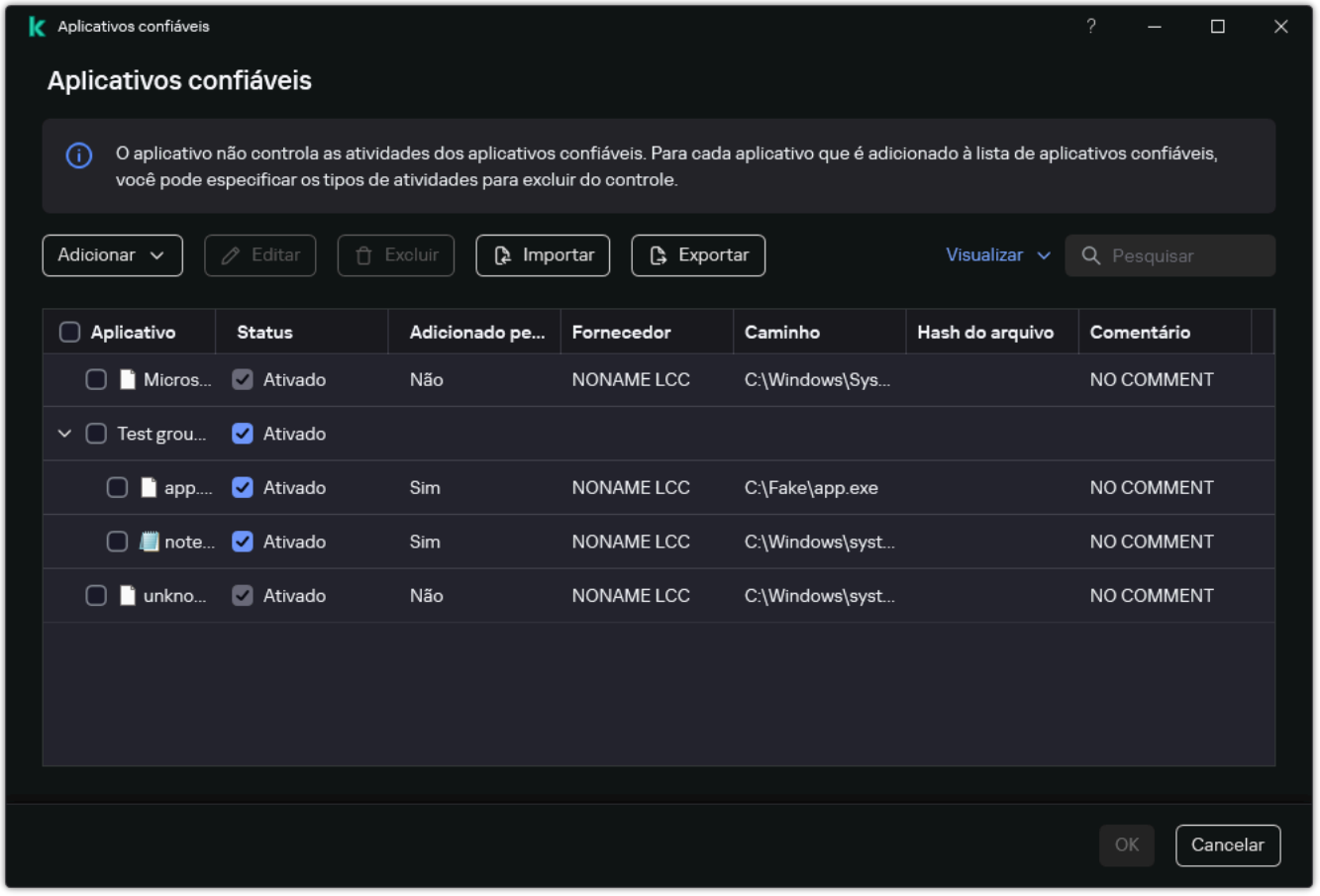
O Kaspersky Endpoint Security é compatível com variáveis de ambiente e converte o caminho para a interface local do aplicativo. Em outras palavras, se o caminho do arquivo `%userprofile%\Documents\File.exe` for inserido, um registro `C:\Users\Fred123\Documents\File.exe` é adicionado na interface local do aplicativo para o usuário Fred123. Consequentemente, o Kaspersky Endpoint 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. 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 **Status**.

8. Salvar alterações.



Lista de aplicativos confiáveis

Exportar e importar a zona confiável

Uma *zona confiável* é uma lista de objetos e aplicativos configuradas pelo administrador de sistema que o Kaspersky Endpoint Security não monitora quando ativado. A zona confiável consiste nas seguintes listas: *exclusões de verificação* e *aplicativos confiáveis*. É possível exportar essas listas para arquivos XML e outros formatos. 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 os seguintes formatos para exportar e importar a *lista de exclusões*:

- O XML está disponível no Console de Administração (MMC), no Web Console e Cloud Console.
- O DAT está disponível apenas para importação no Console de Administração (MMC). O objetivo desse formato é manter a compatibilidade com as versões mais antigas do aplicativo. É possível converter um arquivo DAT em XML no Console de Administração (MMC) para migrar as listas de exclusão para o Web Console.
- CSV só está disponível na interface local do aplicativo.

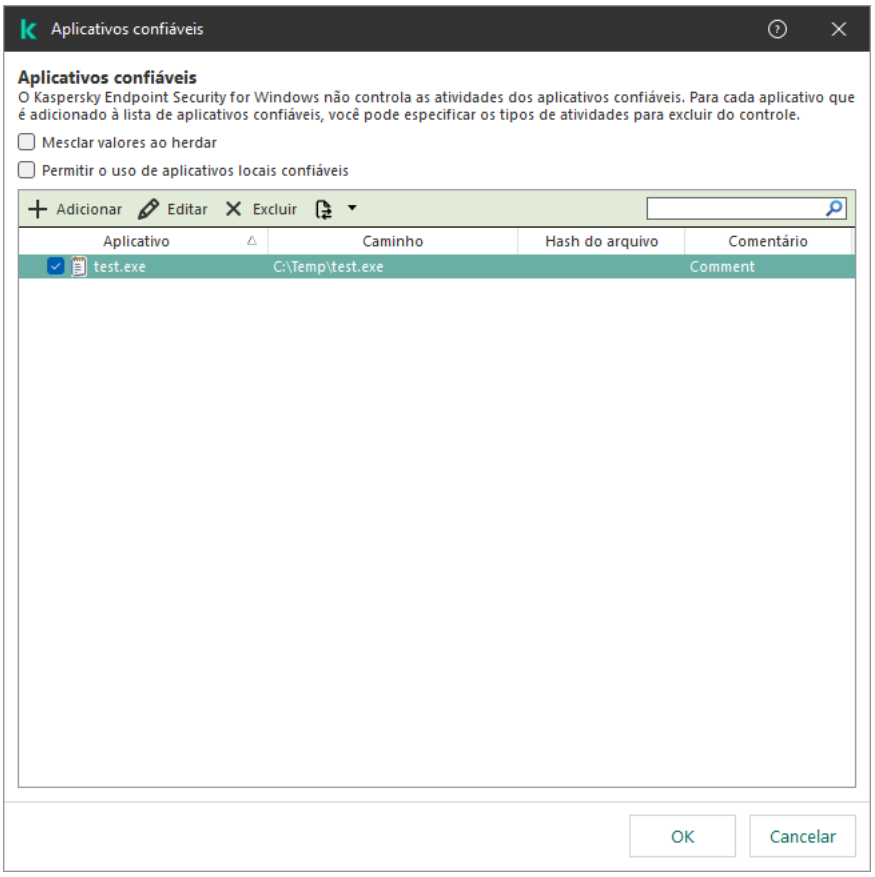
O Kaspersky Endpoint Security usa o formato XML para exportar e importar a *lista de aplicativos confiáveis*.

Como exportar e importar uma zona confiável Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Exclusões e tipos de objetos**.
4. Em **Exclusões de verificação e aplicativos confiáveis**, selecione o componente da zona confiável que deseja exportar ou importar: **Exclusões de verificação** ou **Aplicativos confiáveis**.
5. Clique **Configurações**.
6. Para exportar a lista de regras:
   a. Selecione as exclusões que deseja exportar. Para selecionar várias portas, use as teclas **CTRL** ou **SHIFT**.
      Se você não selecionou nenhuma exclusão, o Kaspersky Endpoint Security exportará todas as exclusões.
   b. Clique no botão → **Exportar**.
   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 Endpoint Security exporta toda a lista de exclusões para o arquivo XML. O Kaspersky Endpoint Security também é compatível com a exportação da lista de exclusões para um arquivo DAT.



Lista de aplicativos confiáveis

7. Para importar a lista de exclusões:

   a. Clique no botão → **Importar**.

   b. Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de exclusões.

   c. Abra o arquivo.

   Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML. O Kaspersky Endpoint Security também é compatível com a importação de uma lista de exclusões de um arquivo DAT.

8. Salvar alterações.

Como exportar ou importar uma zona confiável no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Ir para a seção **Zona Confiável**.

5. Para exportar a lista de regras:

   a. Clique no link **Exclusões de Verificação de malware**.

   b. Selecione as exclusões que deseja exportar.

   c. Clique no botão → **Exportar**.

      O Kaspersky Endpoint Security exporta a lista de exclusões para um arquivo JSON na pasta de downloads padrão.

6. Para exportar a lista de aplicativos confiáveis:

   a. Selecione os aplicativos confiáveis que deseja exportar.

   b. Clique no botão → **Exportar**.

      O Kaspersky Endpoint Security exporta a lista de aplicativos confiáveis para um arquivo JSON na pasta de downloads padrão.

7. Para importar a lista de exclusões:

   a. Clique no link **Exclusões de Verificação de malware**.

   b. Clique no botão → **Importar**.

      Na janela exibida, selecione o arquivo JSON do qual deseja importar a lista de exclusões.

   c. Abra o arquivo.

      Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo JSON.

8. Para importar a lista de aplicativos confiáveis:

   a. Clique no link **Aplicativos**.

   b. Clique no botão → **Importar**.

      Na janela exibida, selecione o arquivo JSON a partir do qual deseja importar a lista de aplicativos confiáveis.

   c. Abra o arquivo.

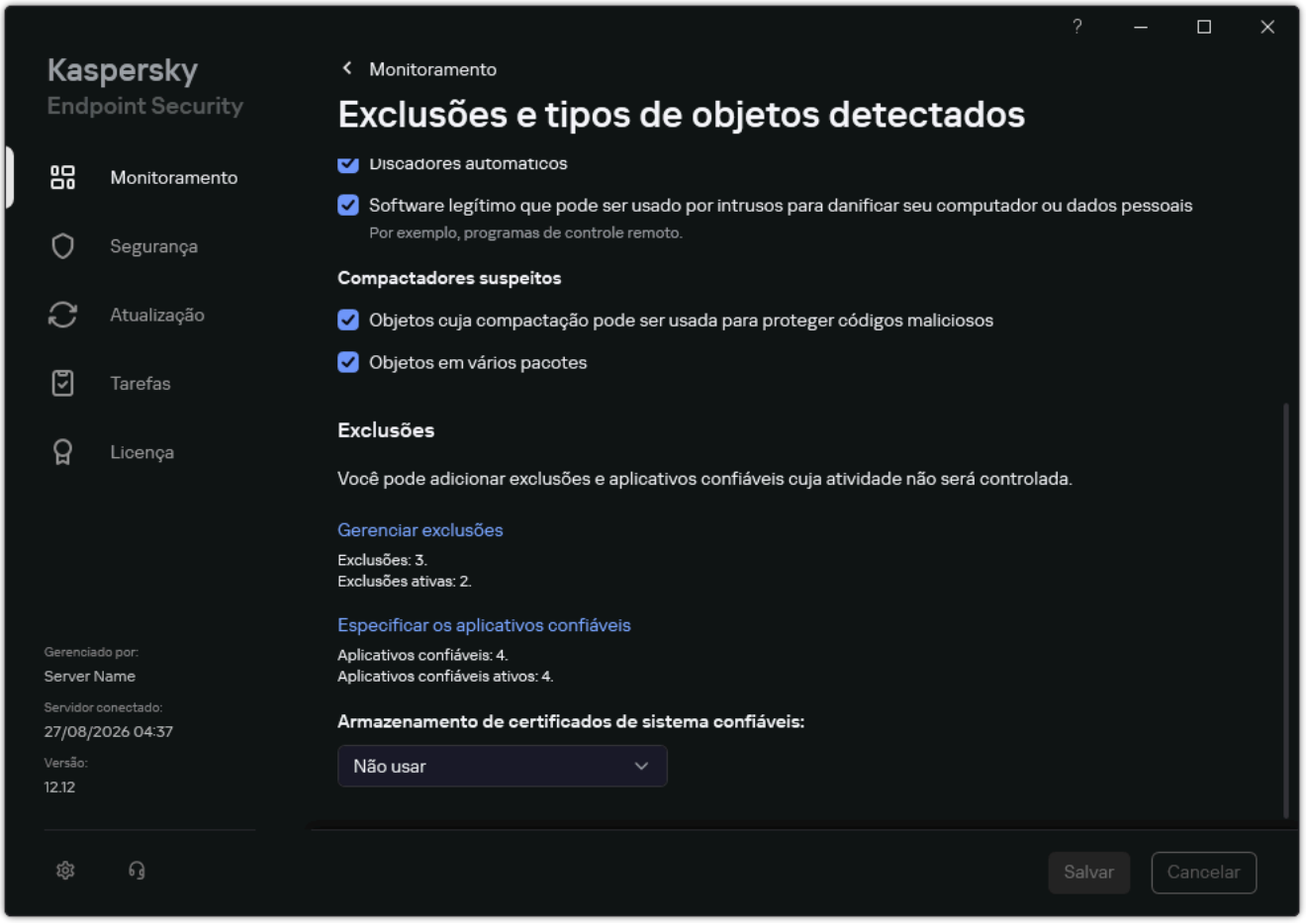
      Se o computador já tiver uma lista de aplicativos confiáveis, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo JSON.

9. Salvar alterações.

Como exportar ou importar a zona confiável na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Exclusões e tipos de objetos detectados**.



Configurações de exclusões

3. Para exportar a lista de regras:

   a. No bloco **Exclusões**, clique no link **Gerenciar exclusões**.

   b. Selecione as exclusões que deseja exportar.

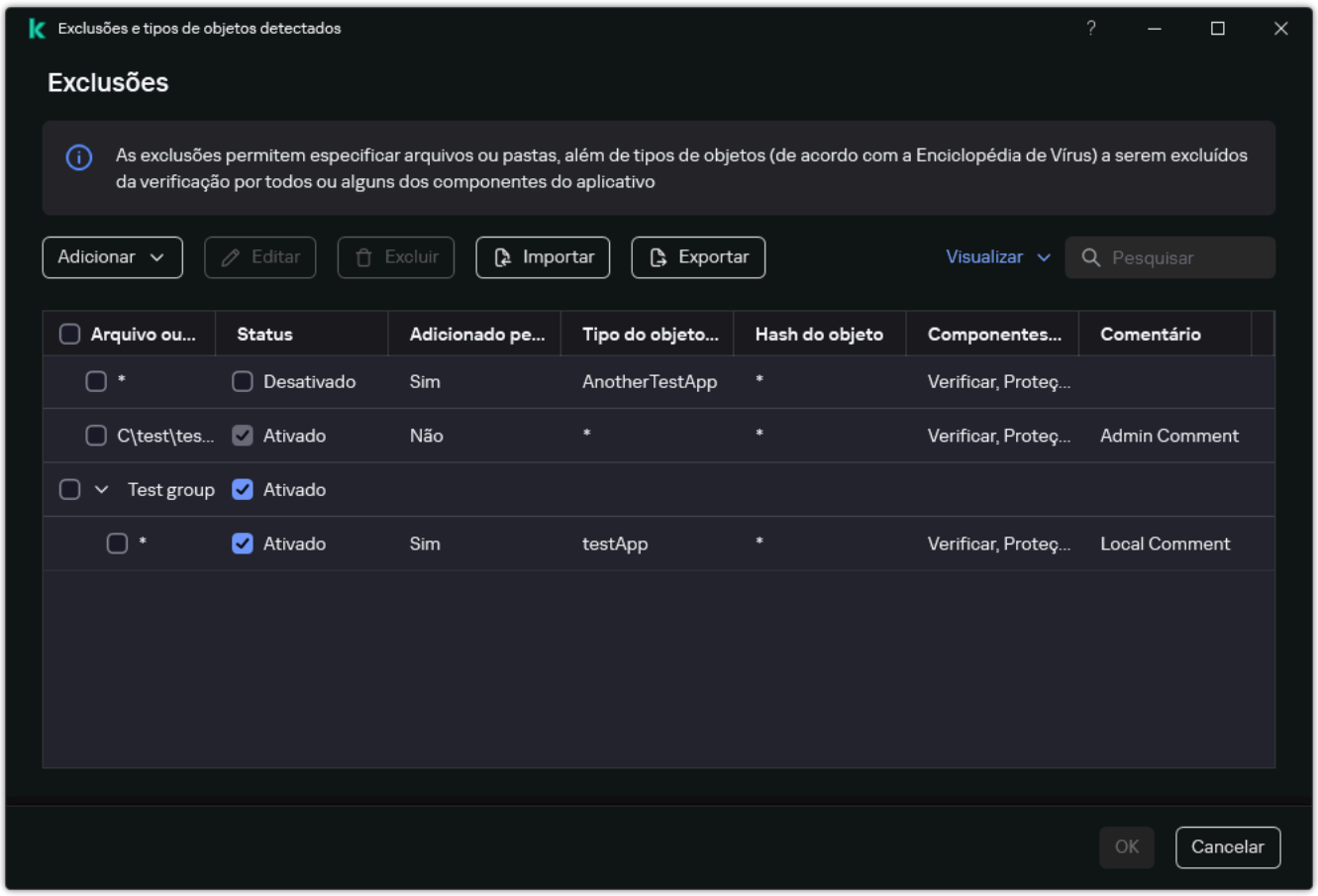
   c. Clique **Exportar**.

   d. Confirme que deseja exportar apenas as exclusões selecionadas ou exportar toda a lista de exclusões.

   e. Na janela exibida, especifique o nome do arquivo CSV para o qual você quer exportar a lista de exclusões e selecione a pasta na qual você quer salvar esse arquivo.

f. Salvar o arquivo.

O Kaspersky Endpoint Security exporta toda a lista de exclusões para o arquivo CSV.



Lista de exclusões

4. Para exportar a lista de aplicativos confiáveis:

a. No bloco **Exclusões**, clique no link **Especificar os aplicativos confiáveis**.

b. Selecione os aplicativos confiáveis que deseja exportar.

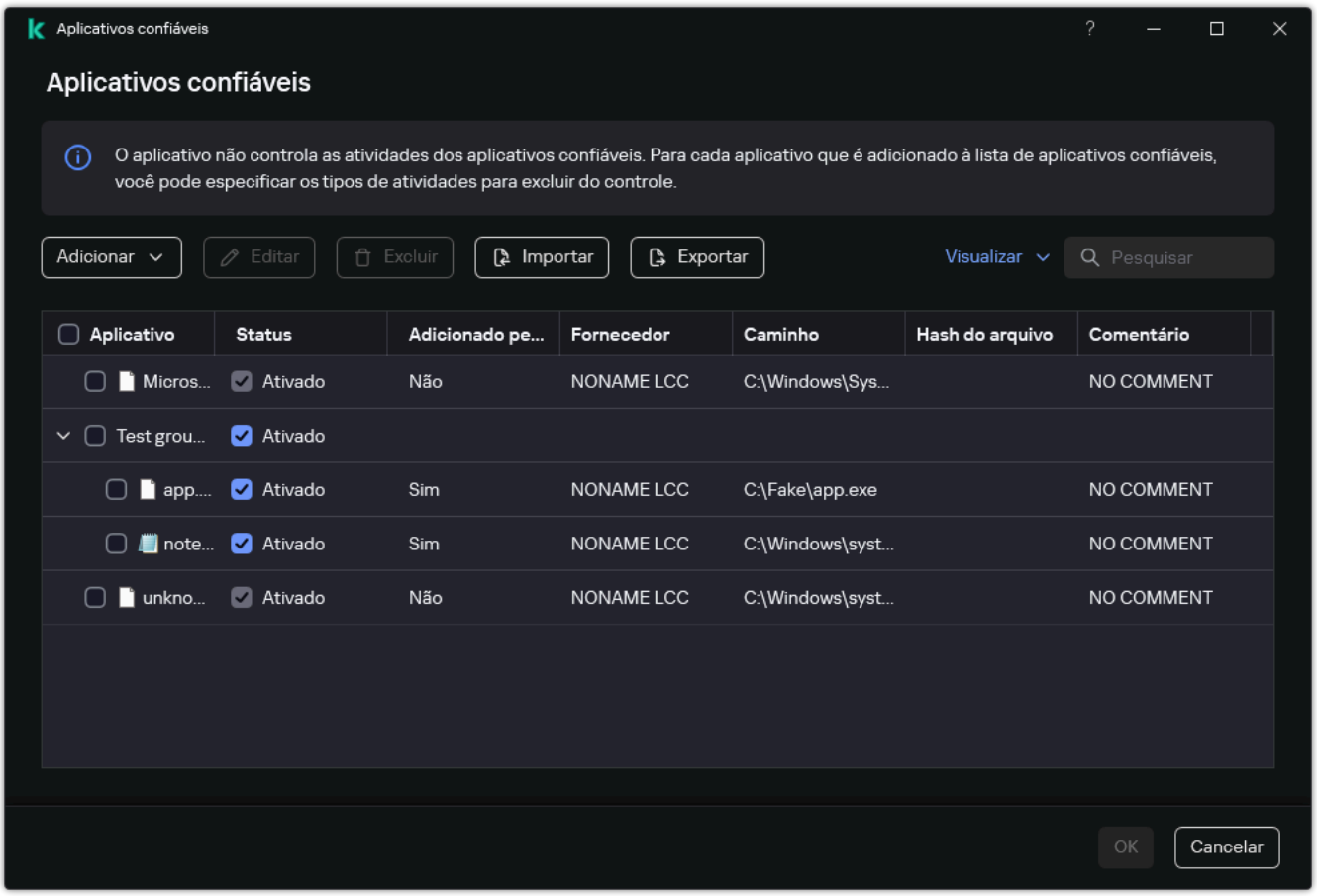
c. Clique **Exportar**.

d. Confirme se deseja exportar apenas os aplicativos confiáveis selecionados ou exportar a lista inteira.

e. 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.

f. Salvar o arquivo.

O Kaspersky Endpoint Security exporta toda a lista de aplicativos confiáveis para o arquivo XML.



Lista de aplicativos confiáveis

5. Para importar a lista de exclusões:

a. No bloco **Exclusões**, clique no link **Gerenciar exclusões**.

b. Clique **Importar**.

c. Na janela exibida, selecione o arquivo CSV do qual deseja importar a lista de exclusões.

d. Abra o arquivo.

Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo CSV.

6. Para importar a lista de aplicativos confiáveis:

a. No bloco **Exclusões**, clique no link **Especificar os 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 Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

7. Salvar alterações.

Manipulação de aplicativos com uma assinatura digital confiável

O uso do armazenamento de certificado de sistema permite excluir aplicativos assinados por uma assinatura digital confiável de verificações de vírus. O Kaspersky Endpoint Security atribui automaticamente esses aplicativos ao grupo *Confiável*.

Como iniciar o uso de um armazenamento de certificados de sistema confiável no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Exclusões e tipos de objetos**.
4. No bloco **Armazenamento de certificados de sistema confiáveis**, marque a caixa de seleção **Usar armazenamento de certificados de sistema confiáveis**.
5. Na lista suspensa, selecione qual armazenamento do sistema deve ser considerado como confiável pelo Kaspersky Endpoint Security.
6. Salvar alterações.

Como iniciar o uso de um armazenamento de certificados de sistema confiável no Web Console e no Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Ir para a seção **Zona Confiável**.
5. Na janela aberta, clique no link **Certificados raiz**.
6. Na janela que é aberta, marque a caixa de seleção **Usar armazenamento de certificados de sistema confiável**.
7. Selecione qual armazenamento do sistema deve ser considerado confiável pelo Kaspersky Endpoint Security.
8. Para aplicar a política aos computadores, feche os ícones de cadeado 🔒 e salve as alterações.

Como iniciar o uso de um armazenamento de certificados de sistema confiável na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Exclusões e tipos de objetos detectados**.
3. Na lista suspensa **Armazenamento de certificados de sistema confiáveis**, selecione qual armazenamento do sistema deve ser considerado como confiável pelo Kaspersky Endpoint Security.
4. Salvar alterações.

Apêndice. Exclusões de verificação predefinidas e aplicativos confiáveis

A partir do Kaspersky Endpoint Security 12.6 for Windows, as exclusões de verificação e aplicativos confiáveis são adicionadas na zona confiável. As exclusões predefinidas de verificação e aplicativos confiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, Microsoft Exchange e System Center Configuration Manager. Isso significa que não será necessário configurar manualmente uma zona confiável para o aplicativo nos servidores. A partir do Kaspersky Endpoint Security 12.8 for Windows, é possível instalar o aplicativo no modo Light Agent para proteger ambientes virtuais. Exclusões de verificação e aplicativos confiáveis predefinidos podem ajudar a configurar rapidamente o Kaspersky Endpoint Security em ambientes virtuais Citrix e VMware.

É possível selecionar as exclusões predefinidas e os aplicativos confiáveis das seguintes formas:

- Instalar o aplicativo.
  - Instalar o aplicativo localmente usando o assistente de instalação
  - Propriedades do pacote de instalação
- Configurar a política.
  - Assistente de nova política
  - Propriedades da política: exclusões de verificação e aplicativos confiáveis

Microsoft SQL Server

Ao instalar o Kaspersky Endpoint Security em um servidor SQL, é necessário criar uma zona confiável por meio das exclusões e aplicativos confiáveis predefinidos para garantir que a operação do servidor não sofra interferências.

Exclusões de verificação predefinidas

Caminho	Versão do SQL
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022

Microsoft Exchange Server

Ao instalar o Kaspersky Endpoint Security em um servidor Microsoft Exchange, é necessário criar uma zona confiável por meio de exclusões e aplicativos confiáveis para garantir que a operação do servidor não sofra interferências.

Exclusões de verificação predefinidas

Caminho	Versão do Microsoft Exchange
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl	2013 2016 2019

Caminho	Versão do Microsoft Exchange
`C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue\*.Chk`	2013 2016 2019
`C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue\*.Edb`	2013 2016 2019
`C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue\*.Jrs`	2013 2016 2019
`C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue\*.log`	2013 2016 2019
`C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue\*.Que`	2013 2016 2019
`C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue\*.jsl`	2013 2016 2019

Aplicativos confiáveis predefinidos

Caminho	Versão do Microsoft Exchange
`%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe`	2013 2016 2019
`%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe`	2013 2016 2019

Microsoft System Center Configuration Manager

Se o Microsoft System Center Configuration Manager estiver instalado no sistema operacional do computador protegido, será necessário adicionar uma exclusão predefinida à lista de exclusões de verificação para garantir a operação estável da solução.

Exclusões de verificação predefinidas

Caminho	Versão do System Center Configuration Manager
`%ProgramFiles%\Microsoft Configuration Manager\Inboxes`	2012 2012 R2

Citrix

Ao instalar o Kaspersky Endpoint Security em um ambiente virtual Citrix, é necessário criar uma zona confiável por meio de exclusões e aplicativos confiáveis predefinidos para garantir que a operação do servidor não sofra interferências.

Caminho
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys
%ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll
mcsdif.vhdx
%Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%Temp%\Citrix\HDXRTConnector**.txt
%SystemDrive%\Users*\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys
%ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll
*.vhd
*.avhd
*.vhdx
*.avhdx

Caminho	
*.pvp	
*.lok	
%SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2)	
%SystemRoot%\System32\drivers\CfsDep2.sys	
%ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN	
.vdiskcache	
vdiskdif.vhdx	
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb	

Aplicativos confiáveis predefinidos

Caminho	Solução Ci
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Áreas de trabalho aplicativo virtuais
%SystemRoot%\System32\drivers\CVhdFilter.sys	Áreas de trabalho aplicativo virtuais
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Áreas de trabalho aplicativo virtuais

Caminho	Solução Ci
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Áreas de trabalho aplicativo virtuais
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	Aplicativo espaço d trabalho
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	Aplicativo espaço d trabalho
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	Aplicativo espaço d trabalho
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	Aplicativo espaço d trabalho
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	Aplicativo espaço d trabalho
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	Aplicativo espaço d trabalho

Caminho	Solução Ci
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	Aplicativo espaço c trabalho
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	Aplicativo espaço c trabalho
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	Aplicativo espaço c trabalho
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	Aplicativo espaço c trabalho
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Provisionam
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Provisionam
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Provisionam
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Provisionam
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Provisionam
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Provisionam
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Provisionam
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Provisionam
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Provisionam
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Provisionam
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Provisionam
%SystemRoot%\System32\drivers\bnistack6.sys	Provisionam
%SystemRoot%\System32\drivers\CfsDep2.sys	Provisionam
%SystemRoot%\System32\drivers\cnicteam.sys	Provisionam
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Provisionam
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Provisionam
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Provisionam
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Provisionam
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Provisionam
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	Vitrine
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	Vitrine

VMware

Ao instalar o Kaspersky Endpoint Security em um ambiente virtual VMware, é necessário criar uma zona confiável a partir de aplicativos confiáveis predefinidos para garantir que a operação do servidor não sofra interferências.

Aplicativos confiáveis predefinidos

Caminho	Solução VMware
C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	Horizon

Caminho	Solução VMware
C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll	Horizon
C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe	Horizon
C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe	Horizon

Desduplicação de dados no Microsoft Windows Server

Se a desduplicação de dados estiver ativada no sistema operacional Microsoft Windows Server no qual o Kaspersky Endpoint Security está instalado, será necessário adicionar um aplicativo confiável predefinido à lista de aplicativos confiáveis para otimizar o Kaspersky Endpoint Security e reduzir a carga da CPU.

Aplicativos confiáveis predefinidos

Caminho	Versão do Microsoft Windows Server
`%SystemRoot%\system32\fsdmhost.exe`	Todas as versões compatíveis

Gerenciar o Backup

O *Backup* armazena cópias de backup de arquivos que foram excluídos ou modificados durante a desinfecção. Uma *cópia backup* é uma cópia de arquivo criada antes que o arquivo seja desinfectado ou excluído. As cópias de backup de arquivos são armazenadas em um formato especial e não representam uma ameaça.

As cópias de backup dos arquivos são armazenadas na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

Os usuários no grupo de Administradores têm permissão para acessar essa pasta. Direitos de acesso limitados a essa pasta são concedidos ao usuário cuja conta foi usada para instalar o Kaspersky Endpoint Security.

O Kaspersky Endpoint Security não fornece a capacidade de configurar permissões de acesso de usuário a cópias backup de arquivos.

Em alguns casos não é possível manter a integridade de arquivos durante a desinfecção. Se após a desinfecção você perder o acesso parcial ou total a informações importantes do arquivo desinfectado, pode tentar restaurar o arquivo da cópia backup para a pasta de origem.

Se o Kaspersky Endpoint Security estiver sendo executado sob o gerenciamento do Kaspersky Security Center, as cópias de backup dos arquivos poderão ser transmitidas para o Servidor de Administração do Kaspersky Security Center. Para obter mais detalhes sobre o gerenciamento de cópias de backup de arquivos no Kaspersky Security Center, consulte o sistema de Ajuda do Kaspersky Security Center.

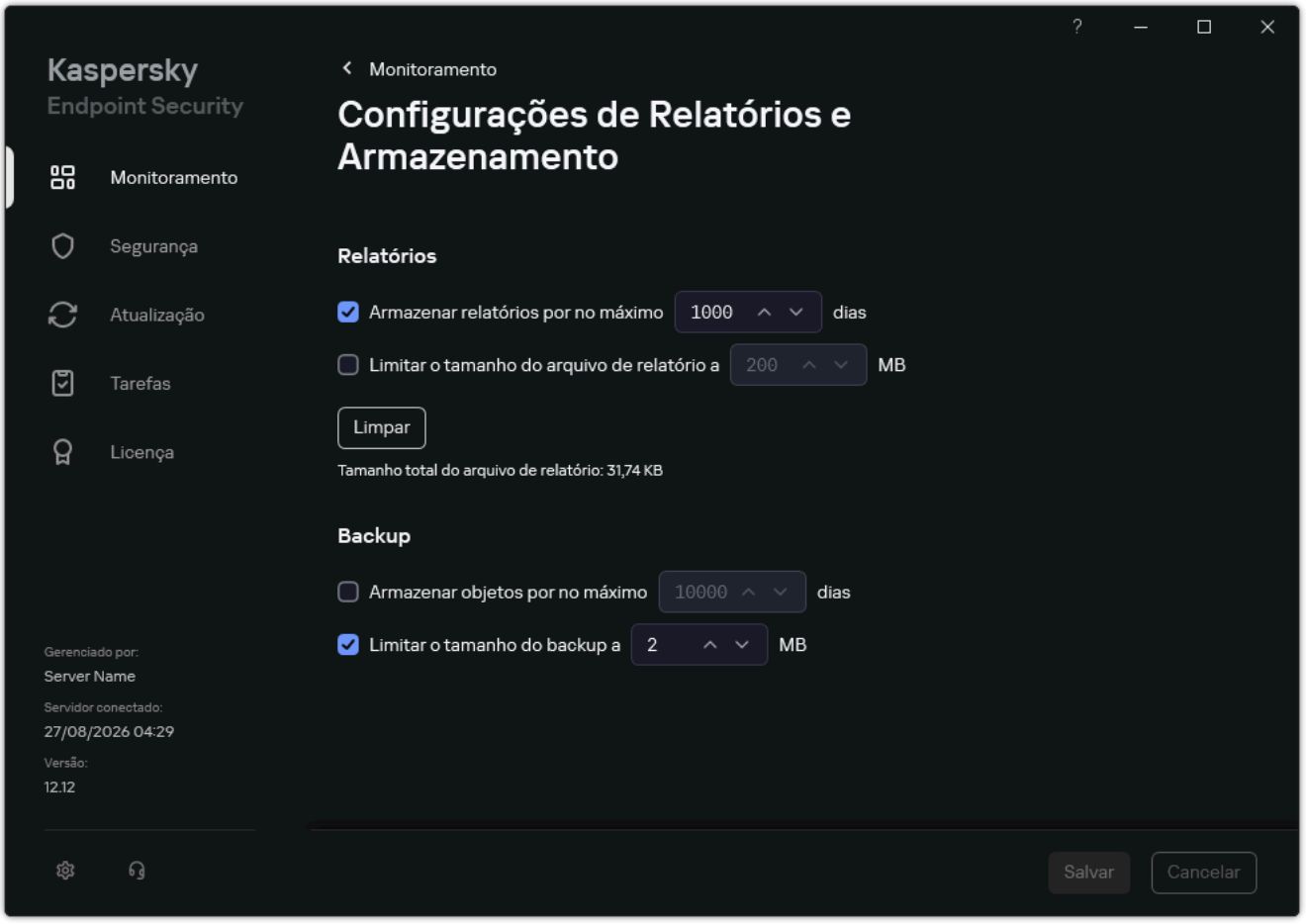
Configurar o período de armazenamento máximo para arquivos no Backup

O período de armazenamento máximo padrão para cópias de arquivos no Backup é de 30 dias. Depois da expiração do período máximo de armazenamento, o Kaspersky Endpoint Security excluirá os arquivos mais antigos do Backup.

Para configurar o período de armazenamento máximo para arquivos no Backup:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, em **Configurações gerais**, clique no bloco **Relatórios e armazenamento**.



Configurações de backup

3. Caso queira limitar o período de armazenamento para cópias de arquivos no Backup, marque a caixa de seleção **Armazenar objetos por no máximo N dias** no bloco **Backup**. Insira o período de armazenamento máximo para arquivos no backup.

4. Salvar alterações.

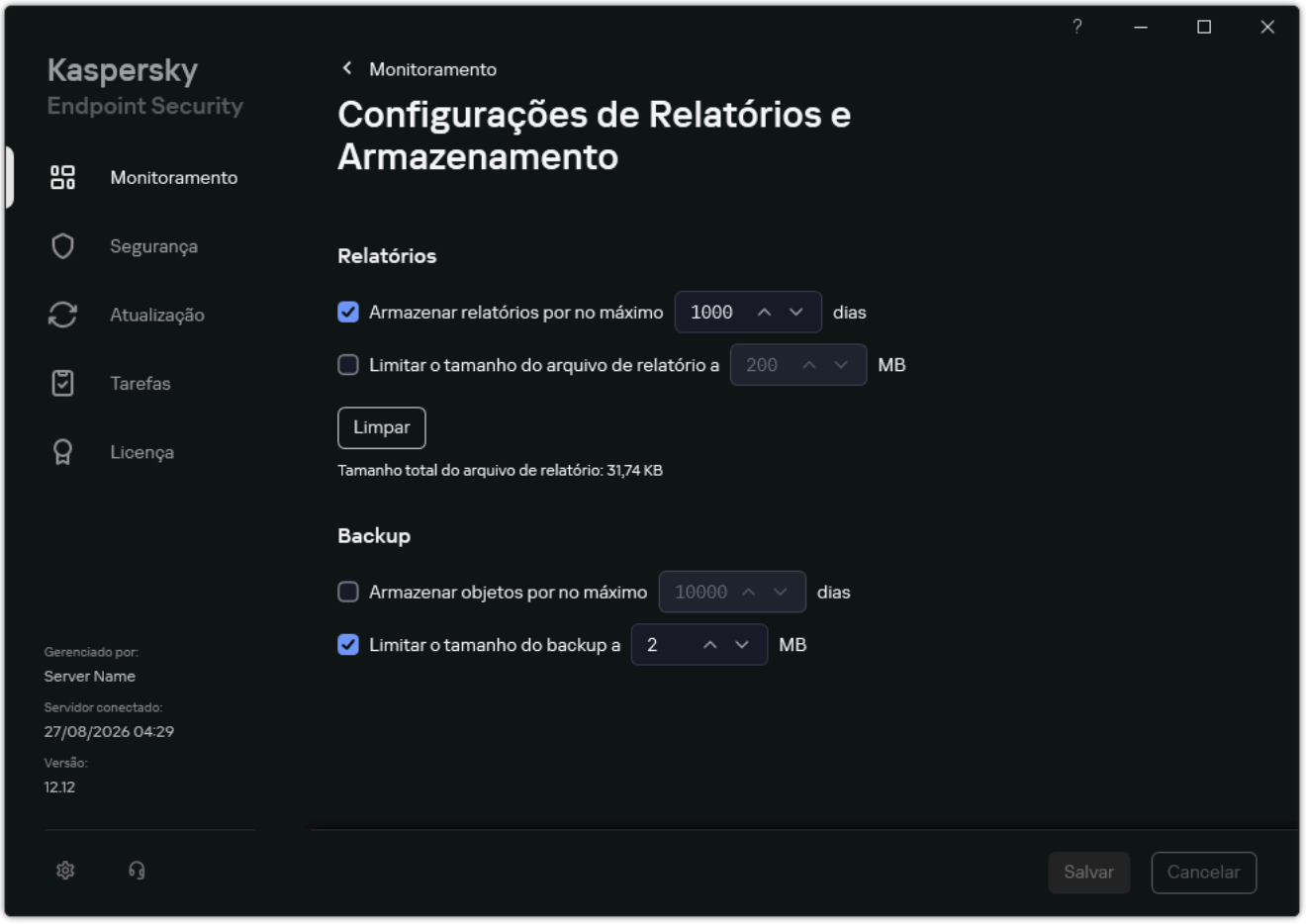
Configurar o tamanho máximo de Backup

Você pode especificar o tamanho máximo do backup. O tamanho do Backup é ilimitado por padrão. Após o tamanho máximo ser atingido, o Kaspersky Endpoint Security exclui automaticamente os arquivos mais antigos do Backup.

Para configurar o tamanho máximo de Backup:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, em **Configurações gerais**, clique no bloco **Relatórios e armazenamento**.



Configurações de backup

3. No bloco **Backup**, marque a caixa de seleção **Limitar o tamanho do backup a N MB**. Se a caixa de seleção estiver marcada, o tamanho máximo de armazenamento será limitado ao valor definido. Por padrão, a dimensão máxima é 1024 MB. Para evitar ultrapassar o tamanho máximo de armazenamento, o Kaspersky Endpoint Security exclui os arquivos mais antigos do arquivo automaticamente quando o tamanho máximo é atingido.

4. Salvar alterações.

Restaurar arquivos do Backup

Caso um código malicioso seja detectado em um arquivo, o Kaspersky Endpoint Security bloqueará o arquivo, atribuirá o status *Não desinfectado*, colocará uma cópia no Backup e tentará desinfectá-lo. Se a desinfecção for bem-sucedida, o status da cópia de backup do arquivo será alterado para *Desinfectado(s)*. O arquivo fica disponível na sua pasta original. Se um arquivo não puder ser desinfectado, o Kaspersky Endpoint Security o exclui da sua pasta original. É possível restaurar o arquivo da cópia de backup para a respectiva pasta de origem.

Os arquivos com o status *Será excluído ao reiniciar* não podem ser restaurados. Reinicie o computador e o status do arquivo será alterado para *Desinfectado(s)* ou *Excluído(s)*. É possível também restaurar o arquivo da cópia de backup para a respectiva pasta de origem.

Ao detectar código malicioso em um arquivo que faça parte do aplicativo Windows Store, o Kaspersky Endpoint Security exclui imediatamente o arquivo sem mover uma cópia dele para Backup. É possível restaurar a integridade do aplicativo Windows Store com o uso das ferramentas adequadas do sistema operacional (consulte os arquivos de ajuda do Microsoft Windows para obter informações sobre a restauração do aplicativo Windows Store).

O conjunto de cópias de backup de arquivos é apresentado como uma tabela. Para uma cópia backup de um arquivo, o caminho até a pasta original do arquivo é exibido. O caminho até a pasta original do arquivo pode conter dados pessoais.

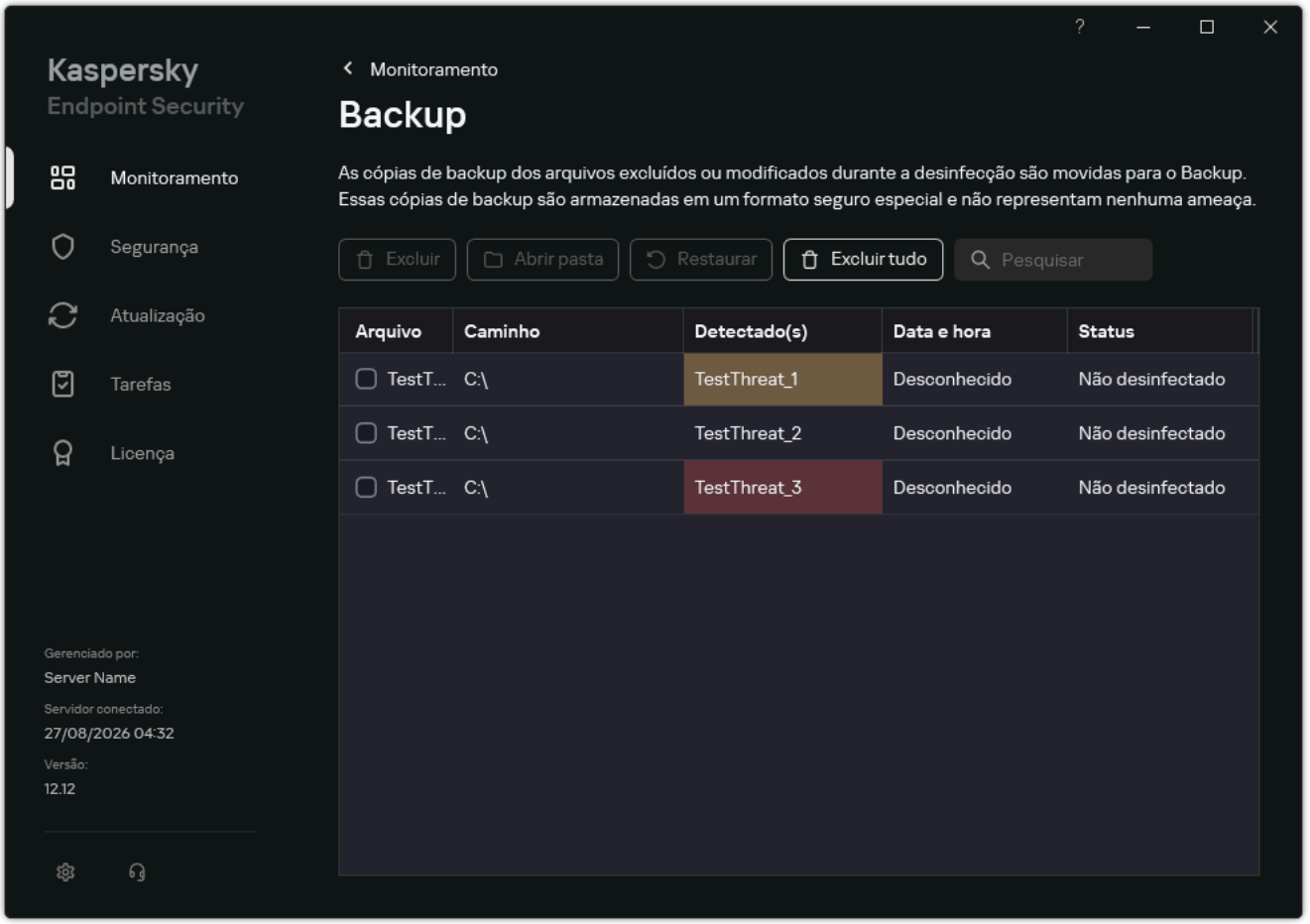
Se vários arquivos com nomes idênticos e conteúdo diferente localizados na mesma pasta forem movidos para o Backup, somente o último arquivo colocado poderá ser restaurado.

Para restaurar arquivos do Backup:

1. Na janela principal do aplicativo, na seção **Monitoramento**, clique no bloco **Backup**.

2. Isso abre a lista de arquivos no Backup; nessa lista, selecione os arquivos que deseja restaurar e clique em **Restaurar**.

O Kaspersky Endpoint Security restaura os arquivos das cópias de backup selecionadas para as respectivas pastas de origem.



Backup

Excluir cópias de backup de arquivos do Backup

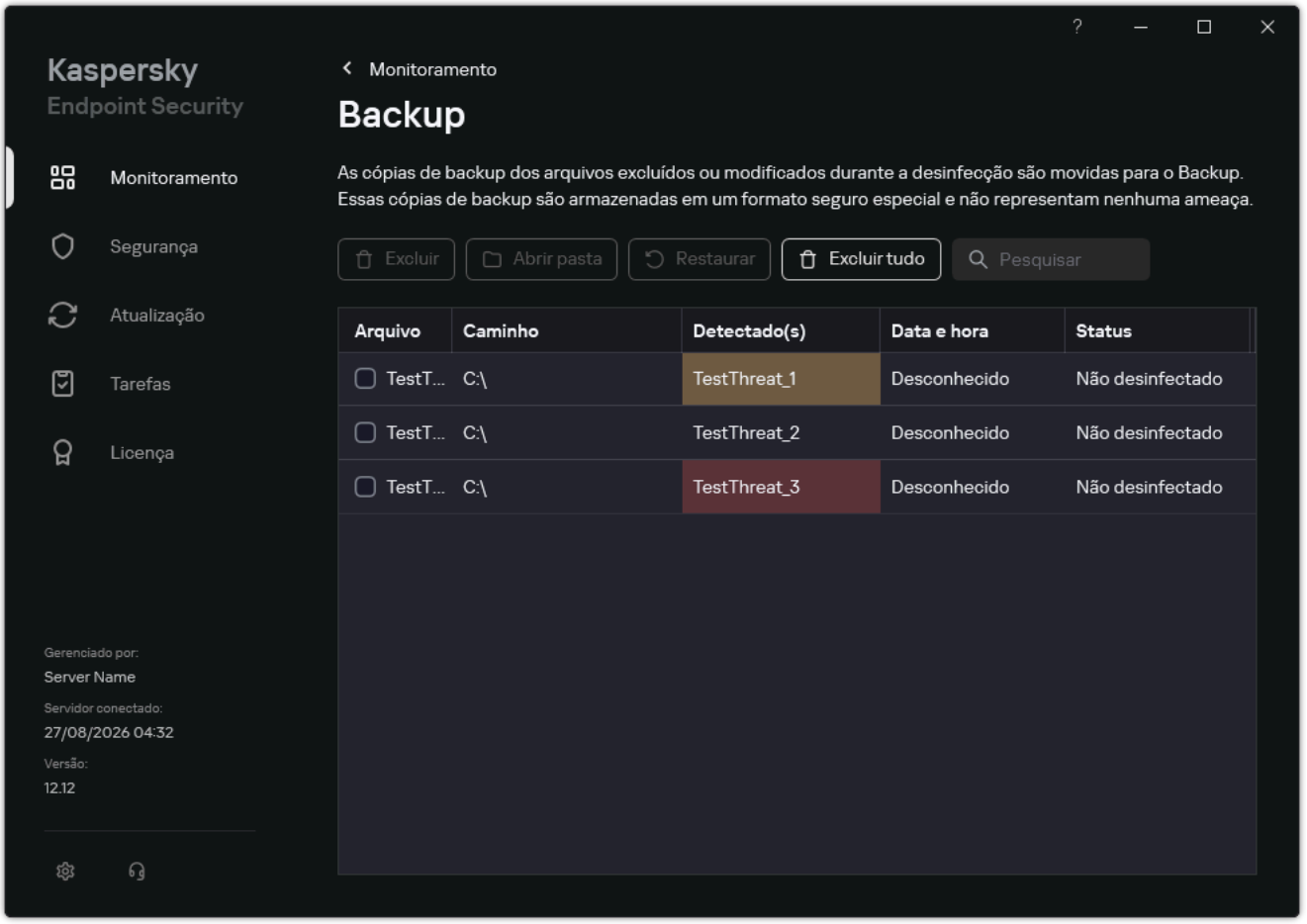
O Kaspersky Endpoint Security exclui automaticamente as cópias de arquivos de backup com qualquer status de Backup após o termo de armazenamento definido nas configurações do aplicativo ter decorrido. Também é possível excluir manualmente qualquer cópia de um arquivo do Backup.

Para excluir cópias backup de arquivos do Backup:

1. Na janela principal do aplicativo, na seção **Monitoramento**, clique no bloco **Backup**.

2. Isso abre a lista de arquivos no backup; nesta lista, selecione os arquivos que deseja excluir do backup e clique em **Excluir**.

O Kaspersky Endpoint Security exclui as cópias de backup dos arquivos selecionados do Backup.



Backup

Serviço de notificações

Vários tipos de eventos ocorrem durante a operação do Kaspersky Endpoint Security. As Notificações destes eventos podem ser puramente informativas ou conter informações importantes. Por exemplo, as notificações podem informar sobre uma atualização bem-sucedida de módulos de aplicativos e bancos de dados ou registrar erros de componentes que precisam ser corrigidos.

O Kaspersky Endpoint Security dá suporte ao registo de informações sobre eventos na operação do registro do aplicativo do Microsoft Windows e/ou do registro de eventos do Kaspersky Endpoint Security.

O Kaspersky Endpoint Security transmite as notificações das seguintes formas:

- usando notificações pop-up na área de notificação da barra de tarefas do Microsoft Windows;
- por e-mail.

Você pode configurar a transmissão de notificações de eventos. O método de transmissão de notificações é configurado para cada tipo de evento.

Usando a tabela de eventos para configurar o serviço de notificação, você pode executar as seguintes ações:

- Filtre o serviço de notificações por valores da coluna ou por condições de filtragem personalizadas.
- Utilize a função de busca para eventos do serviço de notificações.
- Classifique os eventos do serviço de notificações.
- Altere a ordem e a configuração das colunas que são exibidas na lista de eventos do serviço de notificações.

Definir as configurações do registro de eventos

Para definir as configurações do registro de eventos:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Interface**.
3. No bloco **Notificações**, clique no botão **Configurar notificações**.

   Os componentes e as tarefas do Kaspersky Endpoint Security são exibidos na parte esquerda da janela. A parte direita da janela lista os eventos gerados para o componente ou a tarefa selecionados.

   Os eventos podem conter os seguintes dados de usuário:

   - Caminhos para arquivos verificados pelo Kaspersky Endpoint Security.
   - Caminhos para as chaves de registro modificadas durante a operação do Kaspersky Endpoint Security.
   - Nome de usuário do Microsoft Windows.
   - Endereços de páginas da Web abertas pelo usuário.

4. Na parte esquerda da janela, selecione o componente ou a tarefa para os quais deseja definir as configurações do registro de eventos.

5. Marque as caixas de seleção ao lado dos eventos relevantes nas colunas **Salvar no relatório local** e **Salvar no Log de eventos do Windows**.

   Os eventos cujas caixas de seleção são marcadas na coluna **Salvar no relatório local** são exibidos nos logs do aplicativo. Os eventos cujas caixas de seleção são marcadas na coluna **Salvar no Log de eventos do Windows** são exibidos nos logs do Windows no canal `Application`.

6. Salvar alterações.

Configurar a exibição e entrega de notificações

Para configurar a exibição e entrega de notificações:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Interface**.

3. No bloco **Notificações**, clique no botão **Configurar notificações**.

   Os componentes e as tarefas do Kaspersky Endpoint Security são exibidos na parte esquerda da janela. A parte direita da janela lista os eventos gerados para o componente ou a tarefa selecionados.

   Os eventos podem conter os seguintes dados de usuário:

   - Caminhos para arquivos verificados pelo Kaspersky Endpoint Security.
   - Caminhos para as chaves de registro modificadas durante a operação do Kaspersky Endpoint Security.
   - Nome de usuário do Microsoft Windows.
   - Endereços de páginas da Web abertas pelo usuário.

4. Na parte esquerda da janela, selecione o componente ou a tarefa para os quais deseja configurar a transmissão de notificações.

5. Na coluna **Notificar na tela**, marque as caixas de seleção ao lado dos eventos desejados.

   As informações sobre os eventos selecionados são exibidas na tela em mensagens pop-up na área de notificação da barra de tarefas do Microsoft Windows.

6. Na coluna **Notificar por e-mail**, marque as caixas de seleção ao lado dos eventos desejados.

   As informações sobre os eventos selecionados são entregues pelo e-mail se as configurações de entrega de notificação de correio forem configuradas.

7. Clique **OK**.

8. Se você ativou as notificações por e-mail, defina as configurações para entrega de e-mail:

   a. Clique **Configurar notificações por e-mail**.

   b. Marque a caixa de seleção **Notificar sobre os eventos** para ativar a transmissão de informações de eventos do Kaspersky Endpoint Security selecionados na coluna **Notificar por e-mail**.

c. Especifique as configurações de transmissão de notificação por e-mail.

d. Clique **OK**.

9. Salvar alterações.

Configurar a exibição de avisos sobre o status do aplicativo na área de notificação

Para configurar a exibição de avisos de status do aplicativo na área de notificação:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Interface**.
3. No bloco **Mostrar o status do aplicativo na área de notificações**, marque as caixas de seleção ao lado das categorias de eventos sobre os quais deseja ver notificações na área de notificação do Microsoft Windows.
4. Salvar alterações.

Quando os eventos associados às categorias selecionadas ocorrerem, o ícone de aplicativo na área de notificação vai se modificar para ou , dependendo da gravidade do aviso.

Mensagens entre usuários e o administrador

Os componentes Controle de Aplicativos, Controle de Dispositivos, Controle da Web e Controle Adaptativo de Anomalias permitem que usuários da LAN enviem mensagens ao administrador a partir de computadores com o Kaspersky Endpoint Security instalado.

Talvez um usuário precise enviar uma mensagem ao administrador de rede corporativa local nos seguintes casos:

- Acesso bloqueado do Controle de Dispositivos ao dispositivo.

  O modelo da mensagem de uma solicitação para acessar um dispositivo bloqueado está disponível na interface Kaspersky Endpoint Security na seção Controle de Dispositivos.

- O Controle de Aplicativos bloqueou a inicialização de um aplicativo.

  O modelo de mensagem de uma solicitação para permitir a inicialização de um aplicativo bloqueado está disponível na interface do Kaspersky Endpoint Security na seção Controle de Aplicativos.

- Acesso bloqueado do Controle da Web ao recurso da Web.

  O modelo de mensagem de uma solicitação para acessar um recurso da Web bloqueado está disponível na interface do Kaspersky Endpoint Security na seção Controle da Web.

O método usado para enviar mensagens e o modelo utilizado depende de haver ou não uma política do Kaspersky Security Center ativa em execução no computador que possui o Kaspersky Endpoint Security instalado e de haver ou não uma conexão com o servidor de administração do Kaspersky Security Center. Os seguintes cenários são possíveis:

- Se uma política do Kaspersky Security Center não estiver executando no computador que possui o Kaspersky Endpoint Security instalado, a mensagem de um usuário será enviada ao administrador de rede local por e-mail.

  Os campos de mensagem são preenchidos com os valores de campos do modelo definido na interface local do Kaspersky Endpoint Security.

- Se uma política do Kaspersky Security Center estiver em execução no computador que possui o Kaspersky Endpoint Security instalado, a mensagem padrão será enviada ao Servidor de Administração do Kaspersky Security Center.

  Nesse caso, as mensagens do usuário estão disponíveis para visualização no armazenamento de eventos do Kaspersky Security Center (consulte as instruções abaixo). Os campos de mensagem são povoados com os valores de campos do modelo definido na política do Kaspersky Security Center.

- Se uma política de ausência do Kaspersky Security Center estiver em execução no computador com o Kaspersky Endpoint Security instalado, o método usado para enviar mensagens dependerá se há ou não uma conexão com Kaspersky Security Center.

  - Se uma conexão com o Kaspersky Security Center for estabelecida, o Kaspersky Endpoint Security enviará a mensagem padrão ao Servidor de Administração do Kaspersky Security Center.

  - Se uma conexão com o Kaspersky Security Center estiver ausente, a mensagem de um usuário será enviada ao administrador de rede local por e-mail.

  Em ambos os casos, os campos de mensagem são preenchidos com os valores de campos do modelo definido na política do Kaspersky Security Center.

Para visualizar uma mensagem do usuário no armazenamento de eventos do Kaspersky Security Center:

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

2. No nó **Servidor de Administração** da árvore do Console de Administração, selecione a guia **Eventos**.

   A área de trabalho do Kaspersky Security Center exibe todos os eventos que ocorrem durante a operação do Kaspersky Endpoint Security, inclusive mensagens ao administrador que são recebidas de usuários da rede local.

3. Para configurar o filtro de evento, na lista suspensa **Seleções de eventos**, selecione **Pedidos de usuário**.

4. Selecione a mensagem enviada ao administrador.

5. Clicar no botão **Abrir janela de propriedades do evento** na parte direita da área de trabalho do Console de administração.

Gerenciar relatórios

As informações sobre a operação de cada componente do Kaspersky Endpoint Security, os eventos de criptografia de dados, o desempenho de cada tarefa de verificação, a tarefa de atualização e de verificação de integridade e a operação geral do aplicativo são registrados nos relatórios.

Os relatórios são armazenados na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\Report`.

Os relatórios podem conter os seguintes dados de usuário:

- Caminhos para arquivos verificados pelo Kaspersky Endpoint Security.
- Caminhos para as chaves de registro modificadas durante a operação do Kaspersky Endpoint Security.
- Nome de usuário do Microsoft Windows.
- Endereços de páginas da Web abertas pelo usuário.

Os dados no relatório são apresentados em forma de tabela. Cada linha da tabela contém informações sobre um evento diferente. Os atributos do evento estão dispostos nas colunas da tabela. Algumas colunas são compostas, contendo colunas aninhadas que incluem atributos adicionais. Para exibir atributos adicionais, você deve pressionar o botão ⊞ ao lado do nome da coluna. Os eventos registrados na execução dos diversos componentes ou durante o desempenho de várias tarefas têm conjuntos de atributos diferentes.

Os seguintes relatórios estão disponíveis:

- Relatório de **Auditoria do sistema**. Contém informações sobre os eventos ocorridos durante a interação entre usuário e aplicativo e durante a execução do aplicativo em geral, que não estão relacionadas a nenhum componente ou tarefa do Kaspersky Endpoint Security em particular.
- Relatórios sobre a operação dos componentes do Kaspersky Endpoint Security.
- Relatórios de tarefas do Kaspersky Endpoint Security.
- Relatório de **Criptografia de dados**. Contém informações sobre eventos que ocorrem durante a criptografia e descriptografia de dados.

Os relatórios utilizam os seguintes níveis de importância de eventos:

ⓘ **Mensagens informativas**. Eventos para fins de referência que geralmente não são de importância crítica.

⚠ **Avisos**. Eventos que exigem atenção porque representam situações importantes na execução do Kaspersky Endpoint Security.

⊘ **Eventos críticos**. Eventos de importância crítica que indicam problemas no funcionamento do Kaspersky Endpoint Security ou vulnerabilidades na proteção do computador do usuário.

Para trazer praticidade ao processamento de relatórios, é possível modificar a apresentação dos dados na tela da seguinte forma:

- Filtrar a lista de eventos usando vários critérios.
- Utilizar a função de busca para encontrar um determinado evento.
- Exibir o evento selecionado em uma seção separada.
- Ordenar a lista de eventos por cada coluna do relatório.
- Exibir e ocultar eventos agrupados pelo filtro de evento usando o botão ⊞.
- Alterar a ordem e a configuração das colunas exibidas no relatório.

É possível salvar um relatório gerado em arquivo de texto, se necessário. Você também pode excluir as informações do relatório sobre componentes e tarefas do Kaspersky Endpoint Security que estão arranjadas em grupos.

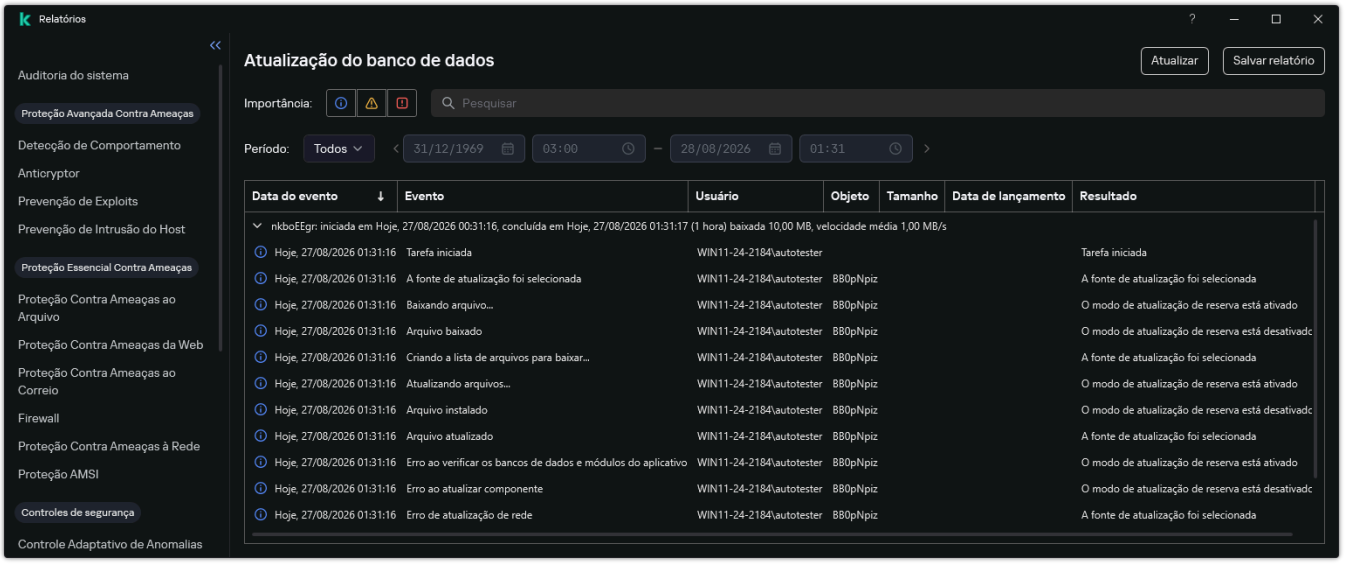
Caso o Kaspersky Endpoint Security esteja sendo executado sob o gerenciamento do Kaspersky Security Center, as informações sobre os eventos poderão ser transmitidas ao Servidor de Administração do Kaspersky Security Center (para obter mais detalhes, consulte a Ajuda do Kaspersky Security Center).

Visualização de relatórios

Se um usuário puder visualizar relatórios, também poderá visualizar todos os eventos refletidos nos relatórios.

Para visualizar relatórios:

1. Na janela principal do aplicativo, na seção **Monitoramento**, clique no bloco **Relatórios**.



Relatórios

2. Na lista de componentes e tarefas, selecione um componente ou uma tarefa.

   O lado direito da janela exibe um relatório contendo uma lista de eventos resultantes da operação do componente selecionado ou da tarefa selecionada do Kaspersky Endpoint Security. Classifique os eventos no relatório com base nos valores em células de uma das colunas.

3. Para visualizar informações detalhadas sobre um evento, selecione o evento no relatório.

Um bloco com o resumo do evento é exibido na parte inferior da janela.

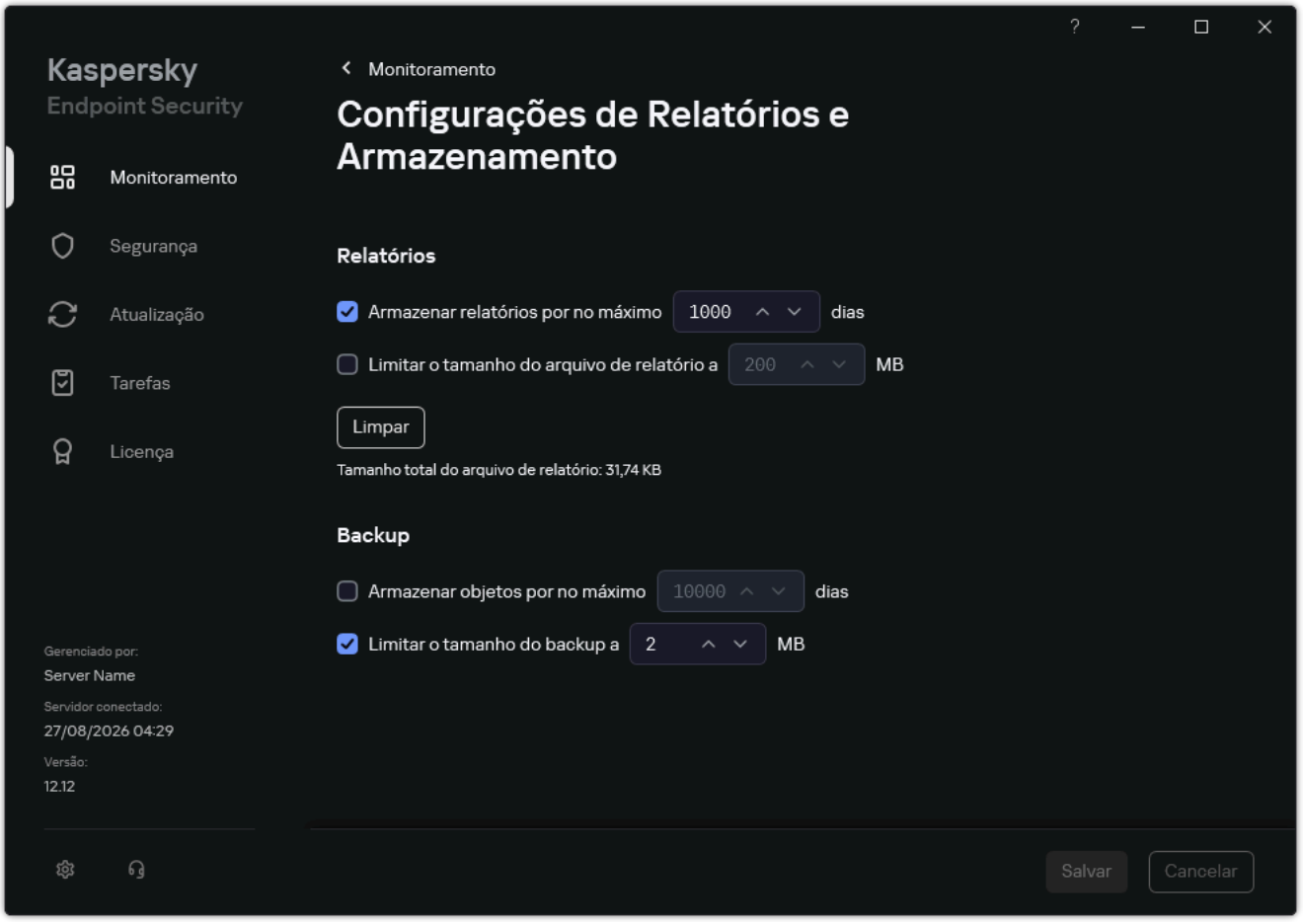
Configurar o período máximo de armazenamento de relatórios

O período máximo padrão de armazenamento de relatórios sobre eventos registrados pelo Kaspersky Endpoint Security é de 30 dias. Após este período, o Kaspersky Endpoint Security exclui as entradas mais antigas do arquivo de relatório automaticamente.

Para modificar o período máximo de armazenamento de relatórios:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, em **Configurações gerais**, clique no bloco **Relatórios e armazenamento**.



Configurações de relatório

3. Caso queira limitar o termo de armazenamento de relatórios, marque a caixa de seleção **Armazenar relatórios por no máximo N dias** no bloco **Relatórios**. Definir o período máximo de armazenamento de relatórios.

4. Salvar alterações.

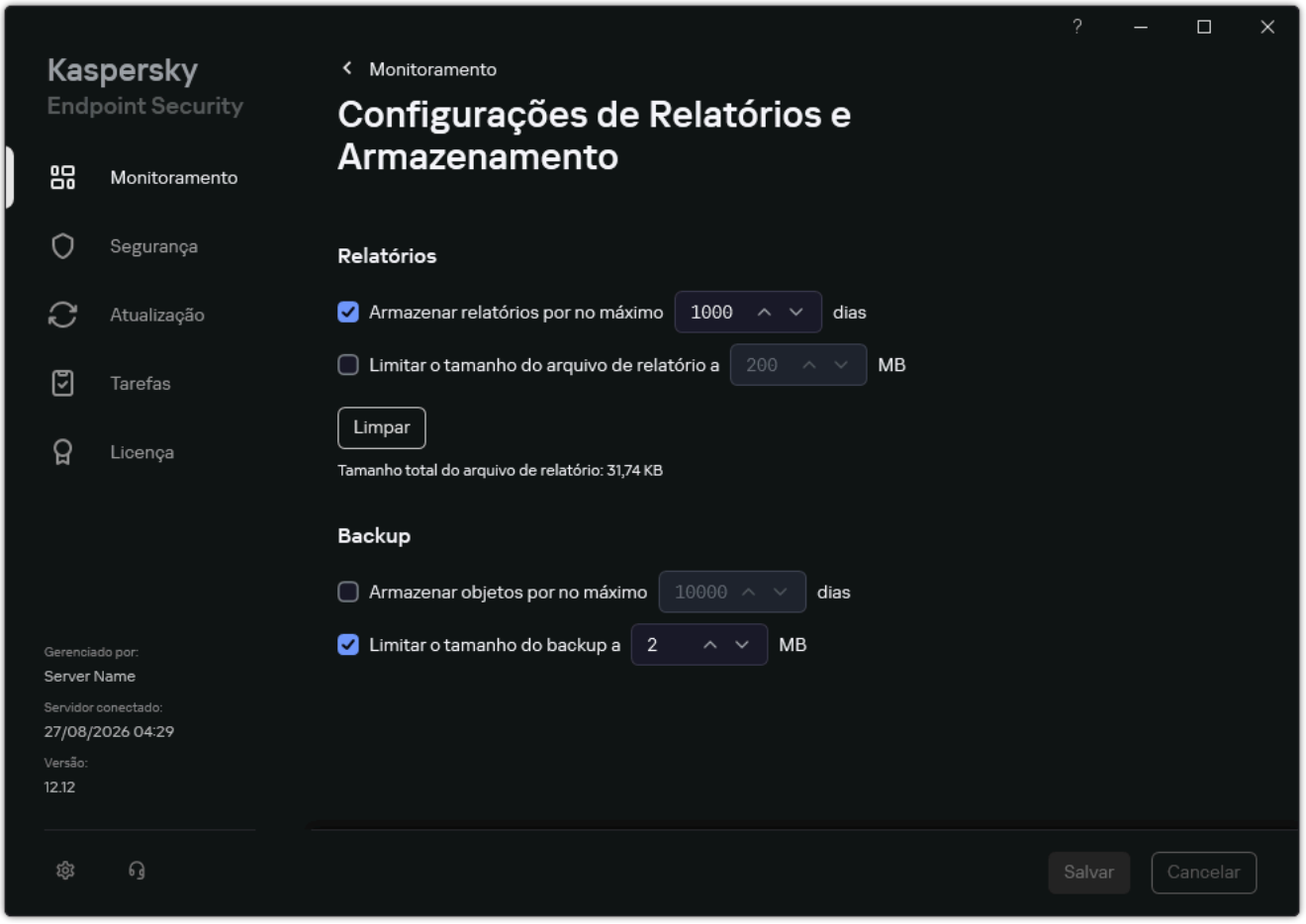
Configurar o tamanho máximo do arquivo de relatório

Você pode especificar o tamanho máximo do arquivo que contém o relatório. Por padrão, o tamanho máximo do arquivo de relatório é 1.024 MB. Para evitar ultrapassar o tamanho máximo do arquivo de relatório, o Kaspersky Endpoint Security exclui as entradas mais antigas do arquivo de relatório automaticamente quando for ultrapassado o tamanho máximo.

Para configurar o tamanho máximo do arquivo de relatório:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, em **Configurações gerais**, clique no bloco **Relatórios e armazenamento**.



Configurações de relatório

3. No bloco **Relatórios**, marque a caixa de seleção **Limitar o tamanho do arquivo de relatório a N MB** caso queira limitar o tamanho de um arquivo de relatório. Definir o tamanho máximo do arquivo de relatório.

4. Salvar alterações.

Salvar um relatório em arquivo

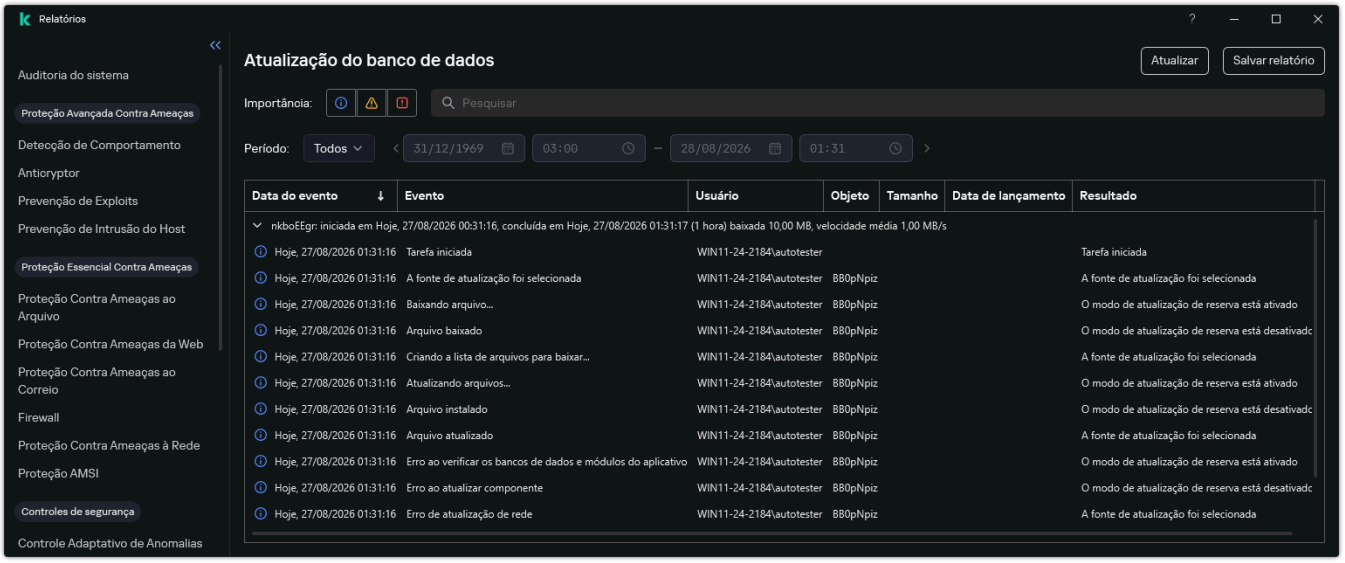
O usuário é pessoalmente responsável por garantir a segurança das informações de um relatório salvo para um arquivo e, em particular, para controlar e restringir o acesso a essas informações.

Você pode salvar o relatório gerado em um arquivo em formato de texto (TXT) ou em um arquivo CSV.

O Kaspersky Endpoint Security registra os eventos no relatório, na forma em que são exibidos na tela, ou seja, com as mesmas combinações e sequências dos atributos do evento.

Para salvar um relatório em arquivo:

1. Na janela principal do aplicativo, na seção **Monitoramento**, clique no bloco **Relatórios**.



Relatórios

2. Isso abre uma janela; nesta janela, selecione o componente ou tarefa.

   Na parte direita da janela é exibido um relatório que contém uma lista de eventos do processamento do componente ou tarefa especificados do Kaspersky Endpoint Security.

3. Se necessário, é possível modificar a apresentação de dados no relatório por meio de:

   - Filtragem de eventos
   - Execução de busca de evento
   - Reordenação de colunas
   - Classificação de eventos

4. Clique no botão **Salvar relatório** no canto superior direito da janela.

5. Na janela aberta, especifique a pasta de destino do arquivo de relatório.

6. Insira o nome do arquivo de relatório.

7. Selecione o formato do arquivo de relatório necessário: TXT ou CSV.

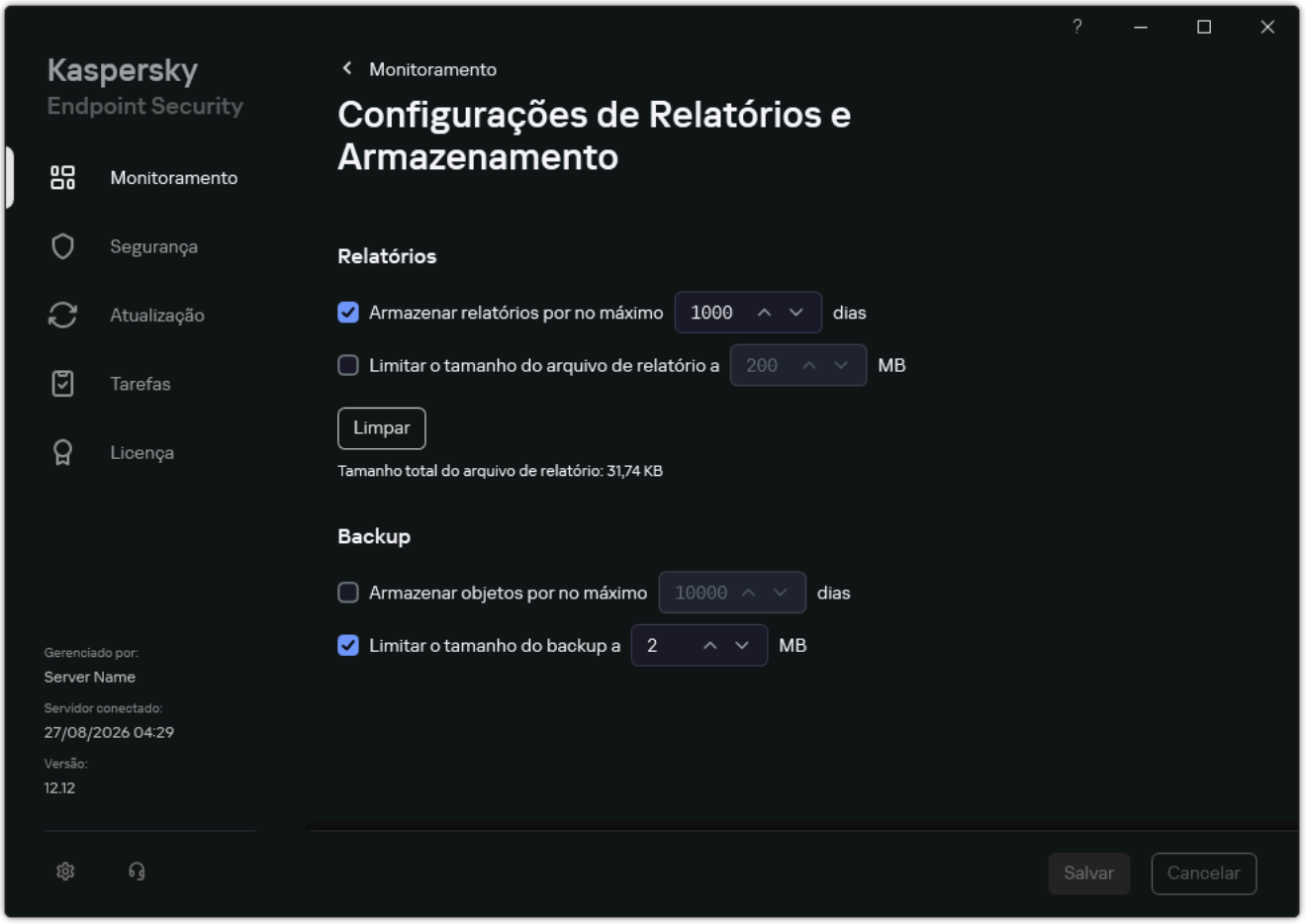
8. Salvar alterações.

Limpando relatórios

Para excluir informações dos relatórios:

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, em **Configurações gerais**, clique no bloco **Relatórios e armazenamento**.



Configurações de relatório

3. No bloco **Relatórios**, clique no botão **Limpar**.

4. Se a Proteção por senha estiver ativada, o Kaspersky Endpoint Security pode solicitar as credenciais da conta do usuário. O aplicativo solicitará as credenciais da conta caso o usuário não tenha as permissões necessárias.

O Kaspersky Endpoint Security excluirá todos os relatórios de todos os componentes e tarefas do aplicativo.

Autodefesa do Kaspersky Endpoint Security

A Autodefesa impede que outros aplicativos executem ações que podem interferir na operação do Kaspersky Endpoint Security e, por exemplo, remover o Kaspersky Endpoint Security do computador. O conjunto de tecnologias de Autodefesa disponíveis para o Kaspersky Endpoint Security depende se o sistema operacional é de 32 ou 64 bits (consulte a tabela abaixo). A Autodefesa também inclui a Proteção por senha e a Proteção da conexão do Servidor de Administração.

A *proteção por senha* permite restringir o acesso dos usuários ao Kaspersky Endpoint Security de acordo com as permissões concedidas a eles (por exemplo, permissão para sair do aplicativo).

A *Proteção da conexão do Servidor de Administração* impede a reconexão não autorizada do computador com um servidor não confiável.

Tecnologias de Autodefesa do Kaspersky Endpoint Security

Tecnologia	Descrição	Computador x86	Computador x64
Mecanismo de autodefesa	A tecnologia bloqueia o acesso aos seguintes componentes do aplicativo: • arquivos na pasta de instalação do Kaspersky Endpoint Security e outros arquivos do aplicativo; • chaves de registro com registros pertencentes ao aplicativo; • processos que o aplicativo executa.	✓	✓
AM-PPL (Antimalware Protected Process Light)	A tecnologia protege os processos do Kaspersky Endpoint Security contra ações maliciosas. Para obter mais detalhes sobre a tecnologia AM-PPL, visite o site da Microsoft. A tecnologia AM-PPL está disponível para os sistemas operacionais Windows 10 versão 1703 (RS2) ou posterior e Windows Server 2019.	✓	✓
Mecanismo de proteção contra o gerenciamento remoto	A tecnologia impede que outros aplicativos (por exemplo, TeamViewer ou RemotelyAnywhere) tenham acesso ao Kaspersky Endpoint Security.	✓	– (exceto para Windows 7)

Ativar ou desativar a Autodefesa

O Kaspersky Endpoint 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 Endpoint Security e outros arquivos do aplicativo;
- chaves de registro com registros pertencentes ao aplicativo;
- processos que o aplicativo executa.

Os mecanismos de autodefesa não se aplicam aos processos do Kaspersky Endpoint Security iniciados por processos pai não confiáveis.

O mecanismo de Autodefesa do Kaspersky Endpoint Security está ativado por padrão.

Como ativar ou desativar a Autodefesa no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Configurações de aplicativos**.
4. Use a caixa de seleção **Ativar a Autodefesa** para habilitar ou desabilitar o mecanismo de Autodefesa.
5. Salvar alterações.

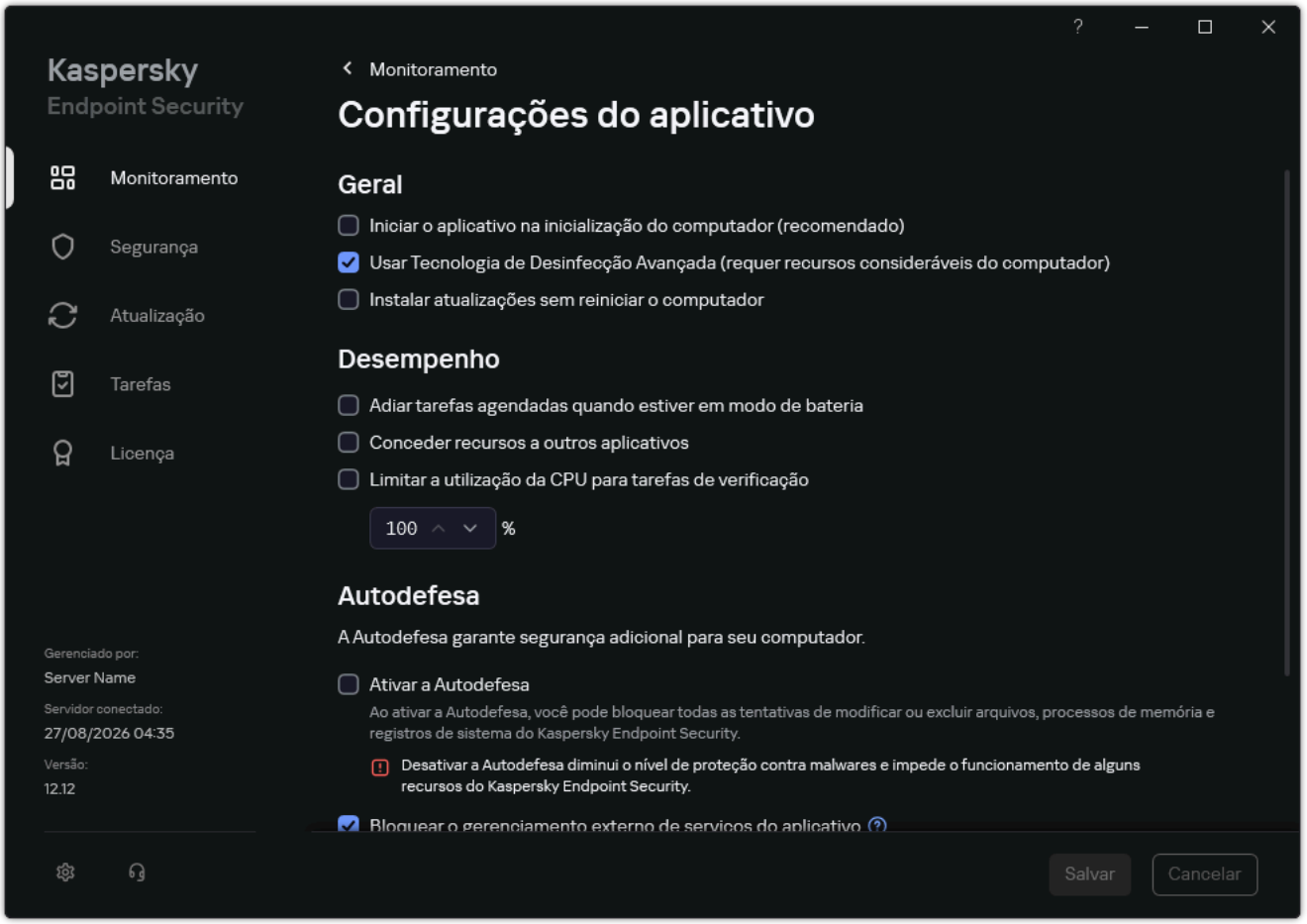
Como ativar ou desativar a Autodefesa no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Autodefesa**.
5. Use o botão de alternância **Autodefesa ATIVADA** para ativar ou desativar o mecanismo de Autodefesa.
6. Salvar alterações.

Como ativar ou desativar a Autodefesa na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações do aplicativo**.



Configurações do Kaspersky Endpoint Security for Windows

3. Use a caixa de seleção **Ativar a Autodefesa** para habilitar ou desabilitar o mecanismo de Autodefesa.

4. Salvar alterações.

Ativar e Desativar o suporte ao AM-PPL

O Kaspersky Endpoint Security é compatível com a tecnologia Antimalware Protected Process Light (doravante denominada "AM-PPL") da Microsoft. O AM-PPL protege os processos do Kaspersky Endpoint Security contra ações maliciosas (por exemplo, encerrando o aplicativo). O AM-PPL permite que apenas processos confiáveis sejam executados. Os processos do Kaspersky Endpoint 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 Endpoint 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.

Usar a tecnologia AM-PPL continuamente. O AM-PPL é um componente importante de proteção do sistema operacional. Desativar o suporte AM-PPL poderá gerar falhas em alguns recursos do Kaspersky Endpoint Security (por exemplo, a integração do aplicativo com o Windows Security Center). Desativar o suporte AM-PPL é permitido apenas em um ambiente de teste separado com o propósito da resolução de problemas.

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.exe) como um administrador.

3. Vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

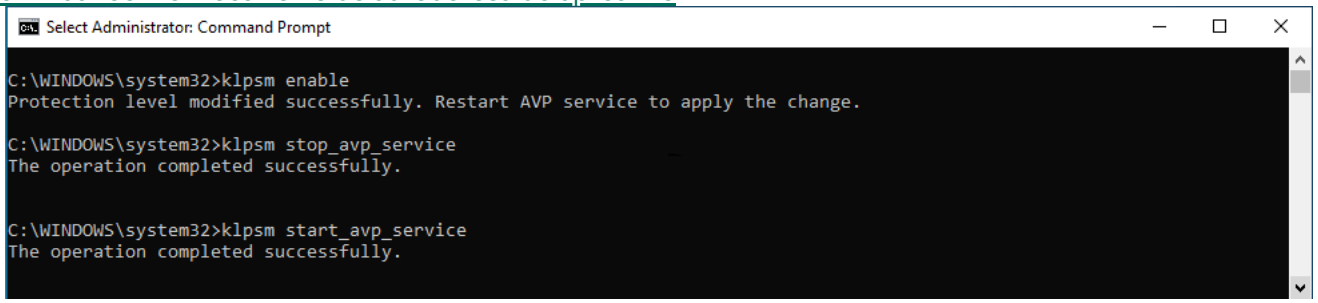
   É possível adicionar o caminho para o arquivo executável à variável de sistema %PATH% durante a instalação do aplicativo.

4. Digite o seguinte na linha de comando:

   - `klpsm.exe enable` – ativa o suporte para a tecnologia AM-PPL (veja a figura a seguir).
   - `klpsm.exe disable` – desativa o suporte à tecnologia AM-PPL.

5. Reiniciar o Kaspersky Endpoint Security.

6. Continuar com o mecanismo de autodefesa do aplicativo.



Habilitação do suporte à tecnologia AM-PPL

Proteção de serviços do aplicativo contra gerenciamento externo

A proteção de serviços do aplicativo contra gerenciamento externo bloqueia tentativas de usuários e outros aplicativos de interromper os serviços do Kaspersky Endpoint Security. A proteção assegura a operação dos seguintes serviços:

- Kaspersky Endpoint Security service (AVP.KES.14.2)
- Kaspersky Seamless Update Service service (AVPSUS.KES.14.2)

Para sair do aplicativo pela linha de comando, desative a proteção dos serviços do Kaspersky Endpoint Security contra gerenciamento externo.

É possível permitir o gerenciamento externo de serviços de aplicativo somente em computadores incompatíveis com a tecnologia AM-PPL ou em computadores com a tecnologia desativada.

Como ativar ou desativar a proteção de serviços de aplicativo contra gerenciamento externo no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Configurações de aplicativos**.
4. Use a caixa de seleção **Bloquear o gerenciamento externo de serviços do aplicativo** para ativar ou desativar a proteção dos serviços do Kaspersky Endpoint Security contra gerenciamento externo.
5. Salvar alterações.

Como ativar ou desativar a proteção de serviços do aplicativo contra gerenciamento externo no Web Console e no Cloud Console

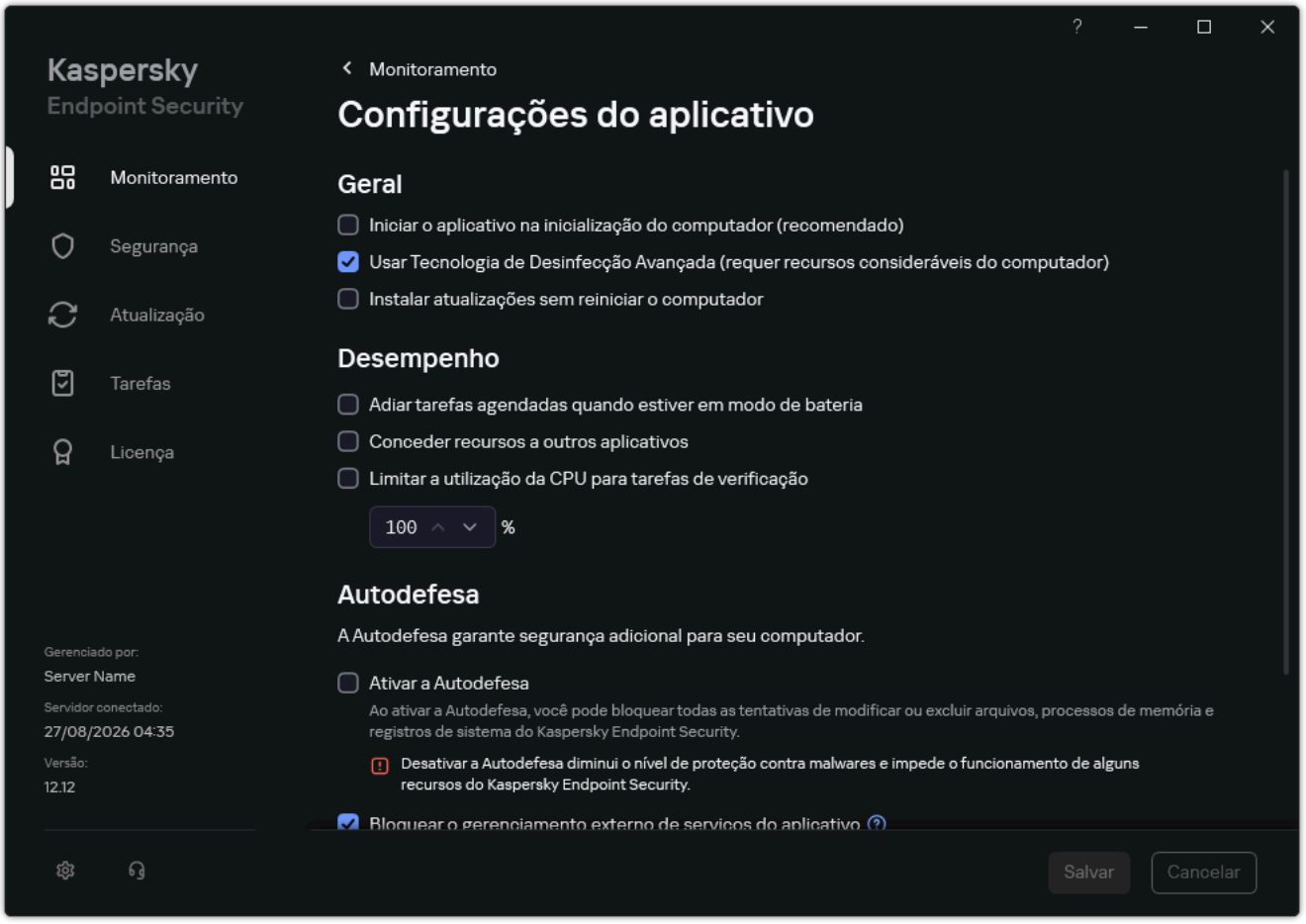
1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Autodefesa**.
5. Use a caixa de seleção **Bloquear o gerenciamento externo de serviços do aplicativo** para ativar ou desativar a proteção dos serviços do Kaspersky Endpoint Security contra gerenciamento externo.
6. Salvar alterações.

Como ativar ou desativar a proteção de serviços do aplicativo contra gerenciamento externo na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações do aplicativo**.

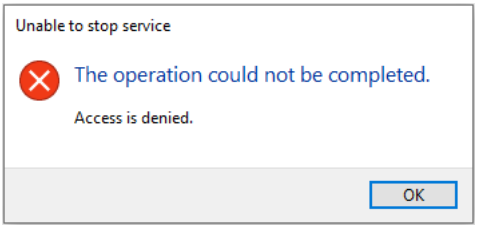


Configurações do Kaspersky Endpoint Security for Windows

3. Use a caixa de seleção **Bloquear o gerenciamento externo de serviços do aplicativo** para ativar ou desativar a proteção dos serviços do Kaspersky Endpoint Security contra gerenciamento externo.

4. Salvar alterações.

Assim, quando um usuário tentar interromper os serviços do aplicativo, 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 Endpoint Security.



Erro de acesso aos serviços do aplicativo

Suportar aplicativos de administração remota

Ocasionalmente, você pode precisar usar um programa de administração remota com a proteção contra o gerenciamento remoto ativada.

Para ativar a execução de aplicativos de administração remota:

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Exclusões e tipos de objetos detectados**.
3. No bloco **Exclusões**, clique no link **Especificar os aplicativos confiáveis**.
4. Na janela que é aberta, clique no botão **Adicionar**.
5. Selecione o arquivo executável do aplicativo de administração remota.

   Também é possível inserir o caminho manualmente. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.
6. Marque a caixa de seleção **Permitir a interação com a interface do Kaspersky Endpoint Security**.
7. Salvar alterações.

Proteção por senha

Vários usuários com diferentes níveis de conhecimentos de informática podem utilizar um computador. Se os usuários têm acesso sem restrições ao Kaspersky Endpoint Security e às configurações deste, talvez haja uma redução do nível geral de proteção. A proteção por senha permite restringir o acesso dos usuários ao Kaspersky Endpoint Security de acordo com as permissões concedidas a eles (por exemplo, permissão para sair do aplicativo).

Se o usuário que iniciou a sessão do Windows (*usuário da sessão*) tiver permissão para executar a ação, o Kaspersky Endpoint Security não solicitará o nome do usuário, senha ou senha temporária. O usuário recebe acesso ao Kaspersky Endpoint Security de acordo com as permissões concedidas.

Se um usuário da sessão não tiver permissão para executar uma ação, ele poderá obter acesso ao aplicativo das seguintes maneiras:

- Inserindo um nome de usuário e senha.

  Este método é adequado para operações diárias. Para executar uma ação protegida por senha, você deve inserir as credenciais da conta de domínio do usuário com a permissão necessária. Nesse caso, o computador deve estar nesse domínio. Caso o computador não esteja no domínio, é possível usar a conta KLAdmin ou uma conta adicionada manualmente.

- Insira uma senha temporária.

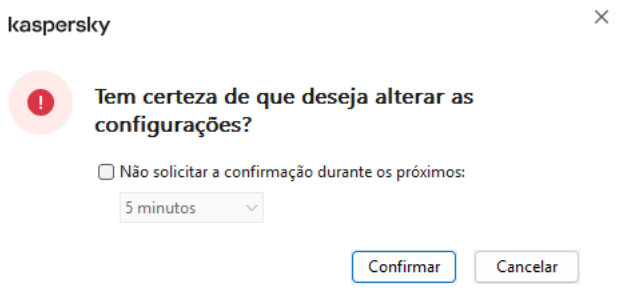
  Esse método é adequado para conceder permissões temporárias para executar ações bloqueadas (por exemplo, sair do aplicativo) a usuários que estão fora da rede corporativa. Quando uma senha temporária expira ou uma sessão termina, o Kaspersky Endpoint Security reverte suas configurações para o estado anterior.

- Token.

  Este método é adequado para usuários privilegiados (como a equipe de Suporte Técnico). A autenticação por token permite usar o modo de logon com cartão inteligente no Active Directory. Isso melhora a segurança da infraestrutura da organização.

Quando um usuário tenta executar uma ação protegida por senha, o Kaspersky Endpoint Security solicita o nome de usuário e a senha, a senha do token ou a senha temporária (veja a figura abaixo).

Na janela de entrada de senha, é possível alternar os idiomas apenas pressionando **ALT+ SHIFT**. O uso de outros atalhos, mesmo que configurados no sistema operacional, não funciona para a troca de idiomas.



Prompt de senha de acesso do Kaspersky Endpoint Security

Nome de usuário e senha

Para acessar o Kaspersky Endpoint Security, é necessário inserir as credenciais da conta. A proteção por senha suporta as seguintes contas:

- **KLAdmin**. Uma conta de administrador com acesso irrestrito ao Kaspersky Endpoint 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 Endpoint 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.

- **Usuário da sessão**. Conta do usuário que iniciou a sessão do Windows. Você pode alternar para outro usuário da sessão quando for solicitada uma senha (a caixa de seleção **Salvar a senha da sessão atual**). Nesse caso, o Kaspersky Endpoint Security considera o usuário cujas credenciais de conta foram inseridas como o usuário da sessão em vez do usuário que iniciou a sessão do Windows.

Senha temporária

Uma senha temporária pode ser usada para conceder acesso temporário ao Kaspersky Endpoint Security para um computador individual fora da rede corporativa. O Administrador gera uma senha temporária para um computador individual nas propriedades do computador no Kaspersky Security Center. O Administrador seleciona as ações que serão protegidas com a senha temporária e especifica o período de validade da senha temporária.

Token

Para acessar a funcionalidade do Kaspersky Endpoint Security, você deve selecionar o certificado de usuário apropriado na lista de certificados armazenados no token conectado e inserir seu PIN. A autenticação por token está disponível somente para usuários do domínio do Active Directory. O administrador pode configurar permissões para um usuário individual ou um grupo. Para que a autenticação por token funcione, é necessário implantar uma infraestrutura de PKI confiável e instalar um software especial para gerenciar o token.

Ativar a proteção por senha

A proteção por senha permite restringir o acesso dos usuários ao Kaspersky Endpoint Security de acordo com as permissões concedidas a eles (por exemplo, permissão para sair do aplicativo).

Como ativar a proteção por senha no console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Interface**.
4. No bloco **Proteção por senha**, clique no botão **Configurações**.
   Essa ação vai abrir uma janela com as configurações de proteção por senha.
5. Use a caixa de seleção **Ativar a proteção por senha** para ativar ou desativar o componente.
6. Em **Permissões**, selecione a conta KLAdmin.
7. Essa ação vai abrir uma janela. Nessa janela, clique em **Senha** e defina uma senha para a conta KLAdmin.
   A conta KLAdmin tem o direito de executar qualquer ação protegida por senha.

   > Caso tenha esquecido a senha da conta KLAdmin, é possível redefinir a senha nas propriedades da política.

8. Volte para a lista de contas.

9. Defina permissões para todos os usuários dentro da rede corporativa:

   a. Em **Permissões**, selecione o grupo "Todos".

      O grupo Todos é um grupo interno do Windows que inclui todos os usuários dentro da rede corporativa.

   b. Na janela que se abriu, marque as caixas de seleção ao lado das ações que os usuários poderão executar sem inserir a senha.

      Se uma caixa de seleção estiver desmarcada, os usuários serão impedidos de executar a ação. Por exemplo, se a caixa de seleção ao lado da permissão **Sair do aplicativo** estiver desmarcada, você poderá sair do aplicativo apenas se estiver registrado como KLAdmin ou como um usuário individual que tem a permissão necessária, ou se você digitar uma senha temporária.

      > As permissões de Proteção por senha têm alguns aspectos importantes a serem considerados. Certifique-se de que todas as condições para acessar o Kaspersky Endpoint Security sejam atendidas.

10. Salvar alterações.

Como ativar a proteção por senha no Web Console e no Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Autodefesa**.

5. Em **Proteção por senha**, use o botão de alternância de **Proteção por senha ATIVADA** para ativar ou desativar o componente.

6. Especifique a senha da conta KLAdmin e confirme-a.

   A conta KLAdmin tem o direito de executar qualquer ação protegida por senha.

   > Caso tenha esquecido a senha da conta KLAdmin, é possível redefinir a senha nas propriedades da política.

7. Volte para a lista de contas.

8. Defina permissões para todos os usuários dentro da rede corporativa:

   a. Na tabela de contas, selecione o grupo "Todos".

      O grupo Todos é um grupo interno do Windows que inclui todos os usuários dentro da rede corporativa.

   b. Na janela que se abriu, marque as caixas de seleção ao lado das ações que os usuários poderão executar sem inserir a senha.

      Se uma caixa de seleção estiver desmarcada, os usuários serão impedidos de executar a ação. Por exemplo, se a caixa de seleção ao lado da permissão **Sair do aplicativo** estiver desmarcada, você poderá sair do aplicativo apenas se estiver registrado como KLAdmin ou como um usuário individual que tem a permissão necessária, ou se você digitar uma senha temporária.

As permissões de Proteção por senha têm alguns aspectos importantes a serem considerados. Certifique-se de que todas as condições para acessar o Kaspersky Endpoint Security sejam atendidas.

9. Salvar alterações.

Como ativar a proteção por senha na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.
2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Interface**.
3. Use o botão de alternância do **Proteção por senha** para ativar ou desativar o componente.
4. Especifique a senha da conta KLAdmin e confirme-a.

   A conta KLAdmin tem o direito de executar qualquer ação protegida por senha.

   Se um computador estiver sendo executado segundo uma política, o Administrador poderá redefinir a senha da conta KLAdmin nas propriedades da política. Se o computador não estiver conectado ao Kaspersky Security Center e você tiver esquecido a senha da conta KLAdmin, não será possível recuperar a senha.

5. Defina permissões para todos os usuários dentro da rede corporativa:

   a. Na tabela de contas, clique em **Editar** para abrir a lista de permissões para o grupo Todos.

      O grupo Todos é um grupo interno do Windows que inclui todos os usuários dentro da rede corporativa.

   b. Marque as caixas de seleção ao lado das ações que os usuários poderão executar sem inserir a senha.

      Se uma caixa de seleção estiver desmarcada, os usuários serão impedidos de executar a ação. Por exemplo, se a caixa de seleção ao lado da permissão **Sair do aplicativo** estiver desmarcada, você poderá sair do aplicativo apenas se estiver registrado como KLAdmin ou como um usuário individual que tem a permissão necessária, ou se você digitar uma senha temporária.

      As permissões de Proteção por senha têm alguns aspectos importantes a serem considerados. Certifique-se de que todas as condições para acessar o Kaspersky Endpoint Security sejam atendidas.

6. Salvar alterações.

Quando a Proteção por senha está ativada, o aplicativo restringirá o acesso dos usuários ao Kaspersky Endpoint Security de acordo com as permissões concedidas ao grupo Todos. Você poderá executar as ações que estão bloqueadas para o grupo Todos somente se usar a conta KLAdmin, outra conta que recebe as permissões necessárias ou se digitar uma senha temporária.

Você pode desativar a Proteção por senha somente se estiver feito o login como KLAdmin. Não é possível desativar a proteção por senha se você estiver usando qualquer outra conta de usuário ou uma senha temporária.

Durante a verificação da senha, você pode marcar a caixa de seleção **Salvar a senha da sessão atual**. Nesse caso, o Kaspersky Endpoint Security não solicitará uma senha quando um usuário tentar executar outra ação protegida por senha durante a sessão.

Conceder permissões a usuários individuais ou grupos

A proteção por senha permite a concessão do acesso do Kaspersky Endpoint Security a contas de usuário individuais do Active Directory, bem como às contas de usuário adicionadas manualmente.

Contas de usuário do Active Directory

É possível conceder o acesso do Kaspersky Endpoint 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. Como resultado, você poderá sair do aplicativo apenas se estiver registrado como esse usuário ou como KLAdmin.

Você pode usar as credenciais da conta para acessar o aplicativo apenas se o computador estiver no domínio. Se o computador não estiver no domínio, você pode usar a conta KLAdmin ou uma senha temporária.

Contas de usuários adicionadas 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 **Visualizar relatórios** 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.

Conceder permissões a usuários individuais ou grupos

Como conceder permissões a usuários individuais ou grupos no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Interface**.
4. No bloco **Proteção por senha**, clique no botão **Configurações**.
   Essa ação vai abrir uma janela com as configurações de proteção por senha.
5. Na tabela de contas, clique em **Adicionar**.

6. Selecione o tipo da conta de usuário a ser adicionada:

   - **Selecionar um usuário/grupo do Active Directory** – contas de usuário do Active Directory

     Para selecionar uma conta de usuário, clique em **Selecionar**. Selecione um usuário ou um grupo no Active Directory e confirme a sua seleção.

   - **Adicionar um usuário/grupo de usuários o manualmente** para uma conta de usuário de serviço adicionada manualmente.

     Para adicionar uma conta de usuário do serviço, insira um nome de usuário e senha (por exemplo, SecureAdmin).

     > É possível redefinir a senha de uma conta de usuário de serviço nas configurações de política. A senha da conta de usuário do serviço deve ser redefinida da mesma maneira que a senha do KLAdmin. Se a edição das configurações de proteção por senha for permitida (o "cadeado" estiver aberto) ou nenhuma política for aplicada no computador, é possível redefinir a senha da conta de usuário do serviço na interface do aplicativo. Para fazer isso, confirme as alterações nas informações da conta de usuário do serviço usando a senha KLAdmin.

7. Na lista **Permissões**, marque as caixas de seleção ao lado das ações que o usuário ou grupo selecionado poderá executar sem precisar inserir uma senha.

   Se uma caixa de seleção estiver desmarcada, os usuários serão impedidos de executar a ação. Por exemplo, se a caixa de seleção ao lado da permissão **Sair do aplicativo** estiver desmarcada, você poderá sair do aplicativo apenas se estiver registrado como KLAdmin ou como um usuário individual que tem a permissão necessária, ou se você digitar uma senha temporária.

   > As permissões de Proteção por senha têm alguns aspectos importantes a serem considerados. Certifique-se de que todas as condições para acessar o Kaspersky Endpoint Security sejam atendidas.

8. Salvar alterações.

Como conceder permissões a usuários individuais ou grupos no Web Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Autodefesa**.

5. No bloco **Proteção por senha**, clique no link **Permissões de usuário**.

   Isso abre o formulário para conceder permissões de Ativação da senha.

6. Clique **Adicionar**.

7. Selecione o tipo da conta de usuário a ser adicionada:

   - **Selecione com base no Diretório Ativo** – contas de usuário do Active Directory

     Para selecionar uma conta de usuário, clique em **Editar**. Selecione um usuário ou um grupo no Active Directory e confirme a sua seleção.

- **Adicionar manualmente** para uma conta de usuário de serviço adicionada manualmente.

  Para adicionar uma conta de usuário do serviço, insira um nome de usuário e senha (por exemplo, SecureAdmin).

  > É possível redefinir a senha de uma conta de usuário de serviço nas configurações de política. A senha da conta de usuário do serviço deve ser redefinida da mesma maneira que a senha do KLAdmin. Se a edição das configurações de proteção por senha for permitida (o "cadeado" estiver aberto) ou nenhuma política for aplicada no computador, é possível redefinir a senha da conta de usuário do serviço na interface do aplicativo. Para fazer isso, confirme as alterações nas informações da conta de usuário do serviço usando a senha KLAdmin.

8. Na lista **Permissões**, marque as caixas de seleção ao lado das ações que o usuário ou grupo selecionado poderá executar sem precisar inserir uma senha.

   Se uma caixa de seleção estiver desmarcada, os usuários serão impedidos de executar a ação. Por exemplo, se a caixa de seleção ao lado da permissão **Sair do aplicativo** estiver desmarcada, você poderá sair do aplicativo apenas se estiver registrado como KLAdmin ou como um usuário individual que tem a permissão necessária, ou se você digitar uma senha temporária.

   > As permissões de Proteção por senha têm alguns aspectos importantes a serem considerados. Certifique-se de que todas as condições para acessar o Kaspersky Endpoint Security sejam atendidas.

9. Clique **Adicionar**.

10. Salvar alterações.

Como conceder permissões a usuários individuais ou grupos na interface de usuário do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Interface**.

3. Na tabela de contas, clique em **Adicionar**.

4. Selecione o tipo da conta de usuário a ser adicionada:

   - **Selecionar um usuário/grupo do Active Directory** – contas de usuário do Active Directory

     Para selecionar uma conta de usuário, clique em **Selecionar usuário ou grupo**. Selecione um usuário ou um grupo no Active Directory e confirme a sua seleção.

   - **Adicionar um usuário manualmente** para uma conta de usuário de serviço adicionada manualmente.

     Para adicionar uma conta de usuário do serviço, insira um nome de usuário e senha (por exemplo, SecureAdmin).

     > É possível redefinir a senha de uma conta de usuário de serviço nas configurações de política. A senha da conta de usuário do serviço deve ser redefinida da mesma maneira que a senha do KLAdmin. Se a edição das configurações de proteção por senha for permitida (o "cadeado" estiver aberto) ou nenhuma política for aplicada no computador, é possível redefinir a senha da conta de usuário do serviço na interface do aplicativo. Para fazer isso, confirme as alterações nas informações da conta de usuário do serviço usando a senha KLAdmin.

5. Na lista **Permissões**, marque as caixas de seleção ao lado das ações que o usuário ou grupo selecionado poderá executar sem precisar inserir uma senha.

   Se uma caixa de seleção estiver desmarcada, os usuários serão impedidos de executar a ação. Por exemplo, se a caixa de seleção ao lado da permissão **Sair do aplicativo** estiver desmarcada, você poderá sair do aplicativo apenas se estiver registrado como KLAdmin ou como um usuário individual que tem a permissão necessária, ou se você digitar uma senha temporária.

   > As permissões de Proteção por senha têm alguns aspectos importantes a serem considerados. Certifique-se de que todas as condições para acessar o Kaspersky Endpoint Security sejam atendidas.

6. Salvar alterações.

Como resultado, se o acesso ao aplicativo for restrito ao grupo Todos, os usuários receberão permissões para acessar o Kaspersky Endpoint Security de acordo com as permissões individuais dos usuários.

Usar uma senha temporária para conceder permissões

Uma senha temporária pode ser usada para conceder acesso temporário ao Kaspersky Endpoint Security para um computador individual fora da rede corporativa. Isso é necessário para permitir que o usuário execute uma ação bloqueada sem obter as credenciais da conta do KLAdmin. Para usar uma senha temporária, o computador deve ser adicionado ao Kaspersky Security Center.

Como permitir que um usuário execute uma ação bloqueada usando uma senha temporária por meio do Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertencem os respectivos computadores clientes.
3. No espaço de trabalho, selecione a guia **Dispositivos**.
4. Clique duas vezes para abrir a janela de propriedades do computador.
5. Na janela de propriedades do computador, selecione a seção **Aplicativos**.
6. Na lista de aplicativos da Kaspersky instalados no computador, selecione **Kaspersky Endpoint Security for Windows (14.2)** e clique duas vezes para abrir as propriedades do aplicativo.
7. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Interface**.
8. No bloco **Proteção por senha**, clique no botão **Configurações**.
9. Na janela exibida, no bloco **Senha temporária**, clique no botão **Lista de senhas temporárias**.

   A janela Gerenciamento de senhas temporárias é exibida.
10. Clique **Adicionar**.
11. No campo **Data de expiração**, especifique a data de expiração quando a senha temporária expirará.
12. Na tabela **Escopo da senha temporária**, marque as caixas de seleção ao lado das ações que estarão disponíveis para o usuário após inserir a senha temporária.

13. Clique **Gerar**.

    Uma janela contendo a senha temporária é aberta (veja a figura abaixo).

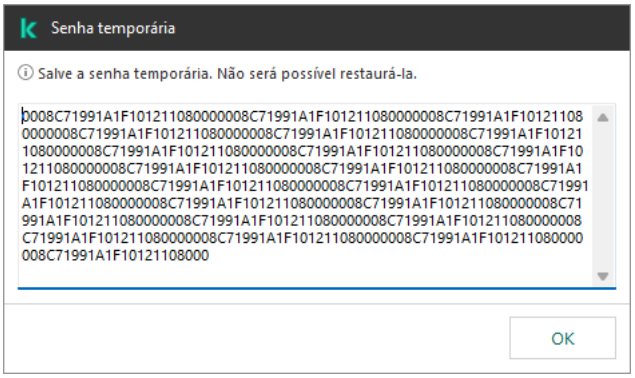
14. Copie a senha e forneça-a ao usuário.

Como permitir que um usuário execute uma ação bloqueada usando uma senha temporária por meio do Web Console e do Cloud Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Ativos (dispositivos)**.
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 Endpoint Security for Windows**.

   Isso abre as configurações locais do aplicativo.
5. Selecione a guia **Configurações do aplicativo**.
6. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Interface**.
7. No bloco **Senhas temporárias**, clique no botão **Adicionar**.
8. No campo **Data de expiração**, especifique a data de expiração quando a senha temporária expirará.
9. Na tabela **Escopo da senha temporária**, marque as caixas de seleção ao lado das ações que estarão disponíveis para o usuário após inserir a senha temporária.
10. Clique **Gerar**.

    Uma janela contendo a senha temporária é aberta.
11. Copie a senha e forneça-a ao usuário.



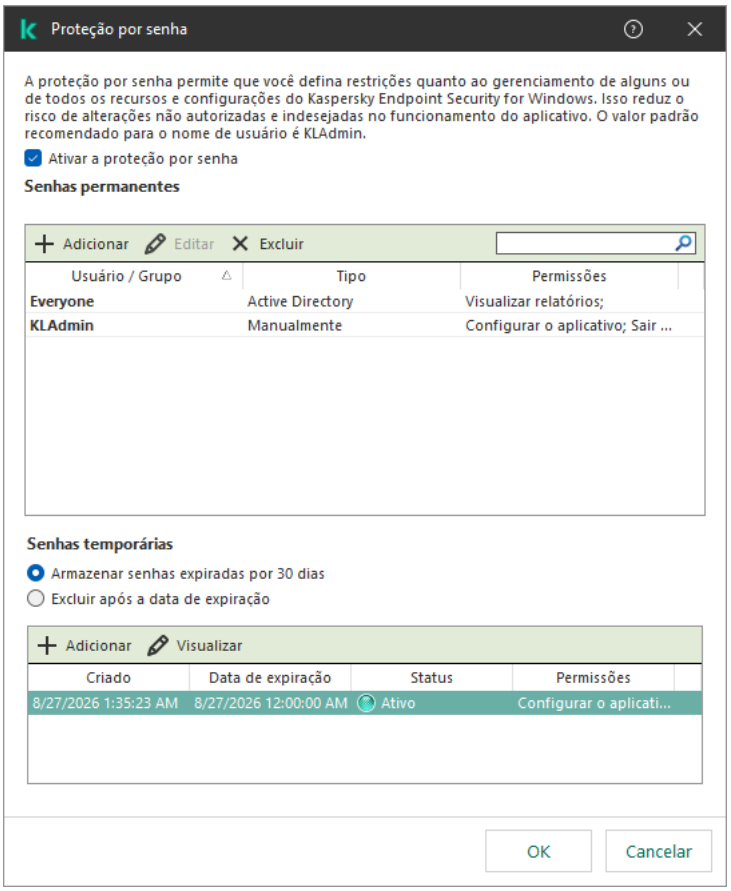
Senha temporária

Revogação da senha temporária

A partir da versão 12.9, o Kaspersky Endpoint Security for Windows inclui a funcionalidade *Gerenciamento de senhas temporárias*. O gerenciamento de senhas temporárias permite executar as seguintes ações:

- Salvar o histórico de senhas (até 30 dias).
- Monitorar o status da senha temporária: *Ativo*, *Expirado*, *Revogado*.

- Revogar senhas temporárias.



Gerenciamento de senhas temporárias

O gerenciamento de senhas temporárias atualiza o status da senha para revogá-la somente após sincronizar o computador com o Kaspersky Security Center.

Como revogar a senha temporária com o uso do Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, abra a pasta com o nome do grupo de administração ao qual pertencem os respectivos computadores clientes.
3. No espaço de trabalho, selecione a guia **Dispositivos**.
4. Clique duas vezes para abrir a janela de propriedades do computador.
5. Na janela de propriedades do computador, selecione a seção **Aplicativos**.
6. Na lista de aplicativos da Kaspersky instalados no computador, selecione **Kaspersky Endpoint Security for Windows (14.2)** e clique duas vezes para abrir as propriedades do aplicativo.
7. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Interface**.
8. No bloco **Proteção por senha**, clique no botão **Configurações**.
9. Uma janela é aberta; nessa janela, em **Senha temporária**, defina as configurações de armazenamento para senhas expiradas.

10. Clique **Lista de senhas temporárias**.

    A janela Gerenciamento de senhas temporárias é exibida. O gerenciamento de senhas temporárias exibe a data de expiração da senha, o status da senha e a lista de permissões.

11. Selecione a senha temporária ativa que deseja revogar e clique duas vezes na senha para abrir suas propriedades.

12. Na janela que é aberta, clique no botão **Revogar**.

13. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Como revogar uma senha temporária com o uso do Web Console e Cloud Console

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

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 Endpoint Security for Windows**.

   Isso abre as configurações locais do aplicativo.

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

6. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Interface**.

7. Em **Senhas temporárias**, configure o armazenamento de senhas expiradas.

8. Clique no link **Senha temporária**.

   A janela Gerenciamento de senhas temporárias é exibida. O gerenciamento de senhas temporárias exibe a data de expiração da senha, o status da senha e a lista de permissões.

9. Selecione a senha temporária ativa que deseja revogar.

10. Na janela que é aberta, clique no botão **Revogar senha**.

11. Salvar alterações. Para aplicar a política em computadores, feche os cadeados .

Assim, o gerenciamento de senhas temporárias define o status da senha como *Revogar (sincronizando com um host)*. Depois de sincronizar o computador com o Kaspersky Security Center, o aplicativo revoga a senha temporária e bloqueia as permissões concedidas imediatamente.

Aspectos especiais das permissões de Proteção por senha

As permissões de Proteção por senha têm alguns aspectos e limitações importantes a serem considerados.

Configurar o aplicativo

Se o computador de um usuário estiver sendo executado segundo uma política, verifique se todas as configurações necessárias na política estão disponíveis para edição (os atributos estão abertos).

Sair do aplicativo

Não há considerações ou limitações especiais.

Desativar componentes de proteção

- Não é possível conceder a permissão para desativar os componentes de proteção para o grupo Todos. Para permitir que usuários que não sejam KL Admin desativem componentes de proteção, adicione um usuário ou grupo que tenha a permissão **Desativar componentes de proteção** nas configurações de proteção por senha.
- Se o computador de um usuário estiver sendo executado segundo uma política, verifique se todas as configurações necessárias na política estão disponíveis para edição (os atributos estão abertos).
- Para desativar componentes de proteção nas configurações do aplicativo, um usuário deve ter a permissão **Configurar o aplicativo**.
- Para desativar componentes de proteção a partir do menu de contexto (usando o item de menu **Pausar a proteção**), um usuário deve ter a permissão **Desativar componentes de proteção** além da permissão **Desativar componentes de controle**.

Desativar componentes de controle

- Não é possível conceder a permissão para desativar os componentes de controle para o grupo Todos. Para permitir que usuários que não sejam KL Admin desativem componentes de proteção, adicione um usuário ou grupo que tenha a permissão **Desativar componentes de controle** nas configurações de proteção por senha.
- Se o computador de um usuário estiver sendo executado segundo uma política, verifique se todas as configurações necessárias na política estão disponíveis para edição (os atributos estão abertos).
- Para desativar componentes de controle nas configurações do aplicativo, um usuário deve ter a permissão **Configurar o aplicativo**.
- Para desativar componentes de controle a partir do menu de contexto (usando o item de menu **Pausar a proteção**), um usuário deve ter a permissão **Desativar componentes de controle** além da permissão **Desativar componentes de proteção**.

Desativar política do Kaspersky Security Center

Você não pode conceder ao grupo "Todos" a permissão para desativar a política do Kaspersky Security Center. Para permitir que usuários que não sejam KL Admin desativem a política, adicione um usuário ou grupo que tenha a permissão **Desativar política do Kaspersky Security Center** nas configurações de proteção por senha.

Remover a chave

Não há considerações ou limitações especiais.

Remover/modificar/restaurar o aplicativo

Se você permitiu a remoção, modificação e restauração do aplicativo para o grupo "Todos", o Kaspersky Endpoint Security não solicitará uma senha quando o usuário tentar realizar essas operações. Portanto, qualquer usuário, incluindo usuários de fora do domínio, pode instalar, modificar ou restaurar o aplicativo.

Restaurar o acesso a dados em unidade criptografada

Você pode restaurar o acesso a dados em discos criptografados somente se estiver registrado como KLAdmin. A permissão para executar esta ação não pode ser concedida a nenhum outro usuário.

Visualizar relatórios

Não há considerações ou limitações especiais.

Restaurar do backup

Não há considerações ou limitações especiais.

Exportar configurações

Por padrão, a exportação de configurações do aplicativo é negada ao grupo "Todos". Você pode exportar as configurações do aplicativo utilizando a conta de usuário KLAdmin. A exportação das configurações do aplicativo inclui somente a criação de um arquivo de configuração com as configurações do Kaspersky Endpoint Security na interface do aplicativo. A permissão não restringe a exportação de listas de exclusões de verificação, endereços da Web confiáveis, dispositivos confiáveis ou outras listas mantidas por componentes do aplicativo.

Redefinir a senha do KLAdmin

Caso tenha esquecido a senha da conta KLAdmin, é possível redefinir a senha nas propriedades da política. Não é possível redefinir a senha na interface do aplicativo.

É possível executar ações protegidas por senha usando uma senha temporária. Nesse caso, não é preciso inserir credenciais do KLAdmin.

Se o computador não estiver conectado ao Kaspersky Security Center e você tiver esquecido a senha da conta KLAdmin, não será possível recuperar a senha.

Como redefinir a senha da conta KLAdmin usando o Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Interface**.
4. No bloco **Proteção por senha**, clique no botão **Configurações**.
5. Na janela aberta, desmarque a caixa de seleção **Ativar a proteção por senha**.
6. Salvar alterações.
7. Marque a caixa de seleção **Ativar a proteção por senha** novamente.
8. Clique em **OK**.
   Essa ação abre a janela da senha do administrador.
9. Especifique a nova senha da conta KLAdmin e confirme-a.
10. Salvar alterações.

Como redefinir a senha da conta KLAdmin no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Ativos (dispositivos)**.
2. Selecione o computador para o qual você deseja definir as configurações locais do aplicativo.
   Isso abre as propriedades do computador.
3. Selecione a guia **Aplicativos**.
4. Clique **Kaspersky Endpoint Security for Windows 14.2**.
   Isso abre as configurações locais do aplicativo.
5. Selecione a guia **Configurações do aplicativo**.
6. Selecione **Configurações gerais** → **Autodefesa**.
7. Em **Proteção por senha**, desligue o botão de alternância **Proteção por senha**.
8. Salvar alterações.
9. Ative o botão de alternância **Proteção por senha** novamente.

10. Especifique a nova senha da conta KLAdmin e confirme-a.

11. Salvar alterações.

Como resultado, a senha da conta KLAdmin é atualizada após a aplicação da política.

Proteção da conexão do Servidor de Administração

A conexão do computador com o Servidor de Administração é feita com o uso do componente do *Agente de Rede* do Kaspersky Security Center. Caso um invasor tenha direitos suficientes para modificar as configurações de conexão do servidor, existe um risco de conexão do computador com um servidor não confiável. Isso permitiria que um invasor aplicasse suas próprias políticas de grupo e, por exemplo, desativasse a autodefesa do aplicativo. O Kaspersky Endpoint Security pode evitar a reconexão não autorizada de um computador a um servidor diferente. Para proteger a conexão com o servidor, o aplicativo sugere definir uma senha e usar a Password-Based key Derivation Function (PBKDF2). Como resultado, o acesso ao aplicativo sem senha é impossível.

Para garantir a proteção completa do Kaspersky Endpoint Security e do Agente de Rede contra acesso não autorizado, recomendamos ativar a proteção adicional. Para o Kaspersky Endpoint Security, recomendamos ativar a proteção por senha. Para proteger o Agente de Rede, recomendamos definir uma senha de desinstalação. Para mais detalhes sobre proteger o Agente de rede da remoção, consulte a Ajuda do Kaspersky Security Center.

O gerenciamento da conexão do computador com o Servidor de Administração é feito utilizando a tarefa *Proteção da conexão do Servidor de Administração*. A tarefa permite executar as seguintes ações:

- Definir uma senha para proteger a conexão do servidor.
- Alterar a senha.
- Reconectar o computador com um servidor diferente.
- Desativar a proteção da conexão do servidor.

Autenticação do computador durante a conexão com o Servidor de Administração

Após definir uma senha, o aplicativo cria um conjunto de dados usando a transformação da senha com PBKDF2. Então, o aplicativo criptografa esse conjunto de dados usando o Agente de Rede. O aplicativo usa o conjunto de dados criptografado para verificar os direitos e privilégios do Servidor de Administração para as conexões subsequentes.

Posteriormente, sempre que for feita uma tentativa de reconexão entre o computador e o Servidor de Administração, o aplicativo descriptografará o conjunto de dados com a chave do Agente de Rede e o comparará com a cópia local. Se não corresponderem, o acesso ao aplicativo ficará restrito.

Proteção da conexão do Servidor de Administração

Como definir uma senha no Console de Administração (MMC) para a proteção da conexão com o servidor

1. No Console de Administração do Kaspersky Security Center, selecione **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

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Proteção da conexão do Servidor de Administração**.

Etapa 2. Proteção da conexão do Servidor de Administração

Defina uma senha para proteger a conexão do Servidor de Administração:

1. Em **Proteção da conexão do Servidor de Administração**, selecione **Proteger com uma senha**.

2. Na lista suspensa **Servidor de Administração**, selecione **Novo servidor**.

3. No campo **Senha para conexão com o Servidor de Administração**, defina uma senha para conexão com o Servidor de Administração e confirme-a.

   Caso esqueça a senha, é possível alterá-la com o uso de uma tarefa.

4. Caso tenha o Kaspersky Endpoint Security 12.7 ou uma versão anterior do aplicativo implementado, marque a caixa de seleção **Ativar a compatibilidade com criptografia de senha para versões anteriores do aplicativo (12.7 e anterior)**.

   A partir do Kaspersky Endpoint Security 12.8 for Windows, o aplicativo usa uma criptografia de senha mais forte. Caso tenha o Kaspersky Endpoint Security 12.8 ou posterior implementado, recomendamos desmarcar essa caixa de seleção e usar a criptografia de senha mais forte. As versões anteriores do aplicativo não são compatíveis com a criptografia de senha forte. Para executar a tarefa, é necessário marcar a caixa de seleção.

Etapa 3. Seleção da conta para executar a tarefa

Selecione **Conta padrão**. Por padrão, o Kaspersky Endpoint Security inicia a tarefa como a conta de usuário do sistema (SISTEMA).

Etapa 4. Configurar um agendamento de início de tarefa

Em **Início agendado**, selecione **Manualmente**.

Etapa 5. Definir o nome da tarefa

Insira um nome para a tarefa, por exemplo, *Senha de conexão do servidor principal*.

Etapa 6. Concluir a criação da tarefa

Conclua o assistente. Marque a caixa de seleção **Executar tarefa após a conclusão do assistente** ou execute a tarefa manualmente. Você pode monitorar o andamento da tarefa nas propriedades da tarefa.

Como definir uma senha no Web Console e no Cloud Console para a proteção da conexão com o servidor

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Proteção da conexão do Servidor de Administração**.

   c. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Senha de conexão do servidor principal*.

   d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Vá para a próxima etapa.

5. Selecione uma conta de usuário padrão. Por padrão, o Kaspersky Endpoint Security inicia a tarefa como a conta de usuário do sistema (SISTEMA).

6. Conclua o assistente.

   Uma nova tarefa será exibida na lista de tarefas.

7. Clique na tarefa **Proteção da conexão do Servidor de Administração** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

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

9. Em **Proteção da conexão do Servidor de Administração**, selecione **Proteger com uma senha**.

10. Na lista suspensa **Conexão com o Servidor de Administração**, selecione **Nova senha**.

11. No campo **Senha para conexão com o Servidor de Administração**, defina uma senha para conexão com o Servidor de Administração e confirme-a.

    Caso esqueça a senha, é possível alterá-la com o uso de uma tarefa.

12. Caso tenha o Kaspersky Endpoint Security 12.7 ou uma versão anterior do aplicativo implementado, marque a caixa de seleção **Ativar a compatibilidade com criptografia de senha para versões anteriores do aplicativo (12.7 e anterior)**.

    A partir do Kaspersky Endpoint Security 12.8 for Windows, o aplicativo usa uma criptografia de senha mais forte. Caso tenha o Kaspersky Endpoint Security 12.8 ou posterior implementado, recomendamos desmarcar essa caixa de seleção e usar a criptografia de senha mais forte. As versões anteriores do aplicativo não são compatíveis com a criptografia de senha forte. Para executar a tarefa, é necessário marcar a caixa de seleção.

13. Salvar alterações.

14. Marque a caixa de seleção ao lado da tarefa.

15. Clique **Iniciar**.

Você pode monitorar o status da tarefa e o número de dispositivos nos quais a tarefa foi concluída com êxito ou concluída com um erro.

Reconexão do computador com um Servidor de Administração diferente

Reconectar o computador a um Servidor de Administração diferente envolve as seguintes etapas:

1. No console do servidor `[KSC1]` atual, execute a tarefa *Alterar o Servidor de Administração* para o Agente de Rede.

   Após executar a tarefa, o computador é reconectado ao novo servidor `[KSC2]`.

   O computador será exibido no console do servidor `[KSC1]` com o status *Crítico*. Não é possível configurar o aplicativo usando políticas ou executando tarefas remotas no computador.

2. No console do novo servidor `[KSC2]`, crie uma nova tarefa *Proteção da conexão do Servidor de Administração* para o Kaspersky Endpoint Security. Nas propriedades da tarefa, insira a senha do servidor anterior e defina uma senha para o novo servidor.

   Como definir uma nova senha no Console de Administração (MMC) para reconectar com um novo servidor

   1. No Console de Administração do Kaspersky Security Center, selecione **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

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Proteção da conexão do Servidor de Administração**.

Etapa 2. Proteção da conexão do Servidor de Administração

Defina uma senha para proteger a conexão com o novo Servidor de Administração:

1. Em **Proteção da conexão do Servidor de Administração**, selecione **Proteger com uma senha**.
2. Na lista suspensa **Servidor de Administração**, selecione **Reconectar a partir de outro servidor**.
3. No campo **Senha atual**, insira a senha definida para a conexão com o servidor confiável utilizado anteriormente.
4. No campo **Nova senha**, defina uma senha para conexão com o novo Servidor de Administração e confirme a senha.

   Caso esqueça a senha, é possível alterá-la com o uso de uma tarefa.
5. Caso tenha o Kaspersky Endpoint Security 12.7 ou uma versão anterior do aplicativo implementado, marque a caixa de seleção **Ativar a compatibilidade com criptografia de senha para versões anteriores do aplicativo (12.7 e anterior)**.

   A partir do Kaspersky Endpoint Security 12.8 for Windows, o aplicativo usa uma criptografia de senha mais forte. Caso tenha o Kaspersky Endpoint Security 12.8 ou posterior implementado, recomendamos desmarcar essa caixa de seleção e usar a criptografia de senha mais forte. As versões anteriores do aplicativo não são compatíveis com a criptografia de senha forte. Para executar a tarefa, é necessário marcar a caixa de seleção.

Etapa 3. Seleção da conta para executar a tarefa

Selecione **Conta padrão**. Por padrão, o Kaspersky Endpoint Security inicia a tarefa como a conta de usuário do sistema (SISTEMA).

Etapa 4. Configurar um agendamento de início de tarefa

Em **Início agendado**, selecione **Manualmente**.

Etapa 5. Definir o nome da tarefa

Insira um nome para a tarefa, por exemplo, *Senha de conexão do servidor principal*.

Etapa 6. Concluir a criação da tarefa

Conclua o assistente. Marque a caixa de seleção **Executar tarefa após a conclusão do assistente** ou execute a tarefa manualmente. Você pode monitorar o andamento da tarefa nas propriedades da tarefa.

Como definir uma nova senha no Web Console e no Cloud Console para reconectar com um novo servidor

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Proteção da conexão do Servidor de Administração**.

   c. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Senha de conexão do servidor principal*.

   d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Vá para a próxima etapa.

5. Selecione uma conta de usuário padrão. Por padrão, o Kaspersky Endpoint Security inicia a tarefa como a conta de usuário do sistema (SISTEMA).

6. Conclua o assistente.

   Uma nova tarefa será exibida na lista de tarefas.

7. Clique na tarefa **Proteção da conexão do Servidor de Administração** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

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

9. Em **Proteção da conexão do Servidor de Administração**, selecione **Proteger com uma senha**.

10. Na lista suspensa **Conexão com o Servidor de Administração**, selecione **Reconectar a partir de outro servidor**.

11. No campo **Senha atual**, insira a senha definida para a conexão com o servidor confiável utilizado anteriormente.

12. No campo **Nova senha**, defina uma senha para conexão com o novo Servidor de Administração e confirme a senha.

    Caso esqueça a senha, é possível alterá-la com o uso de uma tarefa.

13. Caso tenha o Kaspersky Endpoint Security 12.7 ou uma versão anterior do aplicativo implementado, marque a caixa de seleção **Ativar a compatibilidade com criptografia de senha para versões anteriores do aplicativo (12.7 e anterior)**.

    A partir do Kaspersky Endpoint Security 12.8 for Windows, o aplicativo usa uma criptografia de senha mais forte. Caso tenha o Kaspersky Endpoint Security 12.8 ou posterior implementado, recomendamos desmarcar essa caixa de seleção e usar a criptografia de senha mais forte. As versões anteriores do aplicativo não são compatíveis com a criptografia de senha forte. Para executar a tarefa, é necessário marcar a caixa de seleção.

14. Salvar alterações.

15. Marque a caixa de seleção ao lado da tarefa.

16. Clique **Iniciar**.

    Você pode monitorar o status da tarefa e o número de dispositivos nos quais a tarefa foi concluída com êxito ou concluída com um erro.

Após concluir a tarefa, certifique-se de que no console do novo servidor `[KSC2]`, o computador esteja com o status *OK*. Teste se é possível executar tarefas remotamente e configurar o aplicativo usando políticas.

Redefinição da senha de conexão do Servidor de Administração

Se você esqueceu a senha de conexão do Servidor de Administração ou a senha está comprometida, é possível redefini-la nas propriedades da tarefa. Também é possível redefinir a senha e definir uma nova senha para um grupo de computadores com diferentes status de proteção de conexão do Servidor de Administração. Ou seja, se alguns computadores estiverem com a proteção ativada e outros desativada, a tarefa define uma senha para todos os computadores.

> Só é possível redefinir a senha de conexão do Servidor de Administração no console do servidor confiável ao qual o computador está conectado.

Como redefinir a senha de conexão com o Servidor de Administração usando o Console de Administração (MMC)

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

2. Na árvore do console, selecione **Tarefas**.

3. Selecione a tarefa **Proteção da conexão do Servidor de Administração** e clique duas vezes para abrir as propriedades dela.

4. Na janela de propriedades da tarefa, selecione a seção **Configurações**.

5. Em **Proteção da conexão do Servidor de Administração**, selecione **Proteger e alterar senha**.

6. No campo **Senha para conexão com o Servidor de Administração** defina uma nova senha para conexão ao servidor confiável atual e confirme a senha.

7. Salvar alterações.

8. Execute a tarefa.

Como redefinir a senha de conexão com o Servidor de Administração no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **Tarefas**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Proteção da conexão do Servidor de Administração** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

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

4. Em **Proteção da conexão do Servidor de Administração**, selecione **Proteger e alterar senha**.

5. No campo **Senha para conexão com o Servidor de Administração** defina uma nova senha para conexão ao servidor confiável atual e confirme a senha.

6. Salvar alterações.

7. Marque a caixa de seleção ao lado da tarefa.

8. Clique **Iniciar**.

Como resultado, a senha de conexão do Servidor de Administração é redefinida após a conclusão da tarefa.

Desativação da proteção da conexão do Servidor de Administração

Só é possível desativar remotamente a proteção de conexão do Servidor de Administração no console do servidor confiável ao qual o computador está conectado. Também é possível desativar a proteção localmente na linha de comando.

Como desativar a proteção da conexão do servidor no Console de Administração (MMC)

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

2. Na árvore do console, selecione **Tarefas**.

3. Selecione a tarefa **Proteção da conexão do Servidor de Administração** e clique duas vezes para abrir as propriedades dela.

4. Na janela de propriedades da tarefa, selecione a seção **Configurações**.

5. Em **Proteção da conexão do Servidor de Administração**, selecione **Não proteger**.

6. Salvar alterações.

7. Execute a tarefa.

   Você pode monitorar o status da tarefa e o número de dispositivos nos quais a tarefa foi concluída com êxito ou concluída com um erro.

Como desativar a proteção da conexão do servidor no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **Tarefas**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Proteção da conexão do Servidor de Administração** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

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

4. Em **Proteção da conexão do Servidor de Administração**, selecione **Não proteger com uma senha**.

5. Salvar alterações.

6. Marque a caixa de seleção ao lado da tarefa.

7. Clique **Iniciar**.

   Você pode monitorar o status da tarefa e o número de dispositivos nos quais a tarefa foi concluída com êxito ou concluída com um erro.

Como desativar a proteção de conexão do servidor na linha de comando

1. Execute o interpretador da linha de comando (cmd.exe) como um administrador.

2. Vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

3. Execute o seguinte comando:

   ```
   avp.com SERVERBINDINGDISABLE [/password=<password>]
   ```

   onde `<password>` é a senha da Conta de usuário KLAdmin ou a senha da tarefa *Proteção da conexão do Servidor de Administração*. Se o parâmetro não for especificado, o Kaspersky Endpoint Security solicitará que você insira uma senha na próxima linha.

   > Para executar este comando a Proteção por senha deve estar ativada.

Exemplo

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

Criptografia de Dados

O Kaspersky Endpoint Security permite a criptografia de arquivos e pastas armazenados em unidades locais e removíveis ou em unidades removíveis e discos rígidos inteiros. A criptografia de dados minimiza o risco de vazamento de informação que pode resultar quando um computador portátil, uma unidade removível ou um disco rígido é perdido ou roubado ou quando os dados são acessados por usuários ou aplicativos não autorizados. O Kaspersky Endpoint Security usa o algoritmo de criptografia Advanced Encryption Standard (AES).

Se a licença expirou, o aplicativo não criptografa novos dados, os dados criptografados antigos permanecem criptografados e disponíveis para uso. Neste caso, a criptografia de novos dados exige que o aplicativo seja ativado com uma nova licença que permite o uso da criptografia.

Se o Kaspersky Endpoint Security estiver instalado em um computador baseado em Arm, somente a Criptografia de unidade de disco BitLocker estará disponível. O aplicativo não é compatível com outros componentes de criptografia de dados.

Se a sua licença tiver expirado ou o Contrato de Licença do Usuário Final tiver sido violado, a chave de licença, o Kaspersky Endpoint Security ou os componentes de criptografia tiverem sido removidos, o status de criptografado dos arquivos criptografados anteriormente não é garantido. Isso porque alguns aplicativos, como o Microsoft Office Word, criam cópias temporárias de arquivos durante a edição. Quando o arquivo original é salvo, a cópia temporária substitui o arquivo original. Por conseguinte, em um computador que não tem funcionalidade de criptografia ou essa funcionalidade fica inacessível, o arquivo permanece não criptografado.

O Kaspersky Endpoint Security oferece os seguintes aspectos de proteção de dados:

- **Criptografia a Nível de Arquivo em unidades locais de computador**. Você pode compilar listas de arquivos por extensão ou por grupos de extensões e listas de pastas armazenadas em unidades do computador local, bem como criar regras para criptografar arquivos criados por aplicativos específicos. Depois que uma política é aplicada, o Kaspersky Endpoint Security criptografa e descriptografa os seguintes arquivos:
  - adicionados individualmente a listas para criptografia e descriptografia;
  - arquivos armazenados em pastas adicionadas a listas para criptografia e descriptografia;
  - arquivos criados por aplicativos separados.
- **Criptografia de unidades removíveis**. Você pode especificar uma regra de criptografia padrão a ser utilizada pelo aplicativo igualmente em todas as unidades removíveis, ou especificar as regras de criptografia para unidades removíveis específicas.

  A regra de criptografia padrão tem uma prioridade mais baixa do que as regras de criptografia criadas para unidades removíveis individuais. Regras de criptografia criadas para unidades removíveis do modelo de dispositivo especificado têm uma prioridade mais baixa do que as regras de criptografia criadas para unidades removíveis com a ID do dispositivo especificada.

Para selecionar a regra de criptografia para arquivos em uma unidade removível, o Kaspersky Endpoint Security verifica se o modelo do dispositivo e a ID são conhecidos. O aplicativo então executa uma das seguintes operações:

- Se apenas o modelo do dispositivo for conhecido, o aplicativo usa a regra de criptografia (se houver) criada para unidades removíveis com um modelo de dispositivo específico.
- Se a ID do dispositivo for conhecida, o aplicativo usa a regra de criptografia (se houver) criada para unidades removíveis com uma ID do dispositivo específica.
- Se o modelo e a ID do dispositivo forem conhecidos, o aplicativo usa a regra de criptografia (se houver) criada para unidades removíveis com uma ID do dispositivo específica. Se nenhuma regra existir, mas houver uma regra de criptografia criada para unidades removíveis com o modelo de dispositivo específico, o aplicativo aplica essa regra. Se nenhuma regra de criptografia for especificada para a ID do dispositivo específica nem para o modelo de dispositivo específico, o aplicativo aplica a regra de criptografia padrão.
- Se nem o modelo nem o ID do dispositivo forem conhecidos, o aplicativo usa a regra de criptografia padrão.

O aplicativo permite que você prepare uma unidade removível para utilizar dados armazenados no modo portátil. Depois de ativar o modo portátil, você pode acessar os arquivos criptografados em unidades removíveis conectadas a um computador sem a funcionalidade de criptografia.

- **Gerenciar regras de acesso do aplicativo a arquivos criptografados**. Para qualquer aplicativo, você pode criar uma regra de acesso ao arquivo criptografado que bloqueia o acesso a arquivos criptografados ou permite o acesso a arquivos criptografados somente como ciphertext, que é uma sequência de caracteres obtida quando a criptografia é aplicada.
- **Criar pacotes criptografados**. Você pode criar arquivos compactados criptografados e proteger o acesso a esses arquivos com uma senha. O conteúdo dos arquivos compactados criptografados pode ser acessado apenas com a introdução da senha com a qual você protegeu o acesso a esses arquivos. Tais arquivos compactados podem ser transmitidos com segurança pela rede ou em unidades removíveis.
- **Criptografia Completa do Disco**. Você pode selecionar uma tecnologia de criptografia: O Kaspersky Disk Encryption ou criptografia de unidade de disco da BitLocker (aqui também mencionada simplesmente como "BitLocker").

  O BitLocker é uma tecnologia integrante do sistema operacional Windows. Se um computador for equipado com Trusted Platform Module (TPM), o BitLocker utiliza esse recurso para guardar chaves de recuperação que fornecem o acesso a um disco rígido criptografado. Quando o computador é iniciado, o BitLocker solicita as chaves de recuperação de disco rígido do Trusted Platform Module e desbloqueia a unidade. Você pode configurar o uso de uma senha e/ou código PIN para acessar chaves de recuperação.

  Você pode especificar a regra de criptografia completa do disco padrão e criar uma lista de discos rígidos a serem excluídos da criptografia. O Kaspersky Endpoint Security executa a criptografia completa do disco por setor, depois que a política Kaspersky Security Center é aplicada. O aplicativo criptografa todas as partições lógicas dos discos rígidos simultaneamente.

  Após a criptografia dos discos rígidos do sistema, na próxima inicialização do sistema o usuário deve concluir a autenticação usando o Agente de autenticação antes que os discos rígidos possam ser acessados e o sistema operacional seja carregado. Isso requer inserir a senha do token ou cartão inteligente conectado ao computador ou o nome de usuário e a senha da conta do Agente de autenticação criada pelo administrador da rede local usando a tarefa de *Gerenciar contas do Agente de Autenticação*. Estas contas são baseadas nas contas do Microsoft Windows com a qual os usuários fazem login no sistema operacional. Também é possível usar a tecnologia Single Sign-On (SSO) que permite efetuar login automaticamente no sistema operacional com o uso do nome de usuário e da senha da conta do Agente de Autenticação.

Se você fizer o backup do computador, a seguir criptografar os dados do computador e após isso restaurar a cópia de backup do computador e então criptografar os dados do computador novamente, o Kaspersky Endpoint Security cria duplicatas das contas do Agente de Autenticação. Para remover as contas duplicadas, utilize o utilitário klmover com a chave `- dupfix`. O utilitário klmover está incluído na compilação do Kaspersky Security Center. Leia mais sobre a operação na Ajuda do Kaspersky Security Center.

O acesso a discos rígidos criptografados só é possível em computadores nos quais o Kaspersky Endpoint Security está instalado com funcionalidade de criptografia completa do disco. Esta precaução minimiza o risco de vazamento de dados de um disco rígido criptografado quando for feita uma tentativa de acesso fora da rede local da empresa.

Para criptografar discos rígidos e unidades removíveis, você pode usar o modo Criptografar somente espaço usado em disco. Recomenda-se somente usar esta função para novos dispositivos que não foram anteriormente usados. Se você estiver aplicando a criptografia em um dispositivo que já está em uso, recomenda-se criptografar o dispositivo inteiro. Isto assegura que todos os dados estejam protegidos, até os dados excluídos que ainda podem conter informações recuperáveis.

Antes da criptografia começar, o Kaspersky Endpoint Security obtém o mapa de setores de sistema de arquivos. A primeira onda da criptografia inclui setores que são ocupados por arquivos no momento em que a criptografia é iniciada. A segunda onda da criptografia inclui setores que foram gravados depois que a criptografia começou. Depois que a criptografia é concluída, todos os setores que contêm dados estão criptografados.

Depois que a criptografia é concluída e um usuário exclui um arquivo, os setores que guardaram o arquivo apagado ficam disponíveis para guardar novas informações no nível de sistema de arquivos, mas permanecem criptografados. Assim, como os arquivos são gravados em um novo dispositivo e o dispositivo é regularmente criptografado com a função **Criptografar somente espaço usado em disco** ativada, todos os setores serão criptografados depois de algum tempo.

Os dados necessários para a descriptografia de arquivos é fornecido pelo Servidor de Administração do Kaspersky Security Center que controlou o computador no momento da criptografia. Se o computador com objetos criptografados tiver sido gerenciado por um Servidor de Administração diferente por algum motivo, você pode obter acesso aos dados criptografados por meio de uma das seguintes maneiras:

- Servidores de administração na mesma hierarquia:
  - Você não precisa executar nenhuma outra ação. O usuário manterá o acesso aos objetos criptografados. As chaves de criptografia são distribuídas para todos os Servidores de administração.
- Servidores de administração separados:
  - Solicitar acesso à objetos criptografados ao administrador da rede local.
  - Restaure dados em dispositivos criptografados usando o Utilitário de restauração.
  - Restaure a configuração do Servidor de Administração do Kaspersky Security Center que controlou o computador no momento da criptografia a partir de uma cópia de segurança e use essa configuração no Servidor de Administração que agora controla o computador com os objetos criptografados.

Se não houver acesso aos dados criptografados, siga as instruções especiais para trabalhar com dados criptografados (Restaurando o acesso a arquivos criptografados, Trabalhando com dispositivos criptografados quando não houver acesso a eles).

Limitações de funcionalidades da criptografia

A Criptografia de dados tem as seguintes limitações:

- O aplicativo cria arquivos de serviço durante a criptografia. É necessário cerca de 0.5% de espaço livre não fragmentado no disco rígido para armazená-los. Se não houver espaço livre não fragmentado suficiente no disco rígido, a criptografia não será iniciada até que você libere espaço suficiente.

- É possível gerenciar todos os componentes de criptografia de dados no Console de Administração do Kaspersky Security Center e no Kaspersky Security Center Web Console. No Kaspersky Security Center Cloud Console, é possível gerenciar somente o BitLocker.

- A Criptografia de dados está disponível ao usar o Kaspersky Endpoint Security com o sistema de administração do Kaspersky Security Center ou o Kaspersky Security Center Cloud Console (apenas o BitLocker). A Criptografia de dados ao usar o Kaspersky Endpoint Security no modo offline não é possível porque o Kaspersky Endpoint Security armazena chaves de criptografia no Kaspersky Security Center.

- Se o Kaspersky Endpoint Security for instalado em um computador com o Microsoft Windows para servidores, somente a Criptografia completa do disco usando a tecnologia Criptografia de unidade de disco BitLocker estará disponível. Se o Kaspersky Endpoint Security estiver instalado em um computador com o Microsoft Windows para estações de trabalho, a funcionalidade de criptografia de dados está totalmente disponível.

- Caso o Kaspersky Endpoint Security esteja instalado em um computador baseado em Arm, somente a Criptografia completa do disco com uso da tecnologia de Criptografia de Unidade de Disco BitLocker estará disponível e outros componentes de criptografia não serão compatíveis.

A tecnologia de criptografia completa do disco que usa Kaspersky Disk Encryption está indisponível para discos rígidos que não atendem aos requisitos de software e hardware.

A compatibilidade entre a funcionalidade de criptografia completa do disco do Kaspersky Endpoint Security e do Kaspersky Anti-Virus para UEFI não é suportada. O Kaspersky Anti-Virus para UEFI começa antes do carregamento do sistema operacional. Ao usar a criptografia completa do disco, o aplicativo detectará a ausência de um sistema operacional instalado no computador. Consequentemente, a operação do Kaspersky Anti-Virus para UEFI terminará com um erro. A Criptografia a nível de arquivo (FLE) não afeta a operação do Kaspersky Anti-Virus para UEFI.

O Kaspersky Endpoint Security dá suporte às configurações:

- Unidades HDD, SSD e USB.

  A tecnologia Kaspersky Disk Encryption (FDE) oferece suporte ao trabalho com SSD enquanto preserva o desempenho e a vida útil das unidades SSD.

- Unidades conectadas via barramento: SCSI, ATA, IEEE1934, USB, RAID, SAS, SATA, NVME.

- Unidades não removíveis conectadas via barramento SD ou MMC.

- Unidades com setores de 512 bytes.

- Unidades com setores de 4.096 bytes que emulam 512 bytes.

- Unidades com os seguintes tipos de partições: GPT, MBR e VBR (unidades removíveis).
- Software integrado do padrão BIOS Legacy e UEFI 64.
- Software integrado do padrão UEFI com suporte para Secure Boot.

  Secure Boot é uma tecnologia projetada para verificar assinaturas digitais para aplicativos e drivers do carregador UEFI. A inicialização segura bloqueia a inicialização de aplicativos e drivers UEFI não assinados ou assinados por editores desconhecidos. O Kaspersky Disk Encryption (FDE) oferece suporte total à Inicialização Segura. O Agente de Autenticação é assinado por um certificado Microsoft Windows UEFI Driver Publisher.

  Em alguns dispositivos (por exemplo, Microsoft Surface Pro e Microsoft Surface Pro 2), uma lista desatualizada de certificados de verificação de assinatura digital pode ser instalada por padrão. Antes de criptografar a unidade, você precisa atualizar a lista de certificados.
- Software integrado do padrão UEFI com suporte para Fast Boot.

  Fast Boot é uma tecnologia que ajuda o computador a inicializar mais rapidamente. Quando a tecnologia Fast Boot está ativada, normalmente o computador carrega apenas o conjunto mínimo de drivers UEFI necessários para iniciar o sistema operacional. Quando a tecnologia Fast Boot está habilitada, teclados USB, mouses, tokens USB, touchpads e telas sensíveis ao toque podem não funcionar enquanto o Agente de Autenticação estiver em execução.

  > Para usar o Kaspersky Disk Encryption (FDE), é recomendável desativar a tecnologia Fast Boot. Você pode usar o Utilitário de teste FDE para testar a operação do Kaspersky Disk Encryption (FDE).

O Kaspersky Endpoint Security não suporta as seguintes configurações:

- O carregador de inicialização é localizado em uma unidade enquanto o sistema operacional está em uma unidade diferente.
- O sistema contém o software integrado do padrão de UEFI 32.
- O sistema possui Intel® Rapid Start Technology e unidades que possuem uma partição de hibernação mesmo quando o Intel® Rapid Start Technology está desativado.
- Unidades em formato de MBR com mais de 10 partições estendidas.
- O sistema possui um arquivo de troca localizado em uma unidade que não é do sistema.
- Sistema de inicialização múltipla com vários sistemas operacionais simultaneamente instalados.
- As partições dinâmicas (somente partições primárias são suportadas).
- Unidades com espaço livre disponível não fragmentado de menos de 0.5%.
- Unidades com um tamanho de setor diferente de 512 bytes ou 4096 bytes que emulam 512 bytes.
- Unidades híbridas.
- O sistema possui carregadores de terceiros.
- Unidades com diretórios NTFS compactados.
- A tecnologia Kaspersky Disk Encryption (FDE) é incompatível com outras tecnologias de criptografia de disco completo (como BitLocker, McAfee Drive Encryption e WinMagic SecureDoc).

- A tecnologia Kaspersky Disk Encryption (FDE) é incompatível com a tecnologia ExpressCache.
- Não há suporte para a criação, exclusão e modificação de partições em uma unidade criptografada. Você pode perder dados.
- Não há suporte para a formatação do sistema de arquivos. Você pode perder dados.

  Se você precisar formatar uma unidade que foi criptografada com a tecnologia Kaspersky Disk Encryption (FDE), formate a unidade em um computador que não tenha o Kaspersky Endpoint Security for Windows e use apenas a criptografia de disco completo.

  Uma unidade criptografada formatada com a opção de formatação rápida pode ser identificada erroneamente como criptografada na próxima vez que for conectada a um computador com o Kaspersky Endpoint Security for Windows instalado. Os dados do usuário ficarão indisponíveis.
- O Agente de Autenticação não oferece suporte a mais de 100 contas.
- A tecnologia de Login único é incompatível com outras tecnologias de desenvolvedores de terceiros.
- A tecnologia Kaspersky Disk Encryption (FDE) não é compatível com os seguintes modelos de dispositivos:
  - Dell Latitude E6410 (modo UEFI)
  - HP Compaq nc8430 (modo BIOS legado)
  - Lenovo ThinkCentre 8811 (modo Legacy BIOS)
- O Agente de Autenticação não oferece suporte ao trabalho com tokens USB quando Legacy USB Support está ativado. Será possível somente a autenticação baseada em senha no computador.
- Ao criptografar uma unidade no modo BIOS legado, é recomendável habilitar Legacy USB Support nos seguintes modelos de dispositivos:
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T
  - Dell Inspiron 1420
  - Dell Inspiron 1545
  - Dell Inspiron 1750
  - Dell Inspiron N4110
  - Dell Latitude E4300
  - Dell Studio 1537
  - Dell Studio 1569
  - Dell Vostro 1310
  - Dell Vostro 1320

- Dell Vostro 1510
- Dell Vostro 1720
- Dell Vostro V13
- Dell XPS L502x
- Fujitsu Celsius W370
- Fujitsu LifeBook A555
- PC HP Compaq dx2450 Microtower
- Lenovo G550
- Lenovo ThinkPad L530
- Lenovo ThinkPad T510
- Lenovo ThinkPad W540
- Lenovo ThinkPad X121e
- Lenovo ThinkPad X200s (74665YG)
- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 10O
- MSI 760GM-E51 (placa-mãe)

Alteração do comprimento da chave de criptografia (AES56/AES256)

O Kaspersky Endpoint Security usa o algoritmo de criptografia AES (Advanced Encryption Standard). O Kaspersky Endpoint Security suporta o algoritmo de criptografia AES com um comprimento de chave efetivo de 256 ou 56 bits. O algoritmo de criptografia de dados depende da biblioteca de criptografia AES incluída no pacote de distribuição: *Criptografia forte (AES256)* ou *Criptografia Leve (AES56)*. A biblioteca de criptografia AES é instalada junto com o aplicativo.

A alteração do comprimento da chave de criptografia está disponível apenas para o Kaspersky Endpoint Security 11.2.0 ou posterior.

A alteração do comprimento da chave de criptografia consiste das seguintes etapas:

1. Descriptografe os objetos que o Kaspersky Endpoint Security criptografou antes de começar a modificar o comprimento da chave de criptografia:

   a. Descriptografe discos rígidos.

   b. Descriptografe arquivos em unidades locais.

   c. Descriptografe unidades removíveis.

   Depois que o comprimento da chave de criptografia é modificado, os objetos que foram anteriormente criptografados tornam-se indisponíveis.

2. Remova o Kaspersky Endpoint Security.

3. Instale o Kaspersky Endpoint Security a partir do pacote de distribuição do Kaspersky Endpoint Security que contém uma biblioteca de criptografia diferente.

Você também pode alterar o comprimento da chave de criptografia atualizando o aplicativo. O comprimento da chave pode ser alterado por meio da atualização do aplicativo apenas se as seguintes condições forem atendidas:

- O Kaspersky Endpoint Security version 10 Service Pack 2 ou mais recente está instalado no computador.

- Os componentes de criptografia de dados (criptografia a nível de arquivo, Criptografia completa do disco) não estão instalados no computador.

  Por padrão, os componentes de criptografia de dados não estão incluídos no Kaspersky Endpoint Security. O componente BitLocker Management não afeta a alteração no comprimento da chave de criptografia.

Para alterar o comprimento da chave de criptografia, execute o arquivo kes_win.msi ou o setup_kes.exe do pacote de distribuição que contém a biblioteca de criptografia necessária. Você também pode fazer o upgrade remotamente do aplicativo usando o pacote de instalação.

É impossível alterar o comprimento da chave de criptografia usando o pacote de distribuição da mesma versão do aplicativo que está instalado no seu computador sem primeiro desinstalar o aplicativo.

Kaspersky Disk Encryption

O Kaspersky Disk Encryption não é compatível com computadores baseados em Arm.

O Kaspersky Disk Encryption está disponível apenas para computadores que executam um sistema operacional Windows para estações de trabalho. Para computadores que executem um sistema operacional Windows para servidores, use a tecnologia Criptografia de unidade de disco da BitLocker.

O Kaspersky Endpoint Security tem suporte para criptografia completa do disco nos sistemas de arquivos FAT32, NTFS e exFat.

Antes de iniciar a criptografia completa do disco, o aplicativo executa várias verificações para determinar se o dispositivo pode ser criptografado, incluindo a verificação do disco rígido do sistema quanto à compatibilidade com o Agente de Autenticação e com os componentes de criptografia do BitLocker. Para verificar a compatibilidade, o computador deve ser reiniciado. Após o reinício do computador, o aplicativo executa todas as verificações necessárias automaticamente. Se a verificação de compatibilidade for bem sucedida, a criptografia completa do disco começará depois que o sistema operacional for carregado e o aplicativo iniciado. Se o disco rígido do sistema for considerado como incompatível com o Agente de Autenticação ou com os componentes de criptografia do BitLocker, é necessário reinicializar o computador, pressionando o botão de reinício do hardware. O Kaspersky Endpoint Security registra informações sobre a incompatibilidade. Com base nessas informações, o aplicativo não inicia a criptografia completa do disco ao inicializar o sistema operacional. As informações sobre este evento são registradas em relatórios do Kaspersky Security Center.

Se a configuração de hardware do computador tiver sido alterada, as informações de incompatibilidade registradas pelo aplicativo durante a verificação anterior devem ser excluídas para verificar a compatibilidade do disco rígido do sistema com o Agente de Autenticação e com os componentes de criptografia do BitLocker. Para isso, antes da criptografia completa do disco, digite `avp pbatestreset` na linha de comando. Se o sistema operacional não conseguir carregar depois que o disco rígido do sistema tiver sido verificado quanto a compatibilidade com o Agente de Autenticação, você deve remover os objetos e resto de dados depois da operação de teste do Agente de Autenticação usando o Utilitário de restauração e, em seguida, deve iniciar o Kaspersky Endpoint Security e executar o comando `avp pbatestreset` novamente.

Depois que a criptografia completa do disco tiver começado, o Kaspersky Endpoint Security criptografará todos os dados gravados em discos rígidos.

Se o usuário desliga ou reinicia o computador durante uma tarefa de criptografia completa do disco, o Agente de Autenticação é carregado antes da próxima reinicialização do sistema operacional. O Kaspersky Endpoint Security continua a criptografia completa do disco depois da autenticação com êxito no Agente de Autenticação e da inicialização do sistema operacional.

Se o sistema operacional alternar para o modo de hibernação durante a criptografia completa do disco, o Agente de Autenticação será carregado quando o sistema operacional voltar do modo de hibernação. O Kaspersky Endpoint Security continua a criptografia completa do disco depois da autenticação com êxito no Agente de Autenticação e da inicialização do sistema operacional.

Se o sistema operacional entrar no modo de suspensão durante a criptografia completa do disco, o Kaspersky Endpoint Security retomará essa criptografia quando o sistema operacional sair do modo de suspensão sem carregar o Agente de Autenticação.

A autenticação do usuário no Agente de autenticação pode ser realizada de duas formas:

- Insira o nome e a senha da conta do Agente de Autenticação criada pelo administrador de rede local usando as ferramentas do Kaspersky Security Center.
- Insira a senha de um token ou cartão inteligente conectado ao computador.

  O uso de um token ou cartão inteligente estará disponível somente se os discos rígidos do computador tiverem sido criptografados usando o algoritmo de criptografia AES256. Se os discos rígidos do computador foram criptografados usando o algoritmo de criptografia AES56, a adição do arquivo de certificado eletrônico ao comando será negada.

O Agente de autenticação suporta layouts de teclado para os seguintes idiomas:

- Inglês (Reino Unido)
- Inglês (Estados Unidos)

- Árabe (Argélia, Marrocos, Tunísia; layout AZERTY)
- Espanhol (América Latina)
- Italiano
- Alemão (Alemanha e Áustria)
- Alemão (Suíça)
- Português (Brasil, layout ABNT2)
- Russo (para teclados IBM/Windows de 105 teclas com o layout QWERTY)
- Turco (layout QWERTY)
- Francês (França)
- Francês (Suíça)
- Francês (Bélgica, layout AZERTY)
- Japonês (para teclados de 106 teclas com o layout QWERTY)

Um layout de teclado fica disponível no Agente de Autenticação se esse layout tiver sido adicionado às configurações regionais e de idioma do sistema operacional e se tiver ficado disponível na tela de boas-vindas do Microsoft Windows.

Se o nome da conta do Agente de Autenticação contiver símbolos que não possam ser inseridos usando os layouts do teclado disponíveis no Agente de Autenticação, os discos rígidos criptografados poderão ser acessados apenas depois de serem restaurados usando o Utilitário de restauração ou depois de o nome da conta e a senha serem restaurados.

Recursos especiais de criptografia de unidade SSD

O aplicativo oferece suporte à criptografia de unidades SSD, unidades SSHD híbridas e unidades com o recurso Intel Smart Response. O aplicativo não oferece suporte à criptografia de unidades com o recurso Intel Rapid Start. Desative o recurso Intel Rapid Start antes de criptografar a unidade.

A criptografia de unidades SSD possui os seguintes recursos especiais:

- Se uma unidade SSD for nova e não contiver dados confidenciais, ative a criptografia apenas do espaço ocupado. Isso permite sobrescrever os setores relevantes da unidade.
- Se uma unidade SSD estiver em uso e tiver dados confidenciais, selecione uma das seguintes opções:
  - Limpar totalmente a unidade SSD (Secure Erase), instalar o sistema operacional e executar a criptografia da unidade SSD com a opção de criptografar apenas o espaço ocupado ativado.
  - Executar a criptografia da unidade SSD com a opção de criptografar apenas o espaço ocupado desativado.

A criptografia de uma unidade SSD requer 5 a 10 GB de espaço livre. Os requisitos de espaço livre para armazenar dados de administração de criptografia são fornecidos na tabela abaixo.

Requisitos de espaço livre para armazenamento de dados de administração de criptografia

Tamanho da unidade SSD (GB)	Espaço livre na partição primária da unidade SSD (MB)	Espaço livre na partição secundária da unidade SSD (MB)
128	250	64
256	250	640
512	300	128

Iniciar o Kaspersky Disk Encryption

Antes de iniciar a criptografia completa do disco, certifique-se de que o computador não esteja infectado. Para fazer assim, inicie a tarefa de Verificação Completa ou Verificação de Áreas Críticas. Realizar uma criptografia completa do disco em um computador infectado por um rootkit pode fazer com que o computador fique inoperável.

Antes de iniciar a criptografia de disco, é necessário verificar as configurações das contas do Agente de Autenticação. O Agente de Autenticação é necessário para trabalhar com unidades protegidas usando a tecnologia Kaspersky Disk Encryption (FDE). Antes que o sistema operacional seja carregado, o usuário precisa concluir a autenticação com o Agente. O Kaspersky Endpoint Security permite que você crie contas do Agente de Autenticação automaticamente, antes de criptografar uma unidade. É possível ativar a criação automática de contas do Agente de Autenticação nas configurações da política de Criptografia Completa do Disco (consulte as instruções abaixo). Você também pode Usar a tecnologia de Login único (SSO).

O Kaspersky Endpoint Security permite criar automaticamente o Agente de Autenticação para os seguintes grupos de usuários:

- **Todas as contas no computador**. Todas as contas no computador que estiveram ativas em algum momento.
- **Todas as contas de domínio no computador**. Todas as contas no computador que pertencem a algum domínio e que estiveram ativas em algum momento.
- **Todas as contas locais no computador**. Todas as contas locais no computador que estiveram ativas a qualquer momento.
- **Conta de serviço com uma senha única**. A conta de serviço é necessária para obter acesso ao computador, por exemplo, quando o usuário esquece a senha. Também é possível usar a conta de serviço como conta reserva. É necessário inserir o nome da conta (por padrão, `ServiceAccount`). O Kaspersky Endpoint Security cria uma senha automaticamente. É possível encontrar a senha no console do Kaspersky Security Center.
- **Administrador local**. O Kaspersky Endpoint Security cria uma conta de usuário do Agente de Autenticação para o administrador local do computador.
- **Gerente do computador**. O Kaspersky Endpoint Security cria uma conta de usuário do Agente de Autenticação para a conta do gerente do computador. É possível ver qual conta tem a função de gerente de computador nas propriedades do computador no Active Directory. Por padrão, a função de gerente do computador não está definida, ou seja, não corresponde a nenhuma conta.
- **Conta ativa**. O Kaspersky Endpoint Security cria automaticamente uma conta do Agente de Autenticação para a conta que está ativa no momento da criptografia do disco.

A tarefa *Gerenciar contas do Agente de Autenticação* foi projetada para definir as configurações de autenticação do usuário. É possível usar essa tarefa para adicionar novas contas, modificar as configurações de contas atuais ou remover contas, se necessário. Você pode usar tarefas locais para computadores individuais, bem como tarefas de grupo para computadores de grupos de administração separados ou uma seleção de computadores.

Como executar o Kaspersky Disk Encryption pelo Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Criptografia de dados** → **Criptografia completa do disco**.
4. Na lista suspensa **Tecnologia de criptografia**, selecione **Kaspersky Disk Encryption**.

   A tecnologia de Kaspersky Disk Encryption não pode ser usada se o computador tiver discos rígidos que foram criptografados por BitLocker.

5. Na lista suspensa **Modo de criptografia**, selecione **Criptografar todos os discos rígidos**.

   Se o computador tiver vários sistemas operacionais instalados, depois da criptografia de todos os discos rígidos, você poderá carregar apenas o sistema operacional que tenha o aplicativo instalado.

   Se você tiver de excluir alguns discos rígidos da criptografia, crie uma lista de tais discos rígidos.

6. Configure as opções avançadas do Kaspersky Disk Encryption (consulte a tabela abaixo).
7. Salvar alterações.

Como executar o Kaspersky Disk Encryption pelo Web Console e pelo Cloud Console

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

   A janela de propriedades da política é exibida.

3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Criptografia de dados** → **Criptografia completa do disco**.
5. Selecione a tecnologia **Kaspersky Disk Encryption**.

   A tecnologia de Kaspersky Disk Encryption não pode ser usada se o computador tiver discos rígidos que foram criptografados por BitLocker.

6. No bloco **Ação sobre os dispositivos**, selecione **Criptografar todos os discos rígidos**.

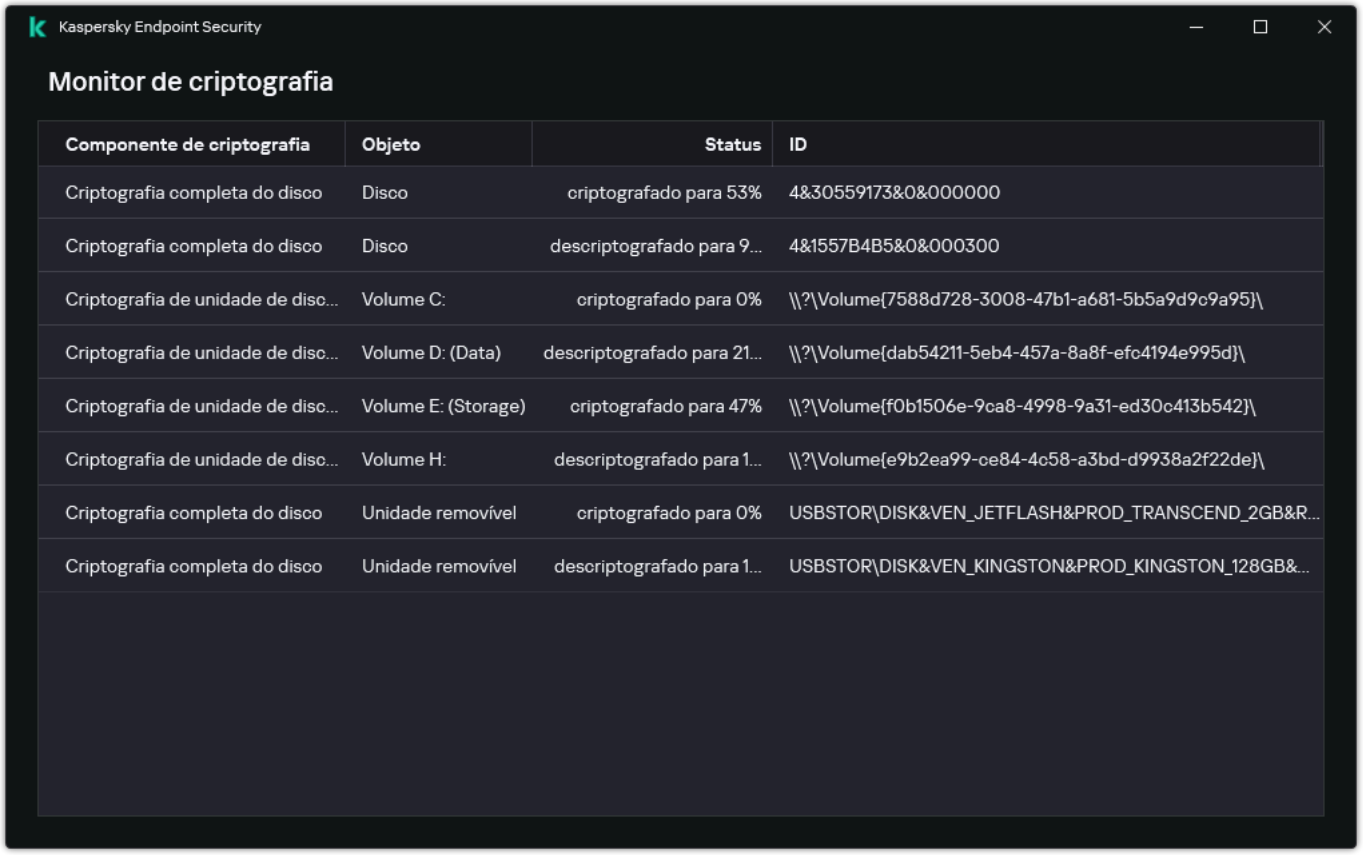
Se o computador tiver vários sistemas operacionais instalados, depois da criptografia você só poderá carregar o sistema em que a criptografia foi realizada.

Se você tiver de excluir alguns discos rígidos da criptografia, crie uma lista de tais discos rígidos.

7. Configure as opções avançadas do Kaspersky Disk Encryption (consulte a tabela abaixo).

8. Salvar alterações.

É possível usar a ferramenta Monitor de criptografia para controlar o processo de criptografia ou descriptografia de disco no computador de um usuário. É possível executar a ferramenta Monitor de criptografia a partir da janela principal do aplicativo.



Componente de criptografia	Objeto	Status	ID
Criptografia completa do disco	Disco	criptografado para 53%	4&30559173&0&000000
Criptografia completa do disco	Disco	descriptografado para 9...	4&1557B4B5&0&000300
Criptografia de unidade de disc...	Volume C:	criptografado para 0%	\\?\Volume{7588d728-3008-47b1-a681-5b5a9d9c9a95}\
Criptografia de unidade de disc...	Volume D: (Data)	descriptografado para 21...	\\?\Volume{dab54211-5eb4-457a-8a8f-efc4194e995d}\
Criptografia de unidade de disc...	Volume E: (Storage)	criptografado para 47%	\\?\Volume{f0b1506e-9ca8-4998-9a31-ed30c413b542}\
Criptografia de unidade de disc...	Volume H:	descriptografado para 1...	\\?\Volume{e9b2ea99-ce84-4c58-a3bd-d9938a2f22de}\
Criptografia completa do disco	Unidade removível	criptografado para 0%	USBSTOR\DISK&VEN_JETFLASH&PROD_TRANSCEND_2GB&R...
Criptografia completa do disco	Unidade removível	descriptografado para 1...	USBSTOR\DISK&VEN_KINGSTON&PROD_KINGSTON_128GB&...

Monitor de criptografia

Se os discos rígidos do sistema forem criptografados, o Agente de Autenticação é carregado antes da inicialização do sistema operacional. Use o Agente de Autenticação para concluir a autenticação a fim de obter acesso aos discos rígidos do sistema criptografado e carregar o sistema operacional. Depois de conclusão bem sucedida do procedimento de autenticação, o sistema operacional é carregado. O processo de autenticação é repetido toda vez que o sistema operacional for reiniciado.

Parâmetro	Descrição
Criar automaticamente contas do Agente de Autenticação para usuários durante a criptografia	Se a caixa de seleção estiver marcada, o aplicativo cria contas do Agente de Autenticação com base na lista de contas de usuários do Windows no computador. Por padrão, o Kaspersky Endpoint Security usa todas as contas locais e de domínio com as quais o usuário efetuou login no sistema operacional nos últimos 30 dias.
Criar automaticamente contas do Agente de Autenticação para todos os usuários do computador ao fazer login	Se a caixa de seleção estiver marcada, o aplicativo verificará as informações sobre as contas de usuários do Windows no computador antes de iniciar o agente de autenticação. Se o Kaspersky Endpoint Security detectar uma conta de usuário do Windows que não tenha uma conta do Agente de Autenticação, o aplicativo criará uma nova conta para acessar unidades criptografadas. A nova conta do Agente de Autenticação terá as seguintes configurações padrão: proteção por senha somente no início da sessão e mudança de senha na primeira autenticação. Portanto, não é necessário adicionar manualmente as contas do Agente de Autenticação usando a tarefa *Gerenciar contas do Agente de Autenticação* para computadores com unidades já criptografadas.
Salvar nome de usuário inserido no Agente de Autenticação	Se a caixa de seleção for marcada, o aplicativo salvará o nome da conta do Agente de autenticação. Não será necessário inserir o nome da conta na próxima vez que você tentar concluir a autorização no Agente de Autenticação na mesma conta.
Criptografar somente espaço usado em disco (reduz o tempo de criptografia)	Esta caixa ativa / desativa a opção que limita a área de criptografia a setores de disco rígido só ocupados. Este limite permite reduzir o tempo de criptografia. Ativar ou desativar o recurso **Criptografar somente espaço usado em disco (reduz o tempo de criptografia)** após o início da criptografia não modifica essa configuração até que os discos rígidos sejam descriptografados. Você deve marcar ou desmarcar a caixa de seleção antes da criptografia inicial. Se a caixa de seleção estiver selecionada, somente as porções da unidade de disco rígido que são ocupadas por arquivos serão criptografadas. O Kaspersky Endpoint Security criptografa automaticamente novos dados à medida que são adicionados. Se a caixa de seleção estiver desmarcada, a unidade de disco rígido inteira será criptografada, inclusive fragmentos residuais de arquivos anteriormente excluídos e modificados. Esta opção é recomendada para novas unidades de disco rígido cujos dados não foram modificados ou excluídos. Se você estiver aplicando a criptografia em um disco rígido que já está no uso, recomenda-se criptografar o disco rígido inteiro. Isso garante a proteção de todos os dados; até mesmo de dados excluídos que podem ser recuperados. Por padrão, a caixa de seleção está desmarcada.
Ativar Legacy USB Support (não recomendado)	Essa caixa de seleção ativa ou desativa a funcionalidade Legacy USB Support. *Legacy USB Support* **é** uma função do BIOS/UEFI que permite usar dispositivos USB (como um token de segurança) durante a fase de inicialização do computador antes de iniciar o sistema operacional (modo BIOS). O Legacy USB Support não afetará o suporte a dispositivos USB depois que o sistema operacional for iniciado. Se a caixa de seleção for marcada, o suporte a dispositivos USB será ativado durante a inicialização do computador. Quando a função Legacy USB Support está ativada, o Agente de Autenticação no modo BIOS não será compatível com o funcionamento de tokens via USB. Recomenda-se usar esta opção somente quando houver um problema de compatibilidade de hardware e somente para os computadores nos quais o problema ocorreu.

Criar uma lista de discos rígidos excluídos da criptografia

Você pode criar uma lista de exclusões da criptografia apenas da tecnologia do Kaspersky Disk Encryption.

Para formar uma lista de discos rígidos excluídos da criptografia:

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Criptografia de dados** → **Criptografia completa do disco**.
4. Na lista suspensa **Tecnologia de criptografia**, selecione **Kaspersky Disk Encryption**.

   Entradas correspondentes a discos rígidos excluídos da criptografia aparecem na tabela **Não criptografar os seguintes discos rígidos**. Esta tabela está vazia caso você não tenha formado anteriormente uma lista de discos rígidos a serem excluídos da criptografia.
5. Para adicionar discos rígidos à lista de discos rígidos excluídos da criptografia:

   a. Clique **Adicionar**.

   b. Na janela que é aberta, especifique os valores para **Nome do dispositivo**, **Computador**, **Tipo de disco**, **Kaspersky Disk Encryption**.

   c. Clique **Atualizar**.

   d. Na coluna **Nome**, marque as caixas de seleção nas linhas da tabela que correspondem aos discos rígidos que você deseja adicionar à lista de discos rígidos excluídos da criptografia.

   e. Clique **OK**.

   Os discos rígidos selecionados aparecem na tabela **Não criptografar os seguintes discos rígidos**.
6. Salvar alterações.

Exportar e importar uma lista de discos rígidos excluídos da criptografia

Você pode exportar a lista de exclusões de criptografia do disco rígido para um arquivo XML. Em seguida, você pode modificar o arquivo para, por exemplo, adicionar um grande número de exclusões do mesmo tipo. Você também pode usar a função de exportação/importação para fazer backup da lista de exclusões ou para migrar as exclusões para um servidor diferente.

Como exportar e importar uma lista de exclusões de criptografia de disco rígido no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Criptografia de dados** → **Criptografia completa do disco**.
4. Na lista suspensa **Tecnologia de criptografia**, selecione **Kaspersky Disk Encryption**.

   Entradas correspondentes a discos rígidos excluídos da criptografia aparecem na tabela **Não criptografar os seguintes discos rígidos**.

5. Para exportar a lista de exclusões:

   a. Selecione as exclusões que deseja exportar. Para selecionar várias portas, use as teclas **CTRL** ou **SHIFT**.

      Se você não selecionou nenhuma exclusão, o Kaspersky Endpoint Security exportará todas as exclusões.

   b. Clique no botão → **Exportar**.

   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 Endpoint Security exporta toda a lista de exclusões para o arquivo XML.

6. Para importar a lista de regras:

   a. Clique no botão → **Importar**.

   b. Na janela exibida, selecione o arquivo XML do qual deseja importar a lista de exclusões.

   c. Abra o arquivo.

      Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint 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 exclusões de criptografia de disco rígido no Web Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Criptografia de dados** → **Criptografia completa do disco**.

   Selecione a tecnologia **Kaspersky Disk Encryption**.

5. Clique no link **Exclusões**.

   A lista de exclusões é aberta.

6. Para exportar a lista de regras:

   a. Selecione as exclusões que deseja exportar.

   b. Clique no botão → **Exportar**.

      O Kaspersky Endpoint Security exporta a lista de exclusões para um arquivo JSON na pasta de downloads padrão.

7. Para importar a lista de exclusões:

   a. Clique no botão → **Importar**.

      Na janela exibida, selecione o arquivo JSON do qual deseja importar a lista de exclusões.

b. Abra o arquivo.

Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo JSON.

8. Salvar alterações.

Ativar a tecnologia de login único (SSO)

A tecnologia Single Sign-On (SSO) permite efetuar o login automaticamente no sistema operacional com o uso das credenciais do Agente de Autenticação. Isso significa que um usuário precisa inserir uma senha apenas uma vez ao entrar no Windows (senha da conta do Agente de Autenticação). A tecnologia Single Sign-On também permite atualizar automaticamente a senha da conta do Agente de Autenticação quando a senha da conta do Windows é alterada.

Ao usar a tecnologia de Login único, o Agente de Autenticação ignora os requisitos de segurança de senha especificados no Kaspersky Security Center. Você pode definir os requisitos de força da senha nas configurações do sistema operacional.

Ativar a tecnologia de login único

Como habilitar o uso da tecnologia Login único no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Criptografia de dados** → **Configurações comuns de criptografia**.
4. No bloco **Configurações da senha**, clique no botão **Configurações**.
5. Na janela que é aberta, na guia **Agente de Autenticação**, selecione a caixa de seleção **Usar a tecnologia de autenticação única (SSO)**.
6. Caso esteja usando um provedor de credenciais de terceiros, marque a caixa de seleção **Encapsular provedores de credenciais de terceiros**.
7. Salvar alterações.

Como resultado, o usuário precisa concluir o procedimento de autenticação apenas uma vez com o Agente. O procedimento de autenticação não é necessário para carregar o sistema operacional. O sistema operacional é carregado automaticamente.

Como habilitar o uso do Login único no Web Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.

4. Selecione **Criptografia de dados** → **Criptografia completa do disco**.

5. Selecione a tecnologia **Kaspersky Disk Encryption**.

6. No bloco **Configurações da senha**, marque a caixa de seleção **Usar a tecnologia de autenticação única (SSO)**.

7. Caso esteja usando um provedor de credenciais de terceiros, marque a caixa de seleção **Encapsular provedores de credenciais de terceiros**.

8. Salvar alterações.

Como resultado, o usuário precisa concluir o procedimento de autenticação apenas uma vez com o Agente. O procedimento de autenticação não é necessário para carregar o sistema operacional. O sistema operacional é carregado automaticamente.

Para que o Login único funcione, a senha da conta do Windows e a senha da conta do Agente de Autenticação devem corresponder. Se as senhas não corresponderem, o usuário precisará executar o procedimento de autenticação duas vezes: na interface do Agente de Autenticação e antes de carregar o sistema operacional. Essas ações precisam ser executadas apenas uma vez para sincronizar as senhas. Depois disso, o Kaspersky Endpoint Security substituirá a senha da conta do Agente de Autenticação pela senha da conta do Windows. Quando a senha da conta do Windows for alterada, o aplicativo atualizará automaticamente a senha da conta do Agente de Autenticação.

Provedores de credenciais de terceiros

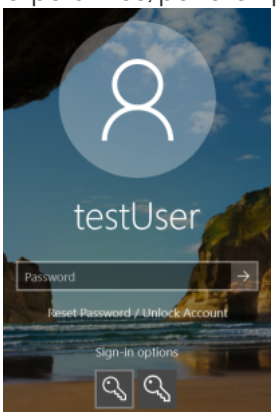
O Kaspersky Endpoint Security é compatível com o provedor de credenciais de terceiros ADSelfService Plus.

Ao trabalhar com provedores de credenciais de terceiros, o Agente de Autenticação intercepta a senha antes que o sistema operacional seja carregado. Isso significa que um usuário precisa inserir uma senha apenas uma vez ao entrar no Windows. Depois de entrar no Windows, o usuário pode utilizar os recursos de um provedor de credenciais de terceiros para autenticação em serviços corporativos, por exemplo. Os provedores de credenciais de terceiros também permitem que os usuários redefinam a própria senha de forma independente. Nesse caso, o Kaspersky Endpoint Security atualizará automaticamente a senha do Agente de Autenticação.

Caso esteja usando um provedor de credenciais de terceiros que não seja compatível com o aplicativo, será possível encontrar algumas limitações na operação da tecnologia Single Sign-On. Ao entrar no Windows, dois perfis estarão disponíveis para o usuário: provedor de credenciais no sistema e provedor de credenciais de terceiros. Os ícones desses perfis serão idênticos (veja a figura abaixo). O usuário terá as seguintes opções para continuar:

- Caso o usuário selecione o *provedor de credenciais de terceiros*, o Agente de Autenticação não poderá sincronizar a senha com a conta do Windows. Portanto, caso o usuário tenha alterado a senha da conta do Windows, o Kaspersky Endpoint Security não poderá atualizar a senha da conta do Agente de Autenticação. Como resultado, o usuário precisará executar o procedimento de autenticação duas vezes: na interface do Agente de Autenticação e antes de carregar o sistema operacional. Nesse caso, o usuário pode utilizar os recursos de um provedor de credenciais de terceiros para autenticação em serviços corporativos, por exemplo.

- Caso o usuário selecione o *provedor de credenciais no sistema*, o Agente de Autenticação sincronizará as senhas com a conta do Windows. Nesse caso, o usuário não poderá utilizar os recursos de um provedor terceirizado para autenticação em serviços corporativos, por exemplo.



Perfil de autenticação do sistema e perfil de autenticação de terceiros para entrada do Windows

Gerenciar contas do Agente de Autenticação

O Agente de Autenticação é necessário para trabalhar com unidades protegidas usando a tecnologia Kaspersky Disk Encryption (FDE). Antes que o sistema operacional seja carregado, o usuário precisa concluir a autenticação com o Agente. A tarefa *Gerenciar contas do Agente de Autenticação* foi projetada para definir as configurações de autenticação do usuário. Você pode usar tarefas locais para computadores individuais, bem como tarefas de grupo para computadores de grupos de administração separados ou uma seleção de computadores.

Você não pode configurar um agendamento para iniciar a tarefa *Gerenciar contas do Agente de Autenticação*. Também é impossível parar à força uma tarefa.

Como criar a tarefa Gerenciar contas do Agente de Autenticação no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **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

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Gerenciar contas do Agente de Autenticação**.

Etapa 2. Selecionar um comando de gerenciamento de conta do Agente de Autenticação

Gere uma lista de comandos de gerenciamento de contas do Agente de autenticação. Os comandos de gerenciamento permitem adicionar, modificar e excluir contas do Agente de autenticação (ver instruções abaixo). Somente usuários que possuem uma conta do Agente de autenticação podem concluir o procedimento de autenticação, carregar o sistema operacional e obter acesso à unidade criptografada.

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. Definir o nome da tarefa

Digite um nome para a tarefa, por exemplo, *Contas de administrador*.

Etapa 5. Concluir a criação da tarefa

Conclua o 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 resultado, após a conclusão da tarefa na próxima inicialização do computador, o novo usuário pode concluir o procedimento de autenticação, carregar o sistema operacional e obter acesso à unidade criptografada.

Como criar a tarefa Gerenciar contas do Agente de Autenticação no Web Console

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.
2. Na lista suspensa **Tipo de tarefa**, selecione **Gerenciar contas do Agente de Autenticação**.
3. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Contas de administrador*.
4. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

Etapa 2. Gerenciar contas do Agente de Autenticação

Gere uma lista de comandos de gerenciamento de contas do Agente de autenticação. Os comandos de gerenciamento permitem adicionar, modificar e excluir contas do Agente de autenticação (ver instruções abaixo). Somente usuários que possuem uma conta do Agente de autenticação podem concluir o procedimento de autenticação, carregar o sistema operacional e obter acesso à unidade criptografada.

Etapa 3. Concluir a criação da tarefa

Conclua o assistente. Uma nova tarefa será exibida na lista de tarefas.

Para executar uma tarefa, marque a caixa de seleção ao lado da tarefa e clique no botão **Iniciar**.

Como resultado, após a conclusão da tarefa na próxima inicialização do computador, o novo usuário pode concluir o procedimento de autenticação, carregar o sistema operacional e obter acesso à unidade criptografada.

Para adicionar uma conta do Agente de Autenticação, você precisa adicionar um comando especial à tarefa *Gerenciar contas do Agente de Autenticação*. É conveniente usar uma tarefa de grupo, por exemplo, para adicionar uma conta de administrador a todos os computadores.

O Kaspersky Endpoint Security permite que você crie contas do Agente de Autenticação automaticamente, antes de criptografar uma unidade. Você pode habilitar a criação automática de contas do Agente de Autenticação nas configurações da política de Criptografia completa do disco. Você também pode Usar a tecnologia de Login único (SSO).

Como adicionar uma conta do Agente de Autenticação por meio do Console de administração (MMC)

1. Abra as propriedades da tarefa *Gerenciar contas do Agente de Autenticação*.
2. Nas propriedades da tarefa, selecione a seção **Configurações**.
3. Clique em **Adicionar** → **Comando de adição de conta**.

4. Na janela exibida, no campo **Conta do Windows**, especifique o nome da conta do Microsoft Windows que será usada para criar a conta do Agente de Autenticação.

5. Se você inseriu manualmente o nome da conta do Windows, clique no botão **Permitir** para definir o SID (identificador de segurança da conta).

   Se você escolher não determinar o identificador de segurança (SID) clicando no botão **Permitir**, o SID será determinado no momento em que a tarefa for executada no computador.

   É necessário definir um identificador de segurança da conta do Windows para verificar se o nome da conta do Windows foi inserido corretamente. Se a conta do Windows não existir no computador ou no domínio confiável, a tarefa *Gerenciar contas do Agente de Autenticação* terminará com um erro.

6. Marque a caixa de seleção **Substituir conta existente** se quiser que a conta existente anteriormente, criada para o Agente de Autenticação, seja substituída pela conta que está sendo criada.

   Esta etapa está disponível quando você adicionar o comando de criação de conta do Agente de Autenticação nas propriedades de uma tarefa de grupo para gerenciar contas do Agente de Autenticação. Esta etapa está indisponível quando o comando de criação de conta do Agente de Autenticação é adicionado nas propriedades da tarefa local do *Gerenciar contas do Agente de Autenticação*.

7. No campo **Nome de usuário**, digite o nome da conta do Agente de Autenticação que deve ser inserido durante o processo de autenticação para acessar os discos rígidos criptografados.

8. Marque a caixa de seleção **Permitir autenticação baseada em senha** se desejar que o aplicativo solicite a inserção da senha da conta do Agente de Autenticação durante o processo de autenticação para acessar os discos rígidos criptografados. Defina uma senha para a conta do Agente de autenticação. Se necessário, você pode solicitar uma nova senha ao usuário após a primeira autenticação.

9. Marque a caixa de seleção **Permitir autenticação baseada em certificado** se desejar que o aplicativo solicite que o usuário conecte um token ou cartão inteligente ao computador durante o processo de autenticação, para acessar os discos rígidos criptografados. Selecione um arquivo de certificado para autenticação com um cartão inteligente ou token.

10. Se necessário, no campo **Descrição do comando**, insira os detalhes da conta do Agente de Autenticação que você precisa para gerenciar o comando.

11. No bloco **Acesso à autenticação no Agente de Autenticação**, configure o acesso à autenticação no Agente de Autenticação para o usuário que utiliza a conta especificada no comando.

12. Salvar alterações.

Como adicionar uma conta do Agente de Autenticação por meio do Web Console

1. Na janela principal do Web Console, selecione **Tarefas**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Gerenciar contas do Agente de Autenticação** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

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

4. Na lista de contas do Agente de autenticação, clique no botão **Adicionar** e selecione o tipo de comando **Adicionar conta**.

5. Selecione uma conta de usuário. Você pode selecionar uma conta na lista de contas de domínio ou inserir manualmente o nome da conta. Vá para a próxima etapa.

   O Kaspersky Endpoint Security determina o identificador de segurança da conta (Security Identifier, SID). Isso é necessário para verificar a conta. Se você digitou o nome de usuário incorretamente, o Kaspersky Endpoint Security encerrará a tarefa com um erro.

6. Defina as configurações da conta do Agente de autenticação.

   - **Criar uma nova conta de Agente de Autenticação para substituir a conta existente**. O Kaspersky Endpoint Security verifica as contas existentes no computador. Se o ID de segurança do usuário no computador e na tarefa corresponderem, o Kaspersky Endpoint Security alterará as configurações da conta de usuário de acordo com a tarefa.

   - **Nome de usuário**. O nome de usuário padrão da conta do Agente de autenticação corresponde ao nome de domínio do usuário.

   - **Permitir autenticação baseada em senha**. Defina uma senha para a conta do Agente de autenticação. Se necessário, você pode solicitar uma nova senha ao usuário após a primeira autenticação. Dessa forma, cada usuário terá sua própria senha exclusiva. Você também pode definir os requisitos de força da senha para a conta do Agente de autenticação na política.

   - **Permitir autenticação baseada em certificado**. Selecione um arquivo de certificado para autenticação com um cartão inteligente ou token. Dessa forma, o usuário precisará digitar a senha do cartão inteligente ou token.

   - **Acesso da conta a dados criptografados**. Configure o acesso do usuário à unidade criptografada. Você pode, por exemplo, desativar temporariamente a autenticação do usuário em vez de excluir a conta do Agente de autenticação.

   - **Comentário**. Digite uma descrição da conta, se necessário.

7. Salvar alterações.

8. Marque a caixa de seleção ao lado da tarefa e clique no botão **Iniciar**.

   Como resultado, após a conclusão da tarefa na próxima inicialização do computador, o novo usuário pode concluir o procedimento de autenticação, carregar o sistema operacional e obter acesso à unidade criptografada.

Para alterar a senha e outras configurações da conta do Agente de Autenticação, você precisa adicionar um comando especial à tarefa *Gerenciar contas do Agente de Autenticação*. É conveniente usar uma tarefa de grupo, por exemplo, para substituir o certificado do token de administrador em todos os computadores.

Como alterar a conta do Agente de Autenticação por meio do Console de administração (MMC)

1. Abra as propriedades da tarefa *Gerenciar contas do Agente de Autenticação*.

2. Nas propriedades da tarefa, selecione a seção **Configurações**.

3. Clique em **Adicionar** → **Comando de edição de conta**.

4. Na janela exibida, no campo **Conta do Windows**, especifique o nome da conta de usuário do Microsoft Windows que você deseja alterar.

5. Se você inseriu manualmente o nome da conta do Windows, clique no botão **Permitir** para definir o SID (identificador de segurança da conta).

Se você escolher não determinar o identificador de segurança (SID) clicando no botão **Permitir**, o SID será determinado no momento em que a tarefa for executada no computador.

> É necessário definir um identificador de segurança da conta do Windows para verificar se o nome da conta do Windows foi inserido corretamente. Se a conta do Windows não existir no computador ou no domínio confiável, a tarefa *Gerenciar contas do Agente de Autenticação* terminará com um erro.

6. Marque a caixa de seleção **Alterar nome de usuário** e insira um novo nome para a conta do Agente de Autenticação se desejar que o Kaspersky Endpoint Security altere o nome de usuário de todas as contas do Agente de Autenticação criadas com base na conta do Microsoft Windows com o nome indicado no campo **Conta do Windows** para o nome inserido no campo abaixo.

7. Marque a caixa de seleção **Modificar configurações de autenticação baseadas em senha** para tornar editáveis as configurações de autenticação baseada em senha.

8. Marque a caixa de seleção **Permitir autenticação baseada em senha** se desejar que o aplicativo solicite a inserção da senha da conta do Agente de Autenticação durante o processo de autenticação para acessar os discos rígidos criptografados. Defina uma senha para a conta do Agente de autenticação.

9. Marque a caixa de seleção **Editar a regra de alteração de senha na autenticação do Agente de Autenticação** caso queira que o Kaspersky Endpoint Security altere o valor da configuração de alteração de senha para todas as contas do Agente de Autenticação criadas usando a conta do Microsoft Windows com o nome indicado no campo **Conta do Windows** para o valor de configuração especificado abaixo.

10. Especifique o valor da configuração de alteração da senha na autenticação do Agente de Autenticação.

11. Marque a caixa de seleção **Modificar configurações de autenticação baseadas em certificado** para tornar editáveis as configurações da autenticação baseadas no certificado eletrônico de um token ou cartão inteligente.

12. Marque a caixa de seleção **Permitir autenticação baseada em certificado** se desejar que o aplicativo solicite que o usuário insira a senha para o token ou cartão inteligente conectado ao computador durante o processo de autenticação, para poder acessar os discos rígidos criptografados. Selecione um arquivo de certificado para autenticação com um cartão inteligente ou token.

13. Marque a caixa de seleção **Editar descrição de comando** e edite a descrição do comando se desejar que o Kaspersky Endpoint Security altere a descrição do comando para todas as contas do Agente de Autenticação criadas com base nas contas do Microsoft Windows com o nome indicado no campo **Conta do Windows**.

14. Marque a caixa de seleção **Editar a regra de acesso à autenticação no Agente de Autenticação** caso queira que o Kaspersky Endpoint Security altere a regra de acesso do usuário do diálogo de autenticação no Agente de Autenticação para o valor especificado abaixo para todas as contas do Agente de Autenticação criadas usando a conta do Microsoft Windows com o nome indicado no campo **Conta do Windows**.

15. Especifique a regra para acessar a caixa de diálogo de autenticação no Agente de Autenticação.

16. Salvar alterações.

Como alterar a conta do Agente de Autenticação por meio do Web Console

1. Na janela principal do Web Console, selecione **Tarefas**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Gerenciar contas do Agente de Autenticação** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

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

4. Na lista de contas do Agente de autenticação, clique no botão **Adicionar** e selecione o tipo de comando **Editar conta**.

5. Selecione uma conta de usuário. Você pode selecionar uma conta na lista de contas de domínio ou inserir manualmente o nome da conta. Vá para a próxima etapa.

   O Kaspersky Endpoint Security determina o identificador de segurança da conta (Security Identifier, SID). Isso é necessário para verificar a conta. Se você digitou o nome de usuário incorretamente, o Kaspersky Endpoint Security encerrará a tarefa com um erro.

6. Marque as caixas de seleção ao lado das configurações que você deseja editar.

7. Defina as configurações da conta do Agente de autenticação.

   - **Criar uma nova conta de Agente de Autenticação para substituir a conta existente**. O Kaspersky Endpoint Security verifica as contas existentes no computador. Se o ID de segurança do usuário no computador e na tarefa corresponderem, o Kaspersky Endpoint Security alterará as configurações da conta de usuário de acordo com a tarefa.

   - **Nome de usuário**. O nome de usuário padrão da conta do Agente de autenticação corresponde ao nome de domínio do usuário.

   - **Permitir autenticação baseada em senha**. Defina uma senha para a conta do Agente de autenticação. Se necessário, você pode solicitar uma nova senha ao usuário após a primeira autenticação. Dessa forma, cada usuário terá sua própria senha exclusiva. Você também pode definir os requisitos de força da senha para a conta do Agente de autenticação na política.

   - **Permitir autenticação baseada em certificado**. Selecione um arquivo de certificado para autenticação com um cartão inteligente ou token. Dessa forma, o usuário precisará digitar a senha do cartão inteligente ou token.

   - **Acesso da conta a dados criptografados**. Configure o acesso do usuário à unidade criptografada. Você pode, por exemplo, desativar temporariamente a autenticação do usuário em vez de excluir a conta do Agente de autenticação.

   - **Comentário**. Digite uma descrição da conta, se necessário.

8. Salvar alterações.

9. Marque a caixa de seleção ao lado da tarefa e clique no botão **Iniciar**.

Para excluir uma conta do Agente de Autenticação, você precisa adicionar um comando especial à tarefa *Gerenciar contas do Agente de Autenticação*. É conveniente usar uma tarefa de grupo, por exemplo, para excluir a conta de um funcionário demitido.

Como excluir uma conta do Agente de Autenticação por meio do Console de administração (MMC)

1. Abra as propriedades da tarefa *Gerenciar contas do Agente de Autenticação*.

2. Nas propriedades da tarefa, selecione a seção **Configurações**.

3. Clique em **Adicionar** → **Comando de exclusão de conta**.

4. No campo **Conta do Windows** da janela exibida, especifique o nome da conta de usuário do Microsoft Windows que foi usada para criar a conta do Agente de Autenticação que você deseja excluir.

5. Se você inseriu manualmente o nome da conta do Windows, clique no botão **Permitir** para definir o SID (identificador de segurança da conta).

   Se você escolher não determinar o identificador de segurança (SID) clicando no botão **Permitir**, o SID será determinado no momento em que a tarefa for executada no computador.

   > É necessário definir um identificador de segurança da conta do Windows para verificar se o nome da conta do Windows foi inserido corretamente. Se a conta do Windows não existir no computador ou no domínio confiável, a tarefa *Gerenciar contas do Agente de Autenticação* terminará com um erro.

6. Salvar alterações.

Como excluir uma conta do Agente de Autenticação por meio do Web Console

1. Na janela principal do Web Console, selecione **Tarefas**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Gerenciar contas do Agente de Autenticação** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

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

4. Na lista de contas do Agente de autenticação, clique no botão **Adicionar** e selecione o tipo de comando **Remover conta**.

5. Selecione uma conta de usuário. Você pode selecionar uma conta na lista de contas de domínio ou inserir manualmente o nome da conta.

6. Salvar alterações.

7. Marque a caixa de seleção ao lado da tarefa e clique no botão **Iniciar**.

Como resultado, após a conclusão da tarefa na próxima inicialização do computador, o usuário não poderá concluir o procedimento de autenticação e carregar o sistema operacional. O Kaspersky Endpoint Security negará o acesso aos dados criptografados.

Para visualizar a lista de usuários que podem concluir a autenticação com o Agente e carregar o sistema operacional, é necessário acessar as propriedades do computador gerenciado.

Como exibir a lista de contas do Agente de Autenticação por meio do Console de administração (MMC)

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

2. Na árvore do console, selecione **Dispositivos**.

3. Clique duas vezes para abrir a janela de propriedades do computador.

4. Na janela de propriedades do computador, selecione a seção **Tarefas**.

5. Na lista de tarefas, selecione **Gerenciar contas do Agente de Autenticação** e abra as propriedades da tarefa clicando duas vezes.

6. Nas propriedades da tarefa, selecione a seção **Configurações**.

Como resultado, você poderá acessar uma lista de contas do Agente de autenticação neste computador. Somente usuários da lista podem concluir a autenticação com o Agente e carregar o sistema operacional.

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

2. Clique no nome do computador no qual deseja visualizar a lista de contas do Agente de Autenticação.

3. Nas propriedades do computador, selecione a guia **Tarefas**.

4. Na lista de tarefas, selecione **Gerenciar contas do Agente de Autenticação**.

5. Nas propriedades da tarefa, selecione a guia **Configurações do aplicativo**.

Como resultado, você poderá acessar uma lista de contas do Agente de autenticação neste computador. Somente usuários da lista podem concluir a autenticação com o Agente e carregar o sistema operacional.

Usar um token ou cartão inteligente com o Agente de Autenticação

É possível usar um token ou cartão inteligente para a autenticação quando acessar discos rígidos criptografados. Para fazer isso, você deve adicionar o arquivo de certificado eletrônico de um token ou cartão inteligente à tarefa *Gerenciar contas do Agente de Autenticação*.

O uso de um token ou cartão inteligente estará disponível somente se os discos rígidos do computador tiverem sido criptografados usando o algoritmo de criptografia AES256. Se os discos rígidos do computador foram criptografados usando o algoritmo de criptografia AES56, a adição do arquivo de certificado eletrônico ao comando será negada.

O Kaspersky Endpoint Security suporte os seguintes tokens, leitores de cartões inteligentes e cartões inteligentes:

- SafeNet eToken PRO 64K (4.2b);
- SafeNet eToken PRO 72K Java;
- SafeNet eToken 4100-72K Java;
- SafeNet eToken 5100;
- SafeNet eToken 5105;
- SafeNet eToken 7300;
- EMC RSA SID 800;
- Gemalto IDPrime.NET 510;
- Gemalto IDPrime.NET 511;
- Rutoken ECP;
- Rutoken ECP Flash;

- Athena IDProtect Laser;
- SafeNet eToken PRO 72K Java;
- Aladdin-RD JaCarta PKI.

Para adicionar o arquivo de certificado eletrônico de um token ou cartão inteligente ao comando para criar uma conta do Agente de Autenticação, primeiro salve o arquivo usando software de terceiros para gerenciar certificados.

O certificado do token ou cartão inteligente tem as seguintes propriedades:

- O certificado deve ser compatível com a norma X.509 e o arquivo do certificado deve ter a codificação DER.
- O certificado contém uma chave RSA com um comprimento de pelo menos 1.024 bits.

Se o certificado eletrônico do token ou cartão inteligente não atender a esses requisitos, você não poderá carregar o arquivo de certificado no comando para criar uma conta do Agente de Autenticação.

O parâmetro `KeyUsage` do certificado deve ter o valor `keyEncipherment` ou `dataEncipherment`. O parâmetro `KeyUsage` determina a finalidade do certificado. Se o parâmetro tiver um valor diferente, o Kaspersky Security Center fará o download do arquivo de certificado, mas exibirá um aviso.

Se um usuário perdeu um token ou um cartão inteligente, o administrador deverá adicionar o arquivo de um certificado eletrônico do token ou do cartão inteligente ao comando para criar uma conta do Agente de Autenticação. Em seguida, o usuário deve concluir o procedimento para receber acesso a dispositivos criptografados ou restaurar dados em dispositivos criptografados.

Descriptografia de disco rígido

É possível descriptografar discos rígidos mesmo se não houver uma licença atualmente em uso que permita a criptografia de dados.

Para descriptografar discos rígidos:

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Criptografia de dados** → **Criptografia completa do disco**.
4. Na lista suspensa **Tecnologia de criptografia**, selecione a tecnologia com a qual os discos rígidos foram criptografados.

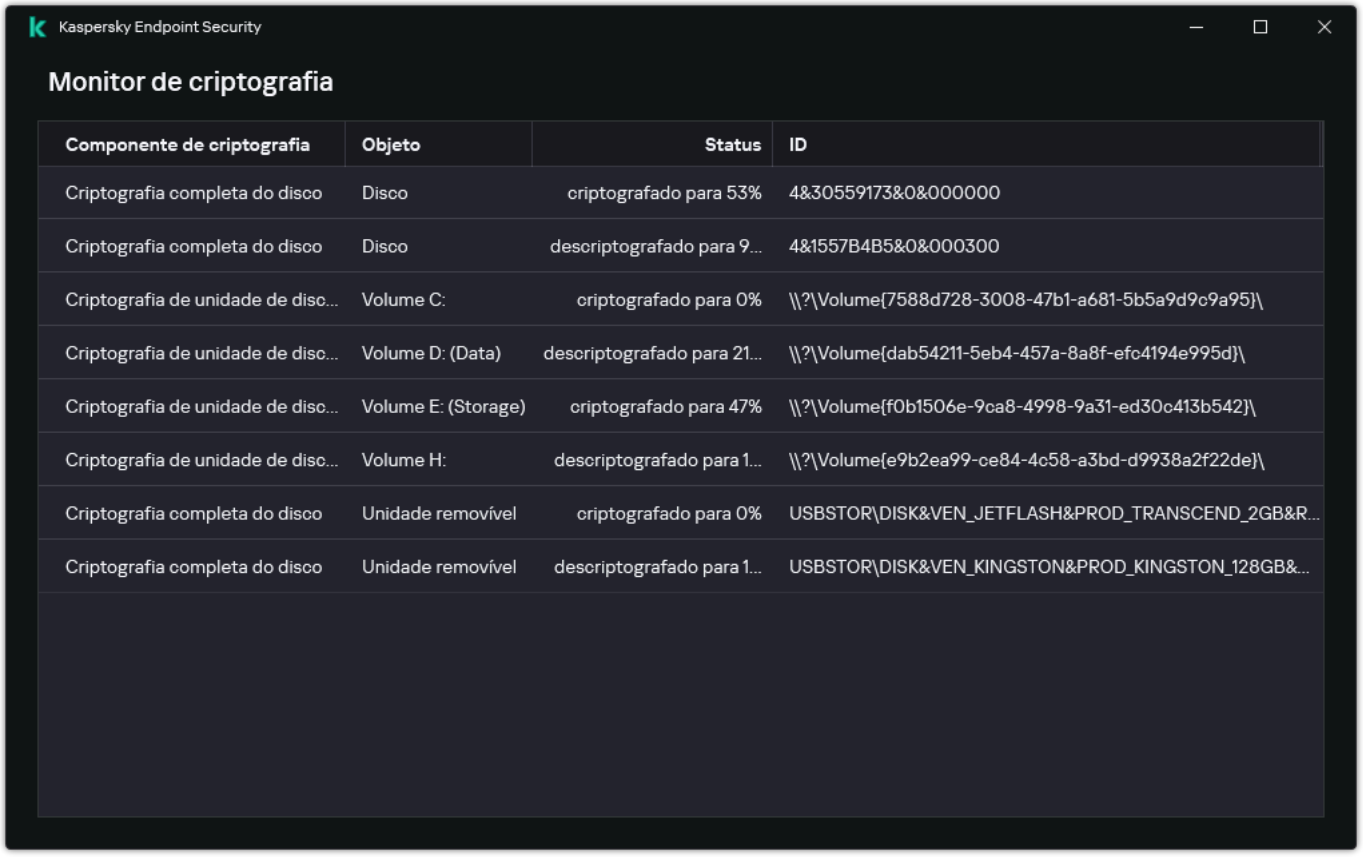
5. Realize uma das seguintes ações:

- Na lista suspensa **Modo de criptografia**, selecione a opção **Descriptografar todos os discos rígidos** para descriptografar todos os discos rígidos criptografados.
- Adicione os discos rígidos criptografados que você deseja descriptografar para a tabela **Não criptografar os seguintes discos rígidos**.

  Esta opção está disponível apenas para a tecnologia do Kaspersky Disk Encryption.

6. Salvar alterações.

É possível usar a ferramenta Monitor de criptografia para controlar o processo de criptografia ou descriptografia de disco no computador de um usuário. É possível executar a ferramenta Monitor de criptografia a partir da janela principal do aplicativo.



Monitor de criptografia

Se o usuário encerrar ou reiniciar o computador durante a descriptografia de discos rígidos que foram criptografados usando a tecnologia do Kaspersky Disk Encryption, o Agente de Autenticação é carregado antes da próxima reinicialização do sistema operacional. O Kaspersky Endpoint Security continua a descriptografia de disco rígido depois da autenticação com êxito no agente de autenticação e da inicialização do sistema operacional.

Se o sistema operacional alternar para o modo de hibernação durante a criptografia de discos rígidos que foram criptografados com a tecnologia do Kaspersky Disk Encryption, o Agente de Autenticação é carregado quando o sistema operacional voltar do modo de hibernação. O Kaspersky Endpoint Security continua a descriptografia de disco rígido depois da autenticação com êxito no agente de autenticação e da inicialização do sistema operacional. Após a descriptografia do disco rígido, o modo de hibernação fica indisponível até que o sistema operacional seja reiniciado da próxima vez.

Se o sistema operacional entrar no modo de suspensão durante a descriptografia do disco rígido, o Kaspersky Endpoint Security reinicia a descriptografia quando o sistema operacional sair do modo de suspensão sem carregar o Agente de Autenticação.

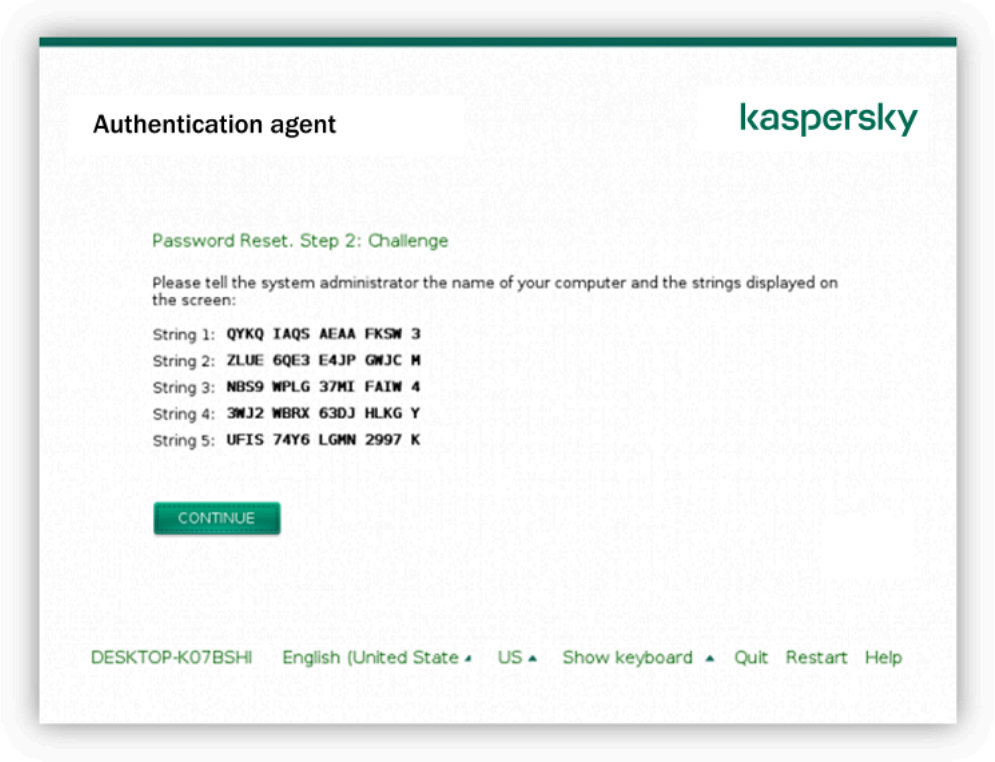
Restaurando o acesso a uma unidade protegida pela tecnologia Kaspersky Disk Encryption

Se um usuário esqueceu a senha para acessar um disco rígido protegido pela tecnologia Kaspersky Disk Encryption, será necessário iniciar o procedimento de recuperação (solicitação e resposta). Também é possível usar a conta de serviço para obter acesso ao disco rígido se esse recurso estiver ativado nas configurações de criptografia de disco.

Restaurando o acesso ao disco rígido do sistema

A restauração do acesso a um disco rígido do sistema protegido pela tecnologia Kaspersky Disk Encryption consiste nas seguintes etapas:

1. O usuário reporta os blocos de solicitação ao administrador (veja a figura abaixo).
2. O administrador insere os blocos de solicitação no Kaspersky Security Center, recebe os blocos de resposta e relata os blocos de resposta ao usuário.
3. O usuário insere os blocos de resposta na interface do Agente de Autenticação e obtém acesso ao disco rígido.



Restaurar acesso a um disco rígido do sistema protegido pela tecnologia Kaspersky Disk Encryption

Para iniciar o procedimento de recuperação, o usuário precisa clicar no botão **Forgot your password** na interface do Agente de Autenticação.

Como obter blocos de resposta para um disco rígido do sistema protegido pela tecnologia Kaspersky Disk Encryption no Console de administração (MMC)

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

2. Na árvore do console, selecione **Dispositivos**.

3. Na guia **Dispositivos**, selecione o computador do usuário que solicitou acesso aos dados criptografados e clique com o botão direito para abrir o menu de contexto.

4. No menu de contexto, selecione **Conceder acesso no modo off-line**.

5. Uma janela será aberta; nessa janela, selecione a guia **Agente de Autenticação**.

6. No bloco **Algoritmo de criptografia em uso**, selecione um algoritmo de criptografia: **AES56** ou **AES256**.

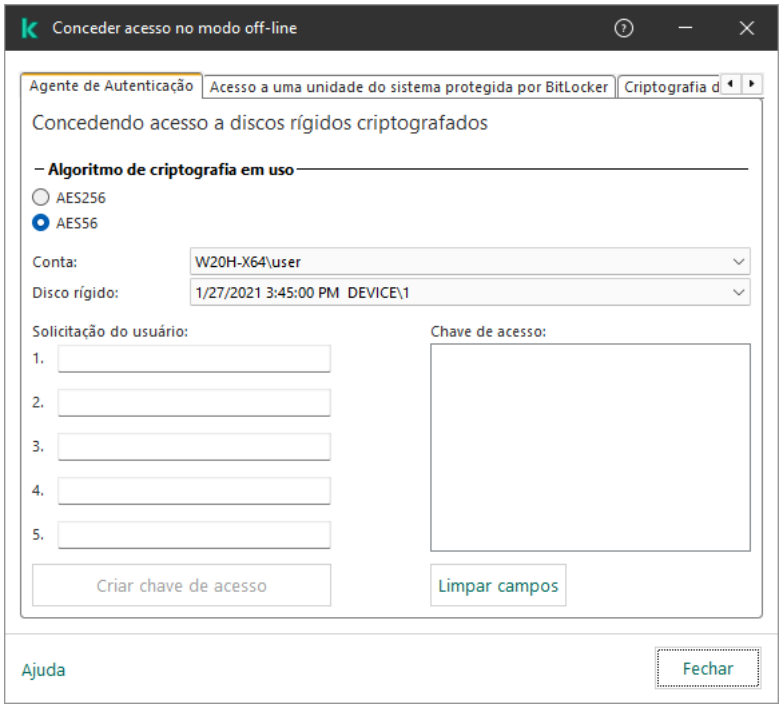
   O algoritmo de criptografia de dados depende da biblioteca de criptografia AES incluída no pacote de distribuição: *Criptografia forte (AES256)* ou *Criptografia leve (AES56)*. A biblioteca de criptografia AES é instalada junto com o aplicativo.

7. Na lista suspensa **Conta**, selecione o nome da conta do Agente de Autenticação criada para o usuário que solicitou a recuperação de acesso à unidade.

8. Na lista suspensa **Disco rígido**, selecione o disco rígido criptografado para o qual você precisa recuperar o acesso.

9. No bloco **Solicitação do usuário**, insira os blocos da solicitação ditada pelo usuário.

Como resultado, o conteúdo das seções da resposta à solicitação do usuário para recuperação do nome de usuário e senha de uma conta do Agente de Autenticação será exibido no campo **Chave de acesso**. Transmitir o conteúdo dos blocos de resposta para o usuário.



Concessão de acesso no modo off-line

Como obter blocos de resposta para um disco rígido do sistema protegido pela tecnologia Kaspersky Disk Encryption no Web Console

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

2. Marque a caixa de seleção ao lado do nome do computador cuja unidade você deseja restaurar o acesso.

3. Clique **Permitir acesso ao dispositivo em modo offline**.

4. Na janela exibida, selecione a seção **Agente de Autenticação**.

5. Na lista suspensa **Conta**, selecione o nome da conta do Agente de Autenticação criada para o usuário que solicitou a recuperação do nome e senha da conta do Agente de Autenticação.

6. Insira os blocos de solicitação transmitidos pelo usuário.

   O conteúdo das seções da resposta à solicitação do usuário para recuperação do nome de usuário e senha de uma conta do Agente de Autenticação será exibido na parte inferior da janela. Transmitir o conteúdo dos blocos de resposta para o usuário.

Após concluir o procedimento de recuperação, o Agente de Autenticação solicitará que o usuário altere a senha.

Restaurar acesso a um disco rígido que não é do sistema

A restauração do acesso a um disco rígido que não é do sistema protegido pela tecnologia Kaspersky Disk Encryption consiste nas seguintes etapas:

1. O usuário envia um arquivo de solicitação de acesso ao administrador.

2. O administrador adiciona o arquivo de solicitação de acesso ao Kaspersky Security Center, cria um arquivo de chave de acesso e envia-o ao usuário.

3. O usuário adiciona o arquivo da chave de acesso ao Kaspersky Endpoint Security e obtém acesso ao disco rígido.

Para iniciar o procedimento de recuperação, o usuário precisa tentar acessar um disco rígido. Como resultado, o Kaspersky Endpoint Security criará um arquivo de solicitação de acesso (um arquivo com a extensão KESDC), que o usuário precisará enviar ao administrador, por exemplo, por e-mail.

Como obter um arquivo de chave de acesso para um disco rígido criptografado que não é do sistema no Console de administração (MMC)

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

2. Na árvore do console, selecione **Dispositivos**.

3. Na guia **Dispositivos**, selecione o computador do usuário que solicitou acesso aos dados criptografados e clique com o botão direito para abrir o menu de contexto.

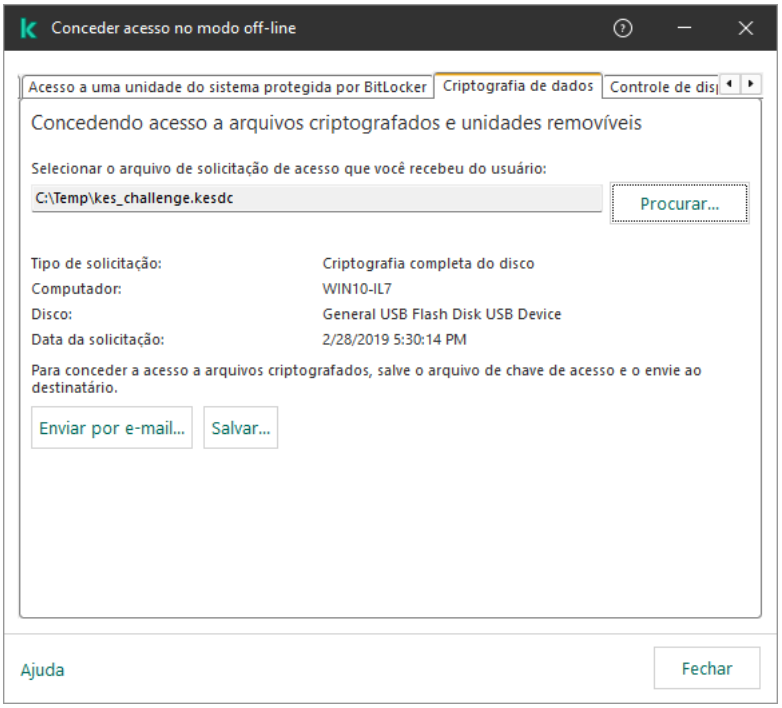
4. No menu de contexto, selecione **Conceder acesso no modo off-line**.

5. Uma janela será aberta; nessa janela, selecione a guia **Criptografia de dados**.

6. Na guia **Criptografia de dados**, clique no botão **Procurar**.

7. Na janela para selecionar um arquivo de solicitação de acesso, especifique o caminho para o arquivo recebido do usuário.

Você verá informações sobre a solicitação do usuário. O Kaspersky Security Center gera um arquivo de chave. Envie por e-mail o arquivo de chave de acesso a dados criptografados gerado para o usuário. Ou salve o arquivo de acesso e use qualquer método disponível para transferir o arquivo.



Concessão de acesso no modo off-line

Como obter um arquivo de chave de acesso criptografado que não é do sistema no Web Console

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

2. Marque a caixa de seleção ao lado do nome do computador cujos dados você deseja restaurar o acesso.

3. Clique **Permitir acesso ao dispositivo em modo offline**.

4. Selecione **Criptografia de dados**.

5. Clique no botão **Selecionar arquivo** e selecione o arquivo de solicitação de acesso que você recebeu do usuário (um arquivo com a extensão KESDC).

   O Web Console exibirá informações sobre a solicitação. Isso incluirá o nome do computador no qual o usuário está solicitando acesso ao arquivo.

6. Clique no botão **Salvar chave** e selecione uma pasta para salvar o arquivo de chave de acesso a dados criptografados (um arquivo com a extensão KESDR).

Como resultado, você poderá obter a chave de acesso a dados criptografados, que precisará transferir para o usuário.

Fazer login com a conta de serviço do Agente de Autenticação

O Kaspersky Endpoint Security permite adicionar uma conta de serviço do Agente de Autenticação ao criptografar uma unidade. A conta de serviço é necessária para obter acesso ao computador, por exemplo, quando o usuário esquece a senha. Também é possível usar a conta de serviço como conta reserva. Para adicionar uma conta, selecione uma conta de serviço nas configurações de criptografia de disco e insira o nome da conta de usuário (por padrão, `ServiceAccount`). Para autenticar usando o agente, você precisará de uma senha de uso único.

Como descobrir a senha de uso único no Console de administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Dispositivos**.
3. Clique duas vezes para abrir a janela de propriedades do computador.
4. Na janela de propriedades do computador, selecione a seção **Tarefas**.
5. Na lista de tarefas, selecione **Gerenciar contas do Agente de Autenticação** e abra as propriedades da tarefa clicando duas vezes.
6. Na janela de propriedades da tarefa, selecione a seção **Configurações**.
7. Na lista de contas, selecione a conta de serviço do Agente de Autenticação (por exemplo, `WIN10-USER\ServiceAccount`).
8. Na lista suspensa **Ação**, selecione **Visualizar conta**.
9. Nas propriedades da conta, marque a caixa de seleção **Exibir senha original**.
10. Copie a senha de uso único para fazer login com a conta de serviço.

Como descobrir a senha de uso único no Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Ativos (dispositivos)**.
2. Clique no nome do computador no qual deseja visualizar a lista de contas do Agente de Autenticação.

   Isso abre as propriedades do computador.
3. Nas propriedades do computador, selecione a guia **Tarefas**.
4. Na lista de tarefas, selecione **Gerenciar contas do Agente de Autenticação**.
5. Nas propriedades da tarefa, selecione a guia **Configurações do aplicativo**.
6. Na lista de contas, selecione a conta de serviço do Agente de Autenticação (por exemplo, `WIN10-USER\ServiceAccount`).
7. Nas propriedades da conta, marque a caixa de seleção **Exibir senha**.
8. Copie a senha de uso único para fazer login com a conta de serviço.

O Kaspersky Endpoint Security atualiza automaticamente a senha sempre que um usuário faz a autenticação com a conta de serviço. Depois de fazer a autenticação usando o agente, é necessário inserir a senha da conta do Windows. Ao fazer login com a conta de serviço, não é possível usar a tecnologia SSO.

Atualização do sistema operacional

Há várias considerações especiais para atualizar o sistema operacional de um computador protegido pela Criptografia Completa do Disco (FDE, na sigla em inglês). Atualize o sistema operacional da seguinte maneira: primeiro, atualize o sistema operacional em um computador, em seguida, em uma pequena parte dos computadores e, por último, em todos os computadores da rede.

Se você estiver usando a tecnologia do Kaspersky Disk Encryption, o Agente de Autenticação será carregado antes que o sistema operacional seja iniciado. Usando o Agente de Autenticação, o usuário pode entrar no sistema e receber acesso às unidades criptografadas. O sistema operacional começa a carregar. Se você iniciar uma atualização do sistema operacional em um computador protegido usando a tecnologia do Kaspersky Disk Encryption, o Assistente de atualização do sistema operacional removerá o Agente de Autenticação. Assim, o computador poderá ser bloqueado porque o carregador do sistema operacional não conseguirá acessar a unidade criptografada.

Recursos da atualização do sistema operacional:

- **Atualização do SO por meio do WSUS**. É possível atualizar o sistema operacional da maneira usual.
- **Atualização do SO por meio do ISO**. Para atualizar o sistema operacional, é necessário especificar a pasta com os drivers de criptografia de disco da Kaspersky. O aplicativo copia automaticamente os drivers para uma pasta separada. Faça o seguinte:

  1. Monte a imagem ISO.
  2. Inicie a instalação da atualização do sistema com a seguinte chave:

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky Lab\KES.14.2\reflect_drivers
     ```

A atualização automática do SO apenas estará disponível se o computador estiver executando o Windows 10 1607 (RS1) ou superior. Recomendamos primeiro descriptografar o disco, atualizar o sistema operacional e, em seguida, criptografar o disco novamente para atualizar versões anteriores.

Se estiver usando a tecnologia de criptografia de unidade de disco da BitLocker, você não precisará descriptografar os discos rígidos para a atualização do Windows 10. Para obter mais detalhes sobre o BitLocker, visite o site da Microsoft.

Eliminar erros de atualização da funcionalidade de criptografia

A criptografia completa do disco é atualizada quando uma versão anterior do aplicativo é atualizada para o Kaspersky Endpoint Security for Windows 14.2.

Ao iniciar a atualização da funcionalidade Criptografia completa do disco, podem ocorrer os seguintes erros:

- Não é possível inicializar a atualização.
- Dispositivo incompatível com o Agente de Autenticação.

Para eliminar os erros que ocorreram quando você iniciou o processo de atualização da funcionalidade Criptografia completa do disco na nova versão do aplicativo:

1. Descriptografe discos rígidos.
2. Criptografe os discos rígidos mais uma vez.

Durante a atualização da funcionalidade Criptografia completa do disco, podem ocorrer os seguintes erros:

- Não é possível concluir a atualização.
- Reversão de atualização da Criptografia completa do disco concluída com um erro.

Para eliminar os erros que ocorreram durante o processo de atualização da funcionalidade Criptografia completa do disco,

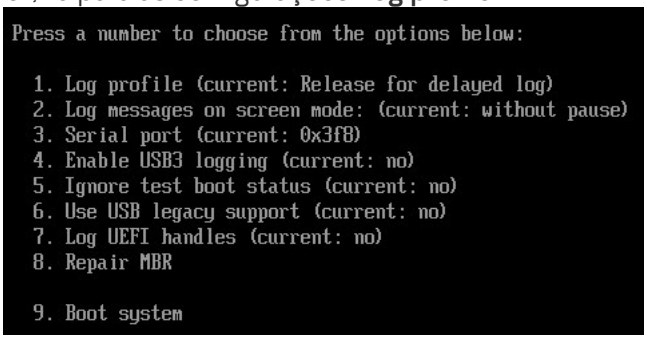
Restaure o acesso a dispositivos criptografados usando o Utilitário de restauração.

Rastreamento do Agente de Autenticação

O aplicativo registra informações de serviço sobre a operação do Agente de Autenticação e informações sobre as operações do usuário com o Agente de Autenticação no arquivo de rastreio.

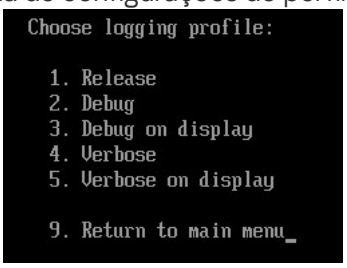
Para ativar o rastreamento do Agente de Autenticação:

1. Ative o rastreamento do Kaspersky Endpoint Security.
2. Reinicie o computador.
3. Logo que um computador com discos rígidos criptografados é inicializado, pressione o botão **F3** para abrir uma janela e especificar as configurações do Agente de Autenticação.
4. Após o carregador do boot FDE iniciar, selecione o gerenciar de boot **KES (FDE <version>)**.
5. No meu do gerenciador de boot, vá para as configurações **Log profile**.



Menu do gerenciar do boot

6. Selecione o nível de rastreamento na janela de configurações do perfil de logs:



Níveis de rastreamento do Agente de Autenticação

- **Release**. Se esta opção for marcada, o aplicativo não registra informações sobre eventos do Agente de Autenticação no arquivo de rastreio.

- **Debug**. Se essa opção for marcada, o aplicativo registra informações sobre a operação do Agente de Autenticação e as operações do usuário realizadas com o Agente de Autenticação no arquivo de rastreio.

- **Debug on display**. Se essa opção for marcada, o aplicativo registra no arquivo de rastreio informações sobre a operação do Agente de Autenticação e as operações do usuário realizadas com o Agente de Autenticação, depois as transmite via porta COM.

  Se um computador com unidades de disco rígido criptografada for conectado a outro computador via porta COM, os eventos do Agente de Autenticação podem ser examinados por esse outro computador.

- **Verbose**. Se essa opção for marcada, o aplicativo registra no arquivo de rastreio informações sobre a operação do Agente de Autenticação e as operações do usuário realizadas com o Agente de Autenticação.

  O nível de detalhe das entradas nessa opção é mais elevado comparado ao nível da opção **Debug**. Um nível elevado de detalhe das entradas pode retardar a inicialização do Agente de Autenticação e do sistema operacional.

- **Verbose on display**. Se essa opção for marcada, o aplicativo registra no arquivo de rastreio informações detalhadas sobre a operação do Agente de Autenticação e as operações do usuário realizadas com o Agente de Autenticação, depois as transmite via porta COM.

  O nível de detalhe das entradas nessa opção é mais elevado comparado ao nível da opção **Debug on display**. Um nível elevado de detalhe das entradas pode retardar a inicialização do Agente de Autenticação e do sistema operacional.

Após selecionar um nível de rastreamento, o gerenciador de boot exibirá o menu novamente.

7. No meu de gerenciamento de boot, selecione **Boot system**.

   O carregador do boot FDE inicia o Agente de Autenticação.

   Reprodução do problema.

   Os dados serão registrados no arquivo de rastreio do Agente de Autenticação se existirem discos rígidos criptografados no computador ou durante a criptografia completa do disco.

8. Para interromper o processo de rastreamento, retorne à janela Ferramentas de suporte e desative o rastreamento.

Como resultado, os arquivos de rastreamento de funcionamento KES.SRV do Agente de Autenticação são criados na pasta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. O arquivo de rastreio do Agente de Autenticação não é enviado à Kaspersky, diferentemente dos outros arquivos de rastreio do aplicativo. Se

necessário, envie manualmente o arquivo de rastreamento do Agente de Autenticação para a Kaspersky para análise.

Editar as textos de ajuda do Agente de autenticação

Antes de editar mensagens de ajuda do Agente de Autenticação, por favor reveja a lista de caracteres suportados em um ambiente de pré-reinicialização.

Para editar as mensagens de ajuda do Agente de Autenticação:

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Criptografia de dados** → **Configurações comuns de criptografia**.
4. No bloco **Modelos**, clique no botão **Ajuda**.
5. Na janela que é aberta, faça o seguinte:
   - Selecione a guia **Autenticação** para editar o texto de ajuda mostrado na janela do Agente de Autenticação quando as credenciais de conta estão sendo inseridas.
   - Selecione a guia **Alterar senha** para editar o texto de ajuda exibido na janela do Agente de Autenticação quando a senha para a conta do Agente de Autenticação estiver sendo alterada.
   - Selecione a guia **Recuperar senha** para editar o texto de ajuda exibido na janela do Agente de Autenticação quando a senha da conta do Agente de Autenticação estiver sendo recuperada.
6. Edite as mensagens de ajuda.

   Se desejar restaurar o texto original, clique no botão **Por padrão**.

   Você pode inserir o texto de ajuda com 16 linhas ou menos. O comprimento máximo de uma linha é de 64 caracteres.
7. Salvar alterações.

O suporte limitado de caracteres nas mensagens de ajuda do Agente de Autenticação

Em um ambiente de pré-reinicialização, os seguintes caracteres Unicode são suportados:

- Alfabeto latino básico (0000 – 007F)
- Caracteres adicionais Latim 1 (0080 – 00FF)
- Latim-A estendido (0100 – 017F)

- Latim-B extenso (0180 – 024F)
- Caracteres de ID estendidos não combinados (02B0 – 02FF)
- Marcas diacríticas combinadas (0300 – 036F)
- Alfabetos gregos e coptos (0370 – 03FF)
- Cirílico (0400 – 04FF)
- Hebraico (0590 – 05FF)
- Script arábico (0600 – 06FF)
- Latim estendido adicional (1E00 – 1EFF)
- Marcas de pontuação (2000 – 206F)
- Símbolos de moeda (20A0 – 20CF)
- Símbolos parecidos com letras (2100 – 214F)
- Números geométricos (25A0 – 25FF)
- Formulários de apresentação de script-B arábico (FE70 – FEFF)

Os caracteres que não são especificados nesta lista não são apoiados em um meio de pré-inicialização. Não se recomenda usar tais caracteres em mensagens de ajuda do Agente de Autenticação.

A remoção de restos de objetos e dados após testar o funcionamento do Agente de Autenticação

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

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

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

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

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

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

2. Inicie o Kaspersky Endpoint Security.

Para usar um Utilitário de Restauração para remover objetos e dados que permaneceram após a operação de teste do Agente de Autenticação:

1. Execute o arquivo chamado fdert.exe, que é o arquivo executável do utilitário de restauração. Este arquivo é criado pelo Kaspersky Endpoint Security.

2. Na janela do Utilitário de Restauração, selecione o dispositivo necessário.

3. Clique **Verificar**.

4. Se, após diagnosticar o disco rígido do sistema, você receber uma mensagem indicando que objetos e dados permaneceram após a operação de teste do Agente de Autenticação, clique em **Excluir objetos e dados AA**.

   O botão **Excluir objetos e dados AA** está disponível somente se forem detectados objetos e dados que permaneceram após a operação de teste do Agente de Autenticação.

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

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

Gerenciamento do BitLocker

O BitLocker é uma tecnologia de criptografia incorporada nos sistemas operacionais Windows. O Kaspersky Endpoint Security permite controlar e gerenciar o Bitlocker usando a infraestrutura do Kaspersky Next. O BitLocker criptografa volumes lógicos. O BitLocker não pode ser usado para criptografia de unidades removíveis. Para obter detalhes sobre o BitLocker, consulte a documentação da Microsoft.

Ao criptografar o disco, o BitLocker coloca o carregador de inicialização e outros arquivos auxiliares no system partition. Esta partição não é criptografada. O sistema operacional cria a partição do sistema automaticamente durante a instalação do Windows. Se o disco estiver totalmente particionado antes da instalação do Windows, o sistema operacional não poderá criar uma partição do sistema. Nesse caso, quando a criptografia de disco do BitLocker for iniciada, o sistema operacional solicitará ao usuário para reparticionar o disco e criar uma partição do sistema. Depois de criar uma partição do sistema, o sistema operacional inicia a criptografia do BitLocker.

O algoritmo de criptografia BitLocker não depende da versão da Biblioteca AES incluída no pacote de distribuição (AES256 ou AES56). A criptografia usa a biblioteca de criptografia integrada do sistema operacional.

Por padrão, o aplicativo usa o algoritmo de criptografia BitLocker com um comprimento de chave efetivo de 256 bits para criptografar dispositivos que nunca foram criptografados. Para um dispositivo que foi criptografado antes da instalação do aplicativo, o algoritmo de criptografia pode ser diferente. Para obter informações detalhadas sobre como selecionar o algoritmo de criptografia, consulte o Site de Suporte Técnico da Microsoft. A partir da versão 12.9, o Kaspersky Endpoint Security envia a chave de recuperação original para dispositivos anteriormente criptografados por aplicativos de terceiros para o Kaspersky Security Center.

O BitLocker fornece armazenamento seguro de chaves de acesso usando um módulo de plataforma confiável. Um *Trusted Platform Module (TPM)* é um microchip desenvolvido para fornecer funções básicas relacionadas à segurança (por exemplo, armazenar chaves de criptografia). Um Módulo de plataforma confiável geralmente é instalado na placa-mãe do computador e interage com todos os outros componentes do sistema através do barramento de hardware. O uso do TPM é a maneira mais segura de armazenar chaves de acesso do BitLocker, pois o TPM fornece verificação de integridade do sistema antes da inicialização. Você ainda pode criptografar unidades em um computador sem um TPM. Nesse caso, a chave de acesso será criptografada com uma senha. O BitLocker usa os seguintes métodos de autenticação:

- TPM.
- TPM e PIN.
- Senha.

Após criptografar o disco rígido do sistema, o usuário precisa passar pela autenticação do BitLocker para inicializar o sistema operacional. Após a autenticação, o BitLocker permite que o usuário faça login. O BitLocker não oferece suporte à tecnologia de login único (SSO).

Após criptografar uma unidade, o BitLocker cria uma chave de recuperação. O Kaspersky Endpoint Security envia a chave de recuperação ao Kaspersky Security Center para que seja possível restaurar o acesso ao disco, por exemplo, caso um usuário esqueça a senha.

Se um usuário criptografar um disco usando o BitLocker, o Kaspersky Endpoint Security enviará a chave de recuperação e informações sobre a criptografia de disco ao Kaspersky Security Center.

Se você estiver usando políticas de grupo do Windows, desative o gerenciamento do BitLocker nas configurações de política. As configurações de política do Windows podem entrar em conflito com as configurações de política do Kaspersky Endpoint Security. Ao criptografar uma unidade, podem ocorrer erros.

Iniciar Criptografia de Unidade de Disco BitLocker

Antes de iniciar a criptografia completa do disco, certifique-se de que o computador não esteja infectado. Para fazer assim, inicie a tarefa de Verificação Completa ou Verificação de Áreas Críticas. Realizar uma criptografia completa do disco em um computador infectado por um rootkit pode fazer com que o computador fique inoperável.

Para usar a criptografia de unidade de disco da BitLocker em computadores executando sistemas operacionais Windows para servidores, pode ser necessário instalar o componente criptografia de unidade de disco da BitLocker. Instale o componente utilizando as ferramentas do sistema operacional (assistente para adicionar funções e componentes). Para obter mais informações sobre a instalação da criptografia de unidade de disco BitLocker, consulte a documentação da Microsoft.

Como executar a criptografia de unidade de disco BitLocker por meio do Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Criptografia de dados** → **Criptografia completa do disco**.
4. Na lista suspensa **Tecnologia de criptografia**, selecione **Criptografia de Unidade de Disco BitLocker**.
5. Na lista suspensa **Modo de criptografia**, selecione **Criptografar todos os discos rígidos**.

   Se o computador tiver vários sistemas operacionais instalados, depois da criptografia você só poderá carregar o sistema em que a criptografia foi realizada.

6. Configure as opções avançadas da criptografia de unidade de disco da BitLocker (consulte a tabela abaixo).
7. Salvar alterações.

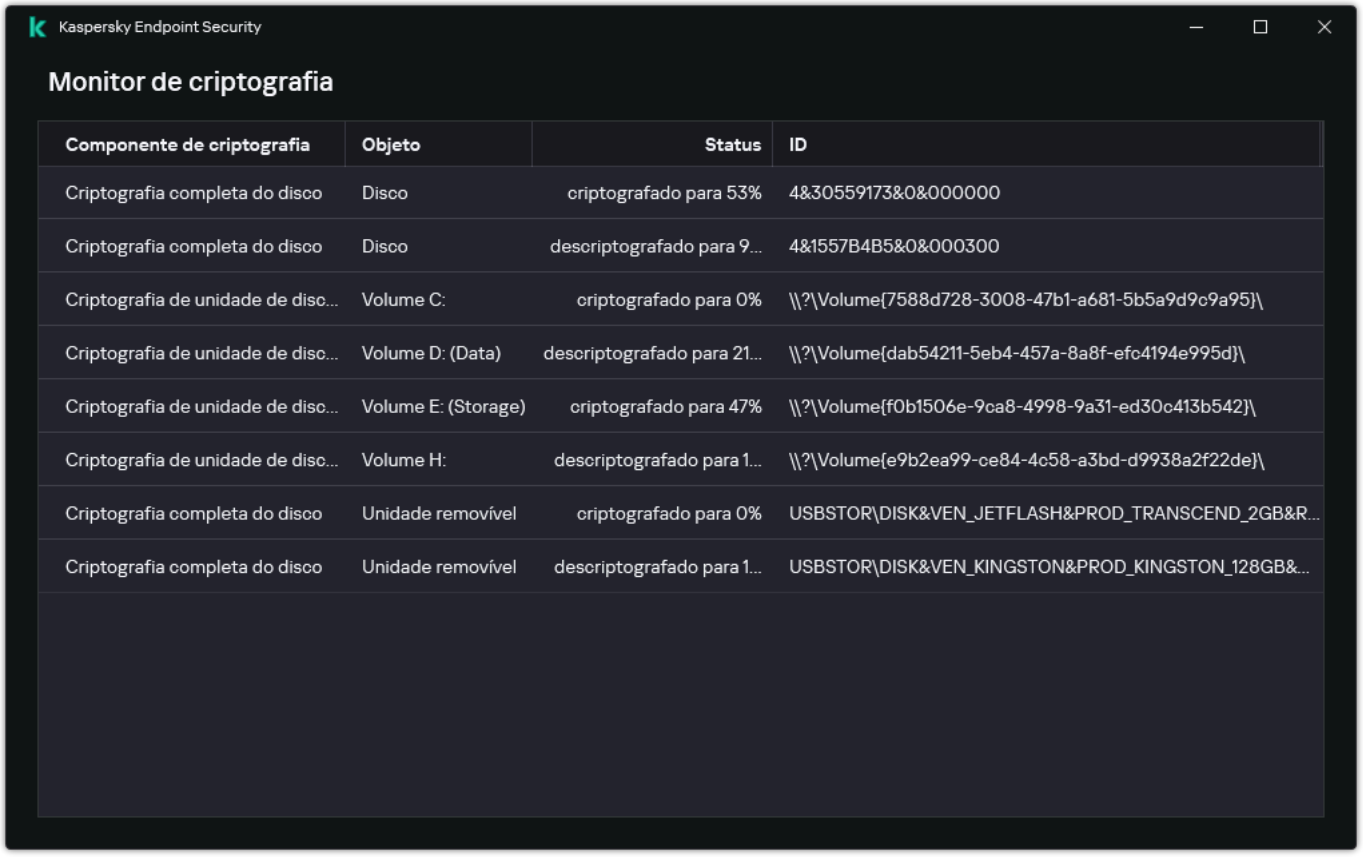
Como executar a Criptografia de Unidade de Disco BitLocker usando o Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Criptografia de dados** → **Criptografia completa do disco**.
5. Selecione a tecnologia **Criptografia do disco BitLocker**.
6. No bloco **Ação sobre os dispositivos**, selecione **Criptografar todos os discos rígidos**.

   Se o computador tiver vários sistemas operacionais instalados, depois da criptografia você só poderá carregar o sistema em que a criptografia foi realizada.

7. Configure as opções avançadas da criptografia de unidade de disco da BitLocker (consulte a tabela abaixo).
8. Salvar alterações.

É possível usar a ferramenta Monitor de criptografia para controlar o processo de criptografia ou descriptografia de disco no computador de um usuário. É possível executar a ferramenta Monitor de criptografia a partir da janela principal do aplicativo.



Monitor de criptografia

Após a aplicação da política, o aplicativo exibirá as seguintes consultas, dependendo das configurações de autenticação:

- Somente TPM. Não é necessária a entrada do usuário. O disco será criptografado quando o computador reiniciar.
- TPM + PIN / Senha. Se um módulo TPM estiver disponível, uma janela de solicitação do código PIN aparece. Se um módulo TPM não estiver disponível, você verá uma janela de solicitação de senha para autenticação da pré-inicialização.
- Somente senha. Será exibida uma janela de solicitação de senha para autenticação pré-iniciação.

Se o modo de compatibilidade padrão do Federal Information Processing estiver ativado para o sistema operacional do computador, no Windows 8 e em versões anteriores do sistema operacional, uma solicitação para conectar um dispositivo de armazenamento será exibida para salvar o arquivo da chave de recuperação. Você pode salvar vários arquivos de chave de recuperação em um único dispositivo de armazenamento.

Após definir uma senha ou PIN, o BitLocker solicitará que você reinicie o computador para concluir a criptografia. Em seguida, o usuário precisa seguir o procedimento de autenticação do BitLocker. Após o procedimento de autenticação, o usuário deve efetuar login no sistema. Após o carregamento do sistema operacional, o BitLocker concluirá a criptografia.

Se não houver acesso a chaves de criptografia, o usuário pode solicitar que o administrador de rede local forneça uma chave de recuperação (se a chave de recuperação não tiver sido salva antes no dispositivo de armazenamento ou tiver sido perdida).

Configurações do componente de Criptografia de unidade de disco da BitLocker

Parâmetro	Descrição
Permitir o uso de autenticação BitLocker que requer entrada de teclado pré-inicialização em tablets	Utilizar uma autenticação que requer a entrada de dados em um ambiente de pré-inicialização, mesmo se a plataforma não oferecer suporte para a entrada de pré-inicialização (por exemplo, com teclados sensíveis ao toque em tablets). A tela sensível ao toque de computadores tablet não está disponível no ambiente de pré-inicialização. Para concluir a autenticação do BitLocker em computadores tablet, o usuário precisa conectar um teclado USB, por exemplo. Se a caixa de seleção for marcada, o uso da autenticação que precisa de entrada de pré-inicialização será permitido. Recomenda-se usar esta definição apenas para dispositivos que têm ferramentas de introdução de dados alternativas em um ambiente de pré-inicialização, como um teclado USB além de teclados sensíveis ao toque. Se a caixa de seleção estiver desmarcada, a criptografia de unidade de disco da BitLocker não é possível em tablets.
Usar criptografia de hardware (Windows 8 e versões posteriores)	Se a caixa de seleção for marcada, o aplicativo aplicará a criptografia de hardware. Isso permite aumentar a velocidade da criptografia e usar menos recursos de computador.
Criptografar somente espaço usado em disco (Windows 8 e versões posteriores)	Esta caixa ativa / desativa a opção que limita a área de criptografia a setores de disco rígido só ocupados. Este limite permite reduzir o tempo de criptografia. Ativar ou desativar o recurso **Criptografar somente espaço usado em disco (reduz o tempo de criptografia)** após o início da criptografia não modifica essa configuração até que os discos rígidos sejam descriptografados. Você deve marcar ou desmarcar a caixa de seleção antes da criptografia inicial. Se a caixa de seleção estiver selecionada, somente as porções da unidade de disco rígido que são ocupadas por arquivos serão criptografadas. O Kaspersky Endpoint Security criptografa automaticamente novos dados à medida que são adicionados. Se a caixa de seleção estiver desmarcada, a unidade de disco rígido inteira será criptografada, inclusive fragmentos residuais de arquivos anteriormente excluídos e modificados. Esta opção é recomendada para novas unidades de disco rígido cujos dados não foram modificados ou excluídos. Se você estiver aplicando a criptografia em um disco rígido que já está no uso, recomenda-se criptografar o disco rígido inteiro. Isso garante a proteção de todos os dados; até mesmo de dados excluídos que podem ser recuperados. Por padrão, a caixa de seleção está desmarcada.

Parâmetro	Descrição
Método de autenticação	**Somente senha (Windows 8 e versões posteriores)** Caso esta opção seja selecionada, o Kaspersky Endpoint Security solicita ao usuário uma senha quando o usuário tenta acessar uma unidade criptografada. Esta opção pode ser selecionada quando o Trusted Platform Module (TPM) não está sendo usado. **Módulo de plataforma confiável (TPM)** Caso esta opção seja selecionada, o BitLocker usará um Trusted Platform Module (TPM). Um *Trusted Platform Module (TPM)* é um microchip desenvolvido para fornecer funções básicas relacionadas à segurança (por exemplo, armazenar chaves de criptografia). Um Módulo de Plataforma Confiável normalmente é instalado na placa mãe do computador e interage com todos os outros componentes do sistema via barramento de hardware. Para computadores que executam o Windows 7 ou Windows Server 2008 R2, somente a criptografia usando um módulo TPM está disponível. Se um módulo TPM não estiver instalado, a criptografia do BitLocker não será possível. O uso de senha nesses computadores não é suportado. Um dispositivo equipado com um Módulo de plataforma confiável pode criar chaves de criptografia que podem ser descriptografados apenas com o dispositivo. Um Trusted Platform Module criptografa chaves de criptografia com a sua própria chave de armazenamento de raiz. A chave de armazenamento de raiz é armazenada dentro do Trusted Platform Module. Isso fornece um nível adicional da proteção contra tentativas de cortar chaves de criptografia. Esta ação é selecionada por padrão. É possível definir uma camada adicional de proteção para o acesso à chave de criptografia e criptografar a chave com uma senha ou um PIN: • **Usar o PIN para TPM**. Se esta caixa de seleção estiver selecionada, um usuário pode usar um código PIN para obter acesso a uma chave de criptografia que é armazenada em Módulo de plataforma confiável (TPM). Se esta caixa de seleção estiver desmarcada, os usuários estão proibidos de usar códigos PIN. Para acessar a chave de criptografia, o usuário deve digitar a senha. • **Módulo de plataforma confiável (TPM), ou senha, caso o TPM não esteja disponível**. Se essa opção for selecionada, o usuário poderá utilizar uma senha para obter acesso a chaves de criptografia quando um Módulo de plataforma confiável (TPM) não estiver disponível. Se a caixa de seleção estiver desmarcada e o TPM não estiver disponível, a criptografia completa do disco não será iniciada. O método de autenticação selecionado deve ser configurado especificando os requisitos de senha ou PIN: • **Comprimento mínimo do PIN (caracteres)** (o valor padrão é 6). • **Comprimento mínimo da senha (caracteres)** (o valor padrão é 8). • **Número máximo de senhas/PINs armazenados** (o valor padrão é 5). • **Limitar período de validade da senha / PIN para TPM (dias)** (desativado por padrão). • **Usar o PIN aprimorado (letras e números)**. O *PIN Aprimorado* permite o uso de outros caracteres além dos caracteres numéricos: letras latinas maiúsculas e minúsculas, caracteres especiais e espaços. Desativado por padrão.
Recriar automaticamente a chave de recuperação (dias)	Atualizar automaticamente a senha para restaurar o acesso a uma unidade protegida pelo BitLocker. Caso a caixa de seleção esteja marcada, especifique o período de validade da senha da chave de recuperação. Isso ajuda a evitar o reuso da senha da chave de recuperação.

Descriptografando um disco rígido protegido pelo BitLocker

Os usuários podem descriptografar um disco usando o sistema operacional (a função *Desativar o BitLocker*). Depois disso, o Kaspersky Endpoint Security solicitará que o usuário criptografe o disco novamente. O Kaspersky Endpoint Security solicitará a criptografia do disco, a menos que você ative a descriptografia de disco na política.

Como descriptografar um disco rígido protegido pelo BitLocker por meio do Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Criptografia de dados** → **Criptografia completa do disco**.

4. Na lista suspensa **Tecnologia de criptografia**, selecione **Criptografia de Unidade de Disco BitLocker**.

5. Na lista suspensa **Modo de criptografia**, selecione **Descriptografar todos os discos rígidos**.

6. Salvar alterações.

Como descriptografar um disco rígido criptografado pelo BitLocker por meio do Web Console e do Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

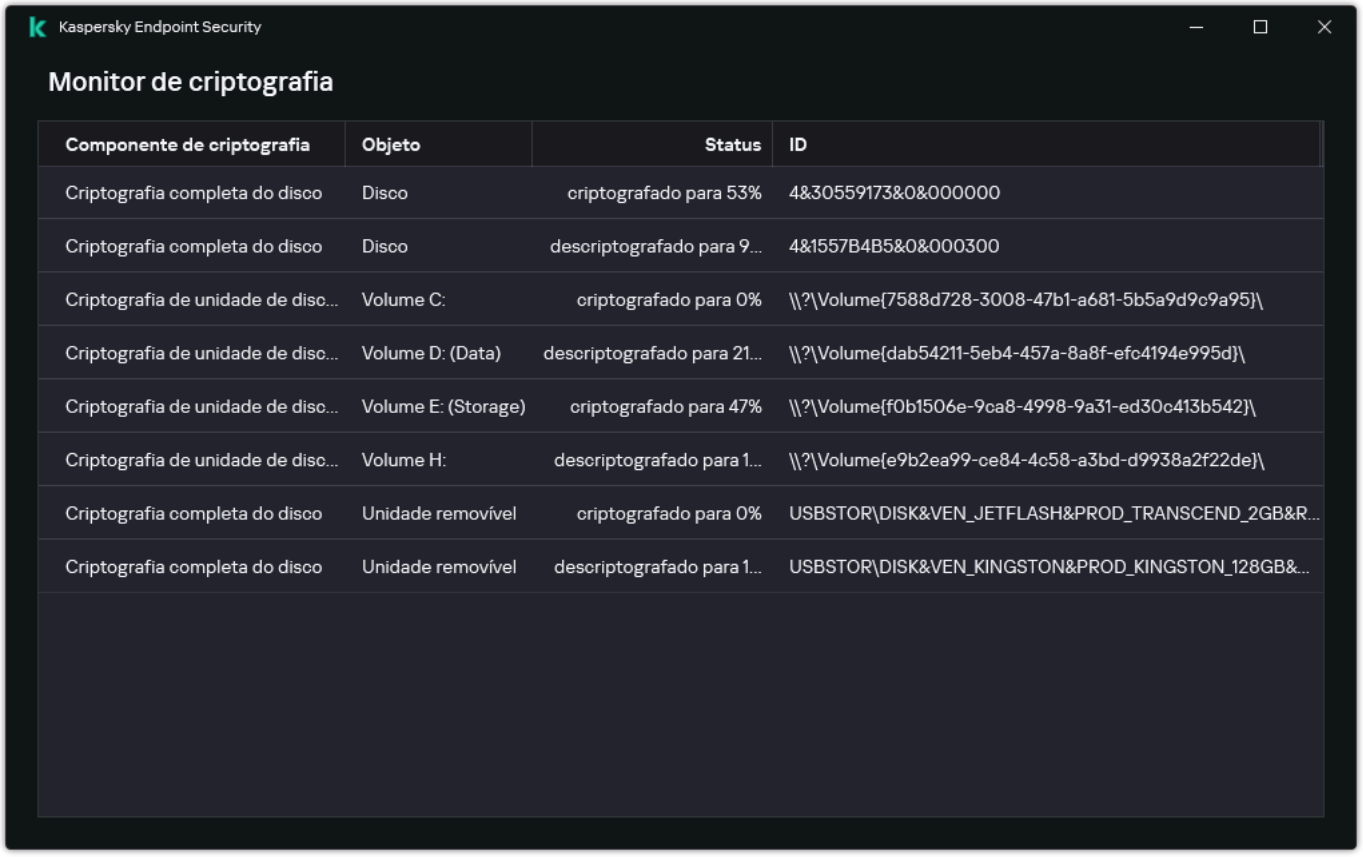
4. Selecione **Criptografia de dados** → **Criptografia completa do disco**.

5. Selecione a tecnologia **Criptografia do disco BitLocker**.

6. No bloco **Ação sobre os dispositivos**, selecione **Descriptografar todos os discos rígidos**.

7. Salvar alterações.

É possível usar a ferramenta Monitor de criptografia para controlar o processo de criptografia ou descriptografia de disco no computador de um usuário. É possível executar a ferramenta Monitor de criptografia a partir da janela principal do aplicativo.



Componente de criptografia	Objeto	Status	ID
Criptografia completa do disco	Disco	criptografado para 53%	4&30559173&0&000000
Criptografia completa do disco	Disco	descriptografado para 9...	4&1557B4B5&0&000300
Criptografia de unidade de disc...	Volume C:	criptografado para 0%	\\?\Volume{7588d728-3008-47b1-a681-5b5a9d9c9a95}\
Criptografia de unidade de disc...	Volume D: (Data)	descriptografado para 21...	\\?\Volume{dab54211-5eb4-457a-8a8f-efc4194e995d}\
Criptografia de unidade de disc...	Volume E: (Storage)	criptografado para 47%	\\?\Volume{f0b1506e-9ca8-4998-9a31-ed30c413b542}\
Criptografia de unidade de disc...	Volume H:	descriptografado para 1...	\\?\Volume{e9b2ea99-ce84-4c58-a3bd-d9938a2f22de}\
Criptografia completa do disco	Unidade removível	criptografado para 0%	USBSTOR\DISK&VEN_JETFLASH&PROD_TRANSCEND_2GB&R...
Criptografia completa do disco	Unidade removível	descriptografado para 1...	USBSTOR\DISK&VEN_KINGSTON&PROD_KINGSTON_128GB&...

Monitor de criptografia

Restauração do acesso a uma unidade protegida pelo BitLocker

Se um usuário esqueceu a senha para acessar um disco rígido criptografado pelo BitLocker, será necessário iniciar o procedimento de recuperação (solicitação e resposta).

Se o modo de compatibilidade Federal Information Processing Standard (FIPS) do sistema operacional do computador estiver ativado, nas versões Windows 8 e anteriores, o arquivo de chave de recuperação é salvo na unidade removível antes da criptografia. Para restaurar o acesso à unidade, insira a unidade removível e siga as instruções na tela.

A restauração do acesso a um disco rígido criptografado pelo BitLocker consiste nas seguintes etapas:

1. O usuário informa ao administrador o ID da chave de recuperação (veja a figura abaixo).
2. O administrador verifica o ID da chave de recuperação nas propriedades do computador no Kaspersky Security Center. O ID que o usuário forneceu deve corresponder ao ID exibido nas propriedades do computador.
3. Se os IDs da chave de recuperação corresponderem, o administrador fornecerá ao usuário a chave de recuperação ou enviará um arquivo de chave de recuperação.

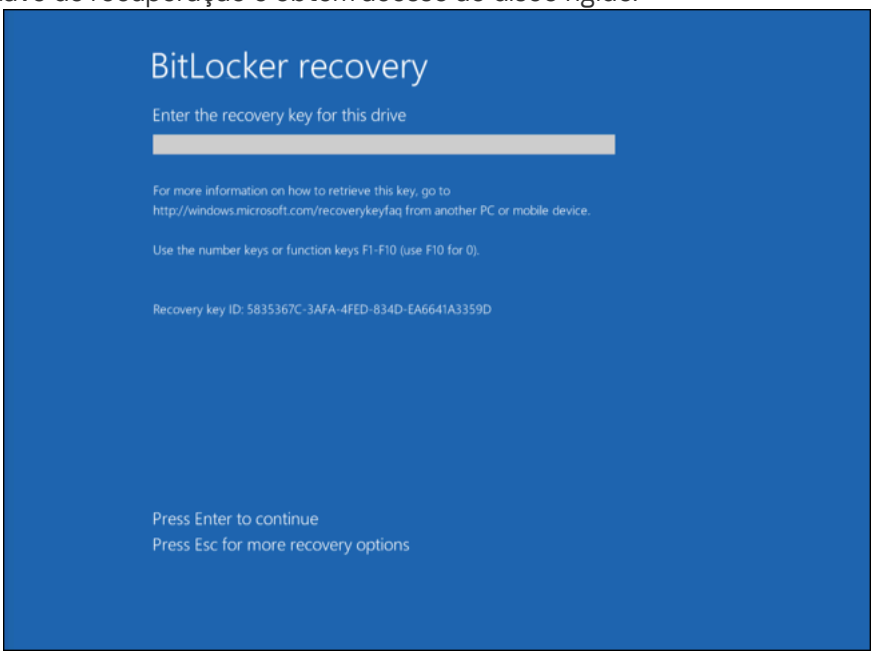
   Um arquivo de chave de recuperação é usado para computadores executando os seguintes sistemas operacionais:

   - Windows 7
   - Windows 8
   - Windows Server 2008;
   - Windows Server 2011;
   - Windows Server 2012;

   Para todos os outros sistemas operacionais, uma chave de recuperação é usada.

   Para evitar o reuso da senha da chave de recuperação, é possível configurar a atualização automática da senha em configurações da política.

4. O usuário digita a chave de recuperação e obtém acesso ao disco rígido.



Restaurando o acesso a um disco rígido criptografado pelo BitLocker

Restaurando o acesso a uma unidade do sistema

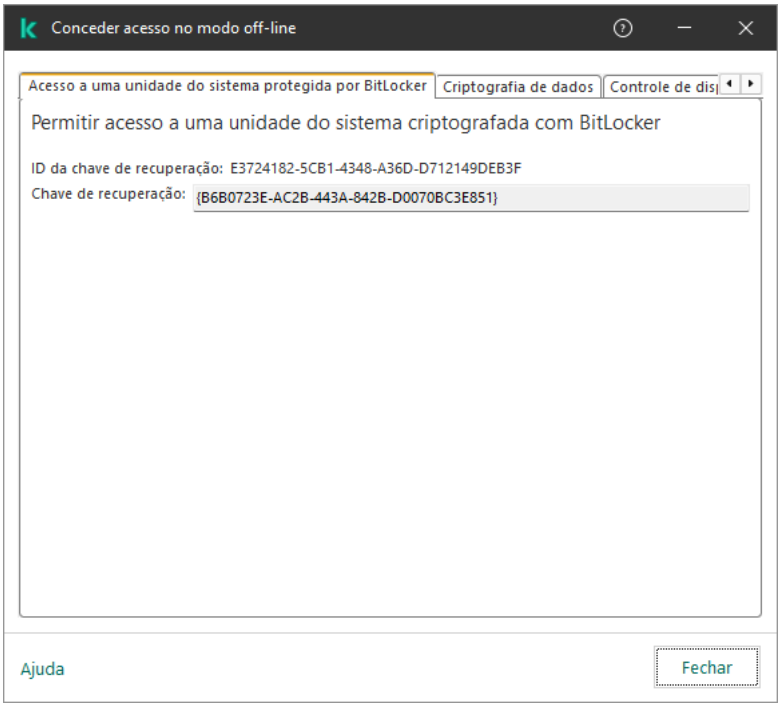
Para iniciar o procedimento de recuperação, o usuário precisa pressionar a tecla **Esc** no estágio de autenticação de pré-inicialização.

Como exibir a chave de recuperação de uma unidade do sistema criptografada pelo BitLocker no Console de administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Dispositivos gerenciados**.
3. Na guia **Dispositivos**, selecione o computador do usuário que solicitou acesso aos dados criptografados e clique com o botão direito para abrir o menu de contexto.
4. No menu de contexto, selecione **Conceder acesso no modo off-line**.
5. Uma janela será aberta; nessa janela, selecione a guia **Acesso a uma unidade do sistema protegida por BitLocker**.
6. Solicite ao usuário o ID de chave de recuperação indicado na janela de entrada de senha de BitLocker e compare-o com o ID no campo **ID da chave de recuperação**.

   Se os IDs não combinarem, essa chave não será válida para restaurar o acesso à unidade de sistema especificada. Assegure que o nome do computador selecionado combina com o nome do computador do usuário.

Como resultado, você terá acesso à chave de recuperação ou ao arquivo da chave de recuperação, que precisará ser transferida para o usuário.



Restaurar o acesso a uma unidade criptografada com BitLocker

Como exibir a chave de recuperação de uma unidade de sistema criptografada pelo BitLocker no Web Console e no Cloud Console

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

2. Marque a caixa de seleção ao lado do nome do computador cuja unidade você deseja restaurar o acesso.

3. Clique **Permitir acesso ao dispositivo em modo offline**.

4. Na janela exibida, selecione a seção **BitLocker**.

5. Verifique o ID da chave de recuperação. O ID fornecido pelo usuário deve corresponder ao ID exibido nas configurações do computador.

   Se os IDs não combinarem, essa chave não será válida para restaurar o acesso à unidade de sistema especificada. Assegure que o nome do computador selecionado combina com o nome do computador do usuário.

6. Clique **Receber chave**.

Como resultado, você terá acesso à chave de recuperação ou ao arquivo da chave de recuperação, que precisará ser transferida para o usuário.

Depois que o sistema operacional é carregado, o Kaspersky Endpoint Security solicita que o usuário altere a senha ou o código PIN. Depois de definir uma nova senha ou código do PIN, o BitLocker criará uma nova chave de recuperação para enviá-la ao Kaspersky Security Center. Como resultado, a chave de recuperação e o arquivo da chave de recuperação serão atualizados. Se o usuário não alterou a senha, você poderá usar a chave de recuperação antiga na próxima vez que o sistema operacional for carregado.

Os computadores com Windows 7 não permitem a alteração da senha ou do código PIN. Depois que a chave de recuperação for inserida e o sistema operacional for carregado, o Kaspersky Endpoint Security não solicitará a alteração da senha ou do código PIN pelo usuário. Assim, é impossível definir uma nova senha ou um código PIN. Esse problema é derivado das peculiaridades do sistema operacional. Para continuar, é necessário criptografar novamente o disco rígido.

Restaurar acesso a uma unidade que não é do sistema

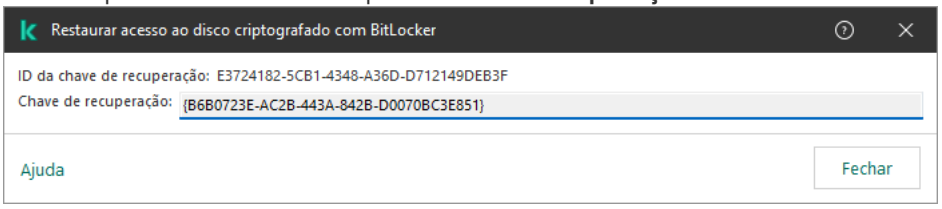
Para iniciar o procedimento de recuperação, o usuário precisa clicar no link **Forgot your password** na janela que fornece acesso à unidade. Após obter acesso à unidade criptografada, o usuário pode habilitar o desbloqueio automático da unidade durante a autenticação do Windows nas configurações do BitLocker.

Como exibir a chave de recuperação de uma unidade que não é do sistema criptografada pelo BitLocker no Console de administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do Console de Administração, selecione a pasta **Avançado** → **Criptografia e proteção de dados** → **Dispositivos criptografados**.
3. Na área de trabalho, selecione o dispositivo criptografado para o qual deseja criar um arquivo de chave de acesso e, no menu de contexto do dispositivo, clique em **Obter acesso ao dispositivo no Kaspersky Endpoint Security**.
4. Solicite ao usuário o ID de chave de recuperação indicado na janela de entrada de senha de BitLocker e compare-o com o ID no campo **ID da chave de recuperação**.

   Se os IDs não combinarem, esta chave não será válida para restaurar o acesso à unidade especificada. Assegure que o nome do computador selecionado combina com o nome do computador do usuário.

5. Envie ao usuário a chave que é indicada no campo **Chave de recuperação**.



Restaurar o acesso a uma unidade criptografada com BitLocker

Como exibir a chave de recuperação de uma unidade que não é do sistema criptografada pelo BitLocker no Web Console e no Cloud Console

1. Na janela principal do Web Console, selecione **Operações** → **Criptografia e proteção de dados** → **Dispositivos criptografados**.

2. Marque a caixa de seleção ao lado do nome do computador cuja unidade você deseja restaurar o acesso.

3. Clique **Permitir acesso ao dispositivo em modo offline**.

   Isso inicia o Assistente para conceder acesso a um dispositivo.

4. Siga as instruções do Assistente para conceder acesso a um dispositivo:

   a. Selecione o plug-in **Kaspersky Endpoint Security for Windows**

   b. Verifique o ID da chave de recuperação. O ID fornecido pelo usuário deve corresponder ao ID exibido nas configurações do computador.

   > Se os IDs não combinarem, essa chave não será válida para restaurar o acesso à unidade de sistema especificada. Assegure que o nome do computador selecionado combina com o nome do computador do usuário.

   c. Clique **Receber chave**.

Como resultado, você terá acesso à chave de recuperação ou ao arquivo da chave de recuperação, que precisará ser transferida para o usuário.

Pausa da proteção do BitLocker para atualizar o software

Há uma série de considerações especiais para atualizar o sistema operacional, instalar pacotes de atualização para o sistema operacional ou atualizar outro software com a proteção BitLocker ativada. A instalação de atualizações pode exigir a reinicialização do computador várias vezes. Após cada reinicialização, o usuário deve concluir a autenticação do BitLocker. Para garantir que as atualizações sejam instaladas corretamente, é possível desativar temporariamente a autenticação do BitLocker. Nesse caso, o disco permanece criptografado e o usuário tem acesso aos dados após entrar no sistema. Para gerenciar a autenticação do BitLocker, é possível usar a tarefa *Gerenciamento de proteção do BitLocker*. É possível usar a tarefa para especificar o número de reinicializações do computador que não exigem autenticação do BitLocker. Dessa forma, após as atualizações serem instaladas e a tarefa *Gerenciamento de proteção do BitLocker* ser concluída, a autenticação do BitLocker é ativada automaticamente. É possível ativar a autenticação do BitLocker a qualquer momento.

Como pausar a proteção do BitLocker usando o console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **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

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Gerenciamento de proteção do BitLocker**.

Etapa 2. Gerenciamento de proteção do BitLocker

Configure a autenticação do BitLocker. Para pausar a proteção do BitLocker, selecione **Permitir que a autenticação do BitLocker seja ignorada temporariamente** e insira o número de reinicializações sem autenticação do BitLocker (1 a 15 vezes). Caso seja necessário, insira uma data e hora de expiração para a tarefa. No horário especificado, a tarefa é desligada automaticamente, e o usuário deve concluir a autenticação do BitLocker quando o computador for reiniciado.

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. Definir o nome da tarefa

Digite o nome da tarefa, por exemplo *atualização para o Windows 10*.

Etapa 5. Concluir a criação da tarefa

Conclua o 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 pausar a proteção do BitLocker usando o Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **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 Endpoint Security for Windows**.
2. Na lista suspensa **Tipo de tarefa**, selecione **Gerenciamento de proteção do BitLocker**.
3. No campo **Nome da tarefa**, insira uma breve descrição, por exemplo, *Atualização para Windows 10*.
4. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

Etapa 2. Gerenciamento de proteção do BitLocker

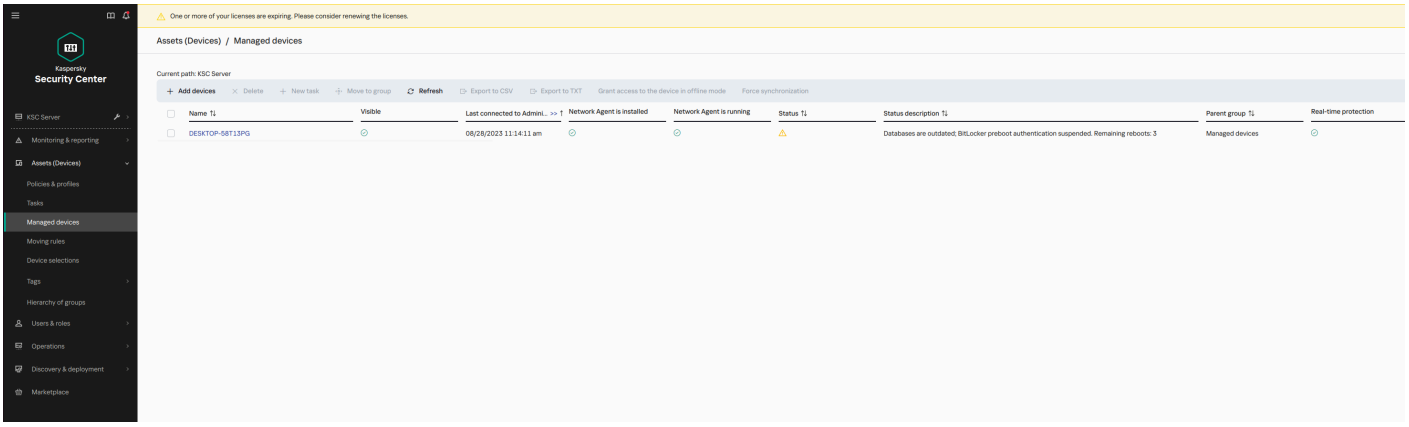
Configure a autenticação do BitLocker. Para pausar a proteção do BitLocker, selecione **Permitir que a autenticação do BitLocker seja ignorada temporariamente** e insira o número de reinicializações sem autenticação do BitLocker (1 a 15 vezes). Caso seja necessário, insira uma data e hora de expiração para a tarefa. No horário especificado, a tarefa é desligada automaticamente, e o usuário deve concluir a autenticação do BitLocker quando o computador for reiniciado.

Etapa 3. Concluir a criação da tarefa

Conclua o assistente. Uma nova tarefa será exibida na lista de tarefas.

Para executar uma tarefa, marque a caixa de seleção ao lado da tarefa e clique no botão **Iniciar**.

Como resultado, quando a tarefa está em execução, após a próxima reinicialização do computador, o BitLocker não solicita a autenticação do usuário. Após cada reinicialização do computador sem autenticação do BitLocker, o Kaspersky Endpoint Security gera um evento correspondente e registra o número de reinicializações restantes. O Kaspersky Endpoint Security então envia o evento ao Kaspersky Security Center para ser monitorado pelo administrador. Você também pode visualizar o número de reinicializações restantes na pasta **Dispositivos gerenciados** do console do Kaspersky Security Center na descrição do status do dispositivo.



A lista de dispositivos gerenciados

Quando o número especificado de reinicializações ou o tempo de expiração da tarefa é atingido, a autenticação do BitLocker é ativada automaticamente. Para obter acesso aos dados, o usuário deve concluir a autenticação do BitLocker.

Em computadores que executam o Windows 7, o BitLocker não pode contar as reinicializações do computador. A contagem de reinicializações em computadores com Windows 7 é feita pelo Kaspersky Endpoint Security. Portanto, para ativar automaticamente a autenticação do BitLocker após cada reinicialização, o Kaspersky Endpoint Security deve ser iniciado.

Para ativar a autenticação do BitLocker com antecedência, abra as propriedades da tarefa *Gerenciamento de proteção do BitLocker* e selecione a opção **Solicitar autenticação a cada pré-inicialização**.

Criptografia a Nível de Arquivo em unidades locais de computador

A criptografia de arquivos não é compatível com computadores baseados em Arm.

O componente estará disponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para computadores pessoais. O componente estará indisponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para servidores.

A criptografia de arquivos possui os seguintes recursos especiais:

- O Kaspersky Endpoint Security criptografa/descriptografa arquivos em pastas predefinidas apenas para perfis de usuários locais do sistema operacional. O Kaspersky Endpoint Security não criptografa ou descriptografa arquivos em pastas predefinidas de perfis de usuários móveis, perfis de usuários obrigatórios, perfis de usuários temporários ou em pastas redirecionadas.

- O Kaspersky Endpoint Security não criptografa arquivos cuja modificação possa prejudicar o sistema operacional e os aplicativos instalados. Por exemplo, os arquivos e pastas a seguir com todas as pastas aninhadas estão na lista de exclusões da criptografia:

  - %WINDIR%;

  - %PROGRAMFILES% e %PROGRAMFILES(X86)%;

  - Arquivos de registro do Windows.

  A lista de exclusões da criptografia não pode ser visualizada nem editada. Embora arquivos e pastas na lista de exclusões da criptografia possam ser adicionados à lista de criptografia, eles não serão criptografados durante a criptografia de arquivos.

Criptografia de arquivos em unidades de computadores locais

O Kaspersky Endpoint Security não criptografa arquivos localizados no armazenamento em nuvem do OneDrive ou em outras pastas que tenham OneDrive como nome. O Kaspersky Endpoint Security também bloqueia a cópia de arquivos criptografados para as pastas do OneDrive caso os arquivos não sejam adicionados à regra de descriptografia.

Para criptografar arquivos em unidades locais:

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Criptografia de dados** → **Criptografia em Nível de Arquivo**.
4. Na lista suspensa **Modo de criptografia**, selecione **De acordo com as regras**.
5. Na guia **Criptografia**, clique no botão **Adicionar** e, na lista suspensa, selecione um dos seguintes itens:
   a. Selecione o item de **Pastas predefinidas** para adicionar arquivos de pastas de perfis de usuário local sugeridos por peritos da Kaspersky a uma regra de criptografia.
      - **Documentos**. Arquivos na pasta *Documentos* padrão do sistema operacional e suas subpastas.
      - **Favoritos**. Arquivos na pasta *Favoritos* padrão do sistema operacional e suas subpastas.
      - **Área de trabalho**. Arquivos na pasta da *Área de trabalho* padrão do sistema operacional e suas subpastas.
      - **Arquivos temporários**. Arquivos temporários relacionados ao funcionamento de aplicativos instalados no computador. Por exemplo, os aplicativos do Microsoft Office criam arquivos temporários que contêm cópias de backup dos documentos.

        Não é recomendado criptografar arquivos temporários, pois isso pode causar perda de dados. Por exemplo, o Microsoft Word cria arquivos temporários ao processar um documento. Caso os arquivos temporários sejam criptografados e o arquivo original não for, o usuário poderá receber um erro de *Acesso Negado* ao tentar salvar o documento. Além disso, o Microsoft Word pode salvar o arquivo, mas não será possível abrir o documento na próxima vez, ou seja, os dados serão perdidos.

      - **Arquivos do Outlook**. Arquivos relacionados ao funcionamento do cliente de e-mail do Outlook: arquivos de dados (PST), arquivos de dados off-line (OST), arquivos de catálogo de endereços off-line (OAB) e arquivos de catálogo de endereços pessoal (PAB).
   b. Selecione o item **Pasta personalizada** para adicionar um caminho de pasta manualmente inserido a uma regra de criptografia.

Ao adicionar um caminho de pasta, siga as seguintes regras:

- Use uma variável de ambiente (por exemplo, `%FOLDER%\UserFolder\`). Você pode usar uma variável de ambiente apenas uma vez e apenas no início do caminho.
- Não use caminhos relativos.
- Não use os caracteres `*` e `?`.
- Não use caminhos UNC.
- Use `;` ou `,` como caracteres de separação.

c. Selecione o item **Arquivos por extensão** para adicionar extensões de arquivo individuais a uma regra de criptografia. O Kaspersky Endpoint Security criptografa arquivos com as extensões especificadas em todas as unidades do computador.

d. Selecione o item **Arquivos por grupos de extensões** para adicionar grupos de extensões de arquivo a uma regra de criptografia (por exemplo, *documentos do Microsoft Office*). O Kaspersky Endpoint Security criptografa arquivos apresentam as extensões listadas nos grupos de extensões em todas as unidades locais do computador.

6. Salvar alterações.

Logo que a política é aplicada, o Kaspersky Endpoint Security criptografa os arquivos que estão incluídos na regra de criptografia e não incluídos na regra de descriptografia.

A criptografia de arquivos possui os seguintes recursos especiais:

- Se o mesmo arquivo for adicionado às regras de criptografia e descriptografia, o Kaspersky Endpoint Security executará as seguintes ações:
  - Se não estiver criptografado, o Kaspersky Endpoint Security não criptografará esse arquivo.
  - Se estiver criptografado, o Kaspersky Endpoint Security descriptografa esse arquivo.
- O Kaspersky Endpoint Security continua a criptografar novos arquivos se esses arquivos atenderem aos critérios da regra de criptografia. Por exemplo, quando você altera as propriedades de um arquivo não criptografado (caminho ou extensão), o arquivo atende aos critérios da regra de criptografia. O Kaspersky Endpoint Security criptografa esse arquivo.
- Quando o usuário cria um novo arquivo cujas propriedades atendem aos critérios da regra de criptografia, o Kaspersky Endpoint Security criptografa o arquivo logo que ele é aberto.
- O Kaspersky Endpoint Security adia a criptografia de arquivos abertos até que eles sejam fechados.
- Se você mover um arquivo criptografado para outra pasta na unidade local, o arquivo permanece criptografado independente da pasta estar ou não na regra de criptografia.
- Se você descriptografar um arquivo e copiá-lo para outra pasta local que não esteja incluída na regra de descriptografia, uma cópia do arquivo poderá estar criptografada. Para impedir que o arquivo copiado seja criptografado, crie uma regra de descriptografia para a pasta de destino.

Formar regras de acesso a arquivos criptografados para aplicativos

Por padrão, todos os aplicativos funcionam com arquivos criptografados em um estado descriptografado. Se você usa frequentemente determinados aplicativos, como navegadores ou editores de texto, pode definir regras de acesso para proteger informações criptografadas.

Recomendamos criar uma regra de acesso aos arquivos criptografados para os navegadores Microsoft Internet Explorer e Microsoft Edge. Como esses navegadores funcionam dessa maneira, um arquivo criptografado será descriptografado automaticamente se for carregado em um site, como um serviço de armazenamento em nuvem. Isso pode causar vazamento de dados. Não é possível carregar um arquivo criptografado com esses navegadores. Recomendamos configurar a regra **Conceder acesso apenas a arquivos criptografados cifrados**. Não é necessário criar uma regra para outros navegadores (como o Google Chrome).

Para formar regras de acesso a arquivos criptografados para aplicativos:

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Criptografia de dados** → **Criptografia em Nível de Arquivo**.
4. Na lista suspensa **Modo de criptografia**, selecione **De acordo com as regras**.

   As regras de acesso são aplicadas somente quando no modo **De acordo com as regras**. Depois de aplicar as regras de acesso no modo **De acordo com as regras**, caso haja alteração para o modo **Manter inalterado**, o Kaspersky Endpoint Security ignorará todas as regras de acesso. Todos os aplicativos terão acesso a todos os arquivos criptografados.

5. Na parte direita da janela, selecione a guia **Regras para aplicativos**.
6. Se desejar selecionar aplicativos exclusivamente na lista do Kaspersky Security Center, clique no botão **Adicionar** e, na lista suspensa, selecione o item **Aplicativos da lista do Kaspersky Security Center**.

   a. Especifique os filtros para restringir a lista de aplicativos na tabela. Para fazer isso, especifique os valores dos parâmetros **Aplicativo**, **Fornecedor** e **Período adicionado** e todas as caixas de seleção do bloco **Grupo**.

   b. Clique **Atualizar**.

   c. A tabela lista os aplicativos que correspondem aos filtros aplicados.

   d. Na coluna **Aplicativo**, marque as caixas de seleção ao lado dos aplicativos para os quais se deseja formar as regras de acesso a arquivos criptografados.

e. Na lista suspensa **Regra para aplicativos**, selecione a regra que determinará o acesso de aplicativos a arquivos criptografados.

f. Na lista suspensa **Ações para aplicativos selecionados anteriormente**, selecione a ação a ser executada pelo Kaspersky Endpoint Security para as regras de acesso que foram formadas anteriormente para os aplicativos já mencionados.

Os detalhes de uma regra de acesso a arquivos criptografados para aplicativos aparecem em uma tabela na guia **Regras para aplicativos**.

7. Se desejar selecionar manualmente os aplicativos, clique no botão **Adicionar** e, na lista suspensa, selecione o item **Aplicativos personalizados**.

   a. No campo de entrada, digite o nomes ou uma lista de nomes de arquivos de aplicativos executáveis, incluindo suas extensões.

      Para adicionar nomes de arquivos executáveis dos aplicativos a partir da lista do Kaspersky Security Center, clique no botão **Adicionar da lista do Kaspersky Security Center**.

   b. Se necessário, no campo **Descrição**, insira uma descrição da lista de aplicativos.

   c. Na lista suspensa **Regra para aplicativos**, selecione a regra que determinará o acesso de aplicativos a arquivos criptografados.

   Os detalhes de uma regra de acesso a arquivos criptografados para aplicativos aparecem em uma tabela na guia **Regras para aplicativos**.

8. Salvar alterações.

Criptografar arquivos que são criados ou modificados por aplicativos específicos

Você pode criar uma regra segundo a qual o Kaspersky Endpoint Security criptografa todos os arquivos criados ou modificados pelos aplicativos especificados na regra.

> Os arquivos que foram criados ou modificados pelos aplicativos especificados antes da regra de criptografia ter sido aplicada não serão criptografados.

Para configurar a criptografia de arquivos que são criados ou modificados por aplicativos específicos:

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Criptografia de dados** → **Criptografia em Nível de Arquivo**.

4. Na lista suspensa **Modo de criptografia**, selecione **De acordo com as regras**.

> As regras de criptografia são aplicadas somente no modo **De acordo com as regras**. Depois de aplicar as regras de criptografia no modo **De acordo com as regras**, se você mudar para modo **Manter inalterado**, o Kaspersky Endpoint Security ignorará todas as regras de criptografia. Os arquivos que foram anteriormente criptografados permanecerão criptografados.

5. Na parte direita da janela, selecione a guia **Regras para aplicativos**.

6. Se desejar selecionar aplicativos exclusivamente na lista do Kaspersky Security Center, clique no botão **Adicionar** e, na lista suspensa, selecione o item **Aplicativos da lista do Kaspersky Security Center**.

   a. Especifique os filtros para restringir a lista de aplicativos na tabela. Para fazer isso, especifique os valores dos parâmetros **Aplicativo**, **Fornecedor** e **Período adicionado** e todas as caixas de seleção do bloco **Grupo**.

   b. Clique **Atualizar**.

      A tabela lista os aplicativos que correspondem aos filtros aplicados.

   c. Na coluna **Aplicativo**, marque as caixas de seleção próximas aos aplicativos cujos arquivos criados deseja criptografar.

   d. Na lista suspensa **Regra para aplicativos**, selecione **Criptografar todos os arquivos criados**.

   e. Na lista suspensa **Ações para aplicativos selecionados anteriormente**, selecione a ação a ser executada pelo Kaspersky Endpoint Security nas regras de criptografia de arquivos formadas anteriormente para os já mencionados aplicativos.

   As informações sobre a regra de criptografia de arquivos criados ou modificados pelos aplicativos selecionados aparecem na tabela na guia **Regras para aplicativos**.

7. Se desejar selecionar manualmente os aplicativos, clique no botão **Adicionar** e, na lista suspensa, selecione o item **Aplicativos personalizados**.

   a. No campo de entrada, digite o nomes ou uma lista de nomes de arquivos de aplicativos executáveis, incluindo suas extensões.

      Para adicionar nomes de arquivos executáveis dos aplicativos a partir da lista do Kaspersky Security Center, clique no botão **Adicionar da lista do Kaspersky Security Center**.

   b. Se necessário, no campo **Descrição**, insira uma descrição da lista de aplicativos.

   c. Na lista suspensa **Regra para aplicativos**, selecione **Criptografar todos os arquivos criados**.

   As informações sobre a regra de criptografia de arquivos criados ou modificados pelos aplicativos selecionados aparecem na tabela na guia **Regras para aplicativos**.

8. Salvar alterações.

Gerar uma regra de descriptografia

Para gerar uma regra de descriptografia:

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Criptografia de dados** → **Criptografia em Nível de Arquivo**.
4. Na lista suspensa **Modo de criptografia**, selecione **De acordo com as regras**.
5. Na guia **Descriptografia**, clique no botão **Adicionar** e, na lista suspensa, selecione um dos seguintes itens:
   a. Selecione o item **Pastas predefinidas** para adicionar arquivos de pastas de perfis de usuário local sugeridos por peritos do Kaspersky a uma regra de descriptografia.
   b. Selecione o item **Pasta personalizada** para adicionar um caminho de pasta inserido manualmente a uma regra de descriptografia.
   c. Selecione o item **Arquivos por extensão** para adicionar extensões de arquivo individuais a uma regra de descriptografia. O Kaspersky Endpoint Security não criptografa arquivos com as extensões especificadas em todas as unidades do computador.
   d. Selecione o item **Arquivos por grupos de extensões** para adicionar grupos de extensões de arquivo a uma regra de descriptografia (por exemplo, *Documentos do Microsoft Office*). O Kaspersky Endpoint Security não criptografa arquivos que apresentam as extensões listadas nos grupos de extensões em todas as unidades locais do computador.
6. Salvar alterações.

Se o mesmo arquivo foi adicionado à lista de criptografia e descriptografia, o Kaspersky Endpoint Security não o criptografa se ele não estiver criptografado e o descriptografa se ele estiver criptografado.

Descriptografar arquivos em unidades de computadores locais

Para descriptografar arquivos em unidades locais:

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Criptografia de dados** → **Criptografia em Nível de Arquivo**.
4. Na parte direita da janela, selecione a guia **Criptografia**.

5. Remova da lista de criptografia os arquivos e pastas que você deseja descriptografar. Para isso, selecione os arquivos e o item **Excluir regra e descriptografar arquivos** no menu de contexto do botão **Excluir**.

   Os arquivos e pastas removidos da lista de criptografia são automaticamente adicionados à lista de descriptografia.

6. Forme a lista de descriptografia.

7. Salvar alterações.

Assim que a política é aplicada, o Kaspersky Endpoint Security descriptografa os arquivos criptografados adicionados à lista de descriptografia.

O Kaspersky Endpoint Security descriptografará os arquivos criptografados se seus parâmetros (caminho/nome/extensão do arquivo) se alterarem para corresponder aos parâmetros dos objetos que foram adicionados à lista de descriptografia.

O Kaspersky Endpoint Security adia a descriptografia de arquivos abertos até que eles sejam fechados.

Criar pacotes criptografados

Para proteger seus dados ao enviar arquivos para usuários fora da rede corporativa, você pode usar pacotes criptografados. Pacotes criptografados podem ser convenientes para a transferência de arquivos grandes em unidades removíveis, pois os programas de e-mail têm restrições de tamanho de arquivo.

Antes de criar pacotes criptografados, o Kaspersky Endpoint Security solicitará uma senha ao usuário. Para proteger os dados de forma confiável, você pode ativar a verificação de força da senha e especificar os requisitos de força da senha. Isto evitará que os usuários utilizem senhas curtas e simples, por exemplo, `1234`.

Como ativar a verificação de força da senha ao criar arquivos compactados criptografados no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Criptografia de dados** → **Configurações comuns de criptografia**.

4. No bloco **Configurações da senha**, clique no botão **Configurações**.

5. Uma janela será aberta; nessa janela, selecione a guia **Pacotes criptografados**.

6. Configure as configurações de complexidade da senha ao criar pacotes criptografados.

Como ativar a verificação de força da senha ao criar arquivos compactados criptografados no Web Console

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

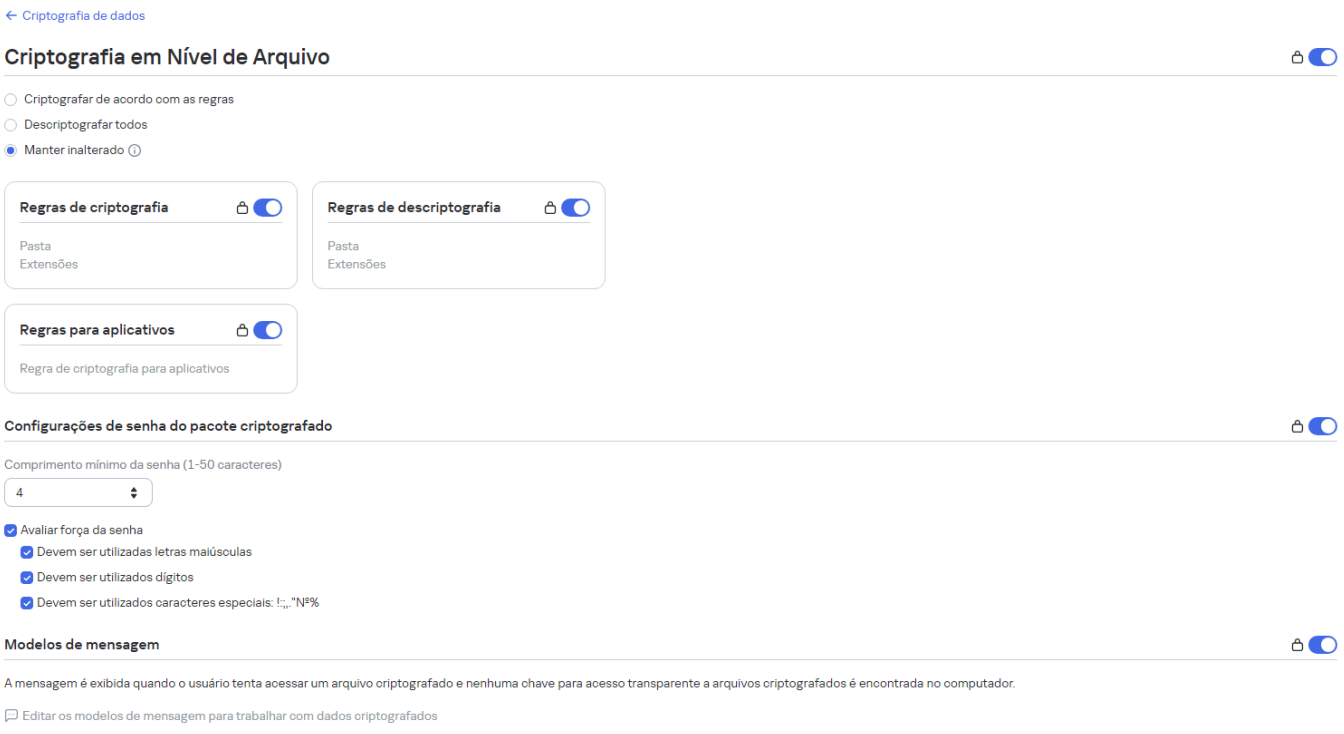
2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é exibida.

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

4. Selecione **Criptografia de dados** → **Criptografia em Nível de Arquivo**.

5. No bloco **Configurações de senha do pacote criptografado**, configure os critérios de força de senha necessários ao criar pacotes criptografados.



Configurações de criptografia de arquivo

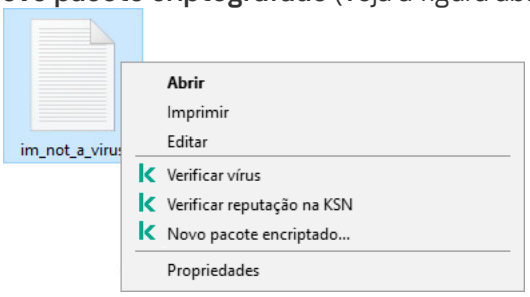
Você pode criar pacotes criptografados em computadores que tenham o Kaspersky Endpoint Security instalado com a Criptografia a nível de arquivo disponível.

> Ao adicionar um arquivo ao pacote criptografado cujo conteúdo reside no armazenamento em nuvem do OneDrive, o Kaspersky Endpoint Security baixa o conteúdo do arquivo e executa a criptografia.

Para criar um pacote criptografado:

1. Em qualquer gerenciador de arquivos, selecione os arquivos ou pastas que você deseja adicionar ao pacote criptografado. Clique com o botão direito do mouse para abrir o menu de contexto.

2. No menu de contexto, selecione **Novo pacote criptografado** (veja a figura abaixo).



Criar um pacote criptografado

3. Na janela exibida, especifique a senha e confirme-a.

   A senha deve atender aos critérios de complexidade especificados na política.

4. Clique **Criar**.

   O processo de criação do pacote criptografado é iniciado. O Kaspersky Endpoint Security não executa a compressão de arquivos ao criar um pacote criptografado. Quando o processo termina, um pacote criptografado autoextraível protegido por senha (um arquivo executável com a extensão .exe -) é criado na pasta de destino selecionada.

Para acessar arquivos em um pacote criptografado, clique duas vezes nele para iniciar o Assistente de descompactação e digite a senha. Se você esqueceu ou perdeu sua senha, não é possível recuperá-la e acessar os arquivos no pacote criptografado. Você pode recriar o pacote criptografado.

Restaurar acesso aos arquivos criptografados.

Quando os arquivos são criptografados, o Kaspersky Endpoint Security recebe uma chave de criptografia necessária para acessar diretamente os arquivos criptografados. Usando essa chave de criptografia, um usuário com qualquer conta Windows que esteve ativa durante a criptografia do arquivo pode acessar os arquivos criptografados diretamente. Um usuário com contas Windows que esteve inativo durante a criptografia do arquivo tem que se conectar ao Kaspersky Security Center para acessar os arquivos criptografados.

Os arquivos criptografados podem ser não acessíveis nas seguintes circunstâncias:

- O computador do usuário armazena chaves de criptografia, mas não há conexão ao Kaspersky Security Center para o gerenciamento das chaves. Neste caso, o usuário deve solicitar acesso aos arquivos criptografados junto ao administrador da rede local.

  Se o acesso ao Kaspersky Security Center não existir, você deve:

  - solicitar uma chave de acesso o acesso a arquivos criptografados em discos rígidos de computador;
  - para acessar arquivos criptografados que estão armazenados em unidades removíveis, solicite chaves de acesso em separado para arquivos criptografados em cada unidade removível.

- Os componentes de criptografia são excluídos do computador do usuário. Neste evento, o usuário pode abrir arquivos criptografados em discos removíveis e locais, mas os conteúdos daqueles arquivos parecerão criptografados.

  O usuário pode trabalhar com arquivos criptografados nas seguintes circunstâncias:

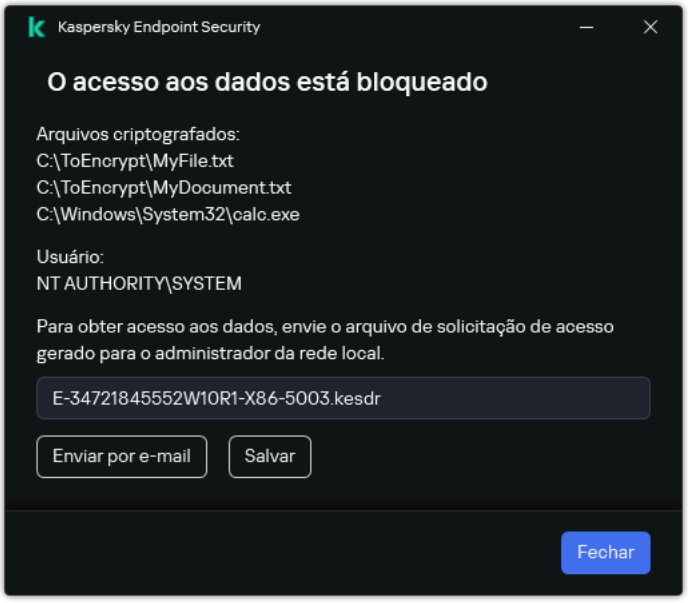
  - Os arquivos são colocados dentro de pacotes criptografados criados em um computador com o Kaspersky Endpoint Security instalado.
  - Os arquivos são armazenados em unidades removíveis nas quais o modo portátil foi permitido.

Para obter acesso aos arquivos criptografados, o usuário precisa iniciar o procedimento de recuperação (solicitação e resposta).

A recuperação de acesso a arquivos criptografados consiste nas seguintes etapas:

1. O usuário envia um arquivo de solicitação de acesso ao administrador (veja a figura abaixo).
2. O administrador adiciona o arquivo de solicitação de acesso ao Kaspersky Security Center, cria um arquivo de chave de acesso e envia-o ao usuário.

3. O usuário adiciona o arquivo da chave de acesso ao Kaspersky Endpoint Security e obtém acesso aos arquivos.



Restaurar acesso aos arquivos criptografados.

Para iniciar o procedimento de recuperação, o usuário precisa tentar acessar um arquivo. Como resultado, o Kaspersky Endpoint Security criará um arquivo de solicitação de acesso (um arquivo com a extensão KESDC), que o usuário precisará enviar ao administrador, por exemplo, por e-mail.

O Kaspersky Endpoint Security gera um arquivo de solicitação de acesso para acessar todos os arquivos criptografados armazenados na unidade do computador (unidade local ou removível).

Como obter um arquivo de chave de acesso a dados criptografados no Console de administração (MMC)

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

2. Na árvore do console, selecione **Dispositivos**.

3. Na guia **Dispositivos**, selecione o computador do usuário que solicitou acesso aos dados criptografados e clique com o botão direito para abrir o menu de contexto.

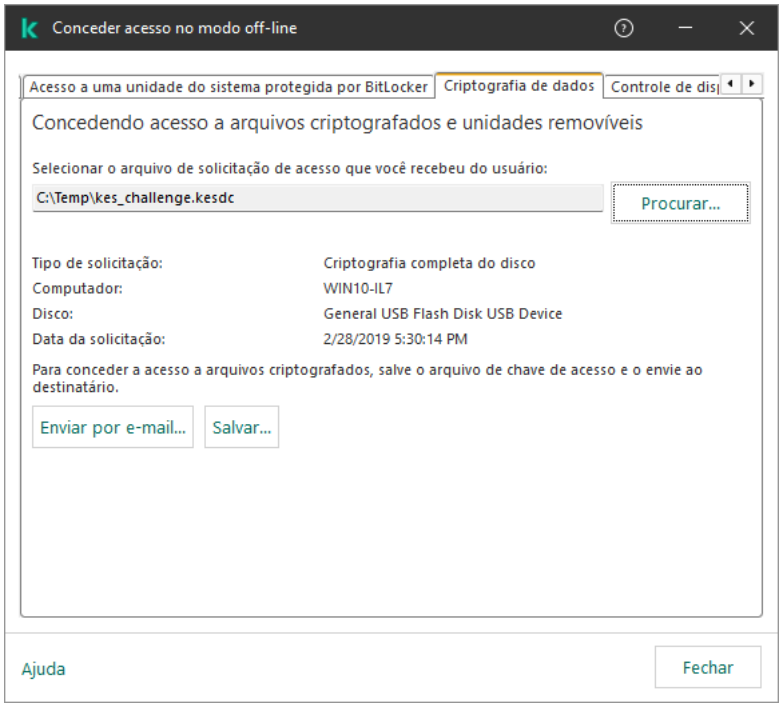
4. No menu de contexto, selecione **Conceder acesso no modo off-line**.

5. Uma janela será aberta; nessa janela, selecione a guia **Criptografia de dados**.

6. Na guia **Criptografia de dados**, clique no botão **Procurar**.

7. Na janela para selecionar um arquivo de solicitação de acesso, especifique o caminho para o arquivo recebido do usuário.

Você verá informações sobre a solicitação do usuário. O Kaspersky Security Center gera um arquivo de chave. Envie por e-mail o arquivo de chave de acesso a dados criptografados gerado para o usuário. Ou salve o arquivo de acesso e use qualquer método disponível para transferir o arquivo.



Concessão de acesso no modo off-line

Como obter um arquivo de chave de acesso a dados criptografados no Web Console

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

2. Marque a caixa de seleção ao lado do nome do computador cujos dados você deseja restaurar o acesso.

3. Clique **Permitir acesso ao dispositivo em modo offline**.

4. Selecione **Criptografia de dados**.

5. Clique no botão **Selecionar arquivo** e selecione o arquivo de solicitação de acesso que você recebeu do usuário (um arquivo com a extensão KESDC).

   O Web Console exibirá informações sobre a solicitação. Isso incluirá o nome do computador no qual o usuário está solicitando acesso ao arquivo.

6. Clique no botão **Salvar chave** e selecione uma pasta para salvar o arquivo de chave de acesso a dados criptografados (um arquivo com a extensão KESDR).

Como resultado, você poderá obter a chave de acesso a dados criptografados, que precisará transferir para o usuário.

Após receber o arquivo de chave de acesso a dados criptografados, o usuário precisa clicar nele duas vezes para executá-lo. Como resultado, o Kaspersky Endpoint Security concederá acesso a todos os arquivos criptografados armazenados na unidade. Para acessar arquivos criptografados armazenados em outras unidades, você deve obter um arquivo de chave de acesso em separado para cada unidade.

Restaurar o acesso a dados criptografados após falha no sistema operacional

Você pode restaurar o acesso aos dados após falha do sistema operacional somente para Criptografia a Nível de Arquivo (FLE, File Level Encryption). Você não pode restaurar o acesso aos dados se a Criptografia Completa do Disco (FDE, Full Disk Encryption) for usada.

Para restaurar o acesso a dados criptografados após falha no sistema operacional:

1. Reinstale o sistema operacional sem formatar o disco rígido.
2. Instalar o Kaspersky Endpoint Security.
3. Estabeleça uma conexão entre o computador e o Servidor de Administração do Kaspersky Security Center que controlou o computador quando os dados foram criptografados.

   O acesso aos dados criptografados será concedido sob as mesmas condições aplicadas antes da falha no sistema operacional.

Editar modelos de mensagens de acesso a arquivos criptografados

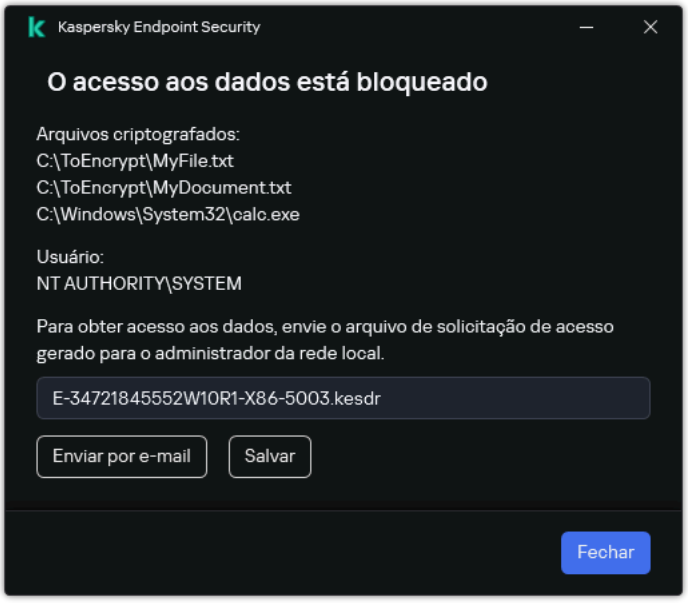
Para editar modelos de mensagens de acesso a arquivos criptografados:

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Criptografia de dados** → **Configurações comuns de criptografia**.
4. No bloco **Modelos**, clique no botão **Modelos**.
5. Na janela que é aberta, faça o seguinte:
   - Se desejar editar o modelo de mensagem do usuário, selecione a guia **Mensagem do usuário**. A janela a seguir é aberta quando o usuário tentar acessar um arquivo criptografado e não há uma chave disponível no computador para acessar os arquivos criptografados (ver figura abaixo). Ao clicar no botão **Enviar por e-mail**, uma mensagem de usuário é criada automaticamente. Esta mensagem é enviada ao administrador da rede local corporativa junto com o arquivo solicitando acesso a arquivos criptografados.
   - Se desejar editar o modelo de mensagem do administrador, selecione a guia **Mensagem do administrador**. O usuário recebe essa mensagem após o acesso aos arquivos criptografados ser concedido.
6. Edite os modelos de mensagem.

   Para inserir uma variável no modelo, posicione o cursor onde necessário, clique em **Variável** e selecione a opção necessária na lista.

   Você também pode restaurar o texto original do modelo clicando no botão **Por padrão**.

7. Salvar alterações.



Restaurar acesso aos arquivos criptografados.

Criptografia de unidades removíveis

A criptografia de unidades removíveis não é compatível em computadores baseados em Arm.

O componente estará disponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para computadores pessoais. O componente estará indisponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para servidores.

O Kaspersky Endpoint Security tem suporte para criptografia de arquivos nos sistemas de arquivos FAT32 e NTFS. Se uma unidade removível com um sistema de arquivos sem suporte for conectada ao computador, a tarefa de criptografia dessa unidade removível terminará com um erro, e o Kaspersky Endpoint Security atribuirá o status somente leitura à unidade removível.

Para proteger dados em unidades removíveis, você pode usar os seguintes tipos de criptografia:

- Full Disk Encryption (FDE).

  Criptografia de toda a unidade removível, incluindo o sistema de arquivos.

  Não é possível acessar dados criptografados fora da rede corporativa. Também é impossível acessar dados criptografados dentro da rede corporativa se o computador não estiver conectado ao Kaspersky Security Center (por exe., em um computador convidado).

- File Level Encryption (FLE).

  Criptografia de apenas arquivos em uma unidade removível. O sistema de arquivos permanece inalterado.

A criptografia de arquivos em unidades removíveis fornece a capacidade de acessar dados fora da rede corporativa usando um modo especial chamado *modo portátil*.

Durante a criptografia, o Kaspersky Endpoint Security cria uma chave mestra. O Kaspersky Endpoint Security salva a chave mestra nos seguintes repositórios:

- Kaspersky Security Center.
- Computador do usuário.

  A chave mestra é criptografada com a chave secreta do usuário.
- Unidade removível.

  A chave mestra é criptografada com a chave pública do Kaspersky Security Center.

Depois que a criptografia estiver concluída, os dados na unidade removível podem ser acessados dentro da rede corporativa, como se estivesse em uma unidade removível comum, sem criptografia.

Acesso a dados criptografados

Quando uma unidade removível com dados criptografados é conectada, o Kaspersky Endpoint Security executa as seguintes ações:

1. Verifica se há uma chave mestra no armazenamento local no computador do usuário.

   Se a chave mestra for encontrada, o usuário obterá acesso aos dados na unidade removível.

   Se a chave mestra não for encontrada, o Kaspersky Endpoint Security executa as seguintes ações:

   a. Envia uma solicitação ao Kaspersky Security Center.

      Após receber a solicitação, o Kaspersky Security Center envia uma resposta que contém a chave mestra.

   b. O Kaspersky Endpoint Security salva a chave mestra no armazenamento local no computador do usuário para operações subsequentes com a unidade removível criptografada.
2. Descriptografa os dados.

Recursos especiais de criptografia de unidade removível

A criptografia de unidades removíveis possui os seguintes recursos especiais:

- A política com configurações predefinidas para criptografia de unidades removíveis é formada por um grupo específico de computadores gerenciados. Portanto, o resultado de aplicar a política do Kaspersky Security Center configurada para criptografia/descriptografia de unidades removíveis depende do computador ao qual a unidade removível está conectada.
- O Kaspersky Endpoint Security não criptografa/descriptografa arquivos de somente leitura armazenados em unidades removíveis.

- Os tipos de dispositivo a seguir têm suporte como unidades removíveis:
  - mídia de dados conectadas por barramento USB
  - discos rígidos conectados por barramento USB e FireWire
  - unidades SSD conectadas por barramento USB e FireWire

Iniciar a criptografia de unidades removíveis

Você pode usar uma política para descriptografar uma unidade removível. Uma política com configurações definidas para criptografia de unidade removível é gerada para um grupo de administração específico. Portanto, o resultado da descriptografia de dados em unidades removíveis dependo do computador em que a unidade removível for conectado.

O Kaspersky Endpoint Security tem suporte para criptografia de arquivos nos sistemas de arquivos FAT32 e NTFS. Se uma unidade removível com um sistema de arquivos sem suporte for conectada ao computador, a tarefa de criptografia dessa unidade removível terminará com um erro, e o Kaspersky Endpoint Security atribuirá o status somente leitura à unidade removível.

Antes de criptografar arquivos em uma unidade removível, verifique se ela está formatada e se não há partições ocultas (como uma partição de sistema EFI). Se a unidade contiver partições não formatadas ou ocultas, a criptografia de arquivo pode falhar.

Para criptografar unidades removíveis:

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Criptografia de dados** → **Criptografia de unidades removíveis**.
4. Na lista suspensa **Modo de criptografia**, selecione a ação padrão que você deseja que o Kaspersky Endpoint Security execute em unidades removíveis:
   - **Criptografar toda a unidade removível** (FDE). Kaspersky Endpoint Security criptografa o conteúdo de uma unidade removível setor por setor. Como resultado, o aplicativo criptografa não apenas os arquivos armazenados na unidade removível, mas também seus sistemas de arquivos, incluindo os nomes de arquivos e estruturas de pastas na unidade removível.
   - **Criptografar todos os arquivos** (FLE). O Kaspersky Endpoint Security criptografa todos os arquivos armazenados em unidades removíveis. O aplicativo não criptografa os sistemas de arquivo de unidades removíveis, incluindo os nomes de arquivos e estruturas de pastas.
   - **Criptografar apenas novos arquivos** (FLE). O Kaspersky Endpoint Security criptografa apenas os arquivos que foram adicionados a unidades removíveis ou que foram armazenados em unidades removíveis e foram modificados após a última aplicação da política do Kaspersky Security Center.

   O Kaspersky Endpoint Security não criptografa unidades removíveis que já foram criptografadas.

5. Se você quiser usar o modo portátil para criptografia de unidades removíveis, selecione a caixa de seleção **Modo portátil**.

   Modo portátil é um modo de criptografia de arquivos (FLE) em unidades removíveis que fornece a capacidade de acessar dados fora de uma rede corporativa. O modo portátil também permite trabalhar com dados criptografados em computadores que não tenham o Kaspersky Endpoint Security instalado.

6. Se você quiser criptografar uma nova unidade removível, é recomendável marcar a caixa de seleção **Criptografar somente espaço usado em disco**. Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security criptografará todos os arquivos, incluindo os fragmentos residuais de arquivos excluídos ou modificados.

7. Se você quiser configurar a criptografia para unidades removíveis individuais, defina as regras de criptografia.

8. Caso queira usar a criptografia completa de unidades removíveis no modo off-line, marque a caixa de seleção **Permitir criptografia de unidades removíveis no modo off-line**.

   O modo de criptografia off-line refere-se a criptografia de unidades removíveis (FDE) quando não há conexão com o Kaspersky Security Center. Durante a criptografia, o Kaspersky Endpoint Security salva a chave mestra somente no computador do usuário. O Kaspersky Endpoint Security enviará a chave mestra para o Kaspersky Security Center durante a próxima sincronização.

   > Se o computador no qual a chave mestra está guardada estiver corrompido e os dados não forem enviados para o Kaspersky Security Center, não será possível obter acesso à unidade removível.

   Caso a caixa de seleção **Permitir criptografia de unidades removíveis no modo off-line** esteja desmarcada e não houver conexão com o Kaspersky Security Center, a criptografia de unidade removível não será possível.

9. Salvar alterações.

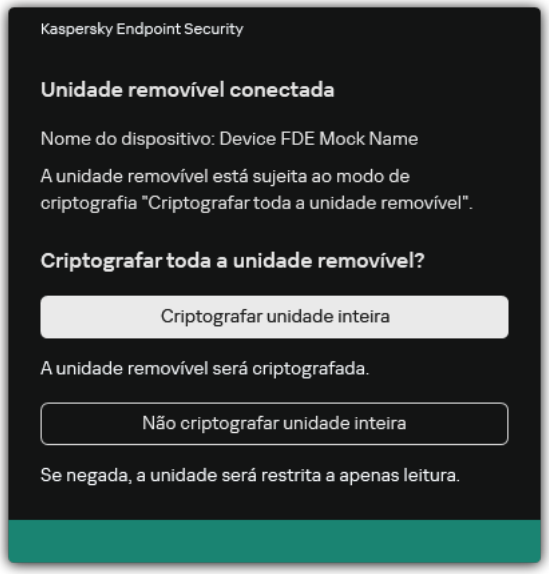
Após a aplicação da política, quando o usuário conecta uma unidade removível ou se uma unidade removível já estiver conectada, o Kaspersky Endpoint Security solicita ao usuário a confirmação para realizar a operação de criptografia (consulte a figura abaixo).

O aplicativo permite que você execute as seguintes ações:

- Se o usuário confirmar a solicitação de criptografia, o Kaspersky Endpoint Security criptografa os dados.
- Se o usuário recusar a solicitação de criptografia, o Kaspersky Endpoint Security deixa os dados inalterados e atribui acesso de somente leitura a essa unidade removível.
- Se o usuário não responder a solicitação de criptografia, o Kaspersky Endpoint Security deixa os dados inalterados e atribui acesso de somente leitura a essa unidade removível. O aplicativo solicita confirmação novamente ao aplicar posteriormente uma política ou na próxima vez que essa unidade removível for conectada.

Se o usuário iniciar a remoção com segurança de uma unidade removível durante a criptografia de dados, o Kaspersky Endpoint Security interrompe a criptografia de dados e permite a remoção da unidade removível antes que o processo de criptografia seja concluído. A criptografia de dados será continuada na próxima vez que a unidade removível for conectada a este computador.

Caso a criptografia de uma unidade removível falhe, visualize o relatório **Criptografia de dados** na interface do Kaspersky Endpoint Security. O acesso a arquivos pode ser bloqueado por outro aplicativo. Neste caso, tente desconectar a unidade removível do computador e conectá-la novamente.



Solicitação de criptografia de unidade removível

Adicionar uma regra de criptografia para unidades removíveis:

Para adicionar uma regra de criptografia para unidades removíveis:

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Criptografia de dados** → **Criptografia de unidades removíveis**.
4. Clique no botão **Adicionar** e, na lista suspensa, selecione um dos seguintes itens:
   - Se desejar adicionar regras de criptografia para unidades removíveis que estão na lista de dispositivos confiáveis do componente Controle de Dispositivos, selecione **Da lista de dispositivos confiáveis desta política**.
   - Se desejar adicionar regras de criptografia para unidades removíveis que estão na lista do Kaspersky Security Center, selecione **Da lista de dispositivos do Kaspersky Security Center**.
5. Na lista suspensa **Modo de criptografia para dispositivos selecionados**, selecione a ação a ser executada pelo Kaspersky Endpoint Security em arquivos armazenados nas unidades removíveis selecionadas.

6. Marque a caixa de seleção **Modo portátil** se desejar que o Kaspersky Endpoint Security prepare as unidades removíveis antes da criptografia, tornando possível usar arquivos criptografados armazenados nessas unidades no modo portátil.

   O modo portátil permite que você utilize arquivos criptografados armazenados nas unidades removíveis que estão conectadas a computadores sem a funcionalidade de criptografia.

7. Marque a caixa de seleção **Criptografar somente espaço usado em disco** se desejar que o Kaspersky Endpoint Security criptografe somente aqueles setores de disco que são ocupados por arquivos.

   Se você estiver aplicando a criptografia em uma unidade que já está em uso, recomenda-se criptografar a unidade inteira. Isto assegura que todos os dados estejam protegidos, até os dados excluídos que ainda podem conter informações recuperáveis. A função **Criptografar somente espaço usado em disco** é recomendada para novas unidades que não foram usadas anteriormente.

   Se um dispositivo tiver sido previamente criptografado usando a função **Criptografar somente espaço usado em disco**, depois de aplicar uma política no modo **Criptografar toda a unidade removível**, os setores que não estejam ocupados por arquivos ainda não serão criptografados.

8. Na lista suspensa **Ações para dispositivos selecionados anteriormente**, selecione a ação a ser executada pelo Kaspersky Endpoint Security de acordo com as regras de criptografia que foram definidas anteriormente para unidades removíveis.

   - Se desejar que a regra de criptografia anteriormente criada da unidade removível permaneça inalterada, selecione **Ignorar**.
   - Se quiser que a regra de criptografia criada anteriormente para a unidade removível seja substituída pela nova regra, selecione **Atualizar**.

9. Salvar alterações.

As regras de criptografia adicionadas para unidades removíveis serão aplicadas às unidades removíveis conectadas a qualquer computador na organização.

Exportar e importar uma lista de regras de criptografia para unidades removíveis

Você pode exportar a lista de regras de criptografia de unidade removível para um arquivo XML. Em seguida, você pode modificar o arquivo para, por exemplo, adicionar um grande número de regras para o mesmo tipo de unidades removíveis. Você também pode usar a função de exportação/importação para fazer backup da lista de regras ou para migrar as regras para um servidor diferente.

Como exportar e importar uma lista de regras de criptografia de unidade removível no Console de Administração (MMC)

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Criptografia de dados** → **Criptografia de unidades removíveis**.

5. No bloco **Regras de criptografia para dispositivos selecionados**, clique no link **<N> regras**.

   Aparecerá uma lista de regras de criptografia para unidades removíveis.

6. Para exportar a lista de regras de criptografia para unidades removíveis:

   a. Selecione as regras que deseja exportar.

   b. Clique **Exportar**.

   c. Confirme se deseja exportar apenas as regras selecionadas ou exportar a lista inteira.

   d. Salvar o arquivo.

      O Kaspersky Endpoint Security exporta a lista de regras para um arquivo XML na pasta de downloads padrão.

7. Para importar a lista de regras:

   a. Clique no link **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 Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

8. Salvar alterações.

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Criptografia de dados** → **Criptografia de unidades removíveis**.

4. Para exportar a lista de regras de criptografia para unidades removíveis:

   a. Selecione as regras que deseja exportar. Para selecionar várias portas, use as teclas **`CTRL`** ou **`SHIFT`**.

      Se você não selecionou nenhuma regra, o Kaspersky Endpoint Security exportará todas as regras.

   b. Clique no link **Exportar**.

   c. 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.

   d. Salvar o arquivo.

      O Kaspersky Endpoint Security exporta toda a lista de regras para o arquivo XML.

5. Para importar uma lista de regras de criptografia para unidades removíveis:

   a. Clique no link **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 Endpoint Security solicitará que você exclua a lista existente ou adicione novas entradas a ela a partir do arquivo XML.

6. Salvar alterações.

Modo portátil para acessar arquivos criptografados em unidades removíveis

Modo portátil é um modo de criptografia de arquivos (FLE) em unidades removíveis que fornece a capacidade de acessar dados fora de uma rede corporativa. O modo portátil também permite trabalhar com dados criptografados em computadores que não tenham o Kaspersky Endpoint Security instalado.

O modo portátil é conveniente para uso nos seguintes casos:

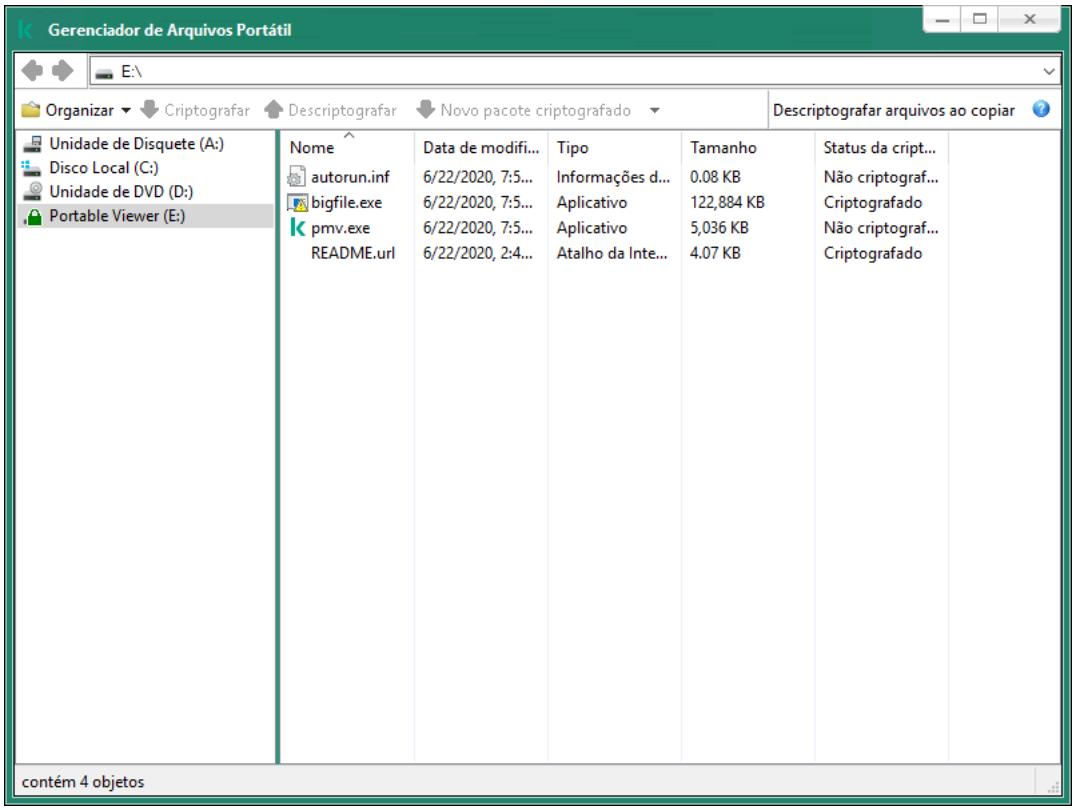
- Não há conexão entre o computador e o Servidor de Administração do Kaspersky Security Center.
- A infraestrutura mudou com a alteração do Servidor de Administração do Kaspersky Security Center.
- O Kaspersky Endpoint Security não está instalado no computador.

Gerenciador de Arquivos Portátil

Para trabalhar no modo portátil, o Kaspersky Endpoint Security instala um módulo de criptografia especial chamado *Gerenciador de arquivos portátil* em uma unidade removível. O Gerenciador de arquivos portátil fornece uma interface para trabalhar com dados criptografados se o Kaspersky Endpoint Security não estiver instalado no computador (veja a figura abaixo). Se o Kaspersky Endpoint Security estiver instalado no seu computador, você poderá trabalhar com unidades removíveis criptografadas usando o gerenciador de arquivos usual (por exemplo, o Explorer).

O Gerenciador de arquivos portátil armazena uma chave para criptografar arquivos em uma unidade removível. A chave é criptografada com a senha do usuário. O usuário define uma senha antes de criptografar arquivos em uma unidade removível.

O Gerenciador de arquivos portátil inicia automaticamente quando uma unidade removível é conectada a um computador no qual o Kaspersky Endpoint Security não está instalado. Se a inicialização automática de aplicativos estiver desativada no computador, inicie manualmente o Gerenciador de arquivos portátil. Para fazer isso, execute o arquivo chamado pmv.exe que está armazenado na unidade removível.



Gerenciador de Arquivos Portátil

Suporte para o modo portátil para trabalhar com arquivos criptografados

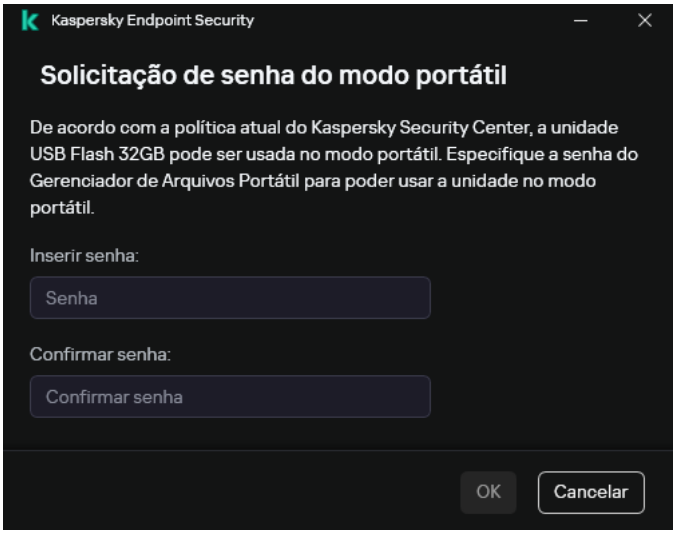
Como ativar o suporte ao modo portátil para trabalhar com arquivos criptografados em unidades removíveis no Console de administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Criptografia de dados** → **Criptografia de unidades removíveis**.
4. Na lista suspensa **Modo de criptografia para dispositivos selecionados**, selecione **Criptografar todos os arquivos** ou **Criptografar apenas novos arquivos**.

   O modo portátil está disponível apenas com Criptografia a nível de arquivo (FLE). Não é possível ativar o suporte ao modo portátil para Criptografia completa do disco (FDE).

5. Marque a caixa de seleção **Modo portátil**.
6. Se necessário, adicione regras de criptografia para unidades removíveis individuais.
7. Salvar alterações.
8. Após aplicar a diretiva, conecte a unidade removível ao computador.
9. Confirme a operação de criptografia de unidade removível.

Com isso, uma janela é aberta na qual é possível criar uma senha do gerenciador de arquivos portátil.



Solicitação de senha do modo portátil

10. Especifique uma senha que atende aos requisitos de força e confirme-o.

11. Salvar alterações.

Como ativar o suporte ao modo portátil para trabalhar com arquivos criptografados em unidades removíveis no Web Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Criptografia de dados** → **Criptografia de unidades removíveis**.

5. No bloco **Ação padrão**, selecione **Criptografar todos os arquivos** ou **Criptografar apenas novos arquivos**.

   O modo portátil está disponível apenas com Criptografia a nível de arquivo (FLE). Não é possível ativar o suporte ao modo portátil para Criptografia completa do disco (FDE).

6. Marque a caixa de seleção **Modo portátil**.

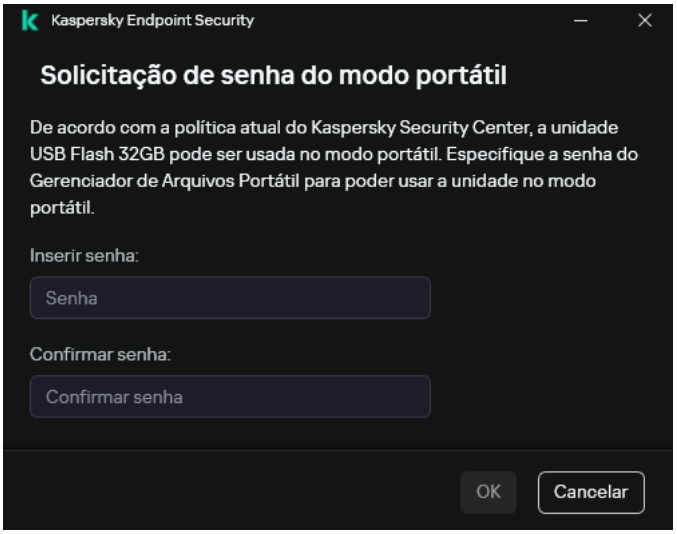
7. Se necessário, adicione regras de criptografia para unidades removíveis individuais.

8. Salvar alterações.

9. Após aplicar a diretiva, conecte a unidade removível ao computador.

10. Confirme a operação de criptografia de unidade removível.

Com isso, uma janela é aberta na qual é possível criar uma senha do gerenciador de arquivos portátil.



Solicitação de senha do modo portátil

11. Especifique uma senha que atende aos requisitos de força e confirme-o.

12. Salvar alterações.

O Kaspersky Endpoint Security criptografará arquivos na unidade removível. O gerenciador de arquivos portátil usado para funcionar com arquivos criptografados também será gravado na unidade removível. Se já houver arquivos criptografados na unidade removível, o Kaspersky Endpoint Security os criptografará novamente usando sua própria chave. Isso permite que o usuário acesse todos os arquivos na unidade removível no modo portátil.

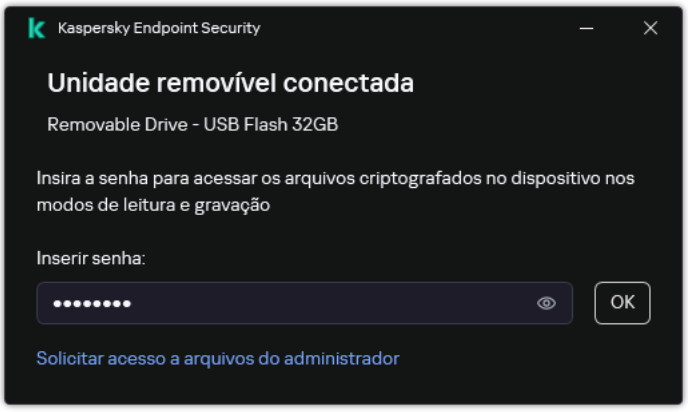
Acessar arquivos criptografados em uma unidade removível

Depois de criptografar arquivos em uma unidade removível com suporte ao modo portátil, os seguintes métodos de acesso a arquivos estão disponíveis:

- Se o Kaspersky Endpoint Security não estiver instalado no computador, o Gerenciador de arquivos portátil solicitará que você digite uma senha. Você precisará digitar a senha sempre que reiniciar o computador ou reconectar a unidade removível.

- Se o computador estiver localizado fora da rede corporativa e o Kaspersky Endpoint Security estiver instalado, o aplicativo solicitará que você digite a senha ou envie ao administrador uma solicitação para acessar os arquivos. Após obter acesso aos arquivos em uma unidade removível, o Kaspersky Endpoint Security armazenará a chave secreta no armazenamento de chaves do computador. Isso permitirá o acesso a arquivos no futuro sem inserir uma senha ou solicitar ao administrador (veja a figura abaixo).

- Se o computador estiver localizado dentro da rede corporativa e o Kaspersky Endpoint Security estiver instalado no computador, você terá acesso ao dispositivo sem inserir uma senha. O Kaspersky Endpoint Security receberá a chave secreta do Servidor de Administração do Kaspersky Security Center ao qual o computador está conectado.



Acessar arquivos criptografados em uma unidade removível

Recuperação da senha para trabalhar no modo portátil

Se esqueceu a senha para trabalhar no modo portátil, você deve conectar a unidade removível a um computador com o Kaspersky Endpoint Security instalado dentro da rede corporativa. Você terá acesso aos arquivos porque a chave secreta é mantida no armazenamento de chaves do computador ou no Servidor de Administração. Descriptografe e recriptografe os arquivos com uma nova senha.

Recursos do modo portátil ao conectar uma unidade removível a um computador de outra rede

Se o computador estiver localizado fora da rede corporativa e o Kaspersky Endpoint Security estiver instalado no computador, você poderá acessar os arquivos das seguintes maneiras:

- **Acesso com base em senha**

  Após digitar a senha, você poderá visualizar, modificar e salvar arquivos na unidade removível (*acesso transparente*). O Kaspersky Endpoint Security pode definir um direito de acesso somente-leitura para uma unidade removível se os seguintes parâmetros estiverem definidos nas configurações da política de criptografia de unidades removíveis:

  - O suporte ao modo portátil está desativado.
  - O modo **Criptografar todos os arquivos** ou **Criptografar apenas novos arquivos** é selecionado.

  Em todos os outros casos, você terá acesso total à unidade removível (permissão de leitura/gravação). Você poderá adicionar e excluir arquivos.

  Você pode alterar as permissões de acesso à unidade removível, mesmo enquanto a unidade removível estiver conectada ao computador. Se as permissões de acesso à unidade removível forem alteradas, o Kaspersky Endpoint Security bloqueará o acesso aos arquivos e solicitará a senha novamente.

  Depois de inserir a senha, você não poderá aplicar as configurações da política de criptografia para a unidade removível. Nesse caso, é impossível descriptografar ou recriptografar os arquivos na unidade removível.

- **Solicitar acesso aos arquivos ao administrador**

Se você esqueceu a senha para trabalhar no modo portátil, peça ao administrador acesso aos arquivos. Para acessar os arquivos, você precisa enviar ao administrador um arquivo de solicitação de acesso (um arquivo com a extensão KESDC). Você pode enviar o arquivo de solicitação de acesso por e-mail, por exemplo. O administrador enviará um arquivo de acesso a dados criptografados (um arquivo com a extensão KESDR).

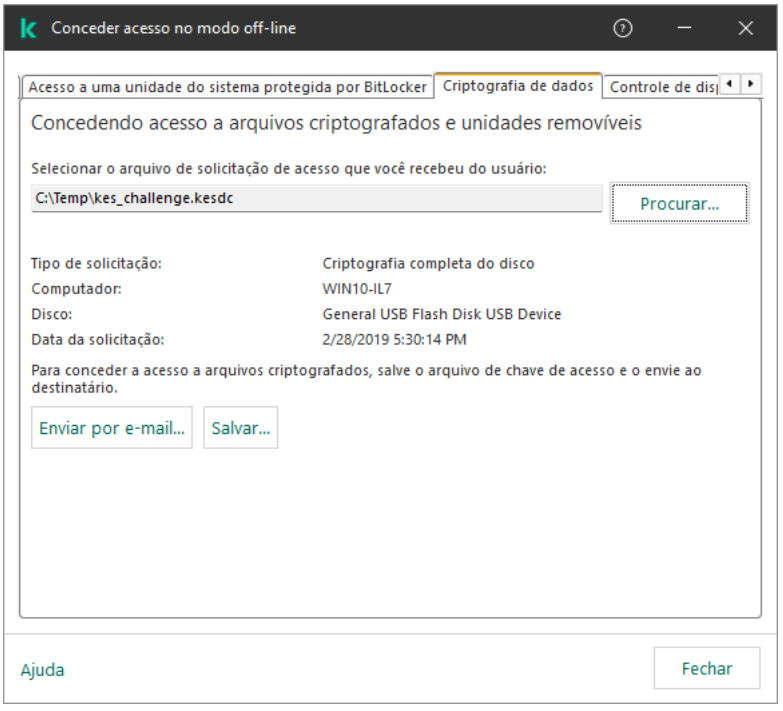
Depois de concluir o procedimento de solicitação e resposta de recuperação da senha, você receberá acesso transparente aos arquivos da unidade removível e acesso total à unidade removível (permissão de leitura/gravação).

Você pode aplicar uma política de criptografia de unidade removível e descriptografar arquivos, por exemplo. Depois de recuperar a senha ou que a política for atualizada, o Kaspersky Endpoint Security solicitará que você confirme as alterações.

Como obter um arquivo de acesso a dados criptografados no Console de administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Dispositivos**.
3. Na guia **Dispositivos**, selecione o computador do usuário que solicitou acesso aos dados criptografados e clique com o botão direito para abrir o menu de contexto.
4. No menu de contexto, selecione **Conceder acesso no modo off-line**.
5. Uma janela será aberta; nessa janela, selecione a guia **Criptografia de dados**.
6. Na guia **Criptografia de dados**, clique no botão **Procurar**.
7. Na janela para selecionar um arquivo de solicitação de acesso, especifique o caminho para o arquivo recebido do usuário.

   Você verá informações sobre a solicitação do usuário. O Kaspersky Security Center gera um arquivo de chave. Envie por e-mail o arquivo de chave de acesso a dados criptografados gerado para o usuário. Ou salve o arquivo de acesso e use qualquer método disponível para transferir o arquivo.



Concessão de acesso no modo off-line

Como obter um arquivo de acesso a dados criptografados no Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Ativos (dispositivos)**.
2. Marque a caixa de seleção ao lado do nome do computador cujos dados você deseja restaurar o acesso.
3. Clique **Permitir acesso ao dispositivo em modo offline**.
4. Selecione **Criptografia de dados**.
5. Clique no botão **Selecionar arquivo** e selecione o arquivo de solicitação de acesso que você recebeu do usuário (um arquivo com a extensão KESDC).

   O Web Console exibirá informações sobre a solicitação. Isso incluirá o nome do computador no qual o usuário está solicitando acesso ao arquivo.
6. Clique no botão **Salvar chave** e selecione uma pasta para salvar o arquivo de chave de acesso a dados criptografados (um arquivo com a extensão KESDR).

Como resultado, você poderá obter a chave de acesso a dados criptografados, que precisará transferir para o usuário.

Descriptografia de unidades removíveis

Você pode usar uma política para descriptografar uma unidade removível. Uma política com configurações definidas para criptografia de unidade removível é gerada para um grupo de administração específico. Portanto, o resultado da descriptografia de dados em unidades removíveis dependo do computador em que a unidade removível for conectado.

Para descriptografar unidades removíveis:

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Criptografia de dados** → **Criptografia de unidades removíveis**.
4. Se desejar descriptografar todos os arquivos criptografados armazenados em unidades removíveis, na lista suspensa **Modo de criptografia**, selecione **Descriptografar toda a unidade removível**.

5. Para descriptografar dados armazenados em unidades removíveis, edite as regras de criptografia para as unidades removíveis cujos dados deseja descriptografar. Para fazer isso:

   a. Na lista de unidades removíveis para a qual as regras de criptografia foram configuradas, selecione uma entrada correspondente à unidade removível que você precisa.

   b. Clique no botão **Definir uma regra** para editar a regra de criptografia para a unidade removível selecionada.

   c. No menu de contexto do botão **Definir uma regra**, selecione o item **Descriptografar toda a unidade removível**.

6. Salvar alterações.

Como resultado, se um usuário conectar uma unidade removível ou se já estiver conectada, o Kaspersky Endpoint Security descriptografará a unidade removível. O aplicativo avisa o usuário que o processo de descriptografia pode demorar algum tempo. Se o usuário iniciar a remoção com segurança de uma unidade removível durante a descriptografia de dados, o Kaspersky Endpoint Security interrompe a descriptografia de dados e permite a remoção da unidade removível antes que a operação de descriptografia seja concluída. A descriptografia de dados será continuada na próxima vez que a unidade removível for conectada ao computador.

Caso a descriptografia de uma unidade removível falhe, visualize o relatório **Criptografia de dados** na interface do Kaspersky Endpoint Security. O acesso a arquivos pode ser bloqueado por outro aplicativo. Neste caso, tente desconectar a unidade removível do computador e conectá-la novamente.

Exibir os detalhes da criptografia de dados

Enquanto a criptografia ou a descriptografia estão em andamento, o Kaspersky Endpoint Security retransmite informações do status dos parâmetros de criptografia aplicadas aos computadores clientes para o Kaspersky Security Center.

Exibir o status da criptografia

É possível ver o status a fim de monitorar a criptografia de dados. O Kaspersky Endpoint Security atribui os seguintes status de criptografia:

- **Não atende à política; cancelado pelo usuário**. O usuário cancelou a criptografia de dados.
- **Não atende a política devido a um erro**. Erro de criptografia de dados, por exemplo, falta de alguma licença.
- **Aplicando a política; a reinicialização é necessária**. A criptografia de dados está em andamento no computador. Reinicie o computador para concluir a criptografia de dados.
- **Nenhuma política de criptografia especificada**. A criptografia de dados está desativada nas configurações de política.
- **Não compatível**. Os componentes de criptografia de dados não estão instalados no computador.
- **Aplicando a política**. A criptografia e/ou descriptografia de dados está em andamento no computador.

Para visualizar o status da criptografia dos dados do computador:

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

2. Na árvore do console, selecione **Dispositivos gerenciados**.

3. Na guia **Dispositivos** na área de trabalho, deslize a barra de rolagem completamente à direita. Se a coluna **Status da criptografia** não for exibida, adicione esta coluna nas configurações do console do Kaspersky Security Center.

   A coluna **Status da criptografia** exibe os status da criptografia dos dados nos computadores no grupo de administração selecionado. Esse status é constituído de informações sobre criptografia de arquivo em unidades locais do computador e sobre criptografia completa de disco.

4. Se o status da criptografia de dados do computador estiver como **Aplicando política**, é possível monitorar o painel de progresso da criptografia:

   a. Abra as propriedades do computador com o status **Aplicando política**, clicando duas vezes nele.

   b. Na janela de propriedades do computador, selecione a seção **Aplicativos**.

   c. Na lista de aplicativos Kaspersky instalados no computador, selecione **Kaspersky Endpoint Security for Windows**.

   d. Clique em **Estatísticas**.

   e. Abaixo de **Criptografia de dispositivos** é possível ver o progresso atual da criptografia de dados em porcentagem.

Visualização das estatísticas de criptografia nos painéis de controle do Kaspersky Security Center

Para exibir o status de criptografia nos painéis de controle do Kaspersky Security Center:

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

2. Na árvore do console, selecione o nó **Servidor de Administração**.

3. Na área de trabalho à direita da árvore do Console de Administração, selecione a guia **Estatísticas**.

4. Crie uma nova página com painéis de detalhes com estatísticas de criptografia de dados. Para fazer isso:

   a. Na guia **Estatísticas**, clique no botão **Personalizar visualização**.

   b. Na janela exibida, clique no botão **Adicionar**.

   c. Uma janela é aberta; nesta janela, na seção **Geral**, insira o nome da página.

   d. Na seção **Painéis de informações**, clique no botão **Adicionar**.

   e. Na janela que é aberta, no grupo **Status da proteção**, selecione o item **Criptografia de dispositivos**.

   f. Clique em **OK**.

g. Caso necessário, edite as configurações no painel de detalhes. Para isso, usar as seções **Exibir** e **Dispositivos**.

h. Clique em **OK**.

i. Repita as etapas d – h das instruções, selecionando o item **Criptografia de unidades removíveis**, na seção **Status da proteção**.

Os painéis de detalhes adicionados aparecem na lista **Painéis de informações**.

j. Clique em **OK**.

O nome da página com painéis de detalhes criados nas etapas anteriores aparece na lista **Páginas**.

k. Clique no botão **Fechar**.

5. Na guia **Estatísticas**, abra a página criada nas etapas anteriores das instruções.

O painel de detalhes aparece, mostrando o status da criptografia dos computadores e unidades removíveis.

Exibir erros de criptografia de arquivos em unidades de computador locais

Para exibir os erros de criptografia de arquivo em unidades de computador locais:

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

2. Na árvore do console, selecione **Dispositivos gerenciados**.

3. Na guia **Dispositivos**, selecione o nome do computador na lista e clique com o botão direito do mouse nele para abrir o menu de contexto.

4. No menu de contexto do computador, selecione o item **Propriedades**. Na janela exibida, selecione a seção **Proteção**.

5. Clique no link **Exibir erros de criptografia de dados** para abrir a janela **Erros de criptografia de dados**.

Esta janela exibe detalhes dos erros de criptografia dos arquivos nas unidades do computador local. Quando um erro é corrigido, o Kaspersky Security Center remove os detalhes dos erros da janela **Erros de criptografia de dados**.

Exibir o relatório de criptografia de dados

O Kaspersky Security Center permite criar relatórios de criptografia de dados:

- **Relatório de status da criptografia dos dispositivos gerenciados**. O relatório inclui informações indicando se o status da criptografia do computador está em conformidade com a política de criptografia.

- **Relatório de status da criptografia dos dispositivos de armazenamento em massa**. O relatório inclui informações sobre o status da criptografia de dispositivos externos e dispositivos de armazenamento.

- **Relatório de direitos de acesso aos dispositivos criptografados**. O relatório inclui informações sobre o status das contas que têm acesso a unidades criptografadas.

- **Relatório de erros na criptografia de arquivos**. O relatório inclui informações sobre os erros ocorridos durante a execução de tarefas de criptografia ou descriptografia de dados em computadores.

- **Relatório de bloqueio de acesso aos arquivos criptografados**. O relatório inclui informações sobre os aplicativos tendo o acesso a bloqueado aos arquivos criptografados.

Para visualizar o relatório de criptografia de dados:

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

2. No nó **Servidor de Administração** da árvore do Console de Administração, selecione a guia **Relatórios**.

3. Clique no botão **Novo modelo de relatório**.

   O Assistente de novo modelo de relatório é iniciado.

4. Siga as instruções do Assistente de Modelo de Relatório. Na janela **Selecionar o tipo de modelo de relatório**, na seção **Outro**, selecione um dos relatórios de criptografia de dados.

   Depois que você terminou com o Novo Assistente de Modelo de Relatório, o novo modelo de relatório aparece na tabela na guia **Relatórios**.

5. Selecione o modelo de relatório que foi criado nas etapas anteriores das instruções.

6. No menu de contexto do modelo, selecione **Exibir o relatório**.

O processo de geração do relatório é iniciado. O relatório é exibido em uma nova janela.

Trabalhar com dispositivos criptografados quando não há acesso a eles

Obter acesso a dispositivos bloqueados

Um usuário pode ter de solicitar o acesso a dispositivos criptografados nos seguintes casos:

- O disco rígido foi criptografado em um computador diferente.

- A chave de criptografia de um dispositivo não está no computador (por exemplo, depois da primeira tentativa de acessar a unidade removível criptografada no computador), e o computador não é conectado ao Kaspersky Security Center.

  Depois que o usuário tiver aplicado a chave de acesso ao dispositivo criptografado, o Kaspersky Endpoint Security salva a chave de criptografia no computador do usuário e permite o acesso a este dispositivo depois de tentativas de acesso subsequentes, mesmo se não houver conexão ao Kaspersky Security Center.

O acesso a dispositivos criptografados pode ser obtido assim:

1. O usuário usa a interface do aplicativo Kaspersky Endpoint Security para criar um arquivo de solicitação de acesso com a extensão kesdc e envia-o ao administrador da rede local corporativa.

2. O administrador usa o Console de administração do Kaspersky Security Center para criar um arquivo de chave de acesso com a extensão kesdr e envia-o ao usuário.

3. O usuário aplica a chave de acesso.

Restaurar dados em dispositivos criptografados

Um usuário pode usar o Utilitário de restauração de Dispositivo Criptografado (denominado aqui como Utilitário de restauração) para trabalhar com dispositivos criptografados. Isso pode ser necessário nos seguintes casos:

- O procedimento para usar uma chave de acesso para obter acesso foi mal sucedido.

- Os componentes de criptografia não foram instalados no computador com o dispositivo criptografado.

Os dados necessários para restaurar o acesso a dispositivos criptografados usando o Utilitário de restauração residem na memória do computador do usuário na forma não criptografada por algum tempo. Para reduzir o risco de acesso não autorizado a esses dados, é recomendável que você restaure o acesso a dispositivos criptografados em computadores confiáveis.

Os dados em dispositivos criptografados podem ser restaurados como se segue:

1. O usuário usa o Utilitário de restauração para criar um arquivo de solicitação de acesso com a extensão fdertc e envia-o ao administrador da rede local corporativa.

2. O administrador usa o Console de administração do Kaspersky Security Center para criar um arquivo de chave de acesso com a extensão fdertr e envia-o ao usuário.

3. O usuário aplica a chave de acesso.

Para restaurar dados em discos rígidos do sistema criptografado, o usuário também pode especificar as credenciais de conta do Agente de Autenticação no Utilitário de restauração. Se os metadados da conta do Agente de Autenticação tiverem sido corrompidos, o usuário deve concluir o procedimento de restauração usando um arquivo de solicitação de acesso.

Antes de restaurar dados em dispositivos criptografados, recomenda-se cancelar a política do Kaspersky Security Center ou desativar a criptografia nas configurações de política do Kaspersky Security Center no computador onde o procedimento será realizado. Isso evita que o dispositivo seja criptografado novamente.

Recuperar dados usando o Utilitário de restauração FDERT

Se o disco rígido falhar, o sistema de arquivos pode estar corrompido. Se for esse o caso, os dados protegidos pela tecnologia Kaspersky Disk Encryption não estarão disponíveis. Você pode descriptografar os dados e copiá-los para uma nova unidade.

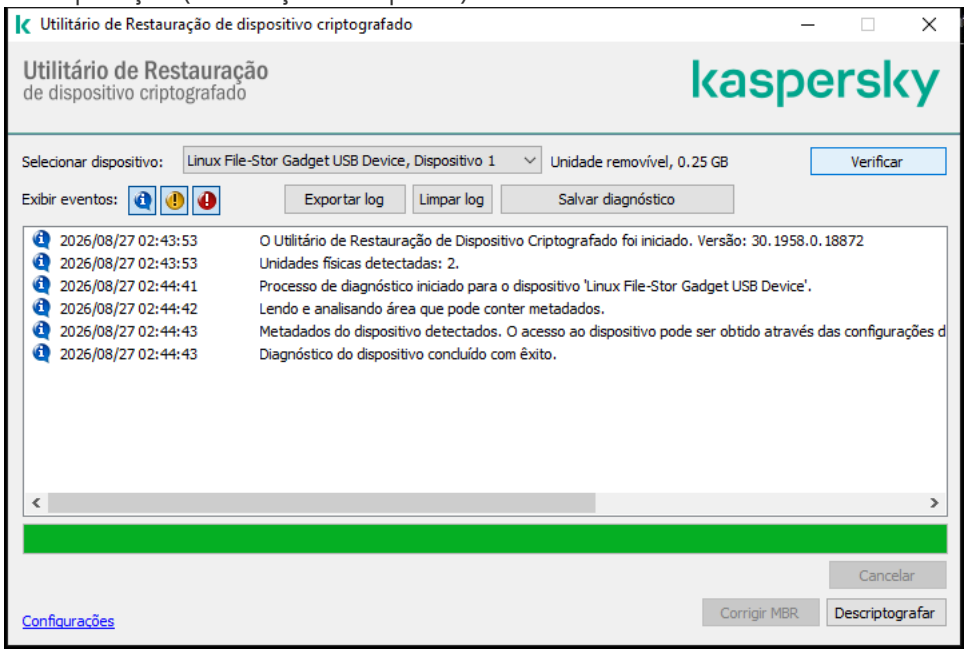
A recuperação de dados em uma unidade protegida pela tecnologia Kaspersky Disk Encryption consiste nas seguintes etapas:

1. Crie um utilitário de restauração independente (veja a figura abaixo).

2. Conecte uma unidade a um computador que não tenha os componentes de criptografia do Kaspersky Endpoint Security instalados.

3. Execute o utilitário de restauração e diagnostique o disco rígido.

4. Acesse os dados na unidade. Para fazer isso, insira as credenciais do Agente de Autenticação ou inicie o procedimento de recuperação (solicitação e resposta).



Utilitário de restauração FDERT

Criação de um utilitário de restauração autônomo

Para criar o arquivo executável do Utilitário de restauração:

1. Na janela principal do aplicativo, clique no botão .

2. Na janela que é aberta, clique no botão **Restaurar dispositivo criptografado**.

   O Utilitário de restauração de dispositivo criptografado é iniciado.

3. Clique no botão **Criar Utilitário de Restauração Independente** na janela do Utilitário de restauração.

4. Salve o utilitário de restauração independente na memória do computador.

   Como resultado, o arquivo executável do utilitário de restauração (fdert.exe) será salvo na pasta especificada. Copie o Utilitário de restauração para um computador que não possua componentes de criptografia do Kaspersky Endpoint Security. Isso evita que a unidade seja criptografada novamente.

Os dados necessários para restaurar o acesso a dispositivos criptografados usando o Utilitário de restauração residem na memória do computador do usuário na forma não criptografada por algum tempo. Para reduzir o risco de acesso não autorizado a esses dados, é recomendável que você restaure o acesso a dispositivos criptografados em computadores confiáveis.

Recuperação dados em um disco rígido

Para restaurar o acesso a um dispositivo criptografado usando o Utilitário de restauração.

1. Execute o arquivo chamado fdert.exe, que é o arquivo executável do utilitário de restauração. Este arquivo é criado pelo Kaspersky Endpoint Security.

2. Na janela Utilitário de restauração, selecione o dispositivo criptografado para o qual deseja restaurar o acesso.

3. Clique no botão **Verificar** para permitir que o utilitário defina quais ações devem ser executadas no dispositivo: se ele deve ser desbloqueado ou descriptografado.

   Se o computador tiver acesso à funcionalidade de criptografia do Kaspersky Endpoint Security, o Utilitário de restauração o avisa para desbloquear o dispositivo. Enquanto o desbloqueio do dispositivo não o descriptografar, o dispositivo se torna diretamente acessível como resultado do desbloqueio. Se o computador não tiver acesso à funcionalidade de criptografia do Kaspersky Endpoint Security, o Utilitário de restauração o avisa para descriptografar o dispositivo.

4. Se você deseja importar informações de diagnóstico, clique no botão **Salvar diagnóstico**.

   O utilitário salvará um arquivo com arquivos contendo informações de diagnóstico.

5. Clique no botão **Corrigir MBR** caso o diagnóstico do disco rígido do sistema criptografado exiba uma mensagem de problemas envolvendo o registro de reinício mestre (MBR) do dispositivo.

   A correção do registro de reinício mestre do dispositivo pode acelerar o processo de obtenção das informações necessárias para desbloquear ou descriptografar o dispositivo.

6. Clique no botão **Desbloquear** ou **Descriptografar** dependendo dos resultados do diagnóstico.

7. Se você deseja restaurar dados usando uma conta do Agente de Autenticação, selecione a opção **Usar parâmetros de conta do Agente de Autenticação** e insira as credenciais do Agente de Autenticação.

   Este método só é possível com a restauração dos dados em um disco rígido do sistema. Se o disco rígido do sistema foi corrompido e os dados de conta do Agente de Autenticação foram perdidos, você deve obter uma chave de acesso do administrador da rede local corporativa para restaurar os dados em um dispositivo criptografado.

8. Se você deseja iniciar o procedimento de recuperação, faça o seguinte:

   a. Selecione a opção **Especificar chave de acesso manualmente**.

   b. Clique no botão **Obter chave de acesso** e salve o arquivo de solicitação de acesso na memória do computador (um arquivo com a extensão FDERTC).

   c. Envie o arquivo de solicitação de acesso ao dispositivo ao administrador da rede local corporativa.

   > Não feche a janela **Receber chave de acesso do dispositivo** até receber a chave de acesso. Quando esta janela for aberta novamente, você não conseguirá aplicar a chave de acesso que foi criada anteriormente pelo administrador.

   d. Receba e salve o arquivo de acesso (um arquivo com a extensão FDERTR) criado e enviado a você pelo administrador da rede local corporativa (consulte as instruções abaixo).

   e. Faça o download do arquivo de acesso na janela **Receber chave de acesso do dispositivo**.

9. Se você estiver descriptografando um dispositivo, deverá definir configurações adicionais de descriptografia:

   - Especifique a área a ser descriptografada:

     - Se você quiser descriptografar o dispositivo inteiro, selecione a opção **Descriptografar dispositivo inteiro**.

     - Se você quiser descriptografar uma parte dos dados em um dispositivo, selecione a opção **Descriptografar áreas individuais do dispositivo** e especifique os limites da área de descriptografia.

   - Selecione a localização para gravar os dados descriptografados:

     - Se você quiser que os dados do dispositivo original sejam regravados com os dados descriptografados, desmarque a caixa de seleção **Descriptografar em um arquivo de imagem de disco**.

     - Se você quiser salvar os dados descriptografados separadamente dos dados criptografados originais, marque a caixa de seleção **Descriptografar em um arquivo de imagem de disco** e use o botão **Procurar** para especificar o caminho no qual salvar o arquivo VHD.

10. Clique **OK**.

    O processo de desbloqueio/descriptografia do dispositivo é iniciado.

Como criar um arquivo de acesso a dados criptografados no Console de administração (MMC)

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

2. Na árvore do Console de Administração, selecione a pasta **Avançado** → **Criptografia e proteção de dados** → **Dispositivos criptografados**.

3. Na área de trabalho, selecione o dispositivo criptografado para o qual deseja criar um arquivo de chave de acesso e, no menu de contexto do dispositivo, clique em **Obter acesso ao dispositivo no Kaspersky Endpoint Security**.

> Caso não tenha certeza para que computador o arquivo de solicitação de acesso foi gerado, na árvore do Console de Administração, selecione a pasta **Avançado** → **Criptografia e proteção de dados** e, na área de trabalho, clique em **Obter a chave de criptografia do dispositivo no Kaspersky Endpoint Security**.

4. Na janela exibida, selecione o algoritmo de criptografia a ser usado: AES256 ou AES56.

   O algoritmo de criptografia de dados depende da biblioteca de criptografia AES incluída no pacote de distribuição: *Criptografia forte (AES256)* ou *Criptografia leve (AES56)*. A biblioteca de criptografia AES é instalada junto com o aplicativo.

5. Clique em **Procurar** para abrir uma janela; nessa janela, especifique o caminho para o arquivo de solicitação com a extensão fdertc recebido do usuário.

6. Clique **Desbloquear**.

Você verá informações sobre a solicitação do usuário. O Kaspersky Security Center gera um arquivo de chave. Envie por e-mail o arquivo de chave de acesso a dados criptografados gerado para o usuário. Ou salve o arquivo de acesso e use qualquer método disponível para transferir o arquivo.

Como criar um arquivo de acesso a dados criptografados no Web Console

1. Na janela principal do Web Console, selecione **Operações** → **Criptografia e proteção de dados** → **Dispositivos criptografados**.

2. Marque a caixa de seleção ao lado do nome do computador no qual você deseja recuperar os dados.

3. Clique **Permitir acesso ao dispositivo em modo offline**.

   Isso inicia o Assistente para conceder acesso a um dispositivo.

4. Siga as instruções do Assistente para conceder acesso a um dispositivo:

   a. Selecione o plug-in Kaspersky Endpoint Security for Windows.

   b. Selecione o algoritmo de criptografia a ser usado: AES256 ou AES56.

      O algoritmo de criptografia de dados depende da biblioteca de criptografia AES incluída no pacote de distribuição: *Criptografia forte (AES256)* ou *Criptografia leve (AES56)*. A biblioteca de criptografia AES é instalada junto com o aplicativo.

   c. Selecione o arquivo de solicitação de acesso recebido do usuário (um arquivo com a extensão FDERTC).

   d. Selecione uma pasta para salvar o arquivo de chave de acesso a dados criptografados (um arquivo com a extensão FDERTR).

Como resultado, você poderá obter a chave de acesso a dados criptografados, que precisará transferir para o usuário.

Criar um disco de recuperação do sistema operacional

O disco de recuperação do sistema operacional pode ser útil quando um disco rígido criptografado não puder ser acessado por alguma razão e o sistema operacional não puser ser carregado.

Você pode carregar uma imagem do sistema operacional do Windows usando o disco de recuperação e restaurar o acesso ao disco rígido criptografado usando o Utilitário de Restauração incluído na imagem de sistema operacional.

Para criar um disco de recuperação do sistema operacional:

1. Crie um arquivo executável do Utilitário de Restauração de Dispositivo Criptografado.

2. Crie uma imagem personalizada do ambiente de pré-inicialização do Windows. Durante a criação da imagem personalizada do ambiente de pré-inicialização do Windows, adicione o arquivo executável do Utilitário de Restauração à imagem.

3. Salve a imagem personalizada do ambiente de pré-instalação do Windows em uma mídia executável, como um CD ou uma unidade removível.

   Consulte os arquivos de ajuda da Microsoft para obter instruções sobre a criação de uma imagem personalizada do ambiente pré-inicialização do Windows (por exemplo, no recurso do Microsoft TechNet).

Soluções de Detection and Response

As soluções de Detection and Response da Kaspersky são sistemas de segurança que detectam ameaças avançadas e indicadores de ataque em diferentes níveis da infraestrutura de uma organização. As soluções de Detection and Response fornecem informações sobre a ameaça detectada e permitem gerenciar ações de Resposta a ameaças.

Assim, a solução de Detection and Response:

- Recebe informações sobre a operação de um computador, servidor ou outros dispositivos (telemetria).
- Analisa automaticamente as informações para detectar ameaças.
- Gera detalhes de alerta como colunas da cadeia de evolução de ameaças para análise e escolha de ações de Resposta a ameaças.
- Executa ações de Resposta a ameaças (por exemplo, isolamento de rede do computador).

O Kaspersky Endpoint Security é compatível com as soluções Detection and Response por meio de um agente integrado. O agente integrado envia telemetria para servidores de soluções e realiza ações de Resposta a ameaças. O agente integrado é compatível com:

- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum)
- Kaspersky Endpoint Detection and Response Expert (EDR Expert)
- Kaspersky Anti Targeted Attack Platform:
  - Endpoint Detection and Response (EDR) versão 7.1 ou anterior
  - Network Detection and Response (NDR)
  - KATA Sandbox
- Kaspersky Endpoint Detection and Response Expert (on-premises)
- Kaspersky Sandbox 2.0

É possível usar o Kaspersky Endpoint Security com a solução de Detection and Response em várias configurações, por exemplo, [EDR Optimum+MDR].

Licenciamento MDR e EDR Optimum

O Kaspersky Endpoint Security é compatível com a funcionalidade das soluções Kaspersky Managed Detection and Response (MDR) e Kaspersky Endpoint Detection and Response Optimum (EDR Optimum). É possível usar o Kaspersky Endpoint Security com essas soluções em várias configurações e criar um sistema de proteção personalizado que atenda aos seus requisitos específicos. Para fazer isso, você deve comprar uma licença para cada uma das soluções. A licença pode abranger o direito de usar uma única solução (por exemplo, solo Add-on MDR) ou várias soluções, Add-on [EDR Optimum+MDR].

O MDR e o EDR Optimum são compatíveis com os seguintes métodos de licenciamento:

- A funcionalidade MDR ou EDR Optimum é coberta pela licença do Kaspersky Endpoint Security for Windows.

  A funcionalidade está disponível imediatamente após a ativação do Kaspersky Endpoint Security for Windows. Você só precisa adicionar uma chave.

- Licenças separadas para o MDR ou EDR Optimum (MDR Add-on, EDR Optimum Add-on, [EDR Optimum+MDR] Add-on).

  A funcionalidade fica disponível depois de adicionada uma chave separada para Add-on MDR, Add-on EDR Optimum ou Add-on [EDR Optimum+MDR]. Como resultado, duas chaves são adicionadas ao computador: uma chave para o Kaspersky Endpoint Security e uma para o MDR ou o EDR Optimum. A chave do Kaspersky Endpoint Security deve ser a primeira a ser adicionada.

O Kaspersky Endpoint Security permite adicionar apenas uma *chave ativa* para licenciamento do MDR e do EDR Optimum. Portanto, se você precisar ativar ambas as soluções, deverá adicionar uma chave do [EDR Optimum+MDR] Add-on em vez de uma chave separada para cada solução. Você também pode adicionar uma *chave reserva*.

Se você usou um arquivo BLOB ao implementar o MDR, não precisará de uma chave separada para ativá-lo. O arquivo BLOB já contém informações de licença.

Licenciamento inicial de soluções

Ao implementar o MDR e o EDR Optimum pela primeira vez, as soluções são ativadas da mesma forma que o aplicativo Kaspersky Endpoint Security. É possível adicionar uma chave usando a tarefa *Adicionar chave* ou a funcionalidade de distribuição automática de chaves. A chave da licença será adicionada ao aplicativo como uma segunda chave ativa ou como uma chave reserva se você marcar a respectiva caixa de seleção.

Alternar de uma licença para outra

Se sua organização já tiver uma dessas soluções implementadas e a chave correspondente tiver sido adicionada ao aplicativo, há algumas considerações especiais envolvidas com o licenciamento da nova configuração. Ao alternar para uma licença diferente, o aplicativo não adiciona a nova chave ao aplicativo, em vez disso, substitui a chave atual pela nova. O motivo disso é a restrição que permite que o aplicativo adicione apenas uma chave para ativar o MDR e o EDR Optimum.

Por exemplo, suponha que sua organização tenha a solução [EDR Optimum+MDR] implementada e você decidiu mudar para a configuração do Add-on MDR. Para alternar para a nova configuração, você deve substituir a chave do [EDR Optimum+MDR] Add-on pela chave do Add-on MDR.

Não está mais disponível uma licença separada para EDR Optimum e MDR (Add-on [EDR Optimum+MDR]). Se você quiser usar essas duas soluções, deverá ativar o MDR usando um arquivo BLOB e o EDR Optimum com uma chave da licença.

Com o recurso de distribuição automática de chaves, o aplicativo rejeita chaves da licença que cobrem o mesmo número de soluções. Ou seja, se você tiver uma chave do Add-on EDR Optimum adicionada, não poderá substituí-la por uma chave do Add-on MDR. No entanto, poderá substituir a chave do Add-on EDR Optimum por uma chave do Add-on [EDR Optimum+MDR]. O aplicativo também rejeitará chaves se você tentar substituir uma chave do Add-on MDR por uma chave do Add-on EDR. Para substituir uma chave, você pode executar a tarefa *Adicionar chave*. A tarefa *Adicionar chave* permite substituir as chaves da licença por qualquer número de soluções.

Caso tenha uma chave reserva do [EDR Optimum+MDR] Add-on, para adicionar corretamente uma chave ativa do Add-on EDR Optimum ou do Add-on MDR, primeiro será necessário substituir a chave reserva por uma chave do Add-on EDR Optimum, Add-on MDR ou, como alternativa, remover a chave reserva e, em seguida, substituir a chave ativa.

Compatibilidade com soluções EDR de terceiros

É possível usar o Kaspersky Endpoint Security para proteger estações de trabalho e servidores juntamente com soluções EDR de terceiros. Para eliminar falsos positivos, recomendamos adicionar arquivos executáveis do Kaspersky Endpoint Security e do Agente de Rede na zona confiável de sua solução EDR de terceiros.

Zona confiável para compatibilidade com soluções EDR de terceiros

	Kaspersky Endpoint Security for Windows	Agente de Rede do Kaspersky Security Center
Pasta de trabalho	`C:\Program Files (x86)\Kaspersky Lab\KES.14.2.0`	`C:\Program Files (x86)\Kaspersky Lab\NetworkAgent`

Arquivos executáveis	`avp.exe`
	`avp.com`
	`avpsus.exe`
	`avpui.exe`
	`dump_writer_agent.exe`
	`kescli.exe`
	`kesdr.exe`
	`kldw.exe`
	`klpsm.exe`
	`kvdb_upgrader.exe`
	`modify_watcher.exe`
	`pmv.exe`
	`remediation.exe`
	`service_stub.exe`
		`AVPDTAgt.exe`
		`fix_gflags.exe`
		`getsysteminfo.exe`
		`integrity_checker.exe`
		`klcpuld.exe`
		`klcsldcl.exe`
		`klcsngtgui.exe`
		`klcspxy.exe`
		`kldumper.exe`
		`klmover.exe`
		`klnagchk.exe`
		`klnagent.exe`
		`klnagntf.exe`
		`klnagwds.exe`
		`klosprep.exe`
		`klrbtagt.exe`
		`klscflag.exe`
		`klscmodchk.exe`
		`klshwmsg.exe`
		`klwd.exe`
		`ksnproxy.exe`
		`Patch.exe`
		`tslauncher.exe`
		`Up2Date.exe`
		`vapm.exe`

Kaspersky Endpoint Agent

O Kaspersky Endpoint Agent tem suporte para a interação entre o aplicativo e outras soluções da Kaspersky para a detecção de ameaças avançadas (por exemplo, o Kaspersky Sandbox). As soluções Kaspersky são compatíveis com versões específicas do Kaspersky Endpoint Agent.

Para usar o Kaspersky Endpoint Agent como parte das soluções da Kaspersky, é necessário ativar as soluções com a chave de licença correspondente.

Para informações detalhadas sobre o Kaspersky Endpoint Agent, incluído na solução de software que você está usando, e para conhecer a solução autônoma, consulte o Guia de ajuda do produto relevante:

- Ajuda do Kaspersky Anti Targeted Attack Platform
- Ajuda do Kaspersky Sandbox
- Ajuda do Kaspersky Endpoint Detection and Response Optimum
- Ajuda do Kaspersky Managed Detection and Response

O kit de distribuição para o Kaspersky Endpoint Security versões 11.2.0 – 11.8.0 inclui o Kaspersky Endpoint Agent. É possível selecionar o Kaspersky Endpoint Agent durante a instalação do Kaspersky Endpoint Security for Windows. Como resultado, dois aplicativos serão instalados no seu computador: KEA e KES. No Kaspersky Endpoint Security 11.9.0, o pacote de distribuição do Kaspersky Endpoint Agent não faz mais parte do kit de distribuição do Kaspersky Endpoint Security.

Correspondência de versões KEA (como parte de KES) para versões KES

Kaspersky Endpoint Security for Windows	Kaspersky Endpoint Agent
11.8.0	3.11.0.216.mr1
11.7.0	3.11
11.6.0	3.10
11.5.0	3.9
11.4.0	3.9
11.3.0	3.9
11.2.0	3.9

A Kaspersky está mudando toda a Detection and Response para trabalhar com o agente integrado do Kaspersky Endpoint Security em vez do Kaspersky Endpoint Agent. Gradualmente, a Kaspersky está adicionando suporte para essas soluções e eliminando o Kaspersky Endpoint Agent (consulte a tabela abaixo). A partir da versão 12.1, o aplicativo é compatível com todas as soluções de Detection and Response. Além disso, a partir da versão 12.1, o aplicativo não é mais compatível com o Kaspersky Endpoint Agent e não é mais possível instalar os dois aplicativos simultaneamente no mesmo computador.

Versão do Kaspersky Endpoint Security	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform (componente do Endpoint Detection and Response)	Kaspersky Anti Targeted Attack Platform (componente do Network Detection and Response)
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.6.0	**Agente integrado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**Agente integrado**	**Agente integrado**	**Agente integrado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12.1	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	Kaspersky Endpoint Agent
12.6	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**	**Agente integrado**

Migração da configuração [KES+KEA] para [KES+built-in agent]

O Kaspersky Endpoint Security inclui agentes integrados para trabalhar com as soluções de Detection and Response. Não é mais preciso um aplicativo separado do Kaspersky Endpoint Agent para trabalhar com estas soluções. Quando o Kaspersky Endpoint Security é implantado em computadores com o Kaspersky Endpoint Agent instalado, as soluções de Detection and Response continuarão funcionando com o Kaspersky Endpoint Security. Além disso, o Kaspersky Endpoint Agent será removido do computador.

O kit de distribuição para o Kaspersky Endpoint Security versões 11.2.0 – 11.8.0 inclui o Kaspersky Endpoint Agent. É possível selecionar o Kaspersky Endpoint Agent durante a instalação do Kaspersky Endpoint Security for Windows. Como resultado, dois aplicativos serão instalados no seu computador: KEA e KES. No Kaspersky Endpoint Security 11.9.0, o pacote de distribuição do Kaspersky Endpoint Agent não faz mais parte do kit de distribuição do Kaspersky Endpoint Security.

A migração da configuração [KES+KEA] para [KES+agente integrado] envolve as seguintes etapas:

1. **Atualização do Kaspersky Security Center**

   Efetue o upgrade de todos os componentes do Kaspersky Security Center para a versão 13.2 ou posterior, inclusive o Agente de Rede nos computadores dos usuários e no Web Console.

2. **Atualização do plug-in da Web do Kaspersky Endpoint Security**

   No Kaspersky Security Center Web Console, atualize o plugin da Web do Kaspersky Endpoint Security para a versão 11.7.0 ou posterior. Para gerenciar os componentes do EDR Optimum e Kaspersky Sandbox, é necessário utilizar o Web Console.

Para usar a Kaspersky Anti Targeted Attack Platform (EDR), será necessário ter um plugin da Web para o Kaspersky Endpoint Security versão 12.1 ou posterior.

Para usar a Kaspersky Anti Targeted Attack Platform (NDR), será necessário ter um plugin da Web para o Kaspersky Endpoint Security versão 12.7 ou posterior.

3. **Migração das políticas e tarefas**

   Utilize o Kaspersky Endpoint Agent Policy e o assistente de tarefa de migração para migrar as configurações do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows.

   Isso cria uma nova política do Kaspersky Endpoint Security. A nova política possui o status *Inativo*. Para aplicar a política, abra as propriedades da política, aceite a Declaração da Kaspersky Security Network e defina o status como *Ativo*.

4. **Licenciamento da funcionalidade**

   Caso utilize uma licença comum do Kaspersky Endpoint Detection and Response Optimum ou do Kaspersky Optimum Security para ativar o Kaspersky Endpoint Security for Windows e Kaspersky Endpoint Agent, a funcionalidade do EDR Optimum será ativada automaticamente após a atualização do aplicativo para a versão 11.7.0. Não é necessário fazer mais nada.

   Caso utilize uma licença autônoma do add-on do Kaspersky Endpoint Detection and Response Optimum para ativar a funcionalidade do EDR Optimum, é necessário garantir que a chave do add-on do EDR Optimum seja adicionada ao repositório do Kaspersky Security Center e que a funcionalidade de distribuição automática da chave de licença seja ativada. Após a atualização do aplicativo para a versão 11.7.0, a funcionalidade do EDR Optimum é ativada automaticamente.

   Caso utilize uma licença do Kaspersky Endpoint Detection and Response Optimum ou do Kaspersky Optimum Security para ativar o Kaspersky Endpoint Agent e uma licença diferente para ativar o Kaspersky Endpoint Security for Windows, é necessário substituir a chave do Kaspersky Endpoint Security for Windows pela chave comum do Kaspersky Endpoint Detection and Response Optimum ou da chave Kaspersky Optimum Security. É possível substituir a chave utilizando a tarefa *Adicionar chave*.

   Não é necessário ativar a funcionalidade do Kaspersky Sandbox. A funcionalidade do Kaspersky Sandbox estará disponível imediatamente após a atualização e ativação do Kaspersky Endpoint Security for Windows.

   Somente a licença da Kaspersky Anti Targeted Attack Platform pode ser usada para ativar o Kaspersky Endpoint Security como parte da solução Kaspersky Anti Targeted Attack Platform. Após a atualização do aplicativo para a versão 12.1, a funcionalidade do EDR (KATA) é ativada automaticamente. Não é necessário fazer mais nada.

5. **Atualização do aplicativo Kaspersky Endpoint Security**

   Para atualizar o aplicativo e migrar a funcionalidade do EDR Optimum e do Kaspersky Sandbox, uma instalação remota é recomendada.

   Para atualizar o aplicativo por meio da tarefa de instalação remota, é necessário editar as seguintes configurações:

   - Selecione os componentes para soluções de detecção e resposta nas configurações do pacote de instalação.
   - Exclua o componente Kaspersky Endpoint Agent nas configurações do pacote de instalação (para Kaspersky Endpoint Security for Windows versões 11.2.0 – 11.8.0).
   - Caso a proteção por senha esteja ativada para restringir o acesso ao Kaspersky Endpoint Agent, insira a senha de desinstalação do aplicativo nas configurações da tarefa *Instalar o aplicativo remotamente*. Você pode inserir a senha de desinstalação a partir do Kaspersky Security Center Linux 15.1.

Também é possível baixar o aplicativo utilizando os seguintes métodos:

- Utilizando o serviço de atualização da Kaspersky (Seamless Update – SMU).
- Localmente, usando o Assistente de configuração.

O Kaspersky Endpoint Security é compatível com a seleção automática de componentes ao atualizar o aplicativo em um computador com o aplicativo Kaspersky Endpoint Agent instalado. A seleção automática dos componentes depende das permissões da conta do usuário que está atualizando o aplicativo.

Caso esteja atualizando o Kaspersky Endpoint Security com um arquivo EXE ou MSI com a conta do sistema (SYSTEM), o Kaspersky Endpoint Security obtém acesso às licenças atualmente em uso das soluções da Kaspersky. Portanto, se o computador possui, por exemplo, o Kaspersky Endpoint Agent instalado e a solução EDR Optimum ativada, o instalador do Kaspersky Endpoint Security configura automaticamente o conjunto de componentes e seleciona o componente EDR Optimum. Isso faz com que o Kaspersky Endpoint Security alterne o uso do agente integrado e remova o Kaspersky Endpoint Agent. A execução do instalador do MSI na conta do sistema (SYSTEM) normalmente é feita com a atualização pelo serviço de atualização da Kaspersky (SMU) ou ao implantar um pacote de instalação pelo Kaspersky Security Center.

Caso esteja atualizando o Kaspersky Endpoint Security com um arquivo MSI com uma conta de usuário não privilegiado, o Kaspersky Endpoint Security perde o acesso das licenças atualmente em uso das soluções da Kaspersky. Neste caso, o Kaspersky Endpoint Security seleciona automaticamente os componentes de acordo com a configuração do Kaspersky Endpoint Agent. Depois disso, o Kaspersky Endpoint Security passa a usar o agente integrado e remove o Kaspersky Endpoint Agent.

6. **Reinicialização do computador**

   Reiniciar o seu computador para concluir a atualização do aplicativo com o agente integrado. Ao atualizar o aplicativo, o instalador remove o Kaspersky Endpoint Agent antes que o computador seja reiniciado. Depois que o computador é reiniciado, o instalador adiciona o agente integrado. Isso significa que o Kaspersky Endpoint Security não executa as funções de EDR e Kaspersky Sandbox até que o computador seja reiniciado.

7. **Verificação da saúde do Kaspersky Endpoint Detection and Response Optimum e Kaspersky Sandbox**

   Se, após a atualização, o computador estiver com o status *Crítico* no console do Kaspersky Security Center:

   - Certifique-se de que o computador possui o Agente de Rede versão 13.2 ou posterior instalado.
   - Verifique o status operacional do agente integrado visualizando o *Relatório de status dos componentes do aplicativo*. Caso o componente tenha o status *Não instalado*, instale o componente usando a tarefa *Alterar componentes do aplicativo*.
   - Certifique-se de aceitar a Declaração da Kaspersky Security Network na nova política do Kaspersky Endpoint Security for Windows.
   - Assegure-se de que a funcionalidade EDR Optimum esteja ativada usando o *Relatório de status dos componentes do aplicativo*. Caso um componente tenha o status *Não coberto pela licença*, certifique-se de que funcionalidade de distribuição automática da chave de licença do EDR Optimum esteja ligada.

Migração de políticas e tarefas para o Kaspersky Endpoint Agent

O Kaspersky Endpoint Security for Windows inclui um assistente para migração do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security. É possível migrar a política e as configurações de tarefa para as seguintes soluções:

- Kaspersky Sandbox
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)
- Kaspersky Anti Targeted Attack Platform

Um assistente para migração do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security funciona apenas no Web Console e no Cloud Console. No Console de Administração (MMC), somente é possível migrar as configurações da solução Kaspersky Anti Targeted Attack Platform (EDR) usando o assistente padrão de migração de tarefas e políticas do Kaspersky Security Center.

É recomendável começar a migração do Kaspersky Endpoint Agent para o Kaspersky Endpoint 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.

Para migrar as configurações de políticas e tarefas do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security,

na janela principal do Web Console, selecione **Operações** → **Migração a partir do Kaspersky Endpoint Agent**.

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

Etapa 1. Migração da política

O assistente de migração cria uma nova política que unifica as configurações das políticas do Kaspersky Endpoint Security e Kaspersky Endpoint Agent. Na lista de política, selecione as políticas do Kaspersky Endpoint Agent cujas configurações deseja unificar as políticas do Kaspersky Endpoint Security. Clique na política do Kaspersky Endpoint Agent para selecionar a política do Kaspersky Endpoint Security com o qual deseja unificar as configurações. Certifique-se de ter selecionado as políticas corretas e vá para a próxima etapa.

Etapa 2. Migração da tarefa

O Assistente de migração cria novas tarefas para o Kaspersky Endpoint Security. Na lista de tarefa, selecione as tarefas do Kaspersky Endpoint Agent para as quais deseja criar uma política do Kaspersky Endpoint Security. O assistente é compatível com as tarefas do Kaspersky Endpoint Detection and Response e Kaspersky Sandbox. Vá para a próxima etapa.

Etapa 3. Conclusão do Assistente

Conclua o assistente. Como resultado, o assistente faz o seguinte:

- Cria uma nova política do Kaspersky Endpoint Security.

  A política unifica as configurações do Kaspersky Endpoint Security e Kaspersky Endpoint Agent. A política é chamada *<nome da política Kaspersky Endpoint Security> & <nome da política Kaspersky Endpoint Agent>*. A nova política possui o status *Inativo*. Para continuar, mude os status das políticas do Kaspersky Endpoint Agent e Kaspersky Endpoint Security para *Inativo* e ative a nova política unificada.

  Após a migração a partir do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows, certifique-se de que a nova política tenha a funcionalidade para transferência de dados para o servidor de administração (dados do arquivo na quarentena e dados da cadeia de evolução de ameaças) configurada. Os valores do parâmetro de transferência de dados não são migrados a partir de uma política do Kaspersky Endpoint Agent.

  Ao migrar do Kaspersky Endpoint Agent para Kaspersky Endpoint Security para a solução Kaspersky Anti Targeted Attack Platform (EDR), pode haver alguns erros ao conectar o computador com os servidores do Central Node. Isso acontece porque o assistente de migração no Web Console ignora as seguintes configurações da política e não as migra:

  - Proibição de modificação de configurações **Conexão com servidores KATA** ("bloqueado").

    Por padrão, as configurações podem ser modificadas (o "cadeado" está aberto). Portanto, as configurações não são aplicadas no computador. É necessário proibir as modificação das configurações e fechar o "cadeado".

  - Crypto-contêiner.

    Caso a autenticação de duas vias seja usada para conexão com os servidores do Central Node, é necessário adicionar novamente o crypto-contêiner. O assistente de migração migra corretamente o certificado TLS do servidor.

  O assistente de migração de tarefas e políticas no Console de Administração (MMC) migra todas as configurações para a solução Kaspersky Anti Targeted Attack Platform (EDR).

- Cria novas tarefas do Kaspersky Endpoint Security.

  Novas tarefas são cópias das tarefas do Kaspersky Endpoint Agent para o Kaspersky Endpoint Detection and Response e Kaspersky Sandbox. Ao mesmo tempo, o assistente deixa as tarefas do Kaspersky Endpoint Agent inalteradas.

Como migrar configurações de política e tarefa do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security no Console de Administração (MMC) (somente para KATA [EDR])

1. No Console de administração, 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**.

O Assistente de Conversão de Políticas e Tarefas em Lotes será iniciado. Siga as instruções do Assistente.

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

Nesta etapa, é preciso selecionar o Kaspersky Endpoint Security for Windows. Vá para a próxima etapa.

Etapa 2. Conversão de políticas

O assistente de migração cria uma nova política do Kaspersky Endpoint Security para a qual as configurações da política do Kaspersky Endpoint Agent serão migradas. Na lista de políticas, selecione as políticas do Kaspersky Endpoint Agent cujas configurações deseja transferir para a política do Kaspersky Endpoint Security. Vá para a próxima etapa.

O Assistente de Migração começará a converter as políticas. Durante a conversão da política, o assistente de migração solicita que o usuário aceite a Declaração da Kaspersky Security Network. As novas políticas serão nomeadas *<Nome da política> (convertida)*.

Etapa 3. Conversão de tarefas

Ignorar esta etapa. O assistente é compatível com as tarefas do Kaspersky Endpoint Detection and Response Optimum e Kaspersky Sandbox. O gerenciamento desses componentes está disponível apenas no Web Console. Vá para a próxima etapa.

Etapa 4. Conclusão do Assistente

Conclua o assistente. Como resultado do assistente, uma nova política do Kaspersky Endpoint Security será criada.

Endpoint Detection and Response Agent (EDR Agent)

A partir do Kaspersky Endpoint Security 12.3 for Windows, o aplicativo inclui a configuração do Endpoint Detection and Response Agent (EDR Agent). O *Endpoint Detection and Response Agent* é um aplicativo instalado em estações de trabalho e servidores individuais na infraestrutura de TI da organização para oferecer suporte às seguintes soluções de Detection and Response da Kaspersky:

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA) (a partir da versão 12.6)

- Kaspersky Anti Targeted Attack Platform (NDR) (a partir da versão 12.7)
- Kaspersky Endpoint Detection and Response Expert (on-premises) (a partir da versão 12.11)

O EDR Agent não é compatível com a integração com a solução Kaspersky Endpoint Detection and Response Expert (cloud).

O EDR Agent monitora continuamente os processos em execução nesses computadores, as conexões de rede abertas e os arquivos em modificação. Os componentes de proteção e controle do aplicativo não estão disponíveis para o EDR Agent.

O EDR Agent é compatível com aplicativos EPP de terceiros. Isso viabiliza o uso de ferramentas de segurança de infraestrutura de terceiros juntamente com o Detection and Response da Kaspersky.

Para implantar o EDR Agent, o computador deve ter o Agente de Rede instalado e o computador deve ser adicionado ao console do Kaspersky Security Center. Para ativar a interação do EDR Agent com o Kaspersky Security Center, é necessário instalar o plug-in de gerenciamento do Kaspersky Endpoint Security for Windows. É possível especificar as configurações do EDR Agent usando uma política de grupo. Para integrar o EDR Agent, é necessário configurar a integração nas seções de política apropriadas.

Os seguintes aplicativos Kaspersky devem ser instalados na infraestrutura para dar suporte às soluções Kaspersky Detection and Response:

	• Agente de Rede • EDR Agent
Endpoint	
	Plug-in de gerenciamento do Kaspersky Endpoint Security for Windows
Kaspersky Security Center	
Soluções de Detection and Response: MDR, KATA (EDR), KATA (NDR), KUMA, EDR Expert (on-premises)	

Instalando o EDR Agent

Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent (EDR Agent) para soluções Kaspersky Detection and Response são instalados da mesma maneira.

O EDR Agent pode ser instalado em um computador em uma das seguintes maneiras:

- Uso remoto do Kaspersky Security Center.
- Localmente, usando o assistente de instalação.
- Localmente na linha de comando (somente para KATA (EDR) e EDR Expert (on-premises)).

Para instalar o EDR Agent, é necessário selecionar a configuração apropriada em configurações do pacote de instalação ou no assistente de instalação.

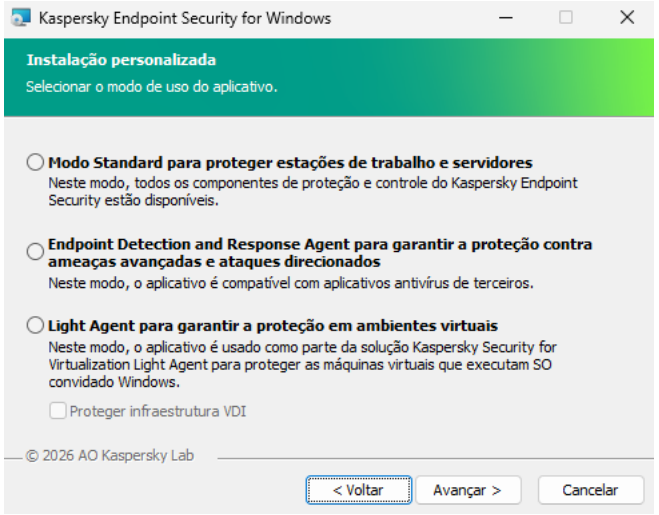
Como instalar o EDR Agent usando o assistente de instalação

1. Copie a pasta Kit de distribuição no computador do usuário.

2. Execute setup_kes.exe.

   O assistente de Instalação é iniciado.

Configuração do Kaspersky Endpoint Security



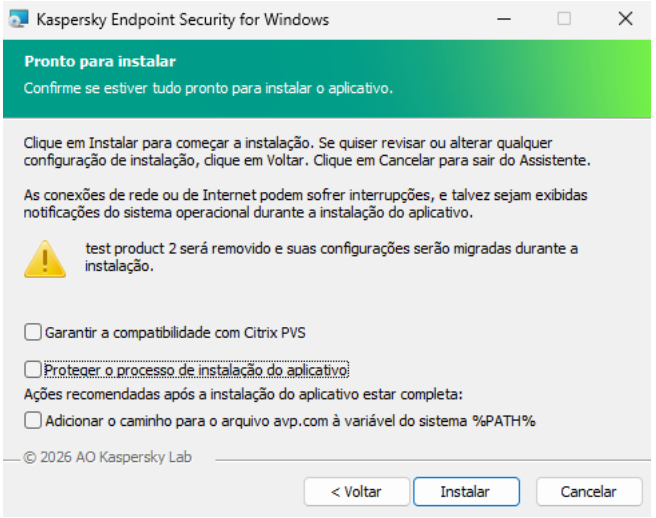
Escolhendo a configuração do aplicativo

Selecione a configuração **Endpoint Detection and Response Agent**. Nesta configuração, é possível instalar apenas os componentes que fornecem suporte para as soluções Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), assim como KUMA. Essa configuração será necessária caso uma Endpoint Protection Platform (EPP) de terceiros seja implantada na sua organização juntamente com uma solução Kaspersky Detection and Response. Isso torna o Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent compatível com os aplicativos EPP de terceiros.

Componentes do Kaspersky Endpoint Security

Selecione os componentes que deseja instalar. Você pode alterar os componentes disponíveis do aplicativo depois de concluir a instalação do aplicativo. Para isso, você precisa executar o Assistente de instalação novamente e optar por alterar os componentes disponíveis.

Configurações avançadas



Configurações avançadas de instalação do aplicativo

Proteger o processo de instalação do aplicativo. 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 Endpoint Security e bloqueio do acesso à seção de registro do sistema que contém chaves do aplicativo. Contudo, 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.

Garantir a compatibilidade com Citrix PVS. É possível ativar o suporte ao Citrix Provisioning Services para instalar o Kaspersky Endpoint Security em uma máquina virtual.

Adicionar o caminho para o arquivo avp.com à variável do sistema %PATH%. É possível adicionar o caminho de instalação à variável %PATH% para uso adequado da interface da linha de comando.

Como instalar o EDR Agent na linha de comando (somente para KATA (EDR) e EDR Expert (on-premises))

1. Execute o interpretador da linha de comando (cmd.exe) como um administrador.

2. Vá até a pasta onde o pacote de distribuição do Kaspersky Endpoint Security está localizado.

3. Execute o seguinte comando:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pSTANDALONEMODE=1 [/s]
   ```

   ou

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
   ```

   Como resultado, o aplicativo EDR Agent para integração com a Kaspersky Anti Targeted Attack Platform (EDR) ou o Kaspersky Endpoint Detection and Response Expert (on-premises) é instalado no computador. É possível confirmar se o aplicativo está instalado e verificar as suas configurações ao enviar o comando `status`.

Como instalar o EDR Agent no Console de Administração (MMC)

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

2. Na árvore do console, selecione a pasta **Avançado** → **Instalação remota** → **Pacotes de instalação**.

   Isso abre uma lista de pacotes de instalação que foram baixados no Kaspersky Security Center.

3. Abra as propriedades do pacote de instalação.

   Caso seja necessário, crie um novo pacote de instalação.

4. Ir para a seção **Componentes de proteção**.

5. Selecione a configuração **Endpoint Detection and Response Agent para garantir a proteção contra ameaças avançadas e ataques direcionados**. Nesta configuração, é possível instalar apenas os componentes que fornecem suporte para as soluções Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), assim como KUMA. Essa configuração será necessária caso uma Endpoint Protection Platform (EPP) de terceiros seja implantada na sua organização juntamente com uma solução Kaspersky Detection and Response. Isso torna o Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent compatível com os aplicativos EPP de terceiros.

6. Selecione os componentes que deseja instalar.

   Você pode alterar os componentes disponíveis do aplicativo depois de concluir a instalação do aplicativo.

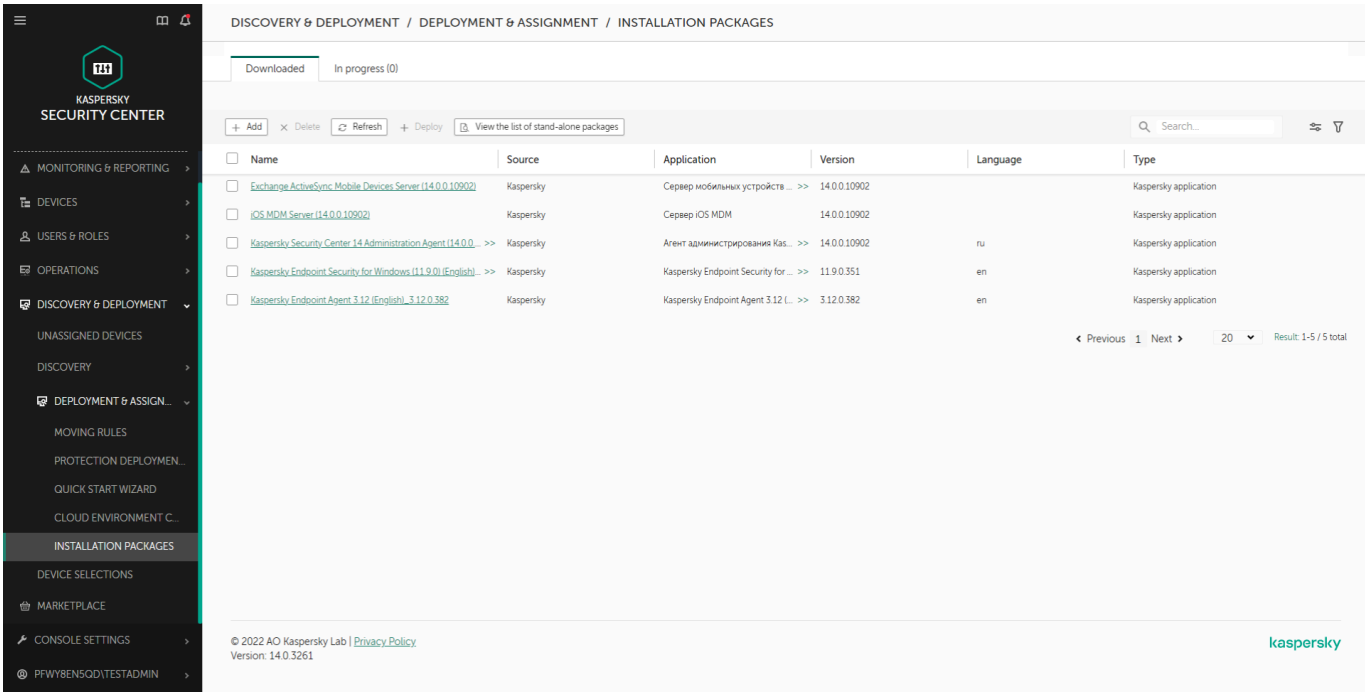
7. Salvar alterações.

8. Crie uma tarefa de instalação remota. Nas propriedades da tarefa, selecione o pacote de instalação criado.

Como instalar o EDR Agent usando o Web Console

1. Na janela principal do Web Console, selecione **Descoberta e implementação** → **Implementação e atribuição** → **Pacotes de instalação**.

   Isso abre uma lista de pacotes de instalação que foram baixados no Kaspersky Security Center.



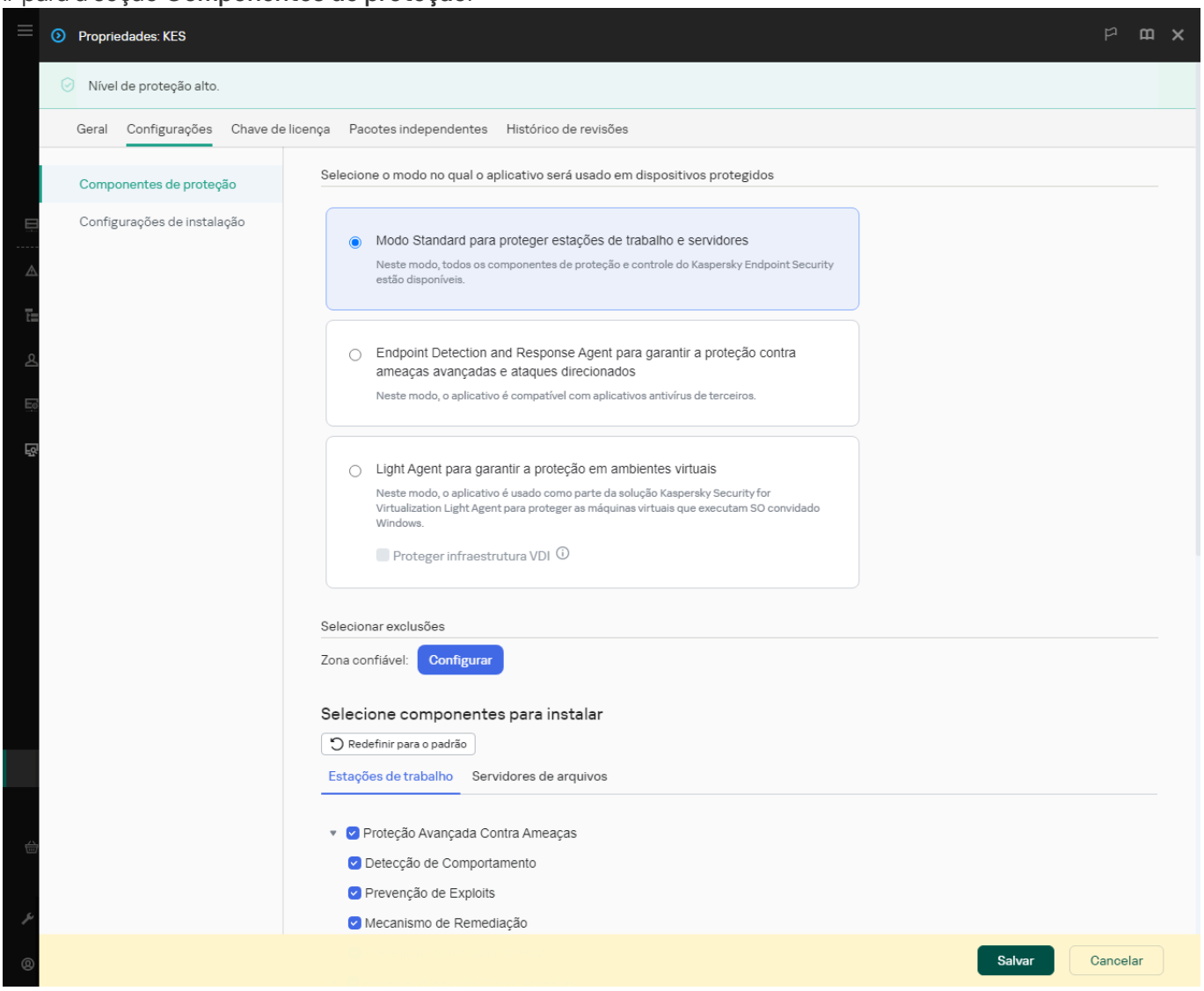
Lista de pacotes de instalação

2. Abra as propriedades do pacote de instalação.

   Caso seja necessário, crie um novo pacote de instalação.

3. Selecione a guia **Configurações**.

4. Ir para a seção **Componentes de proteção**.



Componentes incluídos no pacote de instalação

5. Selecione a configuração **Endpoint Detection and Response Agent**. Nesta configuração, é possível instalar apenas os componentes que fornecem suporte para as soluções Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), assim como KUMA. Essa configuração será necessária caso uma Endpoint Protection Platform (EPP) de terceiros seja implantada na sua organização juntamente com uma solução Kaspersky Detection and Response. Isso torna o Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent compatível com os aplicativos EPP de terceiros.

6. Selecione os componentes que deseja instalar.

   Você pode alterar os componentes disponíveis do aplicativo depois de concluir a instalação do aplicativo.

7. Salvar alterações.

8. Crie uma tarefa de instalação remota. Nas propriedades da tarefa, selecione o pacote de instalação criado.

Assim, o EDR Agent será instalado no computador do usuário. É possível usar a interface do aplicativo. Um um ícone do aplicativo será exibido na área de notificação .

No Kaspersky Security Center, o computador com o aplicativo instalado na configuração do EDR Agent tem o status *Crítico* – . O computador tem esse status porque o componente Proteção Contra Ameaças ao Arquivo está ausente. Não é necessário executar nenhuma outra ação.

Caso não tenha conseguido instalar o EDR Agent em um computador com um aplicativo EPP de terceiros porque o instalador encontrou software incompatível no computador, é possível pular a verificação de compatibilidade de software.

Janela principal do EDR Agent

Agora, é necessário configurar a integração com a solução Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack (EDR) ou Kaspersky Anti Targeted Attack (NDR) Também é possível especificar as configurações avançadas do aplicativo e, por exemplo, criar uma zona confiável ou ocultar a interface do aplicativo. As configurações nas seguintes seções estão disponíveis:

- Kaspersky Security Network
- Configurações do aplicativo
- Configurações de rede
- Exclusões
- Relatórios

- Interface
- Gerenciar configurações

Integrando o EDR Agent com MDR

O EDR Agent é instalado nas estações de trabalho e servidores na infraestrutura de TI da organização. O EDR Agent processa dados e os envia por meio de fluxos da Kaspersky Security Network para o Kaspersky Managed Detection and Response.

Para que o Kaspersky Managed Detection and Response funcione com o Servidor de Administração por meio do Kaspersky Security Center Web Console, é necessário 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 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**

   É possível selecionar o componente MDR durante a instalação ou atualização, assim como usando a tarefa *Alterar componentes do aplicativo*.

   > Para instalar o componente Managed Detection and Response sem reiniciar o computador usando a tarefa *Alterar componentes do aplicativo*, é necessário desativar a opção **Verificar se há aplicativos incompatíveis de terceiros** nas configurações da tarefa.

2. **Configuração da Kaspersky Private Security Network**

   > Ignore esta etapa se estiver usado o Kaspersky Security Center Cloud Console. O Kaspersky Security Center Cloud Console configura automaticamente o Kaspersky Security Network local ao instalar o plugin MDR.

   A *Kaspersky Private Security Network (KPSN)* é uma solução que permite aos usuários de computadores que hospedam o Kaspersky Endpoint 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.

   Carregue o arquivo de configuração da Kaspersky Security Network nas propriedades do Servidor de Administração. O arquivo de configuração da Kaspersky Security Network está localizado dentro do arquivo ZIP do arquivo de configuração MDR. É possível obter o arquivo ZIP no Console do Kaspersky Managed Detection and Response. Para obter detalhes sobre a configuração da Kaspersky Security Network, consulte a ajuda do Kaspersky Security Center. Também é possível carregar um arquivo de configuração da Kaspersky Security Network para o computador a partir da linha de comando (veja as instruções abaixo).

Como configurar o Kaspersky Security Network a partir da linha de comando

1. Execute o interpretador da linha de comando (cmd.exe) como um administrador.

2. Vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

3. Execute o seguinte comando:

```
avp.com KSN /private <file name>
```

onde `<file name>` é o nome do arquivo de configuração contendo as configurações da Kaspersky Private Security Network (formato de arquivo PKCS7 ou PEM).

Exemplo:
```
avp.com KSN /private C:\kpsn_config.pkcs7
```

Como resultado, o Kaspersky Endpoint Security usará a Kaspersky Private Security Network para determinar a reputação dos arquivos, aplicativos e sites. A seção **Kaspersky Security Network** das configurações da política exibirá o seguinte status operacional: *Infraestrutura: Kaspersky Private Security Network*.

É necessário ativar o modo KSN estendido para que a Managed Detection and Response funcione.

3 **Ativação do Kaspersky Managed Detection and Response**

A partir da versão 12.10 do Kaspersky Endpoint Security for Windows, também é possível utilizar um arquivo de chave, como uma alternativa a um código de ativação, para ativar a funcionalidade Managed Detection and Response.

É preciso comprar uma licença separada para o MDR (add-on do Kaspersky Managed Detection and Response).

A funcionalidade estará disponível após a adição de uma chave separada para o add-on do Kaspersky Managed Detection and Response. O licenciamento para a funcionalidade autônoma do Managed Detection and Response é o mesmo do Kaspersky Endpoint Security.

Certifique-se de que a funcionalidade MDR esteja incluída na licença e esteja sendo executada na interface local do aplicativo.

4 **Ativar o componente Managed Detection and Response**

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

A partir do Kaspersky Endpoint Security 12.6 for Windows, a adição de um arquivo BLOB é opcional para o Kaspersky Managed Detection and Response sem locatários caso tenha uma licença atual.

Como ativar o componente Managed Detection and Response no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.

4. Marque a caixa de seleção **Managed Detection and Response (Industrial CyberSecurity)**.

5. No bloco **Configurações**, clique em **Carregar** e selecione o arquivo BLOB recebido no console do Kaspersky Managed Detection and Response. O arquivo tem uma extensão P7.

   Por padrão, o usuário tem permissão para gerenciar as configurações do aplicativo (o "cadeado" fica aberto). Para aplicar a política em computadores, feche os cadeados .

6. Salvar alterações.

Como ativar o componente Managed Detection and Response no Web Console e Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configuração de agentes integrados** → **Managed Detection and Response**.

5. Ative o botão de alternância **Managed Detection and Response ATIVADO**.

6. Clique em **Carregar** e selecione o arquivo BLOB obtido no Console do Kaspersky Managed Detection and Response. O arquivo tem uma extensão P7.

   Por padrão, o usuário tem permissão para gerenciar as configurações da política (o "cadeado" fica aberto). Para aplicar a política em computadores, feche os cadeados .

7. Salvar alterações.

Como ativar o componente Managed Detection and Response a partir da linha de comando

1. Execute o interpretador da linha de comando (cmd.exe) como um administrador.

2. Vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

3. Execute o seguinte comando:

```
avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
```

   Para executar este comando a Proteção por senha deve estar ativada. O usuário deve ter a permissão **Configurar o aplicativo**.

Como resultado, o Kaspersky Endpoint Security verificará o arquivo BLOB. A verificação do arquivo BLOB inclui a verificação da assinatura digital e do período da licença. Caso o arquivo BLOB seja verificado com sucesso, o Kaspersky Endpoint Security baixará e enviará o arquivo para o computador durante a próxima sincronização com o Kaspersky Security Center. Verifique o status operacional do componente visualizando o *Relatório de status dos componentes do aplicativo*. Também é possível visualizar o status operacional de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente do **Managed Detection and Response** será adicionado na lista de componentes do Kaspersky Endpoint Security.

5. **Configuração de outros componentes do aplicativo para receber telemetria**

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

   - Kaspersky Security Network (modo estendido).
   - Detecção de Comportamento.
   - Prevenção de Exploit.
   - Proteção Contra Ameaças da Web.
   - Proteção Contra Ameaças ao Correio.
   - Proteção Contra Ameaças ao Arquivo.
   - Proteção Contra Ameaças à Rede.
   - Firewall.
   - Proteção AMSI.
   - Verificação em segundo plano.

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

        A janela de propriedades da política é exibida.
     3. Selecione a guia **Configurações do aplicativo**.
     4. Selecione **Configuração de agentes integrados** → **Managed Detection and Response**.
     5. Ative o botão de alternância **Managed Detection and Response ATIVADO**.
     6. Salvar alterações.

     1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
     2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
     3. Na janela da política, selecione **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
     4. Marque a caixa de seleção **Managed Detection and Response (Industrial CyberSecurity)**.
     5. Salvar alterações.

Integrando o EDR Agent com EDR (KATA)

O EDR Agent é instalado nas estações de trabalho e servidores na infraestrutura de TI da organização. Nesses computadores, o EDR Agent monitora continuamente os processos, as conexões de rede abertas e os arquivos em modificação, e envia os dados de monitoramento para o servidor com o componente Central Node.

Para se integrar com o EDR (KATA), é necessário ativar o componente Endpoint Detection and Response (KATA) e configurar o EDR Agent.

As seguintes condições devem ser atendidas para que o Endpoint Detection and Response (KATA) funcione:

- Kaspersky Anti Targeted Attack Platform versões 5.0–7.1.
- Kaspersky Security Center versão 14.2 ou posterior. Em versões anteriores do Kaspersky Security Center, é impossível ativar o recurso Endpoint Detection and Response (KATA).

https://www.youtube.com/watch?v=cZzgtBoeC7k

A integração com o Endpoint Detection and Response (KATA) compreende as seguintes etapas:

1. **Ativação do componente Endpoint Detection and Response (KATA)**

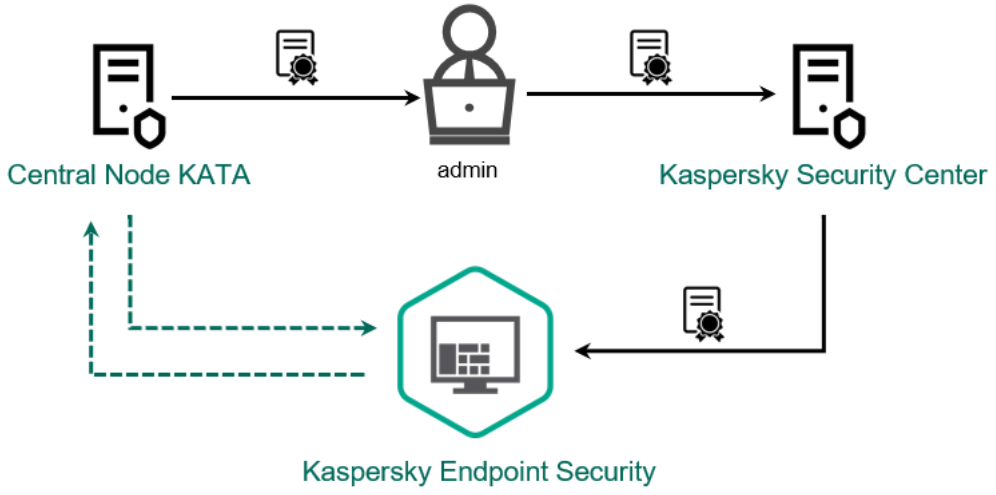
   É preciso comprar uma licença separada para o EDR (KATA) (add-on do Kaspersky Endpoint Detection and Response (KATA)).

   O recurso estará disponível após a adição de uma chave separada para o Kaspersky Endpoint Detection and Response (KATA). A licença para a funcionalidade independente Endpoint Detection and Response (KATA) é a mesma que a licença do Kaspersky Endpoint Security.

   Verifique e confirme se a funcionalidade EDR (KATA) está incluída na licença e se está sendo executada na interface local do aplicativo.

2. **Conexão com o Central Node**

A Kaspersky Anti Targeted Attack Platform requer o estabelecimento de uma conexão confiável entre o Kaspersky Endpoint Security e o componente Central Node. Para configurar uma conexão confiável, é necessário usar um certificado TLS. É possível obter um certificado TLS no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform). Em seguida, é necessário adicionar o certificado TLS ao Kaspersky Endpoint Security (consulte as instruções abaixo).



Adição de um certificado TLS ao Kaspersky Endpoint Security

Por padrão, o Kaspersky Endpoint Security verifica apenas o certificado TLS do Central Node. Para tornar a conexão mais segura, também é possível ativar a verificação do computador no Central Node (autenticação bidirecional). Para ativar essa verificação, é necessário ativar a autenticação bidirecional nas configurações do Central Node e do Kaspersky Endpoint Security. Para usar a autenticação bidirecional, também será necessário um contêiner criptográfico. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner criptográfico no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform).

Como conectar um computador Kaspersky Endpoint Security ao Central Node com o uso do Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Detection and Response** → **Endpoint Detection and Response Expert (on-premises)**.
5. Marque a caixa de seleção **Endpoint Detection and Response Expert (on-premises)**.
6. Clique **Configurações de conexão do servidor**.
7. Configure a conexão do servidor:
   - **Tempo limite (seg)**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite se esgota, o Kaspersky Endpoint Security tenta estabelecer conexão com um servidor de Central Node diferente.
   - **Certificado TLS do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor do Central Node. É possível obter um certificado TLS no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform).

- **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor do Central Node, obter um contêiner de criptografia e definir uma senha para proteger o contêiner criptográfico. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner criptográfico no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform). Depois de definir as configurações do Central Node, é necessário também habilitar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner criptográfico protegido por senha.

  O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.

8. Clique **OK**.

9. Adicionar servidores de Central Node. Para fazer isso, especifique o endereço do servidor (IPv4, IPv6) e a porta para se conectar ao servidor.

   É possível adicionar vários endereços de servidor do nó central. O Kaspersky Endpoint Security tenta se conectar ao servidor usando o primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar usando o segundo endereço IP na lista e assim sucessivamente.

10. Caso necessário, configure a telemetria.

11. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como conectar um computador Kaspersky Endpoint Security ao Central Node usando o Web Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configuração de agentes integrados** → **Endpoint Detection and Response Expert (on-premises)**.

5. Ative o botão de alternância **Endpoint Detection and Response Expert (on-premises) ATIVADO**.

6. Para configurar o EDR (KATA), selecione **Endpoint Detection and Response Expert (versão 7.1 ou anterior)** pela lista de soluções.

7. Clique **Configurações de conexão**.

8. Configure a conexão do servidor:

   - **Tempo limite (s)**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite se esgota, o Kaspersky Endpoint Security tenta estabelecer conexão com um servidor de Central Node diferente.

   - **Certificado do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor do Central Node. É possível obter um certificado TLS no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform).

- **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor do Central Node, obter um contêiner de criptografia e definir uma senha para proteger o contêiner criptográfico. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner criptográfico no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform). Depois de definir as configurações do Central Node, é necessário também habilitar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner criptográfico protegido por senha.

  O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.

9. Clique **OK**.

10. Adicionar servidores de Central Node. Para fazer isso, especifique o endereço do servidor (IPv4, IPv6) e a porta para se conectar ao servidor.

    É possível adicionar vários endereços de servidor do nó central. O Kaspersky Endpoint Security tenta se conectar ao servidor usando o primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar usando o segundo endereço IP na lista e assim sucessivamente.

11. Caso necessário, configure a telemetria.

12. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como resultado, o computador é adicionado ao console da Kaspersky Anti Targeted Attack Platform. Verifique o status operacional do componente visualizando o *Relatório de status dos componentes do aplicativo*. Também é possível visualizar o status operacional de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente do **Endpoint Detection and Response Expert (on-premises)** será adicionado na lista de componentes do Kaspersky Endpoint Security.

Integrando o EDR Agent com NDR (KATA)

O EDR Agent é instalado nas estações de trabalho e servidores na infraestrutura de TI da organização. Nesses computadores, o EDR Agent monitora continuamente os processos, as conexões de rede abertas e os arquivos em modificação, e envia os dados de monitoramento para o servidor com o componente Central Node.

Para se integrar com o NDR (KATA), é necessário ativar o componente Network Detection and Response (KATA) e configurar o EDR Agent.

As seguintes condições devem ser atendidas para que o Network Detection and Response (KATA) funcione:

- Kaspersky Anti Targeted Attack Platform versão 7.0 ou posterior.
- Kaspersky Security Center versão 14.2 ou posterior. Em versões anteriores do Kaspersky Security Center, é impossível ativar o recurso Network Detection and Response (KATA).

https://www.youtube.com/watch?v=gd-rySv0ThQ

A integração com o Network Detection and Response (KATA) compreende as seguintes etapas:

1. **Ativação do componente Network Detection and Response (KATA)**

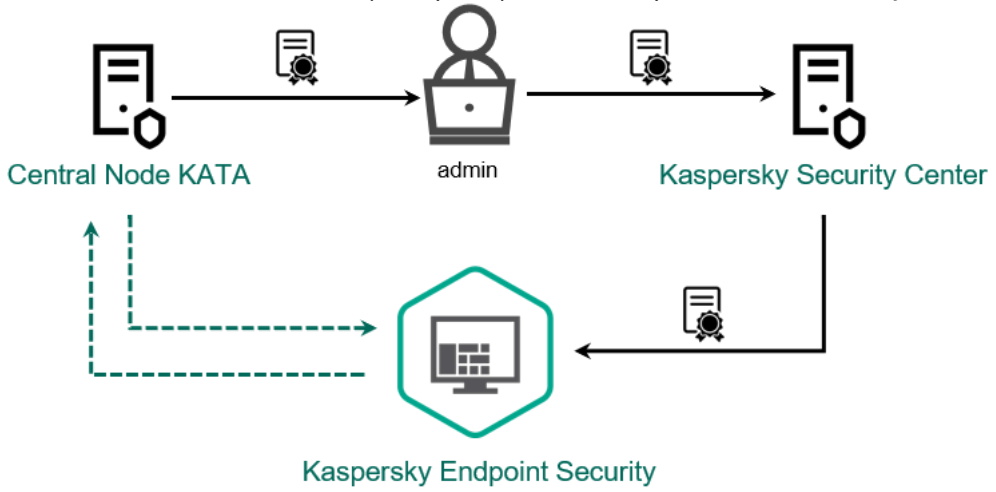
   É preciso comprar uma licença separada para o NDR (KATA) (add-on do Kaspersky Network Detection and Response (KATA)).

   O recurso estará disponível após a adição de uma chave separada para o Kaspersky Network Detection and Response (KATA). A licença para a funcionalidade independente Network Detection and Response (KATA) é a mesma que a licença do Kaspersky Endpoint Security.

   Verifique e confirme se a funcionalidade NDR (KATA) está incluída na licença e se está sendo executada na interface local do aplicativo.

2. **Conexão com o Central Node**

   A Kaspersky Anti Targeted Attack Platform requer o estabelecimento de uma conexão confiável entre o Kaspersky Endpoint Security e o componente Central Node. Para configurar uma conexão confiável, é necessário usar um certificado TLS. É possível obter um certificado TLS no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform). Em seguida, é necessário adicionar o certificado TLS ao Kaspersky Endpoint Security (consulte as instruções abaixo).



Adição de um certificado TLS ao Kaspersky Endpoint Security

Por padrão, o Kaspersky Endpoint Security verifica apenas o certificado TLS do Central Node. Para tornar a conexão mais segura, também é possível ativar a verificação do computador no Central Node (autenticação bidirecional). Para ativar essa verificação, é necessário ativar a autenticação bidirecional nas configurações do Central Node e do Kaspersky Endpoint Security. Para usar a autenticação bidirecional, também será necessário um contêiner criptográfico. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner criptográfico no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform).

Como conectar um computador Kaspersky Endpoint Security ao Central Node com o uso do Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Detection and Response** → **Network Detection and Response (KATA)**.
4. Marque a caixa de seleção **Network Detection and Response (KATA)**.
5. Clique **Configurações de conexão**.
6. Configure a conexão do servidor:
   - **Tempo limite (s)**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite se esgota, o Kaspersky Endpoint Security tenta estabelecer conexão com um servidor de Central Node diferente.
   - **Certificado do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor do Central Node. É possível obter um certificado TLS no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform).
   - **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor do Central Node, obter um contêiner de criptografia e definir uma senha para proteger o contêiner criptográfico. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner criptográfico no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform). Depois de definir as configurações do Central Node, é necessário também habilitar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner criptográfico protegido por senha.

     O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.
7. Clique **OK**.
8. Adicionar servidores de Central Node. Para fazer isso, especifique o endereço do servidor (IPv4, IPv6) e a porta para se conectar ao servidor.
9. É possível adicionar vários endereços de servidor do nó central. O Kaspersky Endpoint Security tenta se conectar ao servidor usando o primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar usando o segundo endereço IP na lista e assim sucessivamente.

10. Caso necessário, configure a telemetria.

11. Salvar alterações.

Como conectar um computador Kaspersky Endpoint Security ao Central Node usando o Web Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configuração de agentes integrados** → **Network Detection and Response (KATA)**.

5. Ative o botão de alternância **Network Detection and Response (KATA) ATIVADO**.

6. Clique **Configurações de conexão**.

7. Configure a conexão do servidor:

   - **Tempo limite (s)**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite se esgota, o Kaspersky Endpoint Security tenta estabelecer conexão com um servidor de Central Node diferente.

   - **Certificado do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor do Central Node. É possível obter um certificado TLS no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform).

   - **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor do Central Node, obter um contêiner de criptografia e definir uma senha para proteger o contêiner criptográfico. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner criptográfico no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform). Depois de definir as configurações do Central Node, é necessário também habilitar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner criptográfico protegido por senha.

     O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.

8. Clique **OK**.

9. Adicionar servidores de Central Node. Para fazer isso, especifique o endereço do servidor (IPv4, IPv6) e a porta para se conectar ao servidor.

10. É possível adicionar vários endereços de servidor do nó central. O Kaspersky Endpoint Security tenta se conectar ao servidor usando o primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar usando o segundo endereço IP na lista e assim sucessivamente.

11. Caso necessário, configure a telemetria.

12. Salvar alterações.

Como resultado, o computador é adicionado ao console da Kaspersky Anti Targeted Attack Platform. Verifique o status operacional do componente visualizando o *Relatório de status dos componentes do aplicativo*. Também é possível visualizar o status operacional de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente do **Network Detection and Response (KATA)** será adicionado na lista de componentes do Kaspersky Endpoint Security.

Integração do EDR Agent com EDR Expert (on-premises)

O EDR Agent é instalado nas estações de trabalho e servidores na infraestrutura de TI da organização. Nesses computadores, o EDR Agent monitora continuamente os processos, as conexões de rede abertas e os arquivos sendo modificados, e envia os dados de monitoramento para o servidor EDR Expert (on-premises).

Para se integrar ao EDR Expert (on-premises), é necessário ativar o componente Endpoint Detection and Response Expert (on-premises) e configurar o EDR Agent.

A integração com o Endpoint Detection and Response Expert (on-premises) compreende as seguintes etapas:

1. **Ativar o Kaspersky Endpoint Detection and Response Expert (on-premises)**

   É preciso comprar uma licença separada para o EDR Expert (on-premises) (add-on do Kaspersky Endpoint Detection and Response Expert (on-premises)).

   A funcionalidade estará disponível após a adição de uma chave separada para o Kaspersky Endpoint Detection and Response Expert (on-premises). A licença para a funcionalidade independente Endpoint Detection and Response Expert (on-premises) é a mesma que a licença do Kaspersky Endpoint Security.

   Verifique se a funcionalidade EDR Expert (on-premises) está incluída na licença e em execução na interface local do aplicativo.

2. **Conexão com servidor de coleta de telemetria e servidor de reposta**

   O Kaspersky Endpoint Detection and Response Expert (on-premises) requer uma conexão confiável entre o Kaspersky Endpoint Security e dois servidores:

   - Um *servidor de coleta de telemetria* é um servidor que faz parte de uma solução SIEM que coleta, normaliza, correlaciona, analisa e armazena informações sobre eventos que ocorrem no computador.
   - Um *servidor de resposta* é um dispositivo que recebe e verifica dados, estuda o comportamento de objetos e publica os resultados desses estudos.

   Para configurar uma conexão confiável, é necessário usar um certificado TLS. É possível obter um certificado TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). Em seguida, é necessário adicionar o certificado TLS ao Kaspersky Endpoint Security (consulte as instruções abaixo).

   Por padrão, o Kaspersky Endpoint Security verifica apenas o certificado TLS dos servidores. Para tornar a conexão mais segura, também é possível ativar a verificação do computador no servidor (autenticação bidirecional). Para ativar essa verificação, é necessário ativar a autenticação bidirecional nas configurações do servidor e do Kaspersky Endpoint Security. Para usar a autenticação bidirecional, também será necessário um contêiner criptográfico. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner de criptografia na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)).

Como conectar um computador com o Kaspersky Endpoint Security ao EDR Expert (on-premises) usando o Web Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configuração de agentes integrados** → **Endpoint Detection and Response Expert (on-premises)**.

5. Ative o botão de alternância **Endpoint Detection and Response Expert (on-premises) ATIVADO**.

6. Para configurar o EDR Expert (on-premises), selecione **Endpoint Detection and Response Expert (versão 8.0 ou posterior)** na lista de soluções.

7. Configure a conexão dos *servidores de coleta de telemetria*:

   a. No bloco **Conexão com servidores de coleta de telemetria**, clique no link **Configurações de conexão**.

   b. Configure a conexão dos servidores de coleta de telemetria:

      - **Tempo limite (s)**. Tempo limite máximo de resposta do servidor. Quando o tempo limite se esgotar, o Kaspersky Endpoint Security tentará estabelecer conexão com um servidor diferente.

      - **Certificado do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor. É possível obter um certificado TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)).

      - **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor, obter um contêiner de criptografia e definir uma senha para protegê-lo. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner de criptografia na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). Depois de definir as configurações do servidor, é necessário também ativar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner de criptografia protegido por senha.

        O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.

   c. Clique **OK**.

d. Adicione servidores de coleta de telemetria. Para fazer isso, especifique o endereço do servidor (IPv4, IPv6) e a porta para se conectar ao servidor.

É possível adicionar vários endereços de servidores de coleta de telemetria. O Kaspersky Endpoint Security tenta se conectar ao servidor usando o primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar usando o segundo endereço IP na lista e assim sucessivamente.

e. Caso necessário, configure a telemetria.

8. Configure a conexão dos *servidores de reposta*:

a. No bloco **Conexão com servidores de resposta**, defina as configurações de **Enviar solicitação de sincronização para o servidor a cada (min.)**. Frequência de solicitações de sincronização enviadas ao servidor. Durante a sincronização, o Kaspersky Endpoint Security receberá tarefas de resposta a ameaças e enviará os resultados da tarefa.

b. Clique no link **Configurações de conexão**.

c. Configure a conexão dos servidores de reposta:

- **Tempo limite (s)**. Tempo limite máximo de resposta do servidor. Quando o tempo limite se esgotar, o Kaspersky Endpoint Security tentará estabelecer conexão com um servidor diferente.

- **Certificado do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor. É possível obter um certificado TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor, obter um contêiner de criptografia e definir uma senha para protegê-lo. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner de criptografia na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). Depois de definir as configurações do servidor, é necessário também ativar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner de criptografia protegido por senha.

  O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.

d. Clique **OK**.

e. Adicione os servidores de reposta. Para fazer isso, especifique o endereço do servidor (IPv4, IPv6) e a porta para se conectar ao servidor.

É possível adicionar vários endereços do servidor de resposta. O Kaspersky Endpoint Security tenta se conectar ao servidor usando o primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar usando o segundo endereço IP na lista e assim sucessivamente.

9. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como resultado, o computador será adicionado na Open Single Management Platform (OSMP). Verifique o status operacional do componente visualizando o *Relatório de status dos componentes do aplicativo*. Também é possível visualizar o status operacional de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente do **Endpoint Detection and Response Expert (on-premises)** será adicionado na lista de componentes do Kaspersky Endpoint Security.

Compatibilidade com aplicativos EPP de terceiros

O EDR Agent oferece suporte à funcionalidade das soluções Kaspersky Detection and Response. Os componentes de proteção e controle não estão disponíveis para o EDR Agent. Essa configuração permite instalar aplicativos EPP de terceiros e implantar soluções Kaspersky Detection and Response na infraestrutura da organização.

O EDR Agent é compatível com aplicativos EPP dos seguintes fornecedores:

- **Dr.Web**

  O Agente EDR é compatível com o Dr.Web Agent for Windows versão 13 e com o Dr.Web Server (x64) 13.0.0.10200.

- **Dallas Lock**

  O Agente EDR é compatível com a versão 843.2 do Dallas Lock 8.0-C.

  Para que o EDR Agent seja executado em um computador que tenha o software Dallas Lock instalado, é necessário permitir a conexão com os serviços externos da Kaspersky nas configurações do módulo Firewall.

- **Secret Net Studio**

  O Agente EDR é compatível com a versão 8.11 (20851) do Secret Net Studio.

  O aplicativo não pode ser instalado em um computador onde o Secret Net Studio estiver implementado com o componente Antivírus. Para possibilitar a interoperabilidade, é necessário remover o componente Antivírus do Secret Net Studio.

- **Trend Micro**

  O Agente EDR é compatível com o Trend Micro Vision One (incluindo a versão 14.0.20731 do Security Agent).

  O Agente EDR é compatível com a versão 20.0.3-18160 do Trend Micro Deep Security (incluindo o Security Agent).

- **Windows Defender**

- **Sophos**

  O Agente EDR é compatível com a versão 2024.1.2 do Sophos Intercept X (incluindo o Endpoint Agent) e com a versão 2026.2.1.3 do Sophos Core Agent.

- **Bitdefender**

  O Agente EDR é compatível com a versão 8.26.7.647 do Bitdefender Endpoint Security Tools.

- **ESET**

  O Agente EDR é compatível com a versão 13.0.2044.0 do ESET Endpoint Security e com a versão 13.2.1189.0 do ESET Management Agent.

O Agente EDR não é compatível com Bitdefender Endpoint Security Tools em computadores que executam o Windows 11 para Arm64.

Os aplicativos devem ser instalados na seguinte ordem: primeiro, instale o aplicativo EPP, depois o Agente de Rede do Kaspersky Security Center e, em seguida, o EDR Agent. Essa ordem é necessária porque o instalador do aplicativo EPP pode detectar o EDR Agent e o Agente de Rede como software incompatível e removê-los. A operação do EDR Agent e do Agente de Rede também deve ser verificada após a atualização do aplicativo EPP de terceiros, pois seu instalador pode verificar novamente o computador em busca de software incompatível e remover os aplicativos.

Caso não tenha conseguido instalar o EDR Agent em um computador com um aplicativo EPP de terceiros porque o instalador encontrou software incompatível no computador, é possível pular a verificação de compatibilidade de software.

Managed Detection and Response

O Kaspersky Endpoint Security for Windows é compatível com a integração da solução Managed Detection and Response. A solução *Kaspersky Managed Detection and Response (MDR)* detecta e analisa automaticamente os incidentes de segurança em sua infraestrutura. Para isso, o MDR usa dados de telemetria recebidos de terminais 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 do Kaspersky Endpoint Security para integração com MDR

As seguintes configurações podem ser usadas para trabalhar com o MDR:

- **[KES+agente integrado]**. Nesta configuração, o Kaspersky Endpoint Security atua como o aplicativo que garante a segurança do computador, assim como o aplicativo que trabalha com o MDR.

- **[EPP de terceiros+EDR Agent]**. Nesta configuração, a segurança da infraestrutura de TI é fornecida pelo Endpoint Protection Platform (EPP) de terceiros. A interação com o MDR é fornecida pelo Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent (Agente EDR). Nesta configuração, o EDR Agent é compatível com aplicativos EPP de terceiros.

Integração do agente integrado com MDR

Para configurar a integração com o Kaspersky Managed Detection and Response, é necessário ativar o componente Managed Detection and Response e configurar o Kaspersky Endpoint Security.

Para que o Kaspersky Managed Detection and Response funcione com o Servidor de Administração por meio do Kaspersky Security Center Web Console, é necessário 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 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**

   É possível selecionar o componente MDR durante a instalação ou atualização, assim como usando a tarefa *Alterar componentes do aplicativo*.

   > Para instalar o componente Managed Detection and Response sem reiniciar o computador usando a tarefa *Alterar componentes do aplicativo*, é necessário desativar a opção **Verificar se há aplicativos incompatíveis de terceiros** nas configurações da tarefa.

2. **Configuração da Kaspersky Private Security Network**

   > Ignore esta etapa se estiver usado o Kaspersky Security Center Cloud Console. O Kaspersky Security Center Cloud Console configura automaticamente o Kaspersky Security Network local ao instalar o plugin MDR.

   A *Kaspersky Private Security Network (KPSN)* é uma solução que permite aos usuários de computadores que hospedam o Kaspersky Endpoint 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.

   Carregue o arquivo de configuração da Kaspersky Security Network nas propriedades do Servidor de Administração. O arquivo de configuração da Kaspersky Security Network está localizado dentro do arquivo ZIP do arquivo de configuração MDR. É possível obter o arquivo ZIP no Console do Kaspersky Managed Detection and Response. Para obter detalhes sobre a configuração da Kaspersky Security Network, consulte a ajuda do Kaspersky Security Center. Também é possível carregar um arquivo de configuração da Kaspersky Security Network para o computador a partir da linha de comando (veja as instruções abaixo).

   Como configurar o Kaspersky Security Network a partir da linha de comando

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

      ```
      avp.com KSN /private <file name>
      ```

onde `<file name>` é o nome do arquivo de configuração contendo as configurações da Kaspersky Private Security Network (formato de arquivo PKCS7 ou PEM).

Exemplo:
```
avp.com KSN /private C:\kpsn_config.pkcs7
```

Como resultado, o Kaspersky Endpoint Security usará a Kaspersky Private Security Network para determinar a reputação dos arquivos, aplicativos e sites. A seção **Kaspersky Security Network** das configurações da política exibirá o seguinte status operacional: *Infraestrutura: Kaspersky Private Security Network*.

É necessário ativar o modo KSN estendido para que a Managed Detection and Response funcione.

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

A partir da versão 12.10 do Kaspersky Endpoint Security for Windows, também é possível utilizar um arquivo de chave, como uma alternativa a um código de ativação, para ativar a funcionalidade Managed Detection and Response.

O Kaspersky Managed Detection and Response é compatível com os seguintes métodos de licenciamento:

- A funcionalidade do Managed Detection and Response está incluída na licença do Kaspersky Endpoint Security for Windows.

  A funcionalidade está disponível imediatamente após a ativação do Kaspersky Endpoint Security for Windows.

- Uma licença separada para o MDR (Kaspersky Managed Detection and Response Add-on) é usada.

  A funcionalidade estará disponível após a adição de uma chave separada para o add-on do Kaspersky Managed Detection and Response. Assim, duas chaves serão instaladas no computador: uma chave para o Kaspersky Endpoint Security e uma para o Kaspersky Managed Detection and Response.

  O licenciamento para a funcionalidade autônoma do Managed Detection and Response é o mesmo do Kaspersky Endpoint Security.

Certifique-se de que a funcionalidade MDR esteja incluída na licença e esteja sendo executada na interface local do aplicativo.

4. **Ativar o componente Managed Detection and Response**

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

A partir do Kaspersky Endpoint Security 12.6 for Windows, a adição de um arquivo BLOB é opcional para o Kaspersky Managed Detection and Response sem locatários caso tenha uma licença atual.

Como ativar o componente Managed Detection and Response no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.

4. Marque a caixa de seleção **Managed Detection and Response (Industrial CyberSecurity)**.

5. No bloco **Configurações**, clique em **Carregar** e selecione o arquivo BLOB recebido no console do Kaspersky Managed Detection and Response. O arquivo tem uma extensão P7.

   Por padrão, o usuário tem permissão para gerenciar as configurações do aplicativo (o "cadeado" fica aberto). Para aplicar a política em computadores, feche os cadeados .

6. Salvar alterações.

Como ativar o componente Managed Detection and Response no Web Console e Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configuração de agentes integrados** → **Managed Detection and Response**.

5. Ative o botão de alternância **Managed Detection and Response ATIVADO**.

6. Clique em **Carregar** e selecione o arquivo BLOB obtido no Console do Kaspersky Managed Detection and Response. O arquivo tem uma extensão P7.

   Por padrão, o usuário tem permissão para gerenciar as configurações da política (o "cadeado" fica aberto). Para aplicar a política em computadores, feche os cadeados .

7. Salvar alterações.

Como ativar o componente Managed Detection and Response a partir da linha de comando

1. Execute o interpretador da linha de comando (cmd.exe) como um administrador.

2. Vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

3. Execute o seguinte comando:

```
avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
```

   Para executar este comando a Proteção por senha deve estar ativada. O usuário deve ter a permissão **Configurar o aplicativo**.

Como resultado, o Kaspersky Endpoint Security verificará o arquivo BLOB. A verificação do arquivo BLOB inclui a verificação da assinatura digital e do período da licença. Caso o arquivo BLOB seja verificado com sucesso, o Kaspersky Endpoint Security baixará e enviará o arquivo para o computador durante a próxima sincronização com o Kaspersky Security Center. Verifique o status operacional do componente visualizando o *Relatório de status dos componentes do aplicativo*. Também é possível visualizar o status operacional de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente do **Managed Detection and Response** será adicionado na lista de componentes do Kaspersky Endpoint Security.

5. **Configuração de outros componentes do aplicativo para receber telemetria**

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

   - Kaspersky Security Network (modo estendido).
   - Detecção de Comportamento.
   - Prevenção de Exploit.
   - Proteção Contra Ameaças da Web.
   - Proteção Contra Ameaças ao Correio.
   - Proteção Contra Ameaças ao Arquivo.
   - Proteção Contra Ameaças à Rede.
   - Firewall.
   - Proteção AMSI.
   - Verificação em segundo plano.

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

        A janela de propriedades da política é exibida.
     3. Selecione a guia **Configurações do aplicativo**.
     4. Selecione **Configuração de agentes integrados** → **Managed Detection and Response**.
     5. Ative o botão de alternância **Managed Detection and Response ATIVADO**.
     6. Salvar alterações.

     1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
     2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
     3. Na janela da política, selecione **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
     4. Marque a caixa de seleção **Managed Detection and Response (Industrial CyberSecurity)**.
     5. Salvar alterações.

Guia de migração do KEA para KES para o MDR

O Kaspersky Endpoint Security for Windows inclui um agente integrado para a solução Kaspersky Managed Detection and Response. Não é mais necessário um aplicativo separado do Kaspersky Endpoint Agent para funcionar com o MDR. Todas as funções do Kaspersky Endpoint Agent serão executadas pelo Kaspersky Endpoint Security.

Quando o Kaspersky Endpoint Security for implantado em computadores com o Kaspersky Endpoint Agent instalado, a solução Kaspersky Managed Detection and Response continuará funcionando com o Kaspersky Endpoint Security. Além disso, o Kaspersky Endpoint Agent será removido do computador. O mesmo comportamento no sistema ocorrerá quando você atualizar o Kaspersky Endpoint Security para a versão 11.6.0 ou posterior.

O Kaspersky Endpoint Security não é compatível com o Kaspersky Endpoint Agent. Não é possível instalar os dois aplicativos no mesmo computador.

As seguintes condições devem ser atendidas para que o Kaspersky Endpoint Security funcione como parte do Kaspersky Managed Detection and Response:

- Kaspersky Security Center versão 13.2 ou posterior (incluindo o Agente de Rede). Em versões anteriores do Kaspersky Security Center, é impossível ativar o recurso Managed Detection and Response.
- A conexão em segundo plano entre o Kaspersky Security Center Web Console e o servidor de administração foi estabelecida. Para que o MDR trabalhe com o Servidor de Administração por meio do Kaspersky Security Center Web Console, é preciso estabelecer uma nova conexão segura, uma *conexão em segundo plano*.

Etapas para migrar a configuração [KES+KEA] para [KES+agente integrado] para o MDR

1. **Atualizar o plug-in de gerenciamento do Kaspersky Endpoint Security**

   O componente MDR pode ser gerenciado usando o plug-in de gerenciamento do Kaspersky Endpoint Security versão 11.6 ou posterior. Dependendo do tipo de console do Kaspersky Security Center que está sendo utilizado, atualize o plug-in de gerenciamento no Console de administração (MMC) ou o plug-in da Web no Web Console.

2. **Migrar as políticas e tarefas**

   Transfira as configurações do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows. As seguintes opções estão disponíveis:

   - Um assistente para migrar do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security. O assistente para migrar do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security funciona apenas no Web Console.

     Como migrar as configurações de políticas e tarefas do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security no Web Console

     Na janela principal do Web Console, selecione **Operações** → **Migração a partir do Kaspersky Endpoint Agent**.

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

Etapa 1. Migração da política

O assistente de migração cria uma nova política que unifica as configurações das políticas do Kaspersky Endpoint Security e Kaspersky Endpoint Agent. Na lista de política, selecione as políticas do Kaspersky Endpoint Agent cujas configurações deseja unificar as políticas do Kaspersky Endpoint Security. Clique na política do Kaspersky Endpoint Agent para selecionar a política do Kaspersky Endpoint Security com o qual deseja unificar as configurações. Certifique-se de ter selecionado as políticas corretas e vá para a próxima etapa.

Etapa 2. Migração da tarefa

O assistente de migração não é compatível com tarefas do MDR. Ignorar esta etapa.

Etapa 3. Conclusão do Assistente

Conclua o assistente. Como resultado do assistente, uma nova política do Kaspersky Endpoint Security será criada. A política unifica as configurações do Kaspersky Endpoint Security e Kaspersky Endpoint Agent. A política é chamada *<nome da política Kaspersky Endpoint Security> & <nome da política Kaspersky Endpoint Agent>*. A nova política possui o status *Inativo*. Para continuar, mude os status das políticas do Kaspersky Endpoint Agent e Kaspersky Endpoint Security para *Inativo* e ative a nova política unificada.

- Um assistente padrão de conversão em lote de políticas e tarefas. O assistente de conversão em lote de políticas e tarefas está disponível apenas no Console de Administração (MMC). Para obter mais informações sobre o assistente de conversão em lote de políticas e tarefas, consulte a Ajuda do Kaspersky Security Center.

3. **Licenciamento da funcionalidade do MDR**

Para ativar o Kaspersky Endpoint Security como parte da solução Kaspersky Managed Detection and Response, é necessária uma licença separada para o add-on do Kaspersky Managed Detection and Response. É possível adicionar a chave utilizando a tarefa *Adicionar chave*. Como resultado, duas chaves serão adicionadas ao aplicativo: *Kaspersky Endpoint Security* e *Kaspersky Managed Detection and Response*.

4. **Instalação/atualização do aplicativo Kaspersky Endpoint Security**

Para migrar a funcionalidade do MDR durante a instalação ou upgrade de um aplicativo, é recomendável usar a tarefa de instalação remota. Ao criar uma tarefa de instalação remota, selecione o componente do MDR nas configurações do pacote de instalação.

Também é possível baixar o aplicativo utilizando os seguintes métodos:

- Uso do serviço de atualização da Kaspersky.
- Localmente, usando o Assistente de configuração.

O Kaspersky Endpoint Security é compatível com a seleção automática de componentes ao atualizar o aplicativo em um computador com o aplicativo Kaspersky Endpoint Agent instalado. A seleção automática dos componentes depende das permissões da conta do usuário que está atualizando o aplicativo.

Caso esteja atualizando o Kaspersky Endpoint Security com um arquivo EXE ou MSI com a conta do sistema (SYSTEM), o Kaspersky Endpoint Security obtém acesso às licenças atualmente em uso das soluções da Kaspersky. Portanto, se o computador tiver o Kaspersky Endpoint Agent instalado e a solução MDR ativada, o instalador do Kaspersky Endpoint Security configurará automaticamente o conjunto de componentes e selecionará o componente MDR. Isso faz com que o Kaspersky Endpoint Security alterne o uso do agente integrado e remova o Kaspersky Endpoint Agent. A execução do instalador do MSI na conta do sistema (SYSTEM) normalmente é feita com a atualização por meio do serviço de atualização da Kaspersky ou ao implementar um pacote de instalação por meio do Kaspersky Security Center.

Caso esteja atualizando o Kaspersky Endpoint Security com um arquivo MSI com uma conta de usuário não privilegiado, o Kaspersky Endpoint Security perde o acesso das licenças atualmente em uso das soluções da Kaspersky. Nesse caso, o Kaspersky Endpoint Security seleciona automaticamente os componentes com base em um conjunto de componentes do Kaspersky Endpoint Agent. Depois disso, o Kaspersky Endpoint Security passa a usar o agente integrado e remove o Kaspersky Endpoint Agent.

O Kaspersky Endpoint Security é compatível com a atualização sem reinicialização do computador. É possível selecionar o modo de atualização do aplicativo nas propriedades da política.

5. **Verificação do funcionamento do aplicativo**

   Se, após a instalação ou atualização do aplicativo, o computador estiver com o status *Crítico* no console do Kaspersky Security Center:

   - Certifique-se de que o computador possui o Agente de Rede versão 13.2 ou posterior instalado.
   - Verifique o status operacional do agente integrado visualizando o *Relatório de status dos componentes do aplicativo*. Caso o componente tenha o status *Não instalado*, instale o componente usando a tarefa *Alterar componentes do aplicativo*. Caso um componente tenha o status *Não coberto pela licença*, certifique-se de que a funcionalidade do agente integrado esteja ativada.
   - Certifique-se de aceitar a Declaração da Kaspersky Security Network na nova política do Kaspersky Endpoint Security for Windows.

Endpoint Detection and Response

O Kaspersky Endpoint Security for Windows inclui um agente integrado para a solução Kaspersky Endpoint Detection and Response Optimum (doravante também "EDR Optimum"). A partir da versão 11.8.0, o Kaspersky Endpoint Security for Windows inclui um agente integrado para a solução Kaspersky Endpoint Detection and Response Expert (doravante também "EDR Expert"). O *Kaspersky Endpoint Detection and Response* é uma gama de soluções para proteger a infraestrutura corporativa de TI contra ameaças cibernéticas avançadas. A funcionalidade das soluções combina a detecção automática de ameaças com a capacidade de reagir a essas ameaças para neutralizar ataques avançados, incluindo novos exploits, ransomwares, ataques sem arquivo, bem como métodos que usam ferramentas de sistema legítimas. O EDR Expert oferece mais monitoramento de ameaças e funcionalidade de resposta do que o EDR Optimum. Para obter informações detalhadas sobre a solução, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

Ferramentas de inteligência contra ameaças

O Kaspersky Endpoint Detection and Response usa as seguintes ferramentas Threat Intelligence:

- Integração com o Kaspersky Threat Intelligence Portal que contém e exibe as informações sobre a reputação de arquivos e endereços da Web.
- Banco de dados de Ameaças da Kaspersky.
- A infraestrutura de serviço na nuvem da Kaspersky Security Network (doravante também chamada de "KSN"), que fornece acesso a arquivos em tempo real, ao site e às informações sobre a reputação de software da base de conhecimento da Kaspersky. A utilização de dados do Kaspersky Security Network garante respostas mais rápidas dos aplicativos da Kaspersky contra as ameaças, melhora o desempenho de alguns componentes de proteção e reduz a possibilidade de falsos positivos.
- Tecnologia Cloud Sandbox que permite executar arquivos detectados em um ambiente isolado e verificar sua reputação.

Princípio de funcionamento da solução

O Kaspersky Endpoint Detection and Response revisa e analisa o desenvolvimento de ameaças e fornece à *equipe de segurança* ou ao *Administrador* as informações sobre o possível ataque necessárias para uma resposta oportuna. O Kaspersky Endpoint Detection and Response exibe os detalhes de alertas e uma janela separada. Um *alerta* é um evento na infraestrutura de TI corporativa que o aplicativo identificou como incomum ou suspeito e que pode representar uma ameaça de segurança para a infraestrutura de TI corporativa. *Detalhes de alertas* é uma ferramenta para visualizar todas as informações coletadas sobre uma ameaça detectada. Os detalhes da alertas incluem, por exemplo, o histórico de arquivos aparentes no computador. Para obter detalhes sobre o gerenciamento dos detalhes de alertas, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

Compatibilidade com versões anteriores do Kaspersky Endpoint Security

Caso esteja usando o Kaspersky Endpoint Security 11.2.0–11.6.0 para interoperabilidade com o Kaspersky Endpoint Detection and Response Optimum, o aplicativo inclui o Kaspersky Endpoint Agent. É possível instalar o Kaspersky Endpoint Agent durante a instalação do Kaspersky Endpoint Security. No Kaspersky Endpoint Security 11.9.0, o pacote de distribuição do Kaspersky Endpoint Agent não faz mais parte do kit de distribuição do Kaspersky Endpoint Security.

A solução Kaspersky Endpoint Detection and Response Expert não oferece suporte à interoperabilidade com o Kaspersky Endpoint Agent. A solução Kaspersky Endpoint Detection and Response Expert usa o Kaspersky Endpoint Security com agente integrado (versão 11.8.0 e posteriores).

Integração do agente integrado com EDR Optimum / EDR Expert

Para configurar a integração com o Kaspersky Endpoint Detection and Response, é necessário adicionar o componente Endpoint Detection and Response Optimum ou o componente Endpoint Detection and Response Expert (cloud) e configurar o Kaspersky Endpoint Security.

Os componentes Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) e Endpoint Detection and Response Expert (on-premises) não são compatíveis entre si.

As seguintes condições devem ser atendidas para que o Endpoint Detection and Response funcione:

- Kaspersky Security Center versão 13.2 ou posterior. Em versões anteriores do Kaspersky Security Center, é impossível ativar o recurso Endpoint Detection and Response.
- Plug-in de gerenciamento do Kaspersky Endpoint Detection and Response.

  A partir do Kaspersky Endpoint Security versão 12.6, a exibição de detalhes do alerta foi movida do plug-in de gerenciamento do Kaspersky Endpoint Security para o plug-in de gerenciamento do EDR. O plug-in de gerenciamento do EDR é um plug-in único voltado para o trabalho com agentes nos sistemas operacionais Windows, Mac e Linux. Agora, ao trabalhar com o EDR Optimum, o plug-in de gerenciamento do Kaspersky Endpoint Security será necessário para a criação de tarefas de resposta a ameaças, e o plug-in de gerenciamento do EDR será necessário para a exibição dos detalhes do alerta.

- O componente Endpoint Detection and Response Optimum como parte do Kaspersky Endpoint Security é compatível com a interação da solução Kaspersky Endpoint Detection and Response Optimum 2.0. A interação com Kaspersky Endpoint Detection and Response Optimum versão 1.0 não é compatível.

- O EDR Optimum pode ser gerenciado no Kaspersky Security Center Web Console e no Kaspersky Security Center Cloud Console.

  O EDR Expert só pode ser gerenciado usando o Kaspersky Security Center Cloud Console. Não é possível gerenciar essa funcionalidade usando o Console de Administração (MMC).

- O aplicativo é ativado e a funcionalidade é contemplada pela licença.

- O componente Endpoint Detection and Response está ativado.

- Os componentes do aplicativo dos quais o Endpoint Detection and Response depende estão ativados e operacionais. O Endpoint Detection and Response depende dos seguintes componentes:

  - Proteção Contra Ameaças ao Arquivo.
  - Proteção Contra Ameaças da Web.
  - Proteção Contra Ameaças ao Correio.
  - Prevenção de Exploit.
  - Detecção de Comportamento.
  - Prevenção de Intrusão do Host.
  - Mecanismo de Remediação.
  - Controle Adaptativo de Anomalias.

A integração com o Kaspersky Endpoint Detection and Response compreende as seguintes etapas:

1. **Instalar os componentes do Endpoint Detection and Response**

   É possível selecionar o componente Endpoint Detection and Response Optimum ou o componente Endpoint Detection and Response Expert (cloud) durante a instalação ou atualização, assim como usar a tarefa *Alterar componentes do aplicativo*.

   > É preciso reiniciar o computador para concluir a atualização do aplicativo com os novos componentes.

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

   É possível adquirir uma licença para utilizar o Kaspersky Endpoint Detection and Response das seguintes maneiras:

   - A funcionalidade Endpoint Detection and Response está incluída na licença do Kaspersky Endpoint Security for Windows.

     A funcionalidade está disponível imediatamente após a ativação do Kaspersky Endpoint Security for Windows.

- Comprar uma licença separada para o EDR Optimum ou o EDR Expert (add-on do Kaspersky Endpoint Detection and Response).

  A funcionalidade estará disponível após a adição de uma chave separada para o Kaspersky Endpoint Detection and Response. Assim, duas chaves serão instaladas no computador: uma chave para o Kaspersky Endpoint Security e uma para o Kaspersky Endpoint Detection and Response.

  A licença para a funcionalidade autônoma Endpoint Detection and Response é a mesma licença do Kaspersky Endpoint Security.

Certifique-se de que a funcionalidade EDR Optimum ou EDR Expert esteja incluído na licença e seja executada na interface local do aplicativo.

Para obter mais informações sobre o Contrato de Licença do Usuário Final do EDR Optimum, consulte a ajuda do Kaspersky Endpoint Detection and Response Optimum.

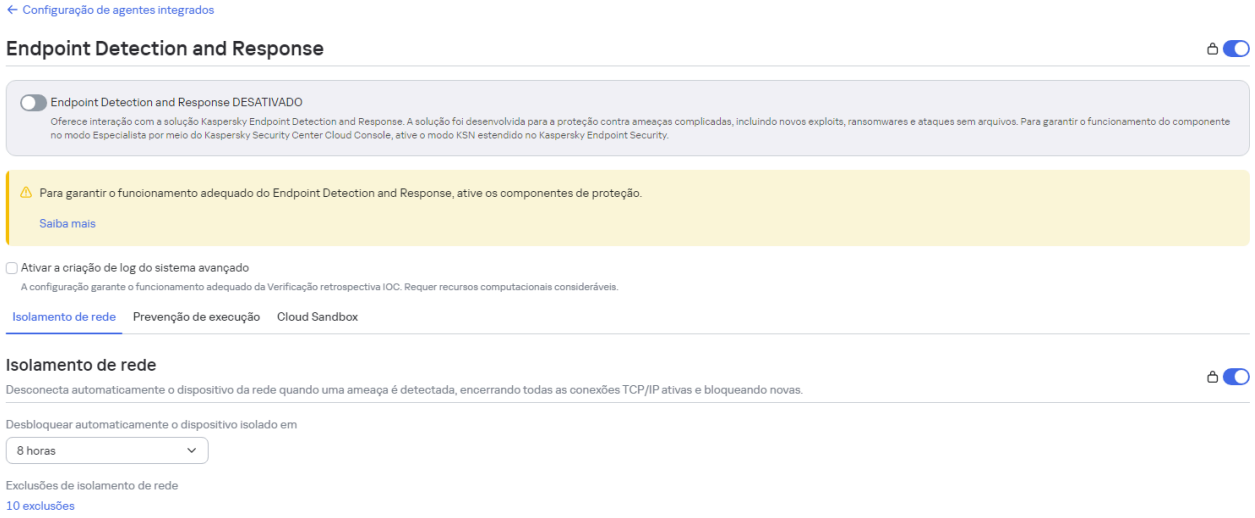
3 Ativar os componentes do Endpoint Detection and Response

É possível ativar ou desativar o componente nas configurações de política do Kaspersky Endpoint Security for Windows.

Como ativar ou desativar o componente Endpoint Detection and Response no Web Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configuração de agentes integrados** → **Endpoint Detection and Response**.
5. Ative o botão de alternância **Endpoint Detection and Response ATIVADO**.
6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.



Configurações de integração do EDR

O componente Kaspersky Endpoint Detection and Response está ativado. Verifique o status operacional do componente visualizando o *Relatório de status dos componentes do aplicativo*. Também é possível visualizar o status operacional de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente **Endpoint Detection and Response Optimum** ou o **Endpoint Detection and Response Expert (cloud)** será adicionado à lista de componentes do Kaspersky Endpoint Security.

4 Ativação da transferência de dados para o servidor de administração

Para ativar todos os recursos do Endpoint Detection and Response, a transferência de dados deve ser ativada para os seguintes tipos de dados:

- Dados dos arquivos na quarentena.

  Os dados são necessários para obter as informações sobre os arquivos em quarentena em um computador por meio do Web Console. Por exemplo, é possível baixar um arquivo a partir da quarentena para a análise no Web Console.

- Dados da cadeia de evolução de ameaças.

  Os dados são necessários para obter informações sobre as ameaças detectadas em um computador no Web Console. É possível visualizar os detalhes de alertas e adotar ações de resposta no Web Console.

Como ativar a transferência de dados para o servidor de administração no Web Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Integração KSC**.
5. No bloco **Transferência de dados para o Servidor de Administração**, clique no link **Configurações avançadas**.
6. Na janela que é aberta, selecione as seguintes caixas de seleção:
   - **Sobre os arquivos na Quarentena**.
   - **Sobre uma cadeia de desenvolvimento de ameaças**.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Verificar os indicadores de comprometimento (tarefa padrão)

Um *Indicador de compromisso (IOC)* é um conjunto de dados sobre um objeto ou atividade que indica acesso não autorizado ao computador (comprometimento de dados). Por exemplo, muitas tentativas malsucedidas de entrar no sistema podem constituir um indicador de compromisso. A *Verificação de IOC* tarefa permite localizar indicadores de comprometimento no computador e tomar as medidas de resposta a ameaças.

O Kaspersky Endpoint Security procura indicadores de comprometimento usando arquivos IOC. *Arquivos IOC* são arquivos contendo os conjuntos de indicadores que o aplicativo tenta combinar para contar uma detecção. Os arquivos IOC devem estar em conformidade com o padrão OpenIOC.

Modo de execução de tarefa de Verificação de IOC

O Kaspersky Endpoint Detection and Response permite criar tarefas padrão de verificação de IOC para detectar dados comprometidos. *Tarefa de verificação de IOC padrão* é um grupo ou tarefa local criado e configurado manualmente no Web Console. As tarefas são executadas usando arquivos IOC preparados pelo usuário. Caso queira adicionar um indicador de comprometimento manualmente, leia os requisitos para arquivos IOC.

O arquivo que pode ser baixado clicando no link abaixo contém uma tabela com a lista completa dos termos de IOC do padrão OpenIOC.

DOWNLOAD DO ARQUIVO IOC TERMS.XLSX

O Kaspersky Endpoint Security também tem suporte para tarefas de verificação de IOC autônomas quando o aplicativo é usado como parte da solução Kaspersky Sandbox.

Criar arquivo IOC

A partir da versão 12.10 do Kaspersky Endpoint Security for Windows, é possível criar arquivos IOC diretamente nas configurações da tarefa. Para criar um arquivo IOC, você deve preparar um arquivo TXT com uma lista de indicadores de comprometimento. Você pode adicionar listas dos seguintes objetos como indicadores de comprometimento:

- Hashes de arquivo (MD5 / SHA256).

  O aplicativo prepara um arquivo IOC com um escopo de verificação FileItem/Md5sum ou FileItem/Sha256sum.

- Endereços IP (IPv4, IPv6).

  O aplicativo prepara um arquivo IOC com um escopo de verificação PortItem/RemoteIP.

- Nomes DNS.

  O aplicativo prepara um arquivo IOC com um escopo de verificação DnsEntryItem/RecordName.

Como criar um arquivo IOC no Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Tarefas**.

   A lista de tarefas é aberta.

2. Selecione a tarefa **Verificação de IOC**.

   A janela de propriedades da tarefa é exibida. Caso seja necessário, crie a tarefa **Verificação de IOC**.

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

4. Ir para a seção **Verificação de ameaças**.

5. Clique **Redefinir arquivos IOC**.

6. Isso abre o formulário para criar um arquivo IOC:

   a. Em **Fonte dos arquivos IOC**, selecione **Gerar por meio do arquivo**.

   b. Insira o nome para o arquivo IOC.

   c. Selecione um arquivo TXT com uma lista de indicadores de comprometimento.

   d. Selecione o tipo do arquivo IOC: **Nomes DNS**, **Hashes dos arquivos**, **Endereços IP**.

   e. Clique **Carregar**.

   O Kaspersky Endpoint Security adiciona arquivos IOC à coleção IOC. Se necessário, é possível fazer a exclusão temporária dos arquivos IOC do escopo da tarefa.

7. Salvar alterações.

Como criar uma tarefa de Verificação de IOC

É possível criar tarefas de *Verificação de IOC* manualmente:

- Em detalhes de alertas (somente para EDR Optimum).

  Detalhes de alertas é uma ferramenta para visualizar todas as informações coletadas sobre uma ameaça detectada. Os detalhes da alertas incluem, por exemplo, o histórico de arquivos aparentes no computador. Para obter detalhes sobre o gerenciamento dos detalhes de alertas, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

- Uso do assistente de tarefa.

A tarefa de grupo *Verificação de IOC* não poderá ser executada se a integração com o Kaspersky Endpoint Detection and Response Expert (on-premises) ou o Kaspersky Endpoint Detection and Response Expert (cloud) estiver configurada nos computadores que estão sendo verificados. Nesse caso, recomendamos usar a ação de resposta *Verificação de IOC* para procurar indicadores de comprometimento. Para obter mais detalhes, consulte a ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises).

É possível configurar a tarefa para o EDR Optimum no Web Console e Cloud Console. As configurações da tarefa para EDR Expert estão disponíveis somente no Cloud Console.

Para criar uma tarefa de Verificação de IOC:

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Verificação de IOC**.

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

   d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Vá para a próxima etapa.

5. Insira as credenciais da conta do usuário cujos direitos deseja usar para executar a tarefa. Vá para a próxima etapa.

   Por padrão, o Kaspersky Endpoint Security inicia a tarefa como a conta de usuário do sistema (SISTEMA).

   A conta do sistema (SYSTEM) não tem permissão para executar a tarefa *Verificação de IOC* nas unidades de rede. Caso queira executar a tarefa para uma unidade de rede, selecione a conta de um usuário que tem acesso a essa unidade.

   Para tarefas de Verificação de IOC autônomas em unidades de rede, é necessário selecionar manualmente a conta de usuário com acesso a esta unidade nas propriedades da tarefa.

6. Conclua o assistente.

   Uma nova tarefa será exibida na lista de tarefas.

7. Clique na Nova Tarefa.

   A janela de propriedades da tarefa é exibida.

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

9. Ir para a seção **Verificação de ameaças**.

10. Carregue os arquivos IOC para pesquisar os indicadores de comprometimento.

    Depois de carregar os arquivos IOC, o aplicativo exibe informações resumidas sobre ele, incluindo a lista de indicadores que não foram aprovados na verificação. Depois de carregar os arquivos IOC, é possível fazer a edição manual deles no editor integrado, diretamente nas propriedades da tarefa. O Kaspersky Endpoint Security oferece suporte para a edição de arquivos IOC compatíveis com o padrão OpenIOC 1.1. Não é possível modificar o conteúdo de arquivos IOC compatíveis com o OpenIOC versão 1.0.

    O Kaspersky Endpoint Security adiciona arquivos IOC à coleção IOC. Se necessário, é possível fazer a exclusão temporária dos arquivos IOC do escopo da tarefa.

    Adicionar ou remover arquivos IOC após a execução da tarefa não é recomendado. Isso pode fazer com que os resultados da verificação de IOC sejam exibidos incorretamente para execuções anteriores da tarefa. Para pesquisar os indicadores de comprometimento por novos arquivos IOC, é recomendável adicionar novas tarefas.

11. Caso seja necessário, marque a caixa de seleção **Verificação retrospectiva IOC**. A *Verificação retrospectiva IOC* é um modo de tarefa de *Verificação de IOC* no qual o Kaspersky Endpoint Security verifica os indicadores de comprometimento com o uso de dados de um determinado período de tempo. Este modo é destinado à pesquisa de indicadores de comprometimento pela telemetria do computador protegido, como atividade de rede, processos, arquivos e outras telemetrias. O Kaspersky Endpoint Security analisa os dados dos logs do sistema operacional e do navegador no computador. A Verificação retrospectiva IOC analisa os logs dos seguintes navegadores: Google Chrome, Mozilla Firefox, Microsoft Edge (versão 79 ou posterior).

12. Configure ações ao detectar IOC:

- **Isolar dispositivo da rede**. Caso a opção seja selecionada, o Kaspersky Endpoint Security isola o computador da rede para evitar que a ameaça se espalhe. É possível configurar a duração do isolamento no componente de configurações do Endpoint Detection and Response.

  Se esta caixa de seleção estiver desmarcada, você poderá isolar o computador da rede depois de executar a tarefa manualmente. Se a tarefa *Verificação de IOC* detectar um IOC, você poderá isolar o computador da rede diretamente do IOC (propriedades da tarefa *Verificação de IOC* → **Configurações do aplicativo** → **Resultados da verificação de IOC**). O Kaspersky Endpoint Security também permite o gerenciamento imediato de configurações adicionais: Período de desativação do Isolamento de rede e Exclusões de isolamento de rede.

- **Mover cópia para a Quarentena, excluir objeto**. Caso a opção seja selecionada, o Kaspersky Endpoint Security exclui o objeto malicioso encontrado no computador. Antes de excluir o objeto, o Kaspersky Endpoint Security cria uma cópia de backup, caso o objeto precise ser restaurado posteriormente. O Kaspersky Endpoint Security move a cópia de backup para a quarentena.

  Se esta caixa de seleção estiver desmarcada, você poderá colocar o arquivo em quarentena manualmente depois de você mesmo ter executado a tarefa. Se a tarefa *Verificação de IOC* detectar um arquivo que pode comprometer os dados, você pode colocar esse arquivo em quarentena diretamente, a partir dos resultados da Verificação de IOC (**Configurações do aplicativo** → **Resultados da verificação de IOC**). Como resultado disso, o Kaspersky Endpoint Security iniciará o assistente de criação de tarefas com dados predefinidos do arquivo detectado. Você só precisará gerenciar configurações de tarefa adicionais, como configurar o agendamento da tarefa, por exemplo.

  Se necessário, marque a caixa de seleção **Aplicar aos objetos críticos do sistema**. Os System Critical Objects (SCOs) incluem arquivos necessários para o funcionamento do sistema operacional.

  > Não recomendamos aplicar ações a arquivos SCO. Isso pode tornar o sistema operacional instável ou impedir sua inicialização.

- **Executar a Verificação de áreas críticas**. Caso essa opção seja selecionada, o Kaspersky Endpoint Security executa a tarefa *Verificação de áreas críticas*. Por padrão, o Kaspersky Endpoint Security verifica a memória kernel, os processos de execução e os setores de inicialização de disco.

13. Ir para a seção **Avançado**.

14. Selecione os tipos de dados (documentos IOC) que devem ser analisados como parte da tarefa.

> O Kaspersky Endpoint Security seleciona automaticamente os tipos de dados (documentos IOC) para a tarefa de *Verificação de IOC* de acordo com o conteúdo dos arquivos IOC carregados. Não é recomendado remover a seleção dos tipos de dados.

Ainda é possível configurar escopos da verificação para os seguintes tipos de dados:

- **Arquivos – FileItem**. Defina o escopo da verificação de IOC no computador utilizando escopos predefinidos.

  Por padrão, o Kaspersky Endpoint Security verifica IOCs somente em áreas importantes do computador, como a pasta Downloads, a área de trabalho, a pasta com arquivos temporários do sistema operacional etc. Também é possível adicionar o escopo da verificação manualmente.

- **Logs de eventos do Windows – EventLogItem**. Insira o período de tempo referente a quando os eventos foram registrados. Também é possível selecionar quais dos logs de eventos do Windows devem ser usados para verificação IOC. Por padrão, os seguintes logos de evento são selecionados: log de eventos do aplicativo, log de eventos do sistema, log de eventos de segurança.

  > Para o termo IOC EventLogItem\source, use o valor **Nome do provedor** do esquema XML do evento.

- **Registro do Windows – RegistryItem**. Configure o escopo da Verificação de IOC no registro.

  Por padrão, o Kaspersky Endpoint Security verifica um conjunto de chaves do registro.

15. Na janela de propriedades da tarefa, selecione a guia **Agendamento**.

16. Configure a tarefa de verificação.

    > Wake-on-LAN não está disponível para esta tarefa. Certifique-se de que o computador está ligado para executar a tarefa.

17. Salvar alterações.

18. Marque a caixa de seleção ao lado da tarefa.

19. Clique **Iniciar**.

Como resultado, o Kaspersky Endpoint Security executa a pesquisa de indicadores de comprometimento do computador. É possível visualizar os resultados da tarefa, nas propriedades da tarefa, na seção **Resultados**. É possível visualizar as informações sobre os indicadores de compromisso detectados nas propriedades da tarefa: **Configurações do aplicativo** → **Resultados da verificação de IOC**. Nos resultados da Verificação de IOC, você também poderá colocar em quarentena o arquivo detectado ou isolar o computador da rede manualmente.

O Kaspersky Endpoint Security procura arquivos duplicados entre os registros criados para o mesmo arquivo IOC e mantém somente os registros exclusivos nos resultados da tarefa. Arquivos duplicados são registros do mesmo tipo que têm os mesmos valores de todos os campos comparados. O aplicativo também pode não criar um registro caso não tenha um valor em um ou mais campos (consulte a tabela abaixo).

Tipo	Campos comparados	Condição para não criar um registro
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• Valor ausente nos campos FullPath, Md5sum, Sha256sum. • Valores ausentes do campo FullPath e valores idênticos dos campos Md5sum, Sha256sum.
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	Valor ausente de pelo menos um dos seguintes campos: Hive, KeyPath, ValueName.
ProcessItem	• startTime • PID	Valores ausentes dos campos startTime ou PID.

A janela **Detalhes do alerta** pode exibir registros RegistryItem com valores de campo idênticos. Esses registros não são duplicados porque têm valores diferentes do campo Texto, que não é exibido na interface.

Os resultados da verificação de IOC são mantidos por 30 dias. Após esse período, o Kaspersky Endpoint Security exclui as entradas mais antigas automaticamente.

Telemetria estendida para verificação de IOC

Recomendamos ativar a telemetria estendida no computador para a verificação retrospectiva IOC. A telemetria estendida melhora a precisão da detecção de IOC, mas usa mais recursos do computador.

A telemetria estendida inclui o suporte dos seguintes termos adicionais:

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

Caso a telemetria estendida esteja desativada, o Kaspersky Endpoint Security poderá alternar as informações sobre os indicadores de comprometimento detectados.

Para ativar a telemetria estendida:

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configuração de agentes integrados** → **Endpoint Detection and Response**.
5. Marque a caixa de seleção **Ativar a criação de log do sistema avançado**.
6. Salvar alterações.

Mover arquivo para a quarentena

Ao reagir a ameaças, o Kaspersky Endpoint Detection and Response pode criar tarefas *Mover arquivo para a Quarentena*. Isso é necessário para minimizar as consequências da ameaça. A *Quarentena* é um armazenamento local especial no computador. O usuário pode colocar em quarentena arquivos que considere perigosos para o computador. Os arquivos em quarentena são armazenados em um estado criptografado e não ameaçam a segurança do dispositivo. O Kaspersky Endpoint Security usa a Quarentena somente quando estiver integrado com as soluções Detection and Response da Kaspersky. Em outros casos, o Kaspersky Endpoint Security coloca o arquivo relevante no Backup. Para obter informações sobre o gerenciamento da Quarentena como parte das soluções, consulte a Ajuda do Kaspersky Sandbox, a Ajuda do Kaspersky Endpoint Detection and Response Optimum, a Ajuda do Kaspersky Endpoint Detection and Response Expert, a Ajuda da Kaspersky Anti Targeted Attack Platform e a Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises).

É possível criar as tarefas *Mover arquivo para a Quarentena* das seguintes maneiras:

- Em detalhes de alertas (somente para EDR Optimum).

  Detalhes de alertas é uma ferramenta para visualizar todas as informações coletadas sobre uma ameaça detectada. Os detalhes da alertas incluem, por exemplo, o histórico de arquivos aparentes no computador. Para obter detalhes sobre o gerenciamento dos detalhes de alertas, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

- Uso do assistente de tarefa.

  É preciso inserir o caminho do arquivo ou hash (SHA256 ou MD5) ou o caminho do arquivo e o hash do arquivo.

- Nas configurações da tarefa de *Verificação de IOC*.

  Se a tarefa *Verificação de IOC* detectar um arquivo que pode comprometer os dados, você pode colocar esse arquivo em quarentena diretamente, a partir dos resultados da Verificação de IOC (**Configurações do aplicativo** → **Resultados da verificação de IOC**). Como resultado disso, o Kaspersky Endpoint Security iniciará o assistente de criação de tarefas com dados predefinidos do arquivo detectado. Você só precisará gerenciar configurações de tarefa adicionais, como configurar o agendamento da tarefa, por exemplo.

A tarefa *Mover arquivo para a Quarentena* tem as seguintes limitações:

1. O tamanho do arquivo não deve exceder 100 MB.
2. Não é possível excluir arquivos necessários para o funcionamento do Kaspersky Endpoint Security for Windows:
   - Arquivos abrangidos pela tecnologia de Autodefesa do Kaspersky Endpoint Security for Windows
   - Arquivos assinados digitalmente pela Kaspersky
3. É possível configurar a tarefa para o EDR Optimum no Web Console e Cloud Console. As configurações da tarefa para EDR Expert estão disponíveis somente no Cloud Console.
4. Não é possível verificar um objeto colocado em quarentena como resultado da tarefa *Mover arquivo para a Quarentena*.

Para criar uma tarefa de Mover arquivo para a Quarentena:

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.
   b. Na lista suspensa **Tipo de tarefa**, selecione **Mover arquivo para a Quarentena**.
   c. No campo **Nome da tarefa**, insira uma breve descrição.
   d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.
4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Clique **Avançar**.
5. Insira as credenciais da conta do usuário cujos direitos deseja usar para executar a tarefa. Clique **Avançar**.

   Por padrão, o Kaspersky Endpoint Security inicia a tarefa como a conta de usuário do sistema (SISTEMA).
6. Finalize o assistente, clicando no botão **Concluir**.

   Uma nova tarefa será exibida na lista de tarefas.
7. Clique na Nova Tarefa.

   A janela de propriedades da tarefa é exibida.
8. Selecione a guia **Configurações do aplicativo**.
9. Caso seja necessário, marque a caixa de seleção **Aplicar aos objetos críticos do sistema**.

   Os System Critical Objects (SCOs) incluem arquivos necessários para o funcionamento do sistema operacional.

Não recomendamos aplicar ações a arquivos SCO. Isso pode tornar o sistema operacional instável ou impedir sua inicialização.

10. Na lista de arquivos, clique em **Adicionar**.

    O assistente de adição de arquivo é iniciado.

11. Para adicionar o arquivo, é necessário inserir o caminho completo para o arquivo ou o hash e o caminho.

    Caso o arquivo esteja localizado em uma unidade de rede, digite o caminho do arquivo começando com `\\`, e não a letra da unidade. Por exemplo, `\\server\shared_folder\file.exe`. Caso o caminho do arquivo contenha uma letra de unidade de rede, será possível obter um erro *Arquivo não encontrado*.

12. Na janela de propriedades da tarefa, selecione a guia **Agendamento**.

13. Configure a tarefa de verificação.

    Wake-on-LAN não está disponível para esta tarefa. Certifique-se de que o computador está ligado para executar a tarefa.

14. Salvar alterações.

15. Marque a caixa de seleção ao lado da tarefa.

16. Clique **Iniciar**.

    Como resultado, o Kaspersky Endpoint Security move o arquivo para a quarentena.

Caso o arquivo esteja bloqueado por outro processo, a tarefa será exibida como Concluído, mas o próprio arquivo será colocado em quarentena somente após o computador ser reiniciado. Após reiniciar o computador, confirme se o arquivo foi excluído.

Caso o arquivo esteja bloqueado por um processo diferente, a tarefa será exibida como *Concluída*, mas o próprio arquivo é colocado em quarentena somente após o computador ser reiniciado. Após reiniciar o computador, confirme se o arquivo foi excluído.

A tarefa *Mover arquivo para a Quarentena* pode terminar com o erro *Acesso negado* caso esteja tentando colocar em quarentena um arquivo executável em execução no momento. Crie uma tarefa de encerramento de processo para o arquivo e tente novamente.

A tarefa *Mover arquivo para a Quarentena* pode terminar com o erro *Não há espaço suficiente no armazenamento da Quarentena* caso esteja tentando colocar em quarentena um arquivo muito grande. Esvazie a quarentena ou aumente o espaço da quarentena. Então, tente novamente.

É possível restaurar um arquivo da quarentena ou esvaziar a quarentena usando o Web Console. É possível restaurar os objetos localmente no computador usando a linha de comando.

Obter arquivo

É possível obter arquivos dos computadores dos usuários. Por exemplo, é possível configurar a obtenção de um arquivo de log de eventos criado por um aplicativo de terceiros. Como resultado da execução da tarefa, uma cópia do arquivo é salva na Quarentena. A *Quarentena* é um armazenamento local especial no computador. É possível baixar esse arquivo da Quarentena para o seu computador usando o Web Console (**Operações** → **Repositórios** → **Quarentena**). No computador do usuário, o arquivo permanece em sua pasta original.

O tamanho do arquivo não deve exceder 2 GB.

É possível configurar a tarefa para o EDR Optimum no Web Console e Cloud Console. As configurações da tarefa para EDR Expert estão disponíveis somente no Cloud Console.

Para criar uma tarefa de Obter o arquivo:

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Obter o arquivo**.

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

   d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Clique **Avançar**.

5. Insira as credenciais da conta do usuário cujos direitos deseja usar para executar a tarefa. Clique **Avançar**.

   Por padrão, o Kaspersky Endpoint Security inicia a tarefa como a conta de usuário do sistema (SISTEMA).

6. Finalize o assistente, clicando no botão **Concluir**.

   Uma nova tarefa será exibida na lista de tarefas.

7. Clique na Nova Tarefa.

   A janela de propriedades da tarefa é exibida.

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

9. Na lista de arquivos, clique em **Adicionar**.

   O assistente de adição de arquivo é iniciado.

10. Para adicionar o arquivo, é necessário inserir o caminho completo para o arquivo ou o hash e o caminho.

    Caso o arquivo esteja localizado em uma unidade de rede, digite o caminho do arquivo começando com `\\`, e não a letra da unidade. Por exemplo, `\\server\shared_folder\file.exe`. Caso o caminho do arquivo contenha uma letra de unidade de rede, será possível obter um erro *Arquivo não encontrado*.

11. Na janela de propriedades da tarefa, selecione a guia **Agendamento**.

12. Configure a tarefa de verificação.

    Wake-on-LAN não está disponível para esta tarefa. Certifique-se de que o computador está ligado para executar a tarefa.

13. Salvar alterações.

14. Marque a caixa de seleção ao lado da tarefa.

15. Clique **Iniciar**.

    Consequentemente, o Kaspersky Endpoint Security cria uma cópia do arquivo e move a cópia para a quarentena. É possível baixar o arquivo da quarentena no Web Console.

Excluir arquivo

É possível excluir os arquivos remotamente usando a tarefa *Excluir arquivo*. Por exemplo, é possível excluir um arquivo remotamente ao responder a ameaças.

Não é possível excluir arquivos necessários para o funcionamento do Kaspersky Endpoint Security for Windows:

- Arquivos abrangidos pela tecnologia de Autodefesa do Kaspersky Endpoint Security for Windows
- Arquivos assinados digitalmente pela Kaspersky

É possível configurar a tarefa para o EDR Optimum no Web Console e Cloud Console. As configurações da tarefa para EDR Expert estão disponíveis somente no Cloud Console.

Para criar uma tarefa de Excluir arquivo:

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Excluir arquivo**.

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

   d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Clique **Avançar**.

5. Insira as credenciais da conta do usuário cujos direitos deseja usar para executar a tarefa. Clique **Avançar**.

   Por padrão, o Kaspersky Endpoint Security inicia a tarefa como a conta de usuário do sistema (SISTEMA).

6. Finalize o assistente, clicando no botão **Concluir**.

   Uma nova tarefa será exibida na lista de tarefas.

7. Clique na Nova Tarefa.

   A janela de propriedades da tarefa é exibida.

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

9. Para adicionar o arquivo, é necessário inserir o caminho completo para o arquivo ou o hash e o caminho.

   Caso o arquivo esteja localizado em uma unidade de rede, digite o caminho do arquivo começando com `\\`, e não a letra da unidade. Por exemplo, `\\server\shared_folder\file.exe`. Caso o caminho do arquivo contenha uma letra de unidade de rede, será possível obter um erro *Arquivo não encontrado*.

10. Caso seja necessário, marque a caixa de seleção **Aplicar aos objetos críticos do sistema**.

    Os System Critical Objects (SCOs) incluem arquivos necessários para o funcionamento do sistema operacional.

    Não recomendamos aplicar ações a arquivos SCO. Isso pode tornar o sistema operacional instável ou impedir sua inicialização.

11. Na janela de propriedades da tarefa, selecione a guia **Agendamento**.

12. Configure a tarefa de verificação.

    Wake-on-LAN não está disponível para esta tarefa. Certifique-se de que o computador está ligado para executar a tarefa.

13. Salvar alterações.

14. Marque a caixa de seleção ao lado da tarefa.

15. Clique **Iniciar**.

Como resultado, o Kaspersky Endpoint Security exclui o arquivo do computador. Caso o arquivo esteja bloqueado por um processo diferente, a tarefa será exibida como *Concluído*, mas o próprio arquivo é excluído somente após o computador ser reiniciado. Após reiniciar o computador, confirme se o arquivo foi excluído.

A tarefa *Excluir arquivo* pode terminar com o erro *Acesso negado ou arquivo não encontrado* caso esteja tentando excluir um arquivo executável em execução no momento. Crie uma tarefa de encerramento de processo para o arquivo e tente novamente.

Início do processo

É possível executar arquivos remotamente usando a tarefa *Início do processo*. Por exemplo, é possível executar remotamente um utilitário que cria o arquivo de configuração do computador. Em seguida, é possível usar a *Obter o arquivo* para receber o arquivo criado no Kaspersky Security Center Web Console.

É possível configurar a tarefa para o EDR Optimum no Web Console e Cloud Console. As configurações da tarefa para EDR Expert estão disponíveis somente no Cloud Console.

Para criar uma tarefa de Início do processo:

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Início do processo**.

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

   d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Clique **Avançar**.

5. Insira as credenciais da conta do usuário cujos direitos deseja usar para executar a tarefa. Clique **Avançar**.

   Por padrão, o Kaspersky Endpoint Security inicia a tarefa como a conta de usuário do sistema (SISTEMA).

6. Finalize o assistente, clicando no botão **Concluir**.

   Uma nova tarefa será exibida na lista de tarefas.

7. Clique na Nova Tarefa.

8. A janela de propriedades da tarefa é exibida.

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

10. Digite o comando de início do processo.

    Por exemplo, se quiser executar um utilitário (`utility.exe`) que salva as informações de configuração do computador em um arquivo chamado `conf.txt` na pasta atual (por padrão). O utilitário está na pasta `C:\Users\admin\Diagnostic\`. Salve o arquivo de configuração na pasta `C:\Users\admin\Documents\Configuration`. Insira os seguintes valores:

    - **Comando executável** – `C:\Users\admin\Diagnostic\utility.exe`
    - **Argumentos da linha de comando (opcionais)** – `/R conf.txt`
    - **Caminho para a pasta de trabalho (opcional)** – `C:\Users\admin\Documents\Configuration`

11. Na janela de propriedades da tarefa, selecione a guia **Agendamento**.

12. Configure a tarefa de verificação.

    > Wake-on-LAN não está disponível para esta tarefa. Certifique-se de que o computador está ligado para executar a tarefa.

13. Salvar alterações.

14. Marque a caixa de seleção ao lado da tarefa.

15. Clique **Iniciar**.

    Consequentemente, o Kaspersky Endpoint Security executa o comando no modo silencioso e inicia o processo. É possível visualizar os resultados da tarefa, nas propriedades da tarefa, na seção **Resultados da execução**.

Encerrar processo

É possível encerrar processos remotamente usando a tarefa *Encerrar processo*. Por exemplo, é possível encerrar remotamente um utilitário de teste de velocidade da Internet iniciado usando a tarefa *Executar processo*.

Caso queira proibir a execução de um arquivo, é possível configurar o componente prevenção de execução. É possível proibir a execução de arquivos executáveis, scripts, arquivos de formato de escritório.

A tarefa *Encerrar processo* tem as seguintes limitações:

Não é possível encerrar processos de arquivos necessários para o funcionamento do Kaspersky Endpoint Security for Windows:

- Arquivos abrangidos pela tecnologia de Autodefesa do Kaspersky Endpoint Security for Windows
- Arquivos assinados digitalmente pela Kaspersky

> É possível configurar a tarefa para o EDR Optimum no Web Console e Cloud Console. As configurações da tarefa para EDR Expert estão disponíveis somente no Cloud Console.

Para criar uma tarefa de Encerrar processo:

1. Na janela principal do Web Console, selecione **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 Endpoint Security for Windows 14.2**.

   b. Na lista suspensa **Tipo de tarefa**, selecione **Encerrar processo**.

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

   d. No bloco **Dispositivos aos quais a tarefa será atribuída**, selecione o escopo da tarefa.

4. Selecione os dispositivos de acordo com a opção de escopo da tarefa selecionada. Clique **Avançar**.

5. Insira as credenciais da conta do usuário cujos direitos deseja usar para executar a tarefa. Clique **Avançar**.

   Por padrão, o Kaspersky Endpoint Security inicia a tarefa como a conta de usuário do sistema (SISTEMA).

6. Finalize o assistente, clicando no botão **Concluir**.

   Uma nova tarefa será exibida na lista de tarefas.

7. Clique na Nova Tarefa.

   A janela de propriedades da tarefa é exibida.

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

9. Caso seja necessário, marque a caixa de seleção **Aplicar aos objetos críticos do sistema**.

   Os System Critical Objects (SCOs) incluem arquivos necessários para o funcionamento do sistema operacional.

   Não recomendamos aplicar ações a arquivos SCO. Isso pode tornar o sistema operacional instável ou impedir sua inicialização.

10. Para concluir o processo, é necessário selecionar o arquivo que deseja encerrar. É possível selecionar um arquivo em uma das seguintes formas:

    - Digite o nome completo do arquivo.
    - Digite o hash e o caminho do arquivo.
    - Digite o PID do processo (somente para tarefas locais).
    - Caso o arquivo esteja localizado em uma unidade de rede, digite o caminho do arquivo começando com `\\`, e não a letra da unidade. Por exemplo, `\\server\shared_folder\file.exe`. Caso o caminho do arquivo contenha uma letra de unidade de rede, será possível obter um erro *Arquivo não encontrado*.

Caso o arquivo esteja localizado em uma unidade de rede, digite o caminho do arquivo começando com `\\`, e não a letra da unidade. Por exemplo, `\\server\shared_folder\file.exe`. Caso o caminho do arquivo contenha uma letra de unidade de rede, será possível obter um erro *Arquivo não encontrado*.

11. Na janela de propriedades da tarefa, selecione a guia **Agendamento**.

12. Configure a tarefa de verificação.

    Wake-on-LAN não está disponível para esta tarefa. Certifique-se de que o computador está ligado para executar a tarefa.

13. Clique **Salvar**.

14. Marque a caixa de seleção ao lado da tarefa.

15. Clique **Iniciar**.

    Como resultado, o Kaspersky Endpoint Security finaliza o processo no computador. Por exemplo, caso um aplicativo GAME esteja em execução e o processo game.exe for encerrado, o aplicativo será fechado sem que os dados sejam salvos. É possível visualizar os resultados da tarefa, nas propriedades da tarefa, na seção **Resultados**.

Prevenção de execução

A prevenção de execução permite o gerenciamento de execução de arquivos executáveis e scripts, assim como a abertura de arquivos no formato Office. Nesse sentido, é possível, por exemplo, prevenir a execução de aplicativos que possam ser considerados inseguros. Como resultado, a propagação da ameaça pode ser interrompida. A prevenção de execução é compatível com um conjunto de extensões de arquivos do office e um conjunto de intérpretes de script.

Regra de prevenção de execução

A prevenção de execução gerencia o acesso do usuário aos arquivos com regras de prevenção de execução. A *Regra de prevenção de execução* é um conjunto de critérios que o aplicativo leva em consideração ao reagir à execução de um objeto, por exemplo, ao bloquear a execução de um objeto. O aplicativo identifica os arquivos por seus caminhos ou somas de verificação calculados usando algoritmos de hash MD5 e SHA256.

É possível criar regras de prevenção de execução:

- Em detalhes de alertas (somente para EDR Optimum).

  Detalhes de alertas é uma ferramenta para visualizar todas as informações coletadas sobre uma ameaça detectada. Os detalhes da alertas incluem, por exemplo, o histórico de arquivos aparentes no computador. Para obter detalhes sobre o gerenciamento dos detalhes de alertas, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

- Uso da política de grupo ou as configurações locais do aplicativo.

  É preciso inserir o caminho ou o hash do arquivo (SHA256 ou MD5), ou o caminho da pasta e o hash do arquivo.

Também é possível gerenciar a prevenção de execução localmente utilizando a linha de comando.

A Prevenção de execução tem as seguintes limitações:

1. As regras de prevenção não contemplam os arquivos em CD e imagens ISO. O aplicativo não bloqueia a execução ou a abertura destes arquivos.

2. Não é possível aplicar uma regra de prevenção a arquivos necessários para o funcionamento do Kaspersky Endpoint Security for Windows:

   - Arquivos abrangidos pela tecnologia de Autodefesa do Kaspersky Endpoint Security for Windows

   - Arquivos assinados digitalmente pela Kaspersky

3. Não é recomendado criar mais de 5000 regras de prevenção de execução, pois isso pode causar instabilidade no sistema.

Modos das regras de prevenção de execução

O componente prevenção de execução pode trabalhar em dois modos:

- **Somente Estatísticas**

  Neste modo, o Kaspersky Endpoint Security publica um evento sobre tentativas de execução de objetos executáveis ou documentos abertos que correspondem aos critérios da regra de prevenção no log de eventos do Windows e no Kaspersky Security Center, mas não bloqueia a tentativa de executar ou abrir o objeto ou documento. O item está selecionado por padrão.

- **Ativo**

  Neste modo, o aplicativo bloqueia a execução de objetos ou a abertura de documentos que atendam aos critérios da regra de prevenção. O aplicativo também publica um evento sobre as tentativas de execução de objetos ou documentos abertos no log de eventos do Windows e no log de eventos do Kaspersky Security Center.

Gerenciamento da prevenção de execução

O componente só pode ser configurado no Web Console.

Para prevenir a execução:

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configuração de agentes integrados** → **Endpoint Detection and Response**.

5. Selecione a guia **Prevenção de execução**.

6. Ative o botão de alternância **Prevenção de Execução ATIVADA**.

7. No bloco **Ação na execução ou abertura de objeto proibido**, selecione o modo de operação do componente:

   - **Bloquear e adicionar ao log de eventos**. Neste modo, o aplicativo bloqueia a execução de objetos ou a abertura de documentos que atendam aos critérios da regra de prevenção. O aplicativo também publica um evento sobre as tentativas de execução de objetos ou documentos abertos no log de eventos do Windows e no log de eventos do Kaspersky Security Center.

     Se necessário, marque a caixa de seleção **Aplicar aos objetos críticos do sistema**. Os System Critical Objects (SCOs) incluem arquivos necessários para o funcionamento do sistema operacional.

     > Não recomendamos aplicar ações a arquivos SCO. Isso pode tornar o sistema operacional instável ou impedir sua inicialização.

   - **Adicionar ao log de eventos**. Neste modo, o Kaspersky Endpoint Security publica um evento sobre tentativas de execução de objetos executáveis ou documentos abertos que correspondem aos critérios da regra de prevenção no log de eventos do Windows e no Kaspersky Security Center, mas não bloqueia a tentativa de executar ou abrir o objeto ou documento. O item está selecionado por padrão.

8. Crie uma lista de regras de prevenção de execução:

   a. Clique **Adicionar**.

   b. Uma janela é aberta; nesta janela, digite o nome da regra de prevenção de execução (por exemplo, *aplicativo A*).

   c. Na lista suspensa **Tipo**, selecione o objeto que deseja bloquear: **Arquivo executável**, **Script**, **Documento do Microsoft Office**.

      Caso selecione um tipo de objeto incorreto, o Kaspersky Endpoint Security não bloqueia o arquivo ou o script.

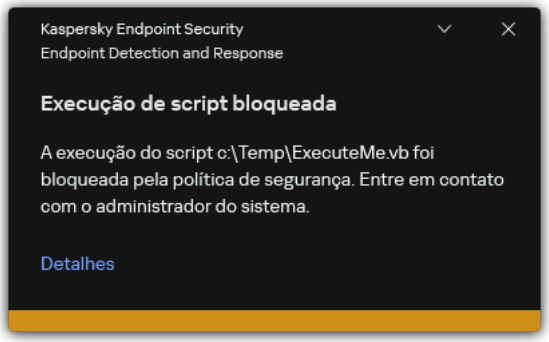
   d. Para adicionar o arquivo, é preciso inserir o hash do arquivo (SHA256 ou MD5), o caminho completo para o arquivo ou o hash e o caminho da pasta.

      > Caso o arquivo esteja localizado em uma unidade de rede, digite o caminho do arquivo começando com `\\`, e não a letra da unidade. Por exemplo, `\\server\shared_folder\file.exe`. Caso o caminho do arquivo contenha uma letra de unidade de rede, o Kaspersky Endpoint Security não bloqueia o arquivo ou script.

      A prevenção de execução é compatível com um conjunto de extensões de arquivos do office e um conjunto de intérpretes de script.

9. Salvar alterações.

Consequentemente, o Kaspersky Endpoint Security bloqueia a execução de objetos: execução de arquivos executáveis e scripts, abertura de arquivos em formato office. Contudo, é possível, por exemplo, abrir um arquivo de script em um editor de texto, mesmo que a execução do script esteja impedida. Ao bloquear a execução de um objeto, o Kaspersky Endpoint Security exibe uma notificação padrão (veja a figura abaixo) caso as notificações estejam ativadas nas configurações do aplicativo.



Notificação sobre as regras de prevenção de execução

Isolamento do computador em relação à rede

O isolamento de rede do computador permite isolar automaticamente um computador da rede em resposta à detecção de um indicador de compromisso (IOC). Esse é *modo automático*. É possível ativar o isolamento de rede manualmente enquanto a ameaça detectada estiver sendo investigada. Esse é o *modo manual*.

Quando o isolamento de rede é ativado, o aplicativo corta todas as conexões ativas e bloqueia todas as novas conexões de rede TCP/IP no computador, exceto as seguintes conexões:

- Conexões listadas em exclusões de isolamento de rede.
- Conexões iniciadas pelos serviços do Kaspersky Endpoint Security.
- Conexões iniciadas pelo Agente de Rede do Kaspersky Security Center.
- Conexões à SVM e ao Servidor de integração se o aplicativo estiver sendo usado no modo Light Agent.
- Conexões com a KSN ao integrar o aplicativo com o Kaspersky Managed Detection and Response.

O componente só pode ser configurado no Web Console.

Modo de isolamento de rede automático

É possível configurar o isolamento de rede para ser ligado automaticamente em resposta a uma detecção de IOC. É possível configurar o modo de isolamento de rede automático com uma política de grupo.

Como configurar o isolamento de rede para ser ligado automaticamente em resposta a uma detecção de IOC

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Tarefas**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Verificação de IOC** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

   Caso seja necessário, crie a tarefa *Verificação de IOC*.

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

4. Selecione a seção **Configurações de resposta**.

5. No bloco **Configure as ações de resposta na detecção de IOC**, selecione **Alerta e resposta** e marque a caixa de seleção **Isolar dispositivo da rede**.

6. Salvar alterações.

Consequentemente, quando um IOC for detectado, o aplicativo isola o computador em relação à rede para prevenir a difusão da ameaça.

É possível configurar a desativação automática do isolamento de rede após um determinado período de tempo. Por padrão, o aplicativo desliga o isolamento de rede após decorrer oito horas em relação ao momento em que ele foi ligado. Também é possível desativar o isolamento de rede manualmente (consulte as instruções abaixo). Após desligar o isolamento de rede, o computador pode utilizar a rede sem restrições.

Como configurar o atraso para o desligamento automático do isolamento de rede de um computador no modo automático

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

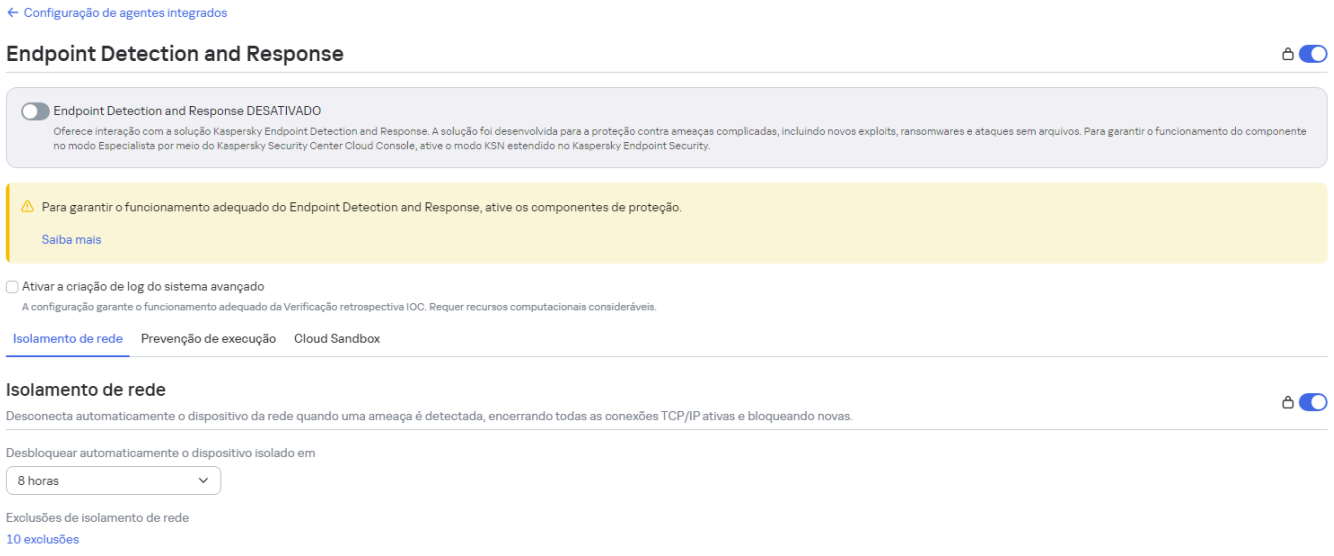
3. Selecione a guia **Configurações do aplicativo**.

4. Selecione **Configuração de agentes integrados** → **Endpoint Detection and Response**.

5. Selecione a guia **Isolamento de rede**.

6. Selecione o atraso para desativar o Isolamento de rede.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.



Configurações de integração do EDR

Modo de isolamento de rede manual

É possível ligar e desligar manualmente o isolamento de rede. É possível configurar o modo de isolamento de rede manual com o uso das propriedades do computador no console do Kaspersky Security Center.

É possível ligar o isolamento de rede:

- Em detalhes de alertas (somente para EDR Optimum).

  Detalhes de alertas é uma ferramenta para visualizar todas as informações coletadas sobre uma ameaça detectada. Os detalhes da alertas incluem, por exemplo, o histórico de arquivos aparentes no computador. Para obter detalhes sobre o gerenciamento dos detalhes de alertas, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

- Uso das configurações locais do aplicativo.

- Nas configurações da tarefa de *Verificação de IOC*.

  Se a tarefa *Verificação de IOC* detectar um IOC, você poderá isolar o computador da rede diretamente do IOC (propriedades da tarefa *Verificação de IOC* → **Configurações do aplicativo** → **Resultados da verificação de IOC**). O Kaspersky Endpoint Security também permite o gerenciamento imediato de configurações adicionais: Período de desativação do Isolamento de rede e Exclusões de isolamento de rede.

Como ligar o isolamento de rede de um computador manualmente

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Ativos (dispositivos)**.
2. Selecione o computador para o qual você deseja definir as configurações locais do aplicativo.

   Isso abre as propriedades do computador.
3. Selecione a guia **Aplicativos**.
4. Clique **Kaspersky Endpoint Security for Windows 14.2**.

   Isso abre as configurações locais do aplicativo.
5. Selecione a guia **Configurações do aplicativo**.
6. Selecione **Detection and Response** → **Endpoint Detection and Response**.
7. No bloco **Isolamento de rede**, clique em **Isolar o computador da rede**.

É possível configurar a desativação automática do isolamento de rede após um determinado período de tempo. Por padrão, o aplicativo desliga o isolamento de rede após decorrer oito horas em relação ao momento em que ele foi ligado. Após desligar o isolamento de rede, o computador pode utilizar a rede sem restrições.

Como configurar o atraso para o desligamento do isolamento de rede de um computador no modo manual

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Ativos (dispositivos)**.
2. Selecione o computador para o qual você deseja definir as configurações locais do aplicativo.

   Isso abre as propriedades do computador.
3. Selecione a guia **Tarefas**.

   A lista de tarefas disponíveis no computador será exibida.

4. Selecione a tarefa **Isolamento de rede**.

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

6. Uma janela será aberta; nessa janela, selecione o atraso para o desligamento do isolamento de rede.

7. Salvar alterações.

Como desligar o isolamento de rede de um computador manualmente

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

2. Selecione o computador para o qual você deseja definir as configurações locais do aplicativo.
   Isso abre as propriedades do computador.

3. Selecione a guia **Aplicativos**.

4. Clique **Kaspersky Endpoint Security for Windows 14.2**.
   Isso abre as configurações locais do aplicativo.

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

6. Selecione **Configuração de agentes integrados** → **Endpoint Detection and Response**.

7. No bloco **Isolamento de rede**, clique em **Desbloquear o computador isolado da rede**.

Também é possível desativar o isolamento de rede localmente usando a linha de comando.

A partir da versão 12.10 do Kaspersky Endpoint Security for Windows, é possível gerenciar o Isolamento de Rede nos detalhes do alerta. Além disso, nos detalhes do alerta, dá para especificar o período de Isolamento de rede do computador. Para obter detalhes sobre o gerenciamento dos detalhes de alertas, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

Exclusões de isolamento de rede

É possível configurar as exclusões de isolamento de rede. As conexões de rede que correspondem às regras não são bloqueadas no computador quando o isolamento de rede é ativado.

Para configurar as exclusões de isolamento de rede, é possível utilizar a lista de *perfis de rede padrão*. Por padrão, as exclusões incluem os perfis de rede contendo as regras que garantem a operação ininterrupta de dispositivos com funções de servidor DNS/DHCP e cliente DNS/DHCP. Também é possível modificar as configurações dos perfis de rede padrão ou definir as exclusões manualmente (consulte as instruções abaixo).

As exclusões especificadas nas propriedades da política são aplicadas apenas se o isolamento de rede for ativado automaticamente em resposta a uma ameaça detectada. As exclusões especificadas nas propriedades do computador são aplicadas apenas se o isolamento de rede for ativado manualmente nas propriedades do computador no console do Kaspersky Security Center ou nos detalhes de alertas.

Uma política ativa não impede a aplicação de exclusões do isolamento de rede configurada nas propriedades do computador, uma vez que estes parâmetros possuem diferentes cenários de uso.

Como adicionar uma exclusão de isolamento de rede no modo automático

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configuração de agentes integrados** → **Endpoint Detection and Response**.
5. Selecione a guia **Isolamento de rede**.
6. No bloco **Exclusões de isolamento de rede**, clique em **<N> exclusões**.
7. Uma janela é aberta; nesta janela, clique em **Adicionar** → **Adicionar a partir do perfil** e selecione os perfis de rede padrão para configurar as exclusões.

   As exclusões de isolamento de rede a partir do perfil são adicionadas à lista de exclusões de isolamento de rede. É possível visualizar as propriedades das conexões de rede. Caso seja necessário, é possível modificar as configurações da conexão de rede.
8. Caso seja necessário, adicione uma exclusão de isolamento de rede manualmente. Para fazer isso, na janela com a lista de exclusões, clique em **Adicionar** → **Adicionar** e edite manualmente as configurações de conexão de rede.
9. Salvar alterações.

Como adicionar uma exclusão de isolamento de rede no modo manual

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Ativos (dispositivos)**.
2. Selecione o computador para o qual você deseja definir as configurações locais do aplicativo.

   Isso abre as propriedades do computador.
3. Selecione a guia **Tarefas**.

   A lista de tarefas disponíveis no computador será exibida.
4. Selecione a tarefa **Isolamento de rede**.
5. Selecione a guia **Configurações do aplicativo**.
6. Uma janela será aberta; nessa janela, clique em **Exclusões**.
7. Uma janela é aberta; nesta janela, clique em **Adicionar a partir do perfil** e selecione os perfis de rede padrão para configurar as exclusões.

   As exclusões de isolamento de rede a partir do perfil são adicionadas à lista de exclusões de isolamento de rede. É possível visualizar as propriedades das conexões de rede. Caso seja necessário, é possível modificar as configurações da conexão de rede.
8. Caso seja necessário, adicione uma exclusão de isolamento de rede manualmente. Para fazer isso, na janela com a lista de exclusões, clique em **Adicionar** e edite manualmente as configurações de conexão de rede.
9. Salvar alterações.

Também é possível visualizar a lista de exclusão de isolamento de rede utilizando a linha de comando. Neste caso, o computador deve estar isolado.

A partir da versão 12.10 do Kaspersky Endpoint Security for Windows, é possível adicionar as Exclusões de isolamento de rede nos detalhes do alerta. Para obter detalhes sobre o gerenciamento dos detalhes de alertas, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

Cloud Sandbox

Cloud Sandbox é uma tecnologia que permite detectar ameaças avançadas em um computador. O Kaspersky Endpoint Security encaminha automaticamente arquivos detectados para a Cloud Sandbox analisar. O Cloud Sandbox executa esses arquivos em um ambiente isolado para identificar atividades maliciosas e avaliar a sua reputação. Os dados desses arquivos são enviados para a Kaspersky Security Network. Portanto, caso o Cloud Sandbox detecte um arquivo malicioso, o Kaspersky Endpoint Security executará a ação apropriada para eliminar essa ameaça em todos os computadores em que esse arquivo for detectado.

Para que o Cloud Sandbox funcione, é necessário habilitar o uso da Kaspersky Security Network.

Caso esteja usando a Kaspersky Private Security Network, a tecnologia Cloud Sandbox não estará disponível.

A tecnologia Cloud Sandbox está habilitada permanentemente e disponível para todos os usuários da Kaspersky Security Network, independentemente do tipo de licença em uso. Caso já tenha implantado a solução Endpoint Detection and Response Optimum, é possível habilitar um contador separado para as ameaças detectadas pelo Cloud Sandbox. É possível usar esse contador para compilar estatísticas ao analisar ameaças detectadas. O Kaspersky Endpoint Security indica a tecnologia de detecção de ameaças Cloud Sandbox em *Relatório de ameaças* no console do Kaspersky Security Center.

Contadores de ameaças

Para ativar o contador do Cloud Sandbox:

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configuração de agentes integrados** → **Endpoint Detection and Response**.
5. Selecione a guia **Cloud Sandbox**.
6. Ative o botão de alternância **Cloud Sandbox ATIVADO**.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Sempre que houver uma ameaça, o Kaspersky Endpoint Security ativa o contador de ameaças detectadas usando o Cloud Sandbox na janela principal do aplicativo debaixo de **Tecnologias de detecção de ameaças**. O Kaspersky Endpoint Security também indicará a tecnologia de detecção de ameaças Cloud Sandbox em *Relatório de ameaças* no console do Kaspersky Security Center.

Guia de migração do KEA para KES para o EDR Optimum

O Kaspersky Endpoint Security for Windows inclui um agente integrado para a solução Kaspersky Endpoint Detection and Response Optimum. Não é mais necessário um aplicativo separado do Kaspersky Endpoint Agent para funcionar com o EDR Optimum. Todas as funções do Kaspersky Endpoint Agent serão executadas pelo Kaspersky Endpoint Security.

Quando o Kaspersky Endpoint Security é implantado em computadores com o Kaspersky Endpoint Agent instalado, a solução Kaspersky Endpoint Detection and Response Optimum continuará funcionando com o Kaspersky Endpoint Security. Além disso, o Kaspersky Endpoint Agent será removido do computador. O mesmo comportamento no sistema ocorrerá quando você atualizar o Kaspersky Endpoint Security para a versão 11.7.0 ou posterior.

O Kaspersky Endpoint Security não é compatível com o Kaspersky Endpoint Agent. Não é possível instalar os dois aplicativos no mesmo computador.

As seguintes condições devem ser atendidas para que o Kaspersky Endpoint Security funcione como parte do Kaspersky Endpoint Detection and Response Optimum:

- Kaspersky Endpoint Detection and Response Optimum versão 2.0 ou superior.
- Kaspersky Security Center versão 13.2 ou posterior (incluindo o Agente de Rede). Em versões anteriores do Kaspersky Security Center, é impossível ativar o recurso EDR Optimum.
- O EDR Optimum só pode ser gerenciado usando o Kaspersky Security Center Web Console.
- A transferência de dados para o Servidor de Administração está ativada. Os dados são necessários para obter as informações sobre os arquivos em quarentena em um computador por meio do Web Console.
- A conexão em segundo plano entre o Kaspersky Security Center Web Console e o servidor de administração foi estabelecida. Para que o EDR Optimum trabalhe com o Servidor de Administração por meio do Kaspersky Security Center Web Console, é preciso estabelecer uma nova conexão segura, uma *conexão em segundo plano*.

Etapas para migrar a configuração [KES+KEA] para [KES+agente integrado] para o EDR Optimum

1. **Atualização do plug-in da Web do Kaspersky Endpoint Security**

   O componente EDR Optimum pode ser gerenciado usando o plug-in da Web do Kaspersky Endpoint Security versão 11.7.0 ou posterior.

2. **Migrar as políticas e tarefas**

   Transfira as configurações do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows. Para fazer isso, use o assistente para migrar do Kaspersky Endpoint Agent no Web Console.

   Como migrar as configurações de políticas e tarefas do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security no Web Console

Na janela principal do Web Console, selecione **Operações** → **Migração a partir do Kaspersky Endpoint Agent**.

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

Etapa 1. Migração da política

O assistente de migração cria uma nova política que unifica as configurações das políticas do Kaspersky Endpoint Security e Kaspersky Endpoint Agent. Na lista de política, selecione as políticas do Kaspersky Endpoint Agent cujas configurações deseja unificar as políticas do Kaspersky Endpoint Security. Clique na política do Kaspersky Endpoint Agent para selecionar a política do Kaspersky Endpoint Security com o qual deseja unificar as configurações. Certifique-se de ter selecionado as políticas corretas e vá para a próxima etapa.

Etapa 2. Migração da tarefa

O Assistente de migração cria novas tarefas para o Kaspersky Endpoint Security. Na lista de tarefa, selecione as tarefas do Kaspersky Endpoint Agent para as quais deseja criar uma política do Kaspersky Endpoint Security. Vá para a próxima etapa.

Etapa 3. Conclusão do Assistente

Conclua o assistente. Como resultado, o assistente faz o seguinte:

- Cria uma nova política do Kaspersky Endpoint Security.

  A política unifica as configurações do Kaspersky Endpoint Security e Kaspersky Endpoint Agent. A política é chamada *<nome da política Kaspersky Endpoint Security> & <nome da política Kaspersky Endpoint Agent>*. A nova política possui o status *Inativo*. Para continuar, mude os status das políticas do Kaspersky Endpoint Agent e Kaspersky Endpoint Security para *Inativo* e ative a nova política unificada.

  > Após a migração a partir do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows, certifique-se de que a nova política tenha a funcionalidade para transferência de dados para o servidor de administração (dados do arquivo na quarentena e dados da cadeia de evolução de ameaças) configurada. Os valores do parâmetro de transferência de dados não são migrados a partir de uma política do Kaspersky Endpoint Agent.

- Cria novas tarefas do Kaspersky Endpoint Security.

  As novas tarefas são cópias das tarefas do Kaspersky Endpoint Agent. Ao mesmo tempo, o assistente deixa as tarefas do Kaspersky Endpoint Agent inalteradas.

3. **Licenciamento da funcionalidade do EDR Optimum**

Caso utilize uma licença comum do Kaspersky Endpoint Detection and Response Optimum ou do Kaspersky Optimum Security para ativar o Kaspersky Endpoint Security for Windows e Kaspersky Endpoint Agent, a funcionalidade do EDR Optimum será ativada automaticamente após a atualização do aplicativo para a versão 11.7.0 ou posterior. Não é necessário fazer mais nada.

Caso utilize uma licença autônoma do add-on do Kaspersky Endpoint Detection and Response Optimum para ativar a funcionalidade do EDR Optimum, é necessário garantir que a chave do EDR Optimum seja adicionada ao repositório do Kaspersky Security Center e que a funcionalidade de distribuição automática da chave de licença seja ativada. Após efetuar upgrade do aplicativo para a versão 11.7.0 ou posterior, a funcionalidade do EDR Optimum é ativada automaticamente.

Caso utilize uma licença do Kaspersky Endpoint Detection and Response Optimum ou do Kaspersky Optimum Security para ativar o Kaspersky Endpoint Agent e uma licença diferente para ativar o Kaspersky Endpoint Security for Windows, é necessário substituir a chave do Kaspersky Endpoint Security for Windows pela chave comum do Kaspersky Endpoint Detection and Response Optimum ou da chave Kaspersky Optimum Security. É possível substituir a chave utilizando a tarefa *Adicionar chave*.

4. **Instalação/atualização do aplicativo Kaspersky Endpoint Security**

Para migrar a funcionalidade do EDR Optimum durante a instalação ou upgrade de um aplicativo, é recomendável usar a tarefa de instalação remota. Ao criar uma tarefa de instalação remota, selecione o componente do EDR Optimum nas configurações do pacote de instalação.

Também é possível baixar o aplicativo utilizando os seguintes métodos:

- Uso do serviço de atualização da Kaspersky.
- Localmente, usando o Assistente de configuração.

O Kaspersky Endpoint Security é compatível com a seleção automática de componentes ao atualizar o aplicativo em um computador com o aplicativo Kaspersky Endpoint Agent instalado. A seleção automática dos componentes depende das permissões da conta do usuário que está atualizando o aplicativo.

Caso esteja atualizando o Kaspersky Endpoint Security com um arquivo EXE ou MSI com a conta do sistema (SYSTEM), o Kaspersky Endpoint Security obtém acesso às licenças atualmente em uso das soluções da Kaspersky. Portanto, se o computador possui, por exemplo, o Kaspersky Endpoint Agent instalado e a solução EDR Optimum ativada, o instalador do Kaspersky Endpoint Security configura automaticamente o conjunto de componentes e seleciona o componente EDR Optimum. Isso faz com que o Kaspersky Endpoint Security alterne o uso do agente integrado e remova o Kaspersky Endpoint Agent. A execução do instalador do MSI na conta do sistema (SYSTEM) normalmente é feita com a atualização por meio do serviço de atualização da Kaspersky ou ao implementar um pacote de instalação por meio do Kaspersky Security Center.

Caso esteja atualizando o Kaspersky Endpoint Security com um arquivo MSI com uma conta de usuário não privilegiado, o Kaspersky Endpoint Security perde o acesso das licenças atualmente em uso das soluções da Kaspersky. Neste caso, o Kaspersky Endpoint Security seleciona automaticamente os componentes de acordo com a configuração do Kaspersky Endpoint Agent. Depois disso, o Kaspersky Endpoint Security passa a usar o agente integrado e remove o Kaspersky Endpoint Agent.

O Kaspersky Endpoint Security é compatível com a atualização sem reinicialização do computador. É possível selecionar o modo de atualização do aplicativo nas propriedades da política.

5. **Verificação do funcionamento do aplicativo**

Se, após a instalação ou atualização do aplicativo, o computador estiver com o status *Crítico* no console do Kaspersky Security Center:

- Certifique-se de que o computador possui o Agente de Rede versão 13.2 ou posterior instalado.
- Verifique o status operacional do agente integrado visualizando o *Relatório de status dos componentes do aplicativo*. Caso o componente tenha o status *Não instalado*, instale o componente usando a tarefa *Alterar componentes do aplicativo*. Caso um componente tenha o status *Não coberto pela licença*, certifique-se de que a funcionalidade do agente integrado esteja ativada.
- Certifique-se de aceitar a Declaração da Kaspersky Security Network na nova política do Kaspersky Endpoint Security for Windows.

Kaspersky Sandbox

O Kaspersky Endpoint Security for Windows inclui um agente interno para integração com a solução Kaspersky Sandbox. O componente *Sandbox* detecta e bloqueia automaticamente ameaças avançadas em computadores. O Sandbox analisa o comportamento do objeto para detectar atividades maliciosas e características de atividades de ataques direcionados à infraestrutura de TI da organização. O Sandbox analisa e verifica objetos em servidores especiais com imagens virtuais implantadas de sistemas operacionais Microsoft Windows (servidores Sandbox). Para obter informações detalhadas sobre a solução, consulte a ajuda do Kaspersky Sandbox e a ajuda da Kaspersky Anti Targeted Attack Platform.

Integração do agente integrado com o Kaspersky Sandbox

A adição do componente Kaspersky Sandbox é necessária para a integração com o Kaspersky Sandbox. É possível selecionar o componente Sandbox durante a instalação ou atualização, assim como usando a tarefa *Alterar componentes do aplicativo*.

Para usar o componente, as seguintes condições devem ser atendidas:

- Kaspersky Security Center 13.2. As versões anteriores do Kaspersky Security Center não permitem a criação de tarefas de Verificação de IOC autônomas em resposta a ameaças.
- O componente só pode ser gerenciado usando o Web Console. Não é possível gerenciar esse componente usando o Console de Administração (MMC).
- O aplicativo é ativado e a funcionalidade é contemplada pela licença.
- A transferência de dados para o Servidor de Administração está ativada.

  Para utilizar todos os recursos do Kaspersky Sandbox, certifique-se que a transferência de dados para arquivos na quarentena esteja ativada. Os dados são necessários para obter as informações sobre os arquivos em quarentena em um computador por meio do Web Console. Por exemplo, é possível baixar um arquivo a partir da quarentena para a análise no Web Console.

  Como ativar a transferência de dados para o servidor de administração no Web Console

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

     A janela de propriedades da política é exibida.
  3. Selecione a guia **Configurações do aplicativo**.
  4. Selecione **Configurações gerais** → **Integração KSC**.
  5. No bloco **Transferência de dados para o Servidor de Administração**, marque a caixa de seleção **Sobre os arquivos na Quarentena**.
  6. Salvar alterações.
- A conexão em segundo plano entre o Kaspersky Security Center Web Console e o servidor de administração foi estabelecida

Para que o Kaspersky Sandbox trabalhe com o Servidor de Administração por meio do Kaspersky Security Center Web Console, é preciso estabelecer uma nova conexão segura, uma *conexão em segundo plano*. Para os detalhes sobre a integração do Kaspersky Security Center com outras soluções Kaspersky, consulte a ajuda do Kaspersky Security Center.

Estabelecimento de uma conexão em segundo plano no 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.

Caso a conexão em segundo plano entre o Kaspersky Security Center Web Console e o Servidor de Administração não seja estabelecida, as tarefas de verificação de IOC autônomas não podem ser criadas como parte da resposta a ameaças.

- Para configurar uma conexão confiável com o servidor Sandbox, é preciso preparar um certificado TLS. Em seguida, é necessário adicionar o certificado ao computador com o uso de uma política. Também é necessário adicionar o certificado ao servidor Sandbox.

  A autenticação bidirecional com o uso de crypto-contêiner não está disponível para o Kaspersky Sandbox.

  Também é possível adicionar um certificado TLS no Web Console ou localmente utilizando a linha de comando.

- O componente Kaspersky Sandbox está ativado.
- Os componentes do aplicativo que garantem a operação do Sandbox estão ativados e operacionais. Os seguintes componentes garantem a operação do Sandbox:
  - Proteção Contra Ameaças ao Arquivo.
  - Prevenção de Intrusão do Host.
  - Firewall.
  - Proteção AMSI.
  - Verificação em segundo plano.

Para ativar ou desativar a integração com o Kaspersky Sandbox:

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configuração de agentes integrados** → **Sandbox**.
5. Use o botão de alternância do **Integração com o Sandbox ATIVADA** para ativar ou desativar o componente.

6. No bloco **Modo de integração**, selecione o modo de operação do componente: **Kaspersky Sandbox**.

7. Clique no link **Configurações de conexão**.

   A janela de configurações de conexão do servidor do Sandbox é aberta.

8. No bloco **Certificado TLS do servidor**, clique em **Carregar** e selecione o arquivo de certificado TLS.

   O Kaspersky Endpoint Security pode ter apenas um certificado TLS para um servidor do Sandbox. Caso tenha adicionado um certificado TLS antes, esse certificado será revogado. Apenas o último certificado adicionado é usado.

9. Defina as configurações de conexão avançadas para os servidores do Sandbox:

   - **Tempo limite (mseg)**. Tempo de conexão esgotado para o Sandbox. Depois de decorrido o tempo limite configurado, o Kaspersky Endpoint Security envia uma solicitação ao próximo servidor. É possível aumentar o tempo de conexão esgotado para o servidor caso a velocidade da sua conexão seja baixa ou instável. O tempo limite de solicitação recomendado é de 0.5 segundo ou menos.

   - **Fila de solicitações**. Tamanho da pasta da fila de solicitações. Ao enviar vários objetos para verificação no Sandbox, o Kaspersky Endpoint Security cria uma fila de solicitações. Por padrão, o tamanho da pasta da fila de solicitações é limitado a 100 MB. Depois que o tamanho máximo é atingido, o Sandbox para de adicionar novas solicitações à fila e envia o evento correspondente ao Kaspersky Security Center. É possível configurar o tamanho da pasta da fila de solicitações dependendo da configuração do seu servidor.

10. No bloco **Conexão com servidores do Sandbox**, clique no botão **Adicionar**.

11. Uma janela é aberta; nela, insira o endereço do servidor Sandbox (IPv4, IPv6, DNS) e a porta.

    Para obter detalhes sobre como implantar imagens virtuais e configurar servidores Sandbox, consulte a ajuda do Kaspersky Sandbox.

12. Salvar alterações.

Como resultado, o Kaspersky Endpoint Security verificará o certificado TLS. Caso o certificado seja verificado com sucesso, o Kaspersky Endpoint Security carregará e enviará o arquivo para o computador durante a próxima sincronização com o Kaspersky Security Center. Caso tenha adicionado dois certificados TLS, o Kaspersky Sandbox utilizará a versão mais atual do certificado para estabelecer uma conexão confiável. Verifique o status operacional do componente visualizando o *Relatório de status dos componentes do aplicativo*. Também é possível visualizar o status operacional de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente do **Sandbox** será adicionado na lista de componentes do Kaspersky Endpoint Security.

É possível ativar ou desativar a integração com o Kaspersky Sandbox no Web Console ou localmente utilizando a linha de comando.

O Kaspersky Endpoint Security salva informações sobre o funcionamento do componente Kaspersky Sandbox em um relatório. O relatório também contém informações sobre erros. Caso receba um erro com uma descrição que corresponda ao formato `Error code: XXX` (por exemplo, `0xa67b01f4`), entre em contato com o Suporte Técnico.

Verificar se há indicadores de comprometimento (tarefa autônoma)

Um *Indicador de compromisso (IOC)* é um conjunto de dados sobre um objeto ou atividade que indica acesso não autorizado ao computador (comprometimento de dados). Por exemplo, muitas tentativas malsucedidas de entrar no sistema podem constituir um indicador de compromisso. A *Verificação de IOC* tarefa permite localizar indicadores de comprometimento no computador e tomar as medidas de resposta a ameaças.

O Kaspersky Endpoint Security procura indicadores de comprometimento usando arquivos IOC. *Arquivos IOC* são arquivos contendo os conjuntos de indicadores que o aplicativo tenta combinar para contar uma detecção. Os arquivos IOC devem estar em conformidade com o padrão OpenIOC. O Kaspersky Endpoint Security gera automaticamente os arquivos IOC para o Kaspersky Sandbox.

Modo de execução de tarefa de Verificação de IOC

O aplicativo cria as tarefas autônomas de verificação de IOC para o Kaspersky Sandbox. *Tarefa Verificação de IOC autônoma* é uma tarefa de grupo criada automaticamente durante a reação contra uma ameaça detectada pelo Kaspersky Sandbox. O Kaspersky Endpoint Security gera automaticamente o arquivo IOC. Arquivos IOC personalizados não são compatíveis. As tarefas são excluídas automaticamente 30 dias após a hora de criação. Para obter mais detalhes sobre as tarefas de verificação de IOC autônomas, consulte a ajuda do Kaspersky Sandbox.

Configurações da tarefa Verificação de IOC

O Kaspersky Sandbox pode criar e executar as tarefas de *Verificação de IOC* automaticamente no momento da reação a ameaças.

As configurações só podem ser definidas no Web Console.

É preciso ter o Kaspersky Security Center 13.2 para que tarefas de verificação de IOC autônomas do Kaspersky Sandbox funcionem.

Para alterar as configurações da tarefa Verificação de IOC:

1. Na janela principal do Web Console, selecione **Tarefas**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Verificação de IOC** do Kaspersky Endpoint Security.

   A janela de propriedades da tarefa é exibida.

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

4. Ir para a seção **Configurações de verificação de IOC**.

5. Configure ações ao detectar IOC:

- **Mover cópia para a Quarentena, excluir objeto**. Caso a opção seja selecionada, o Kaspersky Endpoint Security exclui o objeto malicioso encontrado no computador. Antes de excluir o objeto, o Kaspersky Endpoint Security cria uma cópia de backup, caso o objeto precise ser restaurado posteriormente. O Kaspersky Endpoint Security move a cópia de backup para a quarentena.

- **Executar a Verificação de áreas críticas**. Caso essa opção seja selecionada, o Kaspersky Endpoint Security executa a tarefa *Verificação de áreas críticas*. Por padrão, o Kaspersky Endpoint Security verifica a memória kernel, os processos de execução e os setores de inicialização de disco.

- **Executar apenas quando o computador estiver ocioso**. Início adiado da tarefa quando os recursos do computador estão ocupados. O Kaspersky Endpoint Security inicia a tarefa de verificação se o computador estiver bloqueado ou se a proteção de tela estiver ativada. Caso interrompa a execução da tarefa, por exemplo, desbloqueando o computador, o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que foi interrompido. Essa opção de programação permite conservar os recursos do computador quando ele está sendo utilizado.

6. Salvar alterações.

É possível visualizar os resultados da tarefa, nas propriedades da tarefa, na seção **Resultados**. É possível visualizar as informações sobre os indicadores de compromisso detectados nas propriedades da tarefa: **Configurações do aplicativo** → **Resultados da verificação de IOC**.

Os resultados da verificação de IOC são mantidos por 30 dias. Após esse período, o Kaspersky Endpoint Security exclui as entradas mais antigas automaticamente.

Guia de migração do KEA para KES para o Kaspersky Sandbox

O Kaspersky Endpoint Security for Windows inclui um agente integrado para a solução Kaspersky Sandbox. Não é mais necessário um aplicativo separado do Kaspersky Endpoint Agent para funcionar com o Kaspersky Sandbox. Todas as funções do Kaspersky Endpoint Agent serão executadas pelo Kaspersky Endpoint Security.

Quando o Kaspersky Endpoint Security é implantado em computadores com o Kaspersky Endpoint Agent instalado, a solução Kaspersky Sandbox continuará funcionando com o Kaspersky Endpoint Security. Além disso, o Kaspersky Endpoint Agent será removido do computador. O mesmo comportamento no sistema ocorrerá quando você atualizar o Kaspersky Endpoint Security para a versão 11.7.0 ou posterior.

O Kaspersky Endpoint Security não é compatível com o Kaspersky Endpoint Agent. Não é possível instalar os dois aplicativos no mesmo computador.

As seguintes condições devem ser atendidas para que o Kaspersky Endpoint Security funcione como parte do Kaspersky Sandbox:

- Kaspersky Sandbox versão 2.0 ou posterior.

- Kaspersky Security Center versão 13.2 ou posterior (incluindo o Agente de Rede). Em versões anteriores do Kaspersky Security Center, é impossível ativar o recurso Kaspersky Sandbox.

- O Kaspersky Sandbox só pode ser gerenciado usando o Kaspersky Security Center Web Console.

- A transferência de dados para o Servidor de Administração está ativada. Os dados são necessários para obter as informações sobre os arquivos em quarentena em um computador por meio do Web Console.

- A conexão em segundo plano entre o Kaspersky Security Center Web Console e o servidor de administração foi estabelecida. Para que o Kaspersky Sandbox trabalhe com o Servidor de Administração por meio do Kaspersky Security Center Web Console, é preciso estabelecer uma nova conexão segura, uma *conexão em segundo plano*.

Etapas para migrar a configuração [KES+KEA] para [KES+agente integrado] para o Kaspersky Sandbox

1. **Atualização do plug-in da Web do Kaspersky Endpoint Security**

   O componente Kaspersky Sandbox pode ser gerenciado usando o plug-in da Web do Kaspersky Endpoint Security versão 11.7.0 ou posterior.

2. **Migrar as políticas e tarefas**

   Transfira as configurações do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows. Para fazer isso, use o assistente para migrar do Kaspersky Endpoint Agent no Web Console.

   Como migrar as configurações de políticas e tarefas do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security no Web Console

   Na janela principal do Web Console, selecione **Operações** → **Migração a partir do Kaspersky Endpoint Agent**.

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

Etapa 1. Migração da política

O assistente de migração cria uma nova política que unifica as configurações das políticas do Kaspersky Endpoint Security e Kaspersky Endpoint Agent. Na lista de política, selecione as políticas do Kaspersky Endpoint Agent cujas configurações deseja unificar as políticas do Kaspersky Endpoint Security. Clique na política do Kaspersky Endpoint Agent para selecionar a política do Kaspersky Endpoint Security com o qual deseja unificar as configurações. Certifique-se de ter selecionado as políticas corretas e vá para a próxima etapa.

Etapa 2. Migração da tarefa

O Assistente de migração cria novas tarefas para o Kaspersky Endpoint Security. Na lista de tarefa, selecione as tarefas do Kaspersky Endpoint Agent para as quais deseja criar uma política do Kaspersky Endpoint Security. Vá para a próxima etapa.

Etapa 3. Conclusão do Assistente

Conclua o assistente. Como resultado, o assistente faz o seguinte:

- Cria uma nova política do Kaspersky Endpoint Security.

  A política unifica as configurações do Kaspersky Endpoint Security e Kaspersky Endpoint Agent. A política é chamada *<nome da política Kaspersky Endpoint Security> & <nome da política Kaspersky Endpoint Agent>*. A nova política possui o status *Inativo*. Para continuar, mude os status das políticas do Kaspersky Endpoint Agent e Kaspersky Endpoint Security para *Inativo* e ative a nova política unificada.

  > Após a migração a partir do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows, certifique-se de que a nova política tenha a funcionalidade para transferência de dados para o servidor de administração (dados do arquivo na quarentena e dados da cadeia de evolução de ameaças) configurada. Os valores do parâmetro de transferência de dados não são migrados a partir de uma política do Kaspersky Endpoint Agent.

- Cria novas tarefas do Kaspersky Endpoint Security.

  As novas tarefas são cópias das tarefas do Kaspersky Endpoint Agent. Ao mesmo tempo, o assistente deixa as tarefas do Kaspersky Endpoint Agent inalteradas.

3. **Licenciamento da funcionalidade do Kaspersky Sandbox**

   Para ativar o Kaspersky Endpoint Security como parte da solução Kaspersky Sandbox, é necessária uma licença separada para o add-on do Kaspersky Sandbox. É possível adicionar a chave utilizando a tarefa *Adicionar chave*. Como resultado, duas chaves serão adicionadas ao aplicativo: *Kaspersky Endpoint Security* e *Kaspersky Sandbox*.

4. **Instalação/atualização do aplicativo Kaspersky Endpoint Security**

   Para migrar a funcionalidade do Kaspersky Sandbox durante a instalação ou upgrade de um aplicativo, é recomendável usar a tarefa de instalação remota. Ao criar uma tarefa de instalação remota, selecione o componente do Kaspersky Sandbox nas configurações do pacote de instalação.

   Também é possível baixar o aplicativo utilizando os seguintes métodos:

   - Uso do serviço de atualização da Kaspersky.
   - Localmente, usando o Assistente de configuração.

   O Kaspersky Endpoint Security é compatível com a seleção automática de componentes ao atualizar o aplicativo em um computador com o aplicativo Kaspersky Endpoint Agent instalado. A seleção automática dos componentes depende das permissões da conta do usuário que está atualizando o aplicativo.

   Caso esteja atualizando o Kaspersky Endpoint Security com um arquivo EXE ou MSI com a conta do sistema (SYSTEM), o Kaspersky Endpoint Security obtém acesso às licenças atualmente em uso das soluções da Kaspersky. Portanto, se o computador possui, por exemplo, o Kaspersky Endpoint Agent instalado e a solução Kaspersky Sandbox ativada, o instalador do Kaspersky Endpoint Security configura automaticamente o conjunto de componentes e seleciona o componente do Kaspersky Sandbox. Isso faz com que o Kaspersky Endpoint Security alterne o uso do agente integrado e remova o Kaspersky Endpoint Agent. A execução do instalador do MSI na conta do sistema (SYSTEM) normalmente é feita com a atualização por meio do serviço de atualização da Kaspersky ou ao implementar um pacote de instalação por meio do Kaspersky Security Center.

Caso esteja atualizando o Kaspersky Endpoint Security com um arquivo MSI com uma conta de usuário não privilegiado, o Kaspersky Endpoint Security perde o acesso das licenças atualmente em uso das soluções da Kaspersky. Neste caso, o Kaspersky Endpoint Security seleciona automaticamente os componentes de acordo com a configuração do Kaspersky Endpoint Agent. Depois disso, o Kaspersky Endpoint Security passa a usar o agente integrado e remove o Kaspersky Endpoint Agent.

O Kaspersky Endpoint Security é compatível com a atualização sem reinicialização do computador. É possível selecionar o modo de atualização do aplicativo nas propriedades da política.

5 **Verificação do funcionamento do aplicativo**

Se, após a instalação ou atualização do aplicativo, o computador estiver com o status *Crítico* no console do Kaspersky Security Center:

- Certifique-se de que o computador possui o Agente de Rede versão 13.2 ou posterior instalado.
- Verifique o status operacional do agente integrado visualizando o *Relatório de status dos componentes do aplicativo*. Caso o componente tenha o status *Não instalado*, instale o componente usando a tarefa *Alterar componentes do aplicativo*. Caso um componente tenha o status *Não coberto pela licença*, certifique-se de que a funcionalidade do agente integrado esteja ativada.
- Certifique-se de aceitar a Declaração da Kaspersky Security Network na nova política do Kaspersky Endpoint Security for Windows.

Kaspersky Anti Targeted Attack Platform

O Kaspersky Endpoint Security for Windows é compatível com o funcionamento junto com a solução Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* é uma solução projetada para a detecção oportuna de ameaças sofisticadas, como ataques direcionados, ameaças persistentes avançadas (APT) e ataques de dia zero, entre outros. A Kaspersky Anti Targeted Attack Platform inclui três unidades funcionais:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

É possível adquirir todas as unidades funcionais ou unidades individuais separadamente. Para obter informações detalhadas sobre a solução, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform. O aplicativo inclui agentes integrados para componentes EDR e NDR. O aplicativo também é compatível com o funcionamento junto com o componente Sandbox que faz parte do KATA.

Ferramentas de inteligência contra ameaças

O Kaspersky Endpoint Detection and Response usa as seguintes ferramentas Threat Intelligence:

- Integração com o Kaspersky Threat Intelligence Portal que contém e exibe as informações sobre a reputação de arquivos e endereços da Web.
- Banco de dados de Ameaças da Kaspersky.
- A infraestrutura de serviço na nuvem da Kaspersky Security Network (doravante também chamada de "KSN"), que fornece acesso a arquivos em tempo real, ao site e às informações sobre a reputação de software da base de conhecimento da Kaspersky. A utilização de dados do Kaspersky Security Network garante respostas mais rápidas dos aplicativos da Kaspersky contra as ameaças, melhora o desempenho de alguns componentes de proteção e reduz a possibilidade de falsos positivos.

Princípio de funcionamento da solução

O Kaspersky Endpoint Security é instalado em computadores individuais na infraestrutura corporativa de TI e monitora continuamente os processos, as conexões de rede abertas e os arquivos em modificação. As informações sobre eventos no computador são enviadas para o servidor do Kaspersky Anti Targeted Attack Platform. Nesse caso, o Kaspersky Endpoint Security também envia informações ao servidor do Kaspersky Anti Targeted Attack Platform sobre ameaças descobertas pelo aplicativo, além das informações sobre o processamento dos resultados dessas ameaças.

A integração do EDR (KATA) e NDR (KATA) é configurada no console do Kaspersky Security Center. Então, o agente integrado é gerenciado com o uso do console Kaspersky Anti Targeted Attack Platform, inclusive a execução de tarefas, gerenciamento de objetos em quarentena, exibição de relatórios e outras ações.

Configurações do Kaspersky Endpoint Security para o funcionamento com EDR / NDR (KATA)

As seguintes configurações podem ser usadas para trabalhar com EDR / NDR (KATA)

- **[KES+agente integrado]**. Nesta configuração, o Kaspersky Endpoint Security atua como o aplicativo que garante a segurança do computador, assim como o aplicativo que trabalha com EDR / NDR (KATA) O agente integrado para EDR (KATA) está disponível no Kaspersky Endpoint Security 12.1 for Windows ou posterior. O agente integrado para NDR (KATA) está disponível no Kaspersky Endpoint Security 12.7 for Windows ou posterior.
- **[EPP de terceiros+EDR Agent]**. Nesta configuração, a segurança da infraestrutura de TI é fornecida pelo Endpoint Protection Platform (EPP) de terceiros. A interação com o EDR/NDR (KATA) é fornecida pelo Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent (Agente EDR). Nesta configuração, o EDR Agent é compatível com aplicativos EPP de terceiros. O EDR Agent para EDR (KATA)está disponível no Kaspersky Endpoint Security 12.3 for Windows ou posterior. O EDR Agent para NDR (KATA)está disponível no Kaspersky Endpoint Security 12.7 for Windows ou posterior.

Compatibilidade com versões anteriores do Kaspersky Endpoint Security

Caso esteja usando o Kaspersky Endpoint Security 11.2.0 – 11.8.0 para interoperabilidade com o Kaspersky Anti Targeted Attack Platform (EDR), o aplicativo incluirá o Kaspersky Endpoint Agent. É possível instalar o Kaspersky Endpoint Agent durante a instalação do Kaspersky Endpoint Security.

Se estiver usando o Kaspersky Endpoint Security 11.9.0 – 12.0, você precisará instalar o Kaspersky Endpoint Agent separadamente, pois desde o Kaspersky Endpoint Security 11.9.0 o pacote de distribuição do Kaspersky Endpoint Agent não faz mais parte do kit de distribuição do Kaspersky Endpoint Security.

Integração do agente integrado com EDR / NDR (KATA)

Para a integração com EDR/NDR (KATA), é necessário adicionar o componente pertinente: Endpoint Detection and Response (KATA) ou Network Detection and Response (KATA). É possível selecionar os componentes para integração com EDR/NDR (KATA) durante a instalação ou atualização do aplicativo, assim como usar a tarefa *Alterar componentes do aplicativo*.

Iniciando com a versão 12.11 do Kaspersky Endpoint Security for Windows, o componente EDR (KATA) foi renomeado para **Endpoint Detection and Response Expert (versão 8.0 ou posterior)**. Nesta versão do aplicativo, o componente é compatível com o Kaspersky Anti Targeted Attack Platform 7.1 e versões anteriores, bem como com o Kaspersky Endpoint Detection and Response Expert (on-premises).

Os componentes Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) e Endpoint Detection and Response Expert (on-premises) não são compatíveis entre si.

Para usar a EDR / NDR (KATA), as seguintes condições devem ser atendidas:

- EDR (KATA): Kaspersky Anti Targeted Attack Platform versões 5.0–7.1.
- NDR (KATA): Kaspersky Anti Targeted Attack Platform versão 7.0 ou posterior.
- EDR (KATA): Kaspersky Endpoint Security for Windows 12.1 ou posterior. Para obter mais detalhes sobre a compatibilidade do KATA com diferentes versões do Kaspersky Endpoint Security, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform.
- NDR (KATA): Kaspersky Endpoint Security for Windows 12.7 ou posterior.
- Kaspersky Security Center versão 14.2 ou posterior. Em versões anteriores do Kaspersky Security Center, é impossível ativar a funcionalidade EDR/NDR (KATA).
- O aplicativo é ativado e a funcionalidade é contemplada pela licença.
- Os componentes Endpoint Detection and Response (KATA) e Network Detection and Response (KATA) estão ativados.

- Os componentes do aplicativo que garantem a operação do EDR/NDR (KATA) estão ativados e operacionais. Os seguintes componentes garantem a operação do EDR/NDR (KATA):
  - Proteção Contra Ameaças ao Arquivo.
  - Proteção Contra Ameaças da Web.
  - Proteção Contra Ameaças ao Correio.
  - Prevenção de Exploit.
  - Detecção de Comportamento.
  - Prevenção de Intrusão do Host.
  - Proteção AMSI.
  - Verificação em segundo plano.
  - Kaspersky Security Network.

[▷]

https://www.youtube.com/watch?v=cZzgtBoeC7k

[▷]

https://www.youtube.com/watch?v=gd-rySv0ThQ

A integração com o Endpoint Detection and Response (KATA) compreende as seguintes etapas:

1. **Instalação dos componentes Endpoint Detection and Response (KATA) e Network Detection and Response (KATA)**

   É possível selecionar os componentes EDR (KATA) e NDR (KATA) durante a instalação ou atualização, assim como usar a tarefa *Alterar componentes do aplicativo*.

   É preciso reiniciar o computador para concluir a atualização do aplicativo com os novos componentes.

2. **Ativação do Endpoint Detection and Response (KATA) a Network Detection and Response (KATA)**

   É preciso adquirir uma licença separada para o EDR (KATA) e o NDR (KATA) (por exemplo, add-on do Kaspersky Endpoint Detection and Response (KATA)).

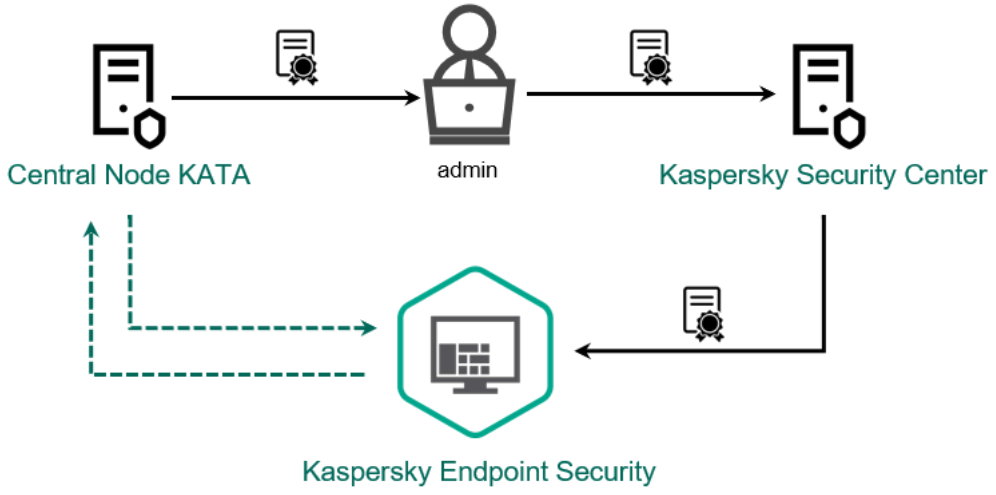
   A funcionalidade fica disponível depois da adição de uma chave separada que abrange as funcionalidades EDR (KATA) e NDR (KATA). Assim, diversas chaves são adicionadas no computador: uma chave para o Kaspersky Endpoint Security e chaves para o Kaspersky Endpoint Detection and Response (KATA) e o Network Detection and Response (KATA).

   A licença para as funcionalidades independentes EDR (KATA) e NDR (KATA) é a mesma que a licença do Kaspersky Endpoint Security.

   Verifique e confirme se as funcionalidades EDR (KATA) e NDR (KATA) estão incluídas na licença e se estão sendo executadas na interface local do aplicativo.

3. **Conexão com o Central Node**

   A Kaspersky Anti Targeted Attack Platform requer o estabelecimento de uma conexão confiável entre o Kaspersky Endpoint Security e o componente Central Node. Para configurar uma conexão confiável, é necessário usar um certificado TLS. É possível obter um certificado TLS no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform). Em seguida, é necessário adicionar o certificado TLS ao Kaspersky Endpoint Security (consulte as instruções abaixo).



Adição de um certificado TLS ao Kaspersky Endpoint Security

   Por padrão, o Kaspersky Endpoint Security verifica apenas o certificado TLS do Central Node. Para tornar a conexão mais segura, também é possível ativar a verificação do computador no Central Node (autenticação bidirecional). Para ativar essa verificação, é necessário ativar a autenticação bidirecional nas configurações do Central Node e do Kaspersky Endpoint Security. Para usar a autenticação bidirecional, também será necessário um contêiner criptográfico. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner criptográfico no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform).

Como conectar um computador Kaspersky Endpoint Security ao Central Node com o uso do Console de Administração (MMC)

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

2. Na árvore do console, selecione **Políticas**.

3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

4. Na janela da política, selecione **Detection and Response** e selecione o componente que deseja configurar: **Endpoint Detection and Response Expert (on-premises)** ou **Network Detection and Response (KATA)**.

5. Marque a caixa de seleção correspondente: **Endpoint Detection and Response Expert (versão 7.1 ou anterior)** ou **Network Detection and Response (KATA)**.

6. Clique **Configurações de conexão do servidor**.

7. Configure a conexão do servidor:

   - **Tempo limite (seg)**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite se esgota, o Kaspersky Endpoint Security tenta estabelecer conexão com um servidor de Central Node diferente.

   - **Certificado TLS do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor do Central Node. É possível obter um certificado TLS no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform).

   - **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor do Central Node, obter um contêiner de criptografia e definir uma senha para proteger o contêiner criptográfico. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner criptográfico no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform). Depois de definir as configurações do Central Node, é necessário também habilitar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner criptográfico protegido por senha.

     O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.

8. Clique **OK**.

9. Adicionar servidores de Central Node. Para fazer isso, especifique o endereço do servidor (IPv4, IPv6) e a porta para se conectar ao servidor.

   É possível adicionar vários endereços de servidor do nó central. O Kaspersky Endpoint Security tenta se conectar ao servidor usando o primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar usando o segundo endereço IP na lista e assim sucessivamente.

10. Caso necessário, configure a telemetria.

11. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como conectar um computador Kaspersky Endpoint Security ao Central Node usando o Web Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Vá para a seção **Configuração de agentes integrados** e selecione o componente que deseja configurar: **Endpoint Detection and Response Expert (on-premises)** ou **Network Detection and Response (KATA)**.

5. Ative o botão de alternância correspondente: **Endpoint Detection and Response Expert (on-premises) ATIVADO** ou **Network Detection and Response (KATA) ATIVADO**.

6. Para configurar o EDR (KATA), selecione **Endpoint Detection and Response Expert (versão 7.1 ou anterior)** pela lista de soluções.

7. Clique **Configurações de conexão**.

8. Configure a conexão do servidor:

   - **Tempo limite (s)**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite se esgota, o Kaspersky Endpoint Security tenta estabelecer conexão com um servidor de Central Node diferente.

   - **Certificado do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor do Central Node. É possível obter um certificado TLS no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform).

   - **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor do Central Node, obter um contêiner de criptografia e definir uma senha para proteger o contêiner criptográfico. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner criptográfico no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform). Depois de definir as configurações do Central Node, é necessário também habilitar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner criptográfico protegido por senha.

     O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.

9. Clique **OK**.

10. Adicionar servidores de Central Node. Para fazer isso, especifique o endereço do servidor (IPv4, IPv6) e a porta para se conectar ao servidor.

    É possível adicionar vários endereços de servidor do nó central. O Kaspersky Endpoint Security tenta se conectar ao servidor usando o primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar usando o segundo endereço IP na lista e assim sucessivamente.

11. Caso necessário, configure a telemetria.

12. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Também é possível adicionar um certificado TLS localmente usando a linha de comando.

Como resultado, o computador é adicionado ao console da Kaspersky Anti Targeted Attack Platform. Verifique o status operacional dos componentes visualizando o *Relatório de status dos componentes do aplicativo*. Também é possível visualizar o status operacional de componentes em relatórios na interface local do Kaspersky Endpoint Security. Os componentes **Endpoint Detection and Response Expert (versão 8.0 ou posterior)** e **Network Detection and Response (KATA)** serão adicionados à lista de componentes do Kaspersky Endpoint Security.

> É possível verificar o status dos componentes no console do Kaspersky Security Center nas propriedades do computador na seção **Componentes**. Considere o seguinte aspecto ao verificar o status do componente no console. Caso o componente não esteja instalado e a funcionalidade não seja abrangida por sua licença, o console exibirá o status **Incompatível com a licença** em vez de **Não instalado**.

A partir do Kaspersky Endpoint Security 12.6 for Windows, é possível monitorar o status do componente EDR (KATA) no Console de Administração do Kaspersky Security Center (MMC). O status atual do componente é exibido nas propriedades do computador, na coluna **Status do Endpoint Sensor** (*Executando*, *Iniciando*, *Parado*, *Pausado*, *Falhou*, *Desconhecido*). O Web Console não exibe o status do Endpoint Sensor.

Configuração da telemetria EDR (KATA)

Telemetria é uma lista de eventos que ocorreram no computador protegido. O Kaspersky Endpoint Security analisa os dados de telemetria e os envia para a Kaspersky Anti Targeted Attack Platform durante a sincronização. Os eventos de telemetria chegam ao servidor quase continuamente. O Kaspersky Endpoint Security inicia a sincronização com o servidor quando qualquer uma das seguintes condições for satisfeita:

- O intervalo de sincronização terminou.
- O número de eventos no buffer excede o limite superior.

Portanto, por padrão, o aplicativo sincroniza a cada 30 segundos ou sempre que o buffer contiver 1024 eventos. É possível configurar o comportamento de sincronização na política do Kaspersky Endpoint Security e selecionar os valores ideais para que correspondam com sua carga de rede (consulte as instruções abaixo).

Se não houver conexão entre o Kaspersky Endpoint Security e o servidor, o aplicativo enfileira novos eventos. Quando a conexão é restaurada, o Kaspersky Endpoint Security envia eventos em fila para o servidor na ordem correta. Para evitar sobrecarregar o servidor, o Kaspersky Endpoint Security pode ignorar alguns eventos. Para ativar essa opção, é possível otimizar as configurações de transmissão de eventos, por exemplo, para definir um valor máximo de eventos por hora (consulte as instruções abaixo).

Caso esteja usando o Kaspersky Anti Targeted Attack Platform junto com outra solução que também use telemetria, é possível desativar a telemetria para KATA (EDR) (consulte as instruções abaixo). Isso permite otimizar a carga do servidor para essas soluções. Por exemplo, caso tenha a solução Managed Detection and Response e o KATA (EDR) implantados, será possível usar a telemetria MDR e criar tarefas de Resposta a Ameaças no KATA (EDR).

Como configurar a telemetria no Console de Administração (MMC)

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

2. Na árvore do console, selecione **Políticas**.

3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

4. Na janela da política, selecione **Detection and Response** e selecione o componente que deseja configurar: **Endpoint Detection and Response Expert (on-premises)** ou **Network Detection and Response (KATA)**.

5. Defina a configuração **Enviar solicitação de sincronização para o servidor KATA a cada (min.)**. Frequência de solicitações de sincronização enviadas ao servidor. Durante a sincronização, o Kaspersky Endpoint Security envia informações sobre as configurações e tarefas modificadas do aplicativo.

6. Certifique-se de que a caixa de seleção **Enviar telemetria à KATA** esteja marcada.

7. Caso necessário, configure a sincronização com as configurações do servidor no bloco **Configurações de transmissão de dados**:

   - **Atraso máximo na transmissão de eventos (segundos)**. O aplicativo sincroniza com o servidor para enviar eventos após expirar o intervalo de sincronização. A configuração padrão é 30 segundos.

   - **Número máximo de pacotes de eventos**. O aplicativo sincroniza com o servidor quando o buffer está cheio de eventos. A configuração padrão é 1024 eventos.

8. Caso seja necessário, marque a caixa de seleção **Ativar a limitação de solicitações** no bloco **Limitação de solicitações**.

   Esse recurso ajuda a otimizar a carga no computador. Se essa funcionalidade estiver ativada, o aplicativo restringirá a transmissão de eventos. Caso o número de eventos exceda os limites configurados, o Kaspersky Endpoint Security interromperá o envio de eventos.

9. Defina as configurações de otimização para enviar eventos ao servidor:

   - **Número máximo de eventos por hora**. O aplicativo analisa o fluxo de dados de telemetria e restringe o envio de eventos caso ele exceda o limite de eventos configurado por hora. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. A configuração padrão é de 3 mil eventos por hora. Caso o aplicativo esteja instalado em um servidor, o fluxo de dados de telemetria será maior. Para servidores, é recomendável aumentar o valor para 60 mil eventos por hora.

   - **Porcentagem de excesso de limite de evento**. O aplicativo ordena os eventos por tipo (por exemplo, eventos "alterações no registro") e restringe a transmissão de eventos caso a proporção de eventos do mesmo tipo para o número total de eventos exceda o limite configurado em porcentagem. O Kaspersky Endpoint Security retoma o envio de eventos quando a proporção de outros eventos para o número total de eventos torna-se volumosa o suficiente novamente. A configuração padrão é 15%.

10. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como configurar a telemetria no Web Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configuração de agentes integrados** → **Endpoint Detection and Response Expert (on-premises)**.

5. Para configurar o EDR (KATA), selecione **Endpoint Detection and Response Expert (versão 7.1 ou anterior)** pela lista de soluções.

6. Verifique e confirme se a caixa de seleção **Enviar telemetria aos servidores da KATA** está marcada no bloco **Configurações de transmissão de dados**.

7. Defina a configuração **Enviar solicitação de sincronização para o servidor a cada (min.)**. Frequência de solicitações de sincronização enviadas ao servidor. Durante a sincronização, o Kaspersky Endpoint Security envia informações sobre as configurações e tarefas modificadas do aplicativo.

8. Certifique-se de que a caixa de seleção **Enviar telemetria aos servidores da KATA** esteja marcada.

9. Caso necessário, configure a sincronização com as configurações do servidor no bloco **Configurações de transmissão de dados**:

   - **Atraso máximo na transmissão de eventos (segundos)**. O aplicativo sincroniza com o servidor para enviar eventos após expirar o intervalo de sincronização. A configuração padrão é 30 segundos.

   - **Número máximo de pacotes de eventos**. O aplicativo sincroniza com o servidor quando o buffer está cheio de eventos. A configuração padrão é 1024 eventos.

10. Caso seja necessário, marque a caixa de seleção **Ativar a limitação de solicitações** no bloco **Limitação de solicitações**.

    Esse recurso ajuda a otimizar a carga no computador. Se essa funcionalidade estiver ativada, o aplicativo restringirá a transmissão de eventos. Caso o número de eventos exceda os limites configurados, o Kaspersky Endpoint Security interromperá o envio de eventos.

11. Defina as configurações de otimização para enviar eventos ao servidor:

    - **Número máximo de eventos por hora**. O aplicativo analisa o fluxo de dados de telemetria e restringe o envio de eventos caso ele exceda o limite de eventos configurado por hora. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. A configuração padrão é de 3 mil eventos por hora. Caso o aplicativo esteja instalado em um servidor, o fluxo de dados de telemetria será maior. Para servidores, é recomendável aumentar o valor para 60 mil eventos por hora.

    - **Porcentagem de excesso de limite de evento**. O aplicativo ordena os eventos por tipo (por exemplo, eventos "alterações no registro") e restringe a transmissão de eventos caso a proporção de eventos do mesmo tipo para o número total de eventos exceda o limite configurado em porcentagem. O Kaspersky Endpoint Security retoma o envio de eventos quando a proporção de outros eventos para o número total de eventos torna-se volumosa o suficiente novamente. A configuração padrão é 15%.

12. Para aplicar a política aos computadores, feche os ícones de cadeado 🔒 e salve as alterações.

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

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

   A janela de propriedades da política é exibida.

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

4. Ir para a seção **Integração KATA** → **Exclusões de telemetria**.

5. Embaixo de **Configurações de transmissão de dados**, marque a caixa de seleção **Exclusões de uso**.

6. Clique **Adicionar** e configure as exclusões:

Os critérios são combinados com a lógica *E*.

- **Caminho**. Caminho completo para o arquivo, incluindo seu nome e extensão. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara. Para que a exclusão funcione, o caminho para o arquivo deve ser especificado.
- **Linha de comando**. Comando usado para executar o objeto.
- **Descrição**. Valor do parâmetro FileDescription a partir de um recurso RT_VERSION (VersionInfo).

  Para obter mais detalhes sobre o recurso VersionInfo, visite o site da Microsoft.
- **Nome do arquivo original**. Valor do parâmetro OriginalFilename a partir de um recurso RT_VERSION (VersionInfo).
- **Versão**. Valor do parâmetro FileVersion a partir de um recurso RT_VERSION (VersionInfo).
- **MD5**. Hash MD5 do arquivo.
- **SHA256**. Hash SHA256 do arquivo.
- **Tipos de eventos**. Para que a exclusão funcione, é preciso selecionar pelo menos um tipo de evento.

7. Salvar alterações.

1. No Console de Administração do Kaspersky Security Center, selecione **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

1. Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Reversão de atualização**.

Etapa 2. 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 3. Configurar um agendamento de início de tarefa

Configure o agendamento da tarefa, por exemplo, manualmente.

Etapa 4. Definir o nome da tarefa

Insira um nome para a tarefa.

Etapa 7. Concluir a criação da tarefa

Conclua o 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.

Exclusões de telemetria EDR (KATA)

Para melhorar o desempenho e otimizar a transmissão de dados para o servidor de telemetria, é possível configurar as exclusões de telemetria. Por exemplo, é possível optar pelo não envio de dados de comunicações de rede para aplicativos individuais.

Como criar uma exclusão de telemetria no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Exclusões e tipos de objetos**.
4. No bloco **Configurações de telemetria** → **Telemetria do EDR (KATA) / NDR (KATA)**, clique no botão **Configurações**.
5. Na janela exibida, configure as exclusões de telemetria (consulte a tabela abaixo).

   O aplicativo combina condições de exclusão com o E lógico. Para criar uma regra, é necessário especificar um valor no campo **Caminho completo** e selecionar pelo menos um tipo de evento na lista **Usar para os seguintes tipos de eventos**.
6. Salvar alterações.

Como criar uma exclusão de telemetria no Web Console e no Cloud Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.

4. Selecione **Configurações gerais** → **Configurações de telemetria**.

5. Selecione a guia **Telemetria do EDR (KATA) / NDR (KATA)**.

6. Na janela exibida, configure as exclusões de telemetria (consulte a tabela abaixo).

   O aplicativo combina condições de exclusão com o E lógico. Para criar uma regra, é necessário especificar um valor no campo **Caminho completo** e selecionar pelo menos um tipo de evento.

7. Salvar alterações.

Parâmetros de exclusão de telemetria

Parâmetro	Descrição
Processos excluídos	**Otimizar o tamanho da telemetria a ser enviada**. O Kaspersky Endpoint Security permite otimizar a quantidade de dados transmitidos e excluir eventos com determinados códigos da telemetria: código 102 (comunicações básicas) e 8 (atividade de rede do processo) para o protocolo SMB da Microsoft, o serviço WinRM e o processo klnagent.exe do Agente de Rede, assim como as informações estendidas sobre os tipos de pacotes de rede para todos os tipos de protocolos de rede. O Kaspersky Endpoint Security combina critérios de acionamento de regra com um E lógico. **Processo** e **Processo pai**: • **Caminho completo**. Caminho completo para o arquivo, incluindo seu nome e extensão. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara. • **Texto da linha de comando**. Comando usado para executar o arquivo. • **Descrição**. Valor do parâmetro FileDescription a partir de um recurso RT_VERSION (VersionInfo). • **Nome do arquivo original**. Valor do parâmetro OriginalFilename a partir de um recurso RT_VERSION (VersionInfo). • **Versão**. Valor do parâmetro FileVersion a partir de um recurso RT_VERSION (VersionInfo). • **Somas de verificação do arquivo**. MD5 e SHA256. Também é possível selecionar manualmente um arquivo e o aplicativo preencherá automaticamente os campos do arquivo selecionado. Em sistemas operacionais de 64 bits, você deve inserir manualmente os parâmetros da versão de 64 bits do arquivo executável de um processo na pasta `C:\windows\system32`. Isso porque o aplicativo preenche os campos de parâmetro do arquivo executável com dados das propriedades da versão de 32 bits do mesmo arquivo executável na pasta `C:\windows\syswow64`. Por exemplo, se `C:\windows\system32\cmd.exe`, for selecionado, o plug-in exibirá os parâmetros de `C:\windows\syswow64\cmd.exe`. Esse comportamento é ditado por peculiaridades do sistema operacional. **Usar para os seguintes tipos de eventos**: • **Modificação de arquivo**. • **Eventos de rede**. • **Processo: entrada interativa no console**. • **Módulo carregado**. • **Registro modificado**. • **Logs de DNS**. • **Acesso ao processo**. • **Invasão de código**. • **Consulta WMI**. • **Pipe**. • **LDAP**. • **AMSI**.

Parâmetro	Descrição
Comunicações de rede excluídas	**Nome da regra**. **Direção**. **Protocolo**. **Soquete bruto**. **Número do protocolo**. **Certificado TLS**. **Porta local ou intervalo**. **Porta remota ou intervalo**. **Endereço local**. O endereço de rede do computador para o qual o Kaspersky Endpoint Security está excluindo a telemetria do tráfego de rede. **Endereço remoto**. O endereço de rede do computador para o qual o Kaspersky Endpoint Security está excluindo a telemetria do tráfego de rede. Somente o formato IPv4 é compatível com endereços IP. **Aplicativos**. Lista de arquivos executáveis de aplicativos para os quais o Kaspersky Endpoint Security está excluindo a telemetria EDR do tráfego de rede.
Operações de arquivo excluídas	**Nome da regra**. **Nome ou máscara do arquivo**. Nome ou máscara de um arquivo ou pasta; o Kaspersky Endpoint Security aplica a regra de exclusão quando esse arquivo ou pasta é acessado. O Kaspersky Endpoint Security tem suporte aos caracteres `*` e `?` ao inserir uma máscara. **Tipo de operação**. **Caminho anterior**. O Kaspersky Endpoint Security combina critérios de acionamento de regra com um E lógico. **Processo** e **Processo pai**: • **Caminho completo**. Caminho completo para o arquivo, incluindo seu nome e extensão. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara. • **Texto da linha de comando**. Comando usado para executar o arquivo. • **Descrição**. Valor do parâmetro FileDescription a partir de um recurso RT_VERSION (VersionInfo). • **Nome do arquivo original**. Valor do parâmetro OriginalFilename a partir de um recurso RT_VERSION (VersionInfo). • **Versão**. Valor do parâmetro FileVersion a partir de um recurso RT_VERSION (VersionInfo). • **Somas de verificação do arquivo**. MD5 e SHA256. Também é possível selecionar manualmente um arquivo e o aplicativo preencherá automaticamente os campos do arquivo selecionado. Em sistemas operacionais de 64 bits, você deve inserir manualmente os parâmetros da versão de 64 bits do arquivo executável de um processo na pasta `C:\windows\system32`. Isso porque o aplicativo preenche os campos de parâmetro do arquivo executável com dados das propriedades da versão de 32 bits do mesmo arquivo executável na pasta `C:\windows\syswow64`. Por exemplo, se `C:\windows\system32\cmd.exe`, for selecionado, o plug-in exibirá os parâmetros de `C:\windows\syswow64\cmd.exe`. Esse comportamento é ditado por peculiaridades do sistema operacional.

Parâmetro	Descrição
Operações de DNS excluídas	**Nome da regra**. O Kaspersky Endpoint Security combina critérios de acionamento de regra com um E lógico. **Processo** e **Processo pai**: • **Caminho completo**. Caminho completo para o arquivo, incluindo seu nome e extensão. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara. • **Texto da linha de comando**. Comando usado para executar o arquivo. • **Descrição**. Valor do parâmetro FileDescription a partir de um recurso RT_VERSION (VersionInfo). • **Nome do arquivo original**. Valor do parâmetro OriginalFilename a partir de um recurso RT_VERSION (VersionInfo). • **Versão**. Valor do parâmetro FileVersion a partir de um recurso RT_VERSION (VersionInfo). • **Somas de verificação do arquivo**. MD5 e SHA256. Também é possível selecionar manualmente um arquivo e o aplicativo preencherá automaticamente os campos do arquivo selecionado. Em sistemas operacionais de 64 bits, você deve inserir manualmente os parâmetros da versão de 64 bits do arquivo executável de um processo na pasta `C:\windows\system32`. Isso porque o aplicativo preenche os campos de parâmetro do arquivo executável com dados das propriedades da versão de 32 bits do mesmo arquivo executável na pasta `C:\windows\syswow64`. Por exemplo, se `C:\windows\system32\cmd.exe`, for selecionado, o plug-in exibirá os parâmetros de `C:\windows\syswow64\cmd.exe`. Esse comportamento é ditado por peculiaridades do sistema operacional. **DNS**: • **Endereço IP do servidor DNS**. • **Opções de consulta**. • **Status**. • **Nome de domínio**. • **ID de tipo de configuração**. • **Dados de resposta**.
Operações LDAP excluídas	**Nome da regra**. **Escopo da pesquisa LDAP**. **Filtro**. **Nome distinto para pesquisa de objetos LDAP**. **Atributos do objeto**. O Kaspersky Endpoint Security combina critérios de acionamento de regra com um E lógico. **Processo** e **Processo pai**: • **Caminho completo**. Caminho completo para o arquivo, incluindo seu nome e extensão. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara. • **Texto da linha de comando**. Comando usado para executar o arquivo. • **Descrição**. Valor do parâmetro FileDescription a partir de um recurso RT_VERSION (VersionInfo). • **Nome do arquivo original**. Valor do parâmetro OriginalFilename a partir de um recurso RT_VERSION (VersionInfo). • **Versão**. Valor do parâmetro FileVersion a partir de um recurso RT_VERSION (VersionInfo). • **Somas de verificação do arquivo**. MD5 e SHA256. Também é possível selecionar manualmente um arquivo e o aplicativo preencherá automaticamente os campos do arquivo selecionado. Em sistemas operacionais de 64 bits, você deve inserir manualmente os parâmetros da versão de 64 bits do arquivo executável de um processo na pasta `C:\windows\system32`. Isso porque o aplicativo preenche os campos de parâmetro do arquivo executável com dados das propriedades da versão de 32 bits do mesmo arquivo executável na pasta `C:\windows\syswow64`. Por exemplo, se `C:\windows\system32\cmd.exe`, for selecionado, o plug-in exibirá os parâmetros de `C:\windows\syswow64\cmd.exe`. Esse comportamento é ditado por peculiaridades do sistema operacional.

Parâmetro	Descrição
Consultas de acesso do processo excluídas	**Nome da regra**. **Tipo de operação**. **Acesso requisitado ao processo**. **Rastreamento de pilha de chamada**. O Kaspersky Endpoint Security combina critérios de acionamento de regra com um E lógico. **Processo**, **Processo pai**, **Arquivo do processo de destino**, **Manuseador do Processo de origem** e **Manuseador do Processo de destino**. • **Caminho completo**. Caminho completo para o arquivo, incluindo seu nome e extensão. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara. • **Texto da linha de comando**. Comando usado para executar o arquivo. • **Especifique os critérios de acionamento da regra e os tipos de eventos para os quais usá-la**. Valor do parâmetro FileDescription a partir de um recurso RT_VERSION (VersionInfo). • **Nome do arquivo original**. Valor do parâmetro OriginalFilename a partir de um recurso RT_VERSION (VersionInfo). • **Versão**. Valor do parâmetro FileVersion a partir de um recurso RT_VERSION (VersionInfo). • **Checksums do arquivo**. MD5 e SHA256. Também é possível selecionar manualmente um arquivo e o aplicativo preencherá automaticamente os campos do arquivo selecionado. Em sistemas operacionais de 64 bits, você deve inserir manualmente os parâmetros da versão de 64 bits do arquivo executável de um processo na pasta `C:\windows\system32`. Isso porque o aplicativo preenche os campos de parâmetro do arquivo executável com dados das propriedades da versão de 32 bits do mesmo arquivo executável na pasta `C:\windows\syswow64`. Por exemplo, se `C:\windows\system32\cmd.exe`, for selecionado, o plug-in exibirá os parâmetros de `C:\windows\syswow64\cmd.exe`. Esse comportamento é ditado por peculiaridades do sistema operacional.
Injeções de código excluídas	**Nome da regra**. **Método de acesso**. **Pilha de chamada**. **Linha de comando modificada**. **Endereço da invasão**. **Nome da DLL inserida**. O Kaspersky Endpoint Security combina critérios de acionamento de regra com um E lógico. **Processo** e **Processo pai**: • **Caminho completo**. Caminho completo para o arquivo, incluindo seu nome e extensão. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara. • **Texto da linha de comando**. Comando usado para executar o arquivo. • **Descrição**. Valor do parâmetro FileDescription a partir de um recurso RT_VERSION (VersionInfo). • **Nome do arquivo original**. Valor do parâmetro OriginalFilename a partir de um recurso RT_VERSION (VersionInfo). • **Versão**. Valor do parâmetro FileVersion a partir de um recurso RT_VERSION (VersionInfo). • **Somas de verificação do arquivo**. MD5 e SHA256. Também é possível selecionar manualmente um arquivo e o aplicativo preencherá automaticamente os campos do arquivo selecionado. Em sistemas operacionais de 64 bits, você deve inserir manualmente os parâmetros da versão de 64 bits do arquivo executável de um processo na pasta `C:\windows\system32`. Isso porque o aplicativo preenche os campos de parâmetro do arquivo executável com dados das propriedades da versão de 32 bits do mesmo arquivo executável na pasta `C:\windows\syswow64`. Por exemplo, se `C:\windows\system32\cmd.exe`, for selecionado, o plug-in exibirá os parâmetros de `C:\windows\syswow64\cmd.exe`. Esse comportamento é ditado por peculiaridades do sistema operacional.

Parâmetro	Descrição
Consultas WMI excluídas	**Nome da regra**. **Tipo de operação WMI**. **Consulta remota**. **Nome de um computador que executou um comando WMI**. **Conta de usuário WMI**. **Comando WMI executado**. **Namespace WMI**. **Filtro de consumidor de evento WMI**. **Nome do consumidor de evento WMI criado**. **Código-fonte de um consumidor de evento WMI**. O Kaspersky Endpoint Security combina critérios de acionamento de regra com um E lógico. **Processo** e **Processo pai**: • **Caminho completo**. Caminho completo para o arquivo, incluindo seu nome e extensão. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara. • **Texto da linha de comando**. Comando usado para executar o arquivo. • **Descrição**. Valor do parâmetro FileDescription a partir de um recurso RT_VERSION (VersionInfo). • **Nome do arquivo original**. Valor do parâmetro OriginalFilename a partir de um recurso RT_VERSION (VersionInfo). • **Versão**. Valor do parâmetro FileVersion a partir de um recurso RT_VERSION (VersionInfo). • **Somas de verificação do arquivo**. MD5 e SHA256. Também é possível selecionar manualmente um arquivo e o aplicativo preencherá automaticamente os campos do arquivo selecionado. Em sistemas operacionais de 64 bits, você deve inserir manualmente os parâmetros da versão de 64 bits do arquivo executável de um processo na pasta `C:\windows\system32`. Isso porque o aplicativo preenche os campos de parâmetro do arquivo executável com dados das propriedades da versão de 32 bits do mesmo arquivo executável na pasta `C:\windows\syswow64`. Por exemplo, se `C:\windows\system32\cmd.exe`, for selecionado, o plug-in exibirá os parâmetros de `C:\windows\syswow64\cmd.exe`. Esse comportamento é ditado por peculiaridades do sistema operacional.
Operações de pipe excluídas	**Nome da regra**. **Nome do pipe**. **Tipo de operação**. O Kaspersky Endpoint Security combina critérios de acionamento de regra com um E lógico. **Processo** e **Processo pai**: • **Caminho completo**. Caminho completo para o arquivo, incluindo seu nome e extensão. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara. • **Texto da linha de comando**. Comando usado para executar o arquivo. • **Descrição**. Valor do parâmetro FileDescription a partir de um recurso RT_VERSION (VersionInfo). • **Nome do arquivo original**. Valor do parâmetro OriginalFilename a partir de um recurso RT_VERSION (VersionInfo). • **Versão**. Valor do parâmetro FileVersion a partir de um recurso RT_VERSION (VersionInfo). • **Somas de verificação do arquivo**. MD5 e SHA256. Também é possível selecionar manualmente um arquivo e o aplicativo preencherá automaticamente os campos do arquivo selecionado. Em sistemas operacionais de 64 bits, você deve inserir manualmente os parâmetros da versão de 64 bits do arquivo executável de um processo na pasta `C:\windows\system32`. Isso porque o aplicativo preenche os campos de parâmetro do arquivo executável com dados das propriedades da versão de 32 bits do mesmo arquivo executável na pasta `C:\windows\syswow64`. Por exemplo, se `C:\windows\system32\cmd.exe`, for selecionado, o plug-in exibirá os parâmetros de `C:\windows\syswow64\cmd.exe`. Esse comportamento é ditado por peculiaridades do sistema operacional.

Parâmetro	Descrição
Alterações de registro excluídas	**Nome da regra**. **Tipo de operação**. **Caminho**. **Nome do valor**. **Valor**. **Nome completo de um arquivo de registro**. O Kaspersky Endpoint Security combina critérios de acionamento de regra com um E lógico. **Processo** e **Processo pai**: • **Caminho completo**. Caminho completo para o arquivo, incluindo seu nome e extensão. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara. • **Texto da linha de comando**. Comando usado para executar o arquivo. • **Descrição**. Valor do parâmetro FileDescription a partir de um recurso RT_VERSION (VersionInfo). • **Nome do arquivo original**. Valor do parâmetro OriginalFilename a partir de um recurso RT_VERSION (VersionInfo). • **Versão**. Valor do parâmetro FileVersion a partir de um recurso RT_VERSION (VersionInfo). • **Somas de verificação do arquivo**. MD5 e SHA256. Também é possível selecionar manualmente um arquivo e o aplicativo preencherá automaticamente os campos do arquivo selecionado. Em sistemas operacionais de 64 bits, você deve inserir manualmente os parâmetros da versão de 64 bits do arquivo executável de um processo na pasta `C:\windows\system32`. Isso porque o aplicativo preenche os campos de parâmetro do arquivo executável com dados das propriedades da versão de 32 bits do mesmo arquivo executável na pasta `C:\windows\syswow64`. Por exemplo, se `C:\windows\system32\cmd.exe`, for selecionado, o plug-in exibirá os parâmetros de `C:\windows\syswow64\cmd.exe`. Esse comportamento é ditado por peculiaridades do sistema operacional.
Operações com dispositivos excluídas	**Nome da regra**. **Tipo do dispositivo**. **ID do dispositivo**. **Nome do dispositivo**.

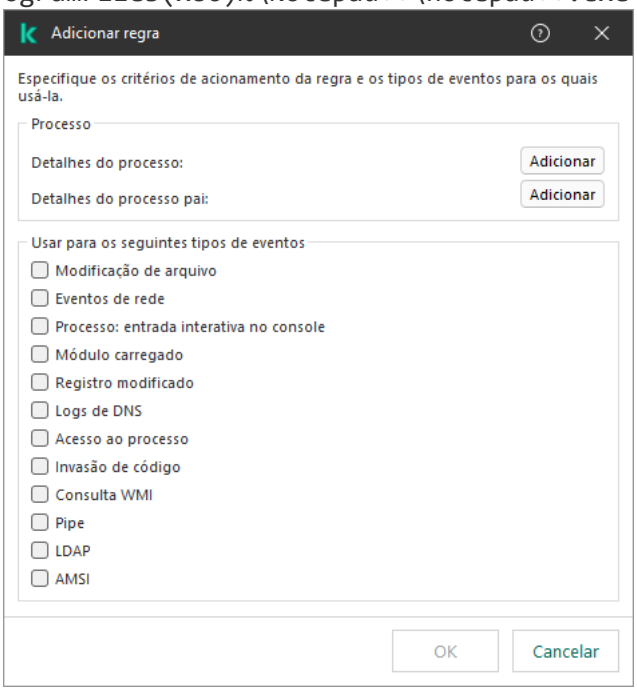
Exemplo 1. Processos excluídos

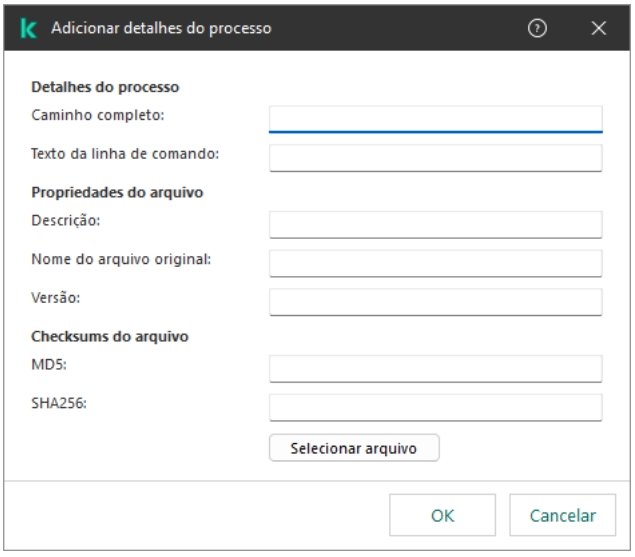
Para excluir eventos de aplicativo (processo) de terceiros da telemetria, abra a janela Exclusões da telemetria EDR em **Processos excluídos** e adicione o arquivo executável do aplicativo.

O Kaspersky Endpoint Security combina critérios de acionamento de regra com um E lógico.

O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara. Por exemplo:

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`





Excluindo um processo

Exemplo 1. Modificação de arquivo

Se você costuma editar scripts no aplicativo Notepad++ e deseja excluir os eventos de modificação para os scripts correspondentes, adicione o arquivo executável do Notepad++ para exclusões da telemetria.

Especifique as configurações da seguinte forma:

- **Caminho completo**: `C:\Program Files\Notepad++\notepad++.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.
- **Usar para os seguintes tipos de eventos**: Modificação de arquivo.

Exemplo 2. Eventos de rede

Se você usar o aplicativo WinSCP para gerenciar arquivos em um servidor remoto e você deseja excluir eventos de rede, adicione o arquivo executável do WinSCP para exclusões da telemetria.

Especifique as configurações da seguinte forma:

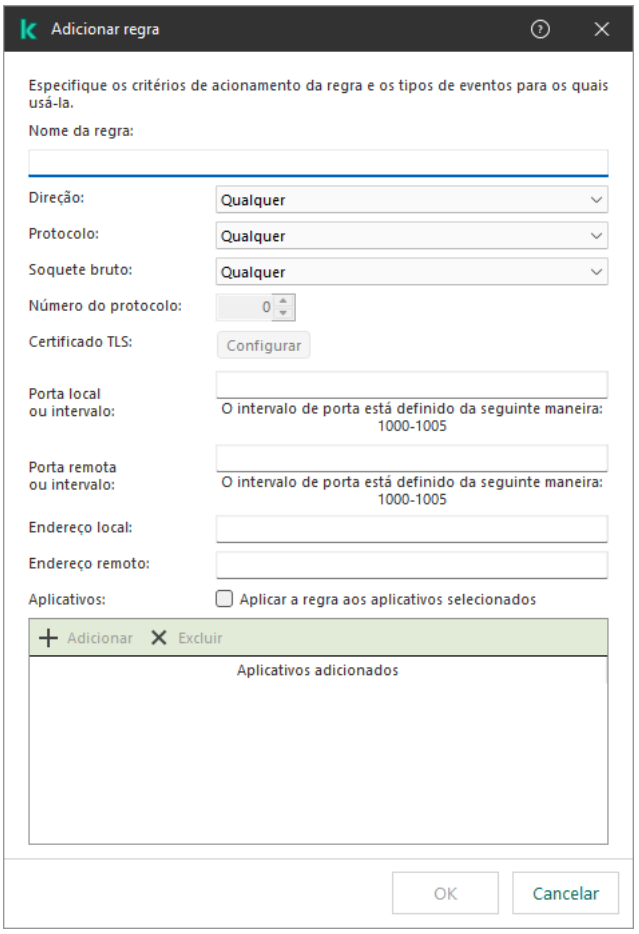
- **Caminho completo**: `C:\Program Files (x86)\WinSCP\WinSCP.exe`.
- **SHA256**: 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (opcional).
- **Usar para os seguintes tipos de eventos**: Eventos de rede.

Exemplo 2. Comunicações de rede excluídas

Para excluir eventos de conexão de serviço remoto da telemetria, abra a janela Exclusões da telemetria EDR na guia **Comunicações de rede excluídas** e adicione configurações de conexão: protocolo, porta, direção, endereço IP, certificado TLS e outros.

O Kaspersky Endpoint Security combina critérios de acionamento de regra com um E lógico.

> Você não pode especificar um endereço de sub-rede (por exemplo, 10.28.0.0/24). O aplicativo só permite especificar um endereço IP (por exemplo, 10.28.0.105).



Exclusão de comunicação de rede

Se você usa um servidor Web corporativo e deseja excluir eventos do navegador ao se conectar a esse servidor da Web, adicione o endereço IP do servidor e o arquivo executável do navegador às exclusões da telemetria.

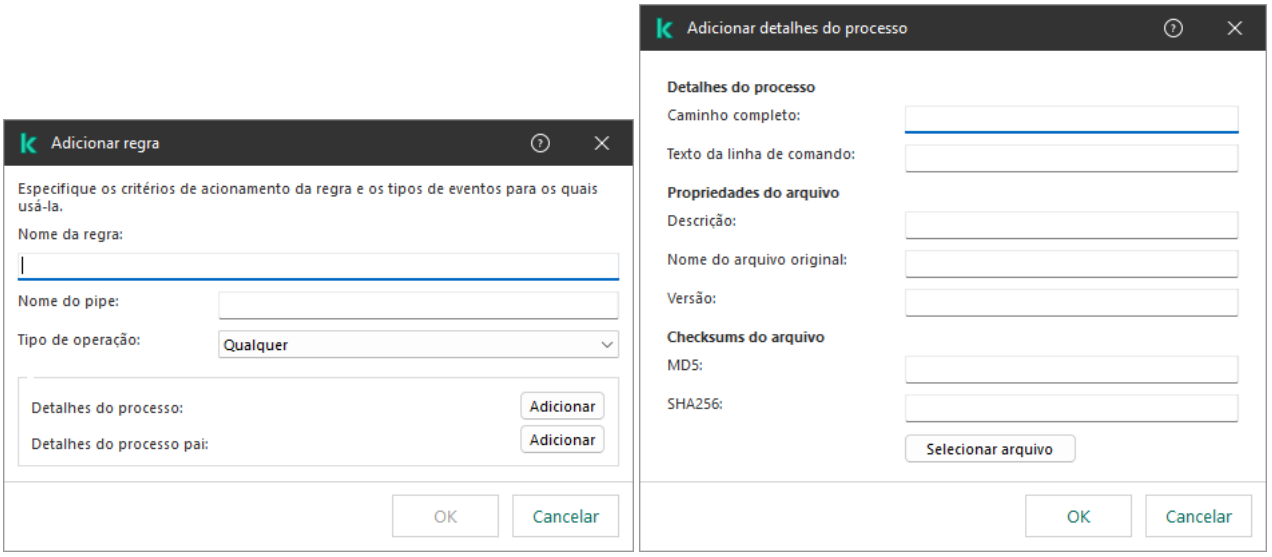
Especifique as configurações da seguinte forma:

- **Protocolo**: TCP.
- **Porta remota ou intervalo**: 443.
- **Endereço remoto**: 10.28.0.105.
- **Aplicativos**: `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`; `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`.

Exemplo 3. Operações de arquivo excluídas

Para excluir eventos envolvendo operações com arquivos confiáveis da telemetria, abra a janela Exclusões da telemetria EDR na guia **Operações de arquivo excluídas** e adicione o arquivo confiável.

O Kaspersky Endpoint Security combina critérios de acionamento de regra com um E lógico.



Excluindo operações de arquivo

Se um aplicativo registrar informações em um log e você quiser excluir eventos de modificação desse log, adicione o arquivo de log e o executável do aplicativo à telemetria.

Especifique as configurações da seguinte forma:

- **Nome ou máscara do arquivo**: `C:\Apache24\logs\error.log`.
- **Tipo de operação**: Modificação de arquivo.
- **Caminho completo**: `C:\Apache24\bin\httpd.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

Exemplo 4. Modificações de registro excluídas

Para excluir eventos de modificação do registro da telemetria, abra a janela Exclusões da telemetria EDR na guia **Alterações de registro excluídas** e adicione uma chave de registro.

O Kaspersky Endpoint Security combina critérios de acionamento de regra com um E lógico.

Se um aplicativo modificar frequentemente os valores de registro e você quiser excluir esses eventos de modificação da telemetria, adicione a chave de registro e o executável do aplicativo às exclusões da telemetria.

Especifique as configurações da seguinte forma:

- **Tipo de operação**: Modificar.
- **Caminho**: HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64.
- **Caminho completo**: `C:\Program Files\PuTTY\putty.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

KATA Sandbox

A Kaspersky Anti Targeted Attack Platform inclui o componente Sandbox (KATA Sandbox). *Sandbox* é uma tecnologia que permite detectar ameaças avançadas em um computador. O Sandbox analisa o comportamento do objeto para detectar atividades maliciosas e características de atividades de ataques direcionados à infraestrutura de TI da organização. O Sandbox analisa e verifica objetos em servidores especiais com imagens virtuais implantadas de sistemas operacionais Microsoft Windows (servidores Sandbox). Para obter informações detalhadas sobre a solução, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform.

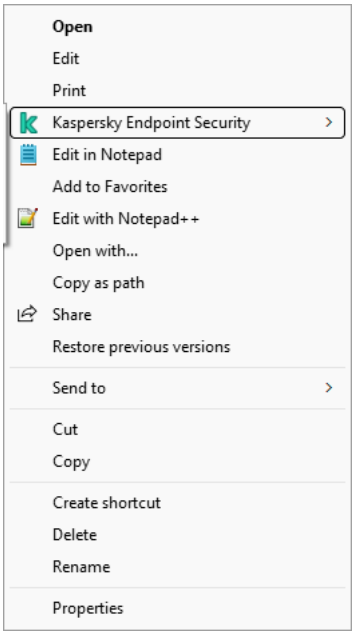
> Para ativar o KATA Sandbox, é necessário ter uma licença que inclua a funcionalidade KATA ou KEDR. Para detalhes sobre a solução, acesse a Ajuda do Kaspersky Anti Targeted Attack Platform.

O KATA Sandbox permite a verificação de arquivos nos seguintes modos:

- *Manualmente*. O usuário envia manualmente o arquivo para verificação pelo menu de contexto (**Enviar para o Sandbox**). Ao enviar um arquivo para o Sandbox, o aplicativo o verifica com o uso do bancos de dados de antivírus.
- *Automaticamente*. O aplicativo detecta os objetos automaticamente para enviá-los ao Sandbox para verificação.

Depois de enviado para o Sandbox, o arquivo permanece acessível ao usuário. O Kaspersky Endpoint Security registra o evento correspondente para enviá-lo ao Kaspersky Security Center e ao console da Kaspersky Anti Targeted Attack Platform. Caso o Sandbox detecte atividade maliciosa, o Kaspersky Endpoint Security executará automaticamente uma ação de resposta a ameaças (por exemplo, ele exclui o objeto e inicia uma Verificação de Áreas Críticas).

Para o KATA Sandbox funcionar no modo manual, a Kaspersky Anti Targeted Attack Platform 7.0 ou posterior deve ser implementada. Para o KATA Sandbox funcionar no modo automático, a Kaspersky Anti Targeted Attack Platform 8.0 ou posterior deve ser implementada.



Verificação no KATA Sandbox pelo menu de contexto

Integração do agente integrado com o KATA Sandbox

A adição do componente KATA Sandbox é necessária para a integração com o Kaspersky Sandbox. É possível selecionar o componente Sandbox durante a instalação ou atualização, assim como usando a tarefa *Alterar componentes do aplicativo*.

Para enviar arquivos para verificação, é necessário ativar a integração com o KATA Sandbox e adicionar um servidor de Central Node implementado dentro da solução. O componente só pode ser gerenciado usando o Kaspersky Security Center Web Console. Não é possível gerenciar esse componente usando o Console de Administração (MMC).

Para ativar ou desativar a integração com o KATA Sandbox:

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configuração de agentes integrados** → **Sandbox**.
5. Use o botão de alternância do **Integração com o Sandbox ATIVADA** para ativar ou desativar o componente.

6. Selecione o modo de operação do KATA Sandbox:

- **Manualmente**. O usuário envia manualmente o arquivo para verificação pelo menu de contexto (**Enviar para o Sandbox**).
- **Automaticamente**. O aplicativo detecta os objetos automaticamente para enviá-los ao Sandbox para verificação.
- **Combinado**.

7. Clique no link **Configurações de conexão**.

8. Definir as configurações de conexão do servidor Central Node:

- **Tempo limite (mseg)**. Tempo de conexão esgotado para o servidor do Central Node. Depois de decorrido o tempo limite configurado, o Kaspersky Endpoint Security envia uma solicitação ao próximo servidor. É possível aumentar o tempo de conexão esgotado para o servidor caso a velocidade da sua conexão seja baixa ou instável. O tempo limite de solicitação recomendado é de 0.5 segundo ou menos.
- **Fila de solicitações**. Tamanho da pasta da fila de solicitações. Ao enviar vários objetos para verificação no Sandbox, o Kaspersky Endpoint Security cria uma fila de solicitações. Por padrão, o tamanho da pasta da fila de solicitações é limitado a 100 MB. Depois que o tamanho máximo é atingido, o Sandbox para de adicionar novas solicitações à fila e envia o evento correspondente ao Kaspersky Security Center. É possível configurar o tamanho da pasta da fila de solicitações dependendo da configuração do seu servidor.
- **Certificado TLS do servidor**. Para configurar uma conexão confiável com o servidor do Central Node, é necessário preparar um certificado TLS. Em seguida, é necessário adicionar o certificado ao computador com o uso de uma política. Também é necessário adicionar o certificado ao servidor do Central Node.
- **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor do Central Node, obter um contêiner de criptografia e definir uma senha para proteger o contêiner criptográfico. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner criptográfico no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform). Depois de definir as configurações do Central Node, é necessário também habilitar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner criptográfico protegido por senha.

9. No bloco **Conexão com servidores do Sandbox**, clique no botão **Adicionar**.

10. Uma janela é aberta; nela, insira o endereço do servidor do nó central (IPv4, IPv6, DNS) e a porta.

    Para obter detalhes sobre como implantar imagens virtuais e configurar servidores do nó central, consulte a ajuda da Kaspersky Anti Targeted Attack Platform.

11. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como resultado, o componente Sandbox é ativado. Verifique o status operacional do componente visualizando o *Relatório de status dos componentes do aplicativo*. Também é possível visualizar o status operacional de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente do **Sandbox** será adicionado na lista de componentes do Kaspersky Endpoint Security.

Configuração das ações de resposta a ameaças

Caso o Sandbox detecte atividade maliciosa, o Kaspersky Endpoint Security executará automaticamente uma ação de resposta a ameaças (por exemplo, ele exclui o objeto e inicia uma Verificação de Áreas Críticas).

Para configurar as ações de resposta a ameaças:

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configuração de agentes integrados** → **Sandbox**.

5. Selecione a ação relevante na seção **Ação ao detectar ameaça**:

   - **Mover cópia para a Quarentena, excluir objeto**. Caso a opção seja selecionada, o Kaspersky Endpoint Security exclui o objeto malicioso encontrado no computador. Antes de excluir o objeto, o Kaspersky Endpoint Security cria uma cópia de backup, caso o objeto precise ser restaurado posteriormente. O Kaspersky Endpoint Security move a cópia de backup para a quarentena.

   - **Executar a Verificação de áreas críticas**. Caso essa opção seja selecionada, o Kaspersky Endpoint Security executa a tarefa *Verificação de áreas críticas*. Por padrão, o Kaspersky Endpoint Security verifica a memória kernel, os processos de execução e os setores de inicialização de disco.

   - **Criar tarefa de Verificação de IOC**. Caso a opção esteja selecionada, o Kaspersky Endpoint Security cria automaticamente uma tarefa de *Verificação de IOC (tarefa Verificação de IOC autônoma)*. Para esta tarefa, é possível configurar o modo de execução, o escopo da verificação e a ação na detecção de IOC (*Mover cópia para a Quarentena, excluir objeto* ou *Executar a Verificação de áreas críticas*). Para modificar outras configurações da tarefa de *Verificação de IOC*, acesse as configurações de tarefa.

6. Caso seja necessário, defina as configurações da tarefa *Verificação de IOC* no bloco **Adicionar escopo da verificação de IOC**.

   - **Áreas críticas de arquivos**. Caso a opção seja selecionada, o Kaspersky Endpoint Security fará uma verificação de IOC apenas em áreas críticas de arquivos do computador: memória kernel e setores de inicialização.

   - **Áreas de arquivo na unidade do sistema do computador**. Se essa opção estiver selecionada, o Kaspersky Endpoint Security verificará a unidade do sistema do computador em busca de IOCs.

7. Caso seja necessário, defina as configurações da tarefa *Verificação de IOC* no bloco **Executar a tarefa de Verificação de IOC**.

   - **Manualmente**. Modo de execução no qual é possível iniciar a tarefa *Verificação de IOC* manualmente, quando conveniente.

   - **Automaticamente**. Modo de execução no qual o Kaspersky Endpoint Security executa a tarefa *Verificação de IOC* automaticamente após a detecção de uma ameaça.

   - **Executar apenas quando o computador estiver ocioso**. Modo de execução no qual o Kaspersky Endpoint Security executa a tarefa de *Verificação de IOC* caso o protetor de tela esteja ativo ou se a tela estiver bloqueada. Caso o usuário desbloqueie o computador, o Kaspersky Endpoint Security pausa a tarefa. Isso significa que a tarefa pode levar vários dias para ser concluída.

8. Defina as configurações de tarefa avançada para *Verificação de IOC*.

9. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Guia de migração do KEA para KES para o EDR (KATA)

A partir da versão 12.1, o Kaspersky Endpoint Security for Windows inclui um agente integrado para gerenciar o componente Kaspersky Endpoint Detection and Response como parte da solução Kaspersky Anti Targeted Attack Platform. Não é mais necessário um aplicativo separado do Kaspersky Endpoint Agent para funcionar com o EDR (KATA). Todas as funções do Kaspersky Endpoint Agent serão executadas pelo Kaspersky Endpoint Security. A carga nos servidores da Kaspersky Anti Targeted Attack Platform permanecerá a mesma.

Quando o Kaspersky Endpoint Security é implementado em computadores com o Kaspersky Endpoint Agent instalado, a solução Kaspersky Anti Targeted Attack Platform (EDR) continua funcionando com o Kaspersky Endpoint Security. Além disso, o Kaspersky Endpoint Agent será removido do computador. O mesmo comportamento no sistema ocorrerá quando você atualizar o Kaspersky Endpoint Security para a versão 12.1 ou posterior.

O Kaspersky Endpoint Security não é compatível com o Kaspersky Endpoint Agent. Não é possível instalar os dois aplicativos no mesmo computador.

As seguintes condições devem ser atendidas para que o Kaspersky Endpoint Security funcione como parte do Endpoint Detection and Response (KATA):

- Kaspersky Anti Targeted Attack Platform versão 5.0 ou posterior.

- Kaspersky Security Center versão 14.2 ou posterior (incluindo o Agente de Rede). Em versões anteriores do Kaspersky Security Center, é impossível ativar o recurso Endpoint Detection and Response (KATA).

Etapas para migrar a configuração [KES+KEA] para [KES+agente integrado] para o EDR (KATA)

1. **Atualizar o plug-in de gerenciamento do Kaspersky Endpoint Security**

   O componente EDR (KATA) pode ser gerenciado usando o plug-in de gerenciamento do Kaspersky Endpoint Security versão 12.1 ou posterior. Dependendo do tipo de console do Kaspersky Security Center que está sendo utilizado, atualize o plug-in de gerenciamento no Console de administração (MMC) ou o plug-in da Web no Web Console.

2 **Migrar as políticas e tarefas**

Transfira as configurações do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows. As seguintes opções estão disponíveis:

- Um assistente para migrar do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security. O assistente para migrar do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security funciona apenas no Web Console.

  Como migrar as configurações de políticas e tarefas do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security no Web Console

  Na janela principal do Web Console, selecione **Operações** → **Migração a partir do Kaspersky Endpoint Agent**.

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

  Etapa 1. Migração da política

  O assistente de migração cria uma nova política que unifica as configurações das políticas do Kaspersky Endpoint Security e Kaspersky Endpoint Agent. Na lista de política, selecione as políticas do Kaspersky Endpoint Agent cujas configurações deseja unificar as políticas do Kaspersky Endpoint Security. Clique na política do Kaspersky Endpoint Agent para selecionar a política do Kaspersky Endpoint Security com o qual deseja unificar as configurações. Certifique-se de ter selecionado as políticas corretas e vá para a próxima etapa.

  Etapa 2. Migração da tarefa

  O assistente de migração não é compatível com tarefas do EDR (KATA). Ignorar esta etapa.

  Etapa 3. Conclusão do Assistente

  Conclua o assistente. Como resultado do assistente, uma nova política do Kaspersky Endpoint Security será criada. A política unifica as configurações do Kaspersky Endpoint Security e Kaspersky Endpoint Agent. A política é chamada *<nome da política Kaspersky Endpoint Security> & <nome da política Kaspersky Endpoint Agent>*. A nova política possui o status *Inativo*. Para continuar, mude os status das políticas do Kaspersky Endpoint Agent e Kaspersky Endpoint Security para *Inativo* e ative a nova política unificada.

  O assistente de migração no Web Console ignora as seguintes configurações da política e não as migra:

  - Proibição de modificação de configurações **Configurações de conexão** ("bloqueado").

    Por padrão, as configurações podem ser modificadas (o "cadeado" está aberto). Portanto, as configurações não são aplicadas no computador. É necessário proibir as modificação das configurações e fechar o "cadeado".

  - Crypto-contêiner.

    Caso a autenticação de duas vias seja usada para conexão com os servidores do Central Node, é necessário adicionar novamente o crypto-contêiner.

Como o assistente de migração não migra essas configurações, você pode encontrar erros ao conectar o computador aos servidores do Central Node. Para corrigir os erros, acesse as propriedades da política e defina as configurações de conexão.

- Um assistente padrão de conversão em lote de políticas e tarefas. O assistente de conversão em lote de políticas e tarefas está disponível apenas no Console de Administração (MMC). Para obter mais informações sobre o assistente de conversão em lote de políticas e tarefas, consulte a Ajuda do Kaspersky Security Center.

Para garantir que o Kaspersky Endpoint Security funcione corretamente nos servidores, é recomendável adicionar arquivos importantes para o funcionamento do servidor na zona confiável. Para servidores SQL, é necessário adicionar arquivos de banco de dados MDF e LDF. Para servidores Microsoft Exchange, é necessário incluir arquivos CHK, EDB, JRS, LOG e JSL. É possível usar as máscaras, por exemplo, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

A partir do Kaspersky Endpoint Security 12.6 for Windows, as exclusões de verificação e aplicativos confiáveis são adicionadas na zona confiável. As exclusões predefinidas de verificação e aplicativos confiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, Microsoft Exchange e System Center Configuration Manager. Isso significa que não será necessário configurar manualmente uma zona confiável para o aplicativo nos servidores.

As exclusões de telemetria do EDR não migram da política do Kaspersky Endpoint Agent para a política do Kaspersky Endpoint Security. O Kaspersky Endpoint Security tem suas próprias ferramentas de exclusão – aplicativos confiáveis. A operação do Kaspersky Endpoint Security é otimizada para que a ausência de exclusões de telemetria individuais do EDR não cause nenhuma carga adicional no computador em comparação com o Kaspersky Endpoint Agent. O Kaspersky Endpoint Security usa telemetria não apenas para EDR (KATA), mas também para a operação de componentes de proteção de aplicativos. Portanto, não há necessidade de transferir exclusões de telemetria EDR individuais. Se o desempenho do computador diminuir, verifique a operação do aplicativo (consulte a etapa 7 Como verificar o desempenho).

3 Licenciamento da funcionalidade do EDR (KATA)

Para ativar o Kaspersky Endpoint Security como parte da solução Kaspersky Anti Targeted Attack Platform, é necessária uma licença separada para o add-on do Kaspersky Endpoint Detection and Response (KATA). É possível adicionar a chave utilizando a tarefa *Adicionar chave*. Como resultado, duas chaves serão adicionadas ao aplicativo: *Kaspersky Endpoint Security* e *Kaspersky Endpoint Detection and Response (KATA).*

O licenciamento do add-on do Kaspersky Endpoint Detection and Response (KATA) em computadores com recursos EDR Optimum ou EDR Expert previamente ativados envolve as seguintes considerações especiais:

- Se você estiver usando um *arquivo de chave* para licenciar o Kaspersky Endpoint Security com os recursos EDR Optimum ou EDR Expert, você não pode ativar uma licença separada do add-on do Kaspersky Endpoint Detection and Response (KATA). Você pode alternar para usar um código de ativação para licenciamento ou entrar em contato com seu provedor de serviços para obter um novo arquivo de chave para ativar os recursos do Kaspersky Endpoint Security e do EDR. O provedor de serviços fornecerá um ou mais arquivos de chave para licenciamento.

- Se você estiver usando um *arquivo de chave* para licenciar o Kaspersky Endpoint Security sem os recursos EDR Optimum ou EDR Expert, você pode adicionar uma chave separada para o add-on do Kaspersky Endpoint Detection and Response (KATA) sem precisar reemitir os arquivos de chave.

- Se você estiver usando um *código de ativação* para licenciamento, o servidor de ativação da Kaspersky reemitirá automaticamente as chaves e os recursos do EDR (KATA) ficarão disponíveis automaticamente. Nesse caso, o EDR Optimum e o EDR Expert serão desabilitados.

- O Kaspersky Endpoint Security permite adicionar até duas chaves ativas: Chave do Kaspersky Endpoint Security e chave do tipo add-on. Você também pode adicionar até duas chaves de reserva. Uma chave de reserva do Kaspersky Endpoint Security e uma chave de reserva do tipo add-on.

4. **Instalação/atualização do aplicativo Kaspersky Endpoint Security**

Para migrar a funcionalidade do EDR (KATA) durante a instalação ou atualização de um aplicativo, é recomendável usar a tarefa de instalação remota. Ao criar uma tarefa de instalação remota, selecione o componente do EDR (KATA) nas configurações do pacote de instalação.

Também é possível baixar o aplicativo utilizando os seguintes métodos:

- Uso do serviço de atualização da Kaspersky.

- Localmente, usando o Assistente de configuração.

O Kaspersky Endpoint Security é compatível com a seleção automática de componentes ao atualizar o aplicativo em um computador com o aplicativo Kaspersky Endpoint Agent instalado. A seleção automática dos componentes depende das permissões da conta do usuário que está atualizando o aplicativo.

Caso esteja atualizando o Kaspersky Endpoint Security com um arquivo EXE ou MSI com a conta do sistema (SYSTEM), o Kaspersky Endpoint Security obtém acesso às licenças atualmente em uso das soluções da Kaspersky. Portanto, se o computador tiver o Kaspersky Endpoint Agent instalado e a solução EDR (KATA) ativada, o instalador do Kaspersky Endpoint Security configurará automaticamente o conjunto de componentes e selecionará o componente EDR (KATA). Isso faz com que o Kaspersky Endpoint Security alterne o uso do agente integrado e remova o Kaspersky Endpoint Agent. A execução do instalador do MSI na conta do sistema (SYSTEM) normalmente é feita com a atualização por meio do serviço de atualização da Kaspersky ou ao implementar um pacote de instalação por meio do Kaspersky Security Center.

Caso esteja atualizando o Kaspersky Endpoint Security com um arquivo MSI com uma conta de usuário não privilegiado, o Kaspersky Endpoint Security perde o acesso das licenças atualmente em uso das soluções da Kaspersky. Nesse caso, o Kaspersky Endpoint Security seleciona automaticamente os componentes com base em um conjunto de componentes do Kaspersky Endpoint Agent. Depois disso, o Kaspersky Endpoint Security passa a usar o agente integrado e remove o Kaspersky Endpoint Agent.

O Kaspersky Endpoint Security é compatível com a atualização sem reinicialização do computador. É possível selecionar o modo de atualização do aplicativo nas propriedades da política.

5. **Verificação do funcionamento do aplicativo**

Se, após a instalação ou atualização do aplicativo, o computador estiver com o status *Crítico* no console do Kaspersky Security Center:

- Certifique-se de que o computador possui o Agente de Rede versão 13.2 ou posterior instalado.

- Verifique o status operacional do agente integrado visualizando o *Relatório de status dos componentes do aplicativo*. Caso o componente tenha o status *Não instalado*, instale o componente usando a tarefa *Alterar componentes do aplicativo*. Caso um componente tenha o status *Não coberto pela licença*, certifique-se de que a funcionalidade do agente integrado esteja ativada.

- Certifique-se de aceitar a Declaração da Kaspersky Security Network na nova política do Kaspersky Endpoint Security for Windows.

6. **Como verificar a conexão com o servidor da Kaspersky Anti Targeted Attack Platform**

Verifique a conexão ao servidor da Kaspersky Anti Targeted Attack Platform. Para fazer isso:

1. Verifique se você tem um certificado válido.

2. Verifique as configurações de conexão do servidor.

3. Verifique o log de eventos.

   Se a conexão com o servidor for estabelecida, o aplicativo envia o evento *Conexão bem-sucedida com o servidor do EDR Expert*. Se não houver nenhum evento de conexão bem-sucedida e não houver eventos com erros de conexão, verifique as configurações do log de eventos e ative o envio de eventos para o Endpoint Detection and Response (KATA).

O status da conexão do servidor não afeta o status do computador no console do Kaspersky Security Center. Portanto, mesmo se não houver conexão com o servidor, o computador ainda pode ter o status *OK*. Verifique o log de eventos para verificar a conexão com o servidor.

7 Como verificar o desempenho

Se o desempenho do seu computador diminuiu após a instalação ou a atualização de um aplicativo, você pode otimizar a transferência de dados. Para fazer isso:

1. Desative o componente EDR (KATA) e verifique se a degradação do desempenho é devida ao EDR (KATA).

2. Para aplicativos confiáveis, desative a coleta de telemetria nas operações de entrada do console (ativada por padrão).

3. Adicione aplicativos que reduzem o desempenho do computador à lista de aplicativos confiáveis.

4. Entre em contato com o Suporte Técnico da Kaspersky. Os especialistas de suporte vão ajudar você a configurar a filtragem de telemetria na Kaspersky Anti Targeted Attack Platform. Isso reduzirá a quantidade de tráfego. Se o desempenho do seu computador for afetado por um determinado aplicativo, anexe o pacote de distribuição desse aplicativo à solicitação.

Endpoint Detection and Response Expert (on-premises)

O Kaspersky Endpoint Security for Windows é compatível com a integração com a solução Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* é uma solução de cibersegurança empresarial que inclui aplicativos da Kaspersky que permitem a uma organização se defender contra a maioria dos tipos de riscos cibernéticos e abranger os cenários mais importantes de propagação de ameaças. Os componentes do EDR Expert (on-premises) são implementados na Open Single Management Platform (OSMP). Esta plataforma executa cenários multiplataforma em uma única interface e permite a integração de aplicativos da Kaspersky com aplicativos de terceiros em um sistema de segurança abrangente.

Um dos elementos centrais da solução é o componente *SIEM*. O componente SIEM rastreia eventos provenientes de todos os componentes e correlaciona esses eventos entre si com o uso de regras definidas pelo fornecedor e pelo usuário. O EDR Expert (on-premises) analisa os logs e a telemetria recebidos da infraestrutura corporativa para detectar automaticamente ataques e permite investigar incidentes usando um gráfico de investigação unificado que combina todos os eventos coletados no EDR Expert (on-premises), inclusive eventos de aplicativos da Kaspersky e de produtos de segurança da informação de terceiros.

Para responder a incidentes avançados, o EDR Expert (on-premises) usa cenários predefinidos e definidos pelo usuário. Também é possível usar ações de resposta de aplicativos de terceiros e cenários de resposta que envolvem vários aplicativos.

Ferramentas de inteligência contra ameaças

O Kaspersky Endpoint Detection and Response usa as seguintes ferramentas Threat Intelligence:

- Integração com o Kaspersky Threat Intelligence Portal que contém e exibe as informações sobre a reputação de arquivos e endereços da Web.
- Banco de dados de Ameaças da Kaspersky.
- A infraestrutura de serviço na nuvem da Kaspersky Security Network (doravante também chamada de "KSN"), que fornece acesso a arquivos em tempo real, ao site e às informações sobre a reputação de software da base de conhecimento da Kaspersky. A utilização de dados do Kaspersky Security Network garante respostas mais rápidas dos aplicativos da Kaspersky contra as ameaças, melhora o desempenho de alguns componentes de proteção e reduz a possibilidade de falsos positivos.

Princípio de funcionamento da solução

O Kaspersky Endpoint Security é instalado em computadores individuais na infraestrutura corporativa de TI e monitora continuamente os processos, as conexões de rede abertas e os arquivos em modificação.

> Quando instalado no modo padrão na infraestrutura VDI, o Kaspersky Endpoint Security é compatível com a integração com o EDR Expert (on-premises). No entanto, a operabilidade das outras funcionalidades do aplicativo não é garantida. Para proteger máquinas virtuais na infraestrutura VDI, recomendamos usar o Kaspersky Endpoint Security no Modo Light Agent.

As informações sobre eventos no computador (telemetria) são enviadas para o servidor do EDR Expert (on-premises). Nesse caso, o Kaspersky Endpoint Security também envia informações sobre ameaças descobertas pelo aplicativo, além das informações sobre o processamento dos resultados dessas ameaças para os servidores de coleta de telemetria.

A integração do EDR Expert (on-premises) é configurada no console do Kaspersky Security Center. Então, o agente integrado é gerenciado com o uso da Open Single Management Platform (OSMP), inclusive a execução de tarefas, gerenciamento de objetos na Quarentena, exibição de relatórios e outras ações.

Configurações do Kaspersky Endpoint Security para trabalhar com o EDR Expert (on-premises)

As seguintes configurações podem ser usadas para trabalhar com o EDR Expert (on-premises):

- **[KES+agente integrado]**. Nesta configuração, o Kaspersky Endpoint Security atua tanto como o aplicativo que garante a segurança do computador quanto como o aplicativo para trabalhar com o EDR Expert (on-premises). O agente integrado para o EDR Expert (on-premises) está disponível no Kaspersky Endpoint Security 12.11 for Windows ou posterior.

- **[EPP de terceiros+EDR Agent]**. Nesta configuração, a segurança da infraestrutura de TI é fornecida pelo Endpoint Protection Platform (EPP) de terceiros. A interação com o EDR Expert (on-premises) é fornecida pelo Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent (Agente EDR). Nesta configuração, o EDR Agent é compatível com aplicativos EPP de terceiros. O EDR Agent para EDR Expert (on-premises) está disponível no Kaspersky Endpoint Security 12.11 for Windows ou posterior.

Integração do agente integrado com o EDR Expert (on-premises)

Para integrar-se à solução Kaspersky Endpoint Detection and Response Expert (on-premises), é necessário adicionar o componente Endpoint Detection and Response Expert (on-premises) e configurar o Kaspersky Endpoint Security.

> Os componentes Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) e Endpoint Detection and Response Expert (on-premises) não são compatíveis entre si.

As seguintes condições devem ser atendidas para que o Endpoint Detection and Response Expert (on-premises) funcione:

- A OSMP (Open Single Management Platform) deve estar instalada.

- O aplicativo é ativado e a funcionalidade é contemplada pela licença.

- O componente Endpoint Detection and Response Expert (on-premises) está ativado.

- Os componentes do aplicativo que garantem a operação do EDR Expert (on-premises) estão ativados e operacionais. Os seguintes componentes garantem a operação do EDR Expert (on-premises):

  - Proteção Contra Ameaças ao Arquivo.

  - Proteção Contra Ameaças da Web.

  - Proteção Contra Ameaças ao Correio.

  - Prevenção de Exploit.

  - Detecção de Comportamento.

  - Prevenção de Intrusão do Host.

- Mecanismo de Remediação.
- Controle Adaptativo de Anomalias.

A configuração da integração do EDR Expert (on-premises) envolve as seguintes etapas:

1. **Instalação do componente EDR Expert (on-premises)**

   É possível selecionar o componente EDR Expert (on-premises) durante a instalação ou atualização, assim como usando a tarefa *Alterar componentes do aplicativo*.

   É necessário reiniciar o computador para concluir a atualização do aplicativo com o novo componente.

2. **Ativar o Kaspersky Endpoint Detection and Response Expert (on-premises)**

   É preciso comprar uma licença separada para o EDR Expert (on-premises) (add-on do Kaspersky Endpoint Detection and Response Expert (on-premises)).

   A funcionalidade estará disponível após a adição de uma chave separada para o Kaspersky Endpoint Detection and Response Expert (on-premises). Assim, duas chaves são adicionadas ao computador: uma chave para o Kaspersky Endpoint Security e uma chave para o Kaspersky Endpoint Detection and Response Expert (on-premises).

   O licenciamento da funcionalidade independente Endpoint Detection and Response Expert (on-premises) é o mesmo que o licenciamento do Kaspersky Endpoint Security.

   Verifique se a funcionalidade EDR Expert (on-premises) está incluída na licença e em execução na interface local do aplicativo.

3. **Conexão com servidor de coleta de telemetria e servidor de reposta**

   O Kaspersky Endpoint Detection and Response Expert (on-premises) requer uma conexão confiável entre o Kaspersky Endpoint Security e dois servidores:

   - Um *servidor de coleta de telemetria* é um servidor que faz parte de uma solução SIEM que coleta, normaliza, correlaciona, analisa e armazena informações sobre eventos que ocorrem no computador.
   - Um *servidor de resposta* é um dispositivo que recebe e verifica dados, estuda o comportamento de objetos e publica os resultados desses estudos.

   Para configurar uma conexão confiável, é necessário usar um certificado TLS. É possível obter um certificado TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). Em seguida, é necessário adicionar o certificado TLS ao Kaspersky Endpoint Security (consulte as instruções abaixo).

   Por padrão, o Kaspersky Endpoint Security verifica apenas o certificado TLS dos servidores. Para tornar a conexão mais segura, também é possível ativar a verificação do computador no servidor (autenticação bidirecional). Para ativar essa verificação, é necessário ativar a autenticação bidirecional nas configurações do servidor e do Kaspersky Endpoint Security. Para usar a autenticação bidirecional, também será necessário um contêiner criptográfico. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner de criptografia na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)).

   Como conectar um computador com o Kaspersky Endpoint Security ao EDR Expert (on-premises) usando o Web Console

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

      A janela de propriedades da política é exibida.

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

4. Selecione **Configuração de agentes integrados** → **Endpoint Detection and Response Expert (on-premises)**.

5. Ative o botão de alternância **Endpoint Detection and Response Expert (on-premises) ATIVADO**.

6. Para configurar o EDR Expert (on-premises), selecione **Endpoint Detection and Response Expert (versão 8.0 ou posterior)** na lista de soluções.

7. Configure a conexão dos *servidores de coleta de telemetria*:

   a. No bloco **Conexão com servidores de coleta de telemetria**, clique no link **Configurações de conexão**.

   b. Configure a conexão dos servidores de coleta de telemetria:

      - **Tempo limite (s)**. Tempo limite máximo de resposta do servidor. Quando o tempo limite se esgotar, o Kaspersky Endpoint Security tentará estabelecer conexão com um servidor diferente.

      - **Certificado do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor. É possível obter um certificado TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)).

      - **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor, obter um contêiner de criptografia e definir uma senha para protegê-lo. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner de criptografia na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). Depois de definir as configurações do servidor, é necessário também ativar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner de criptografia protegido por senha.

        O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.

   c. Clique **OK**.

   d. Adicione servidores de coleta de telemetria. Para fazer isso, especifique o endereço do servidor (IPv4, IPv6) e a porta para se conectar ao servidor.

      É possível adicionar vários endereços de servidores de coleta de telemetria. O Kaspersky Endpoint Security tenta se conectar ao servidor usando o primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar usando o segundo endereço IP na lista e assim sucessivamente.

   e. Caso necessário, configure a telemetria.

8. Configure a conexão dos *servidores de reposta*:

   a. No bloco **Conexão com servidores de resposta**, defina as configurações de **Enviar solicitação de sincronização para o servidor a cada (min.)**. Frequência de solicitações de sincronização enviadas ao servidor. Durante a sincronização, o Kaspersky Endpoint Security receberá tarefas de resposta a ameaças e enviará os resultados da tarefa.

   b. Clique no link **Configurações de conexão**.

   c. Configure a conexão dos servidores de reposta:

      - **Tempo limite (s)**. Tempo limite máximo de resposta do servidor. Quando o tempo limite se esgotar, o Kaspersky Endpoint Security tentará estabelecer conexão com um servidor diferente.

      - **Certificado do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor. É possível obter um certificado TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)).

      - **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor, obter um contêiner de criptografia e definir uma senha para protegê-lo. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner de criptografia na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). Depois de definir as configurações do servidor, é necessário também ativar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner de criptografia protegido por senha.

        O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.

   d. Clique **OK**.

   e. Adicione os servidores de reposta. Para fazer isso, especifique o endereço do servidor (IPv4, IPv6) e a porta para se conectar ao servidor.

      É possível adicionar vários endereços do servidor de resposta. O Kaspersky Endpoint Security tenta se conectar ao servidor usando o primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar usando o segundo endereço IP na lista e assim sucessivamente.

9. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

É possível verificar o status do componente usando o *Relatório de status dos componentes do aplicativo*. Também é possível visualizar o status operacional de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente do **Endpoint Detection and Response Expert (on-premises)** será adicionado na lista de componentes do Kaspersky Endpoint Security.

Definição das configurações de telemetria do EDR Expert (on-premises)

Telemetria é uma lista de eventos que ocorreram no computador protegido. O Kaspersky Endpoint Security analisa os dados de telemetria para enviá-los para a Kaspersky Anti Targeted Attack Platform durante a sincronização. Para obter mais informações sobre os eventos de telemetria transmitidos, consulte a Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises).

Os eventos de telemetria chegam ao servidor quase continuamente. O Kaspersky Endpoint Security inicia a sincronização com o servidor quando qualquer uma das seguintes condições for satisfeita:

- O intervalo de sincronização terminou.
- O número de eventos no buffer excede o limite superior.

Portanto, por padrão, o aplicativo sincroniza a cada 30 segundos ou sempre que o buffer contiver 1024 eventos. É possível configurar o comportamento de sincronização na política do Kaspersky Endpoint Security e selecionar os valores ideais para que correspondam com sua carga de rede (consulte as instruções abaixo).

Se não houver conexão entre o Kaspersky Endpoint Security e o servidor, o aplicativo enfileira novos eventos. Quando a conexão é restaurada, o Kaspersky Endpoint Security envia eventos em fila para o servidor na ordem correta. Para evitar sobrecarregar o servidor, o Kaspersky Endpoint Security pode ignorar alguns eventos. Para ativar essa opção, é possível otimizar as configurações de transmissão de eventos, por exemplo, para definir um valor máximo de eventos por hora (consulte as instruções abaixo).

Para definir as configurações de telemetria, execute as seguintes etapas:

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configuração de agentes integrados** → **Endpoint Detection and Response Expert (on-premises)**.
5. Para configurar o EDR Expert (on-premises), selecione **Endpoint Detection and Response Expert (versão 8.0 ou posterior)** na lista de soluções.
6. Verifique e confirme se a caixa de seleção **Enviar telemetria aos servidores de coleta de telemetria** está marcada no bloco **Configurações de transmissão de dados**.
7. Caso seja necessário, marque a caixa de seleção **Enviar apenas telemetria com IOA**. *Indicadores de ataque (IOA)* é uma regra que contém uma descrição de comportamentos suspeitos no sistema que podem indicar um ataque direcionado. O aplicativo compara o comportamento contínuo no sistema com essas regras e registra os eventos que indicam um ataque direcionado. O aplicativo usa a tecnologia *de verificação de streaming*, que permite fazer o rastreamento de eventos em tempo real.

8. Caso necessário, configure a sincronização com as configurações do servidor no bloco **Configurações de transmissão de dados**:

   - **Atraso máximo na transmissão de eventos (segundos)**. O aplicativo sincroniza com o servidor para enviar eventos após expirar o intervalo de sincronização. A configuração padrão é 30 segundos.

   - **Número máximo de pacotes de eventos**. O aplicativo sincroniza com o servidor quando o buffer está cheio de eventos. A configuração padrão é 1024 eventos.

9. Se necessário, desmarque a caixa de seleção **Ativar a limitação de solicitações** no bloco **Limitação de solicitações**.

   Esse recurso ajuda a otimizar a carga no computador. Se essa funcionalidade estiver ativada, o aplicativo restringirá a transmissão de eventos. Caso o número de eventos exceda os limites configurados, o Kaspersky Endpoint Security interromperá o envio de eventos. Esta opção está ativada por padrão.

10. Defina as configurações de otimização para enviar eventos ao servidor:

    - **Número máximo de eventos por hora**. O aplicativo analisa o fluxo de dados de telemetria e restringe o envio de eventos caso ele exceda o limite de eventos configurado por hora. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. A configuração padrão é de 3 mil eventos por hora. Caso o aplicativo esteja instalado em um servidor, o fluxo de dados de telemetria será maior. Para servidores, é recomendável aumentar o valor para 60 mil eventos por hora.

    - **Porcentagem de excesso de limite de evento**. O aplicativo ordena os eventos por tipo (por exemplo, eventos "alterações no registro") e restringe a transmissão de eventos caso a proporção de eventos do mesmo tipo para o número total de eventos exceda o limite configurado em porcentagem. O Kaspersky Endpoint Security retoma o envio de eventos quando a proporção de outros eventos para o número total de eventos torna-se volumosa o suficiente novamente. A configuração padrão é 15%.

11. No bloco **Conexão com servidores de resposta**, insira um valor para o parâmetro **Enviar solicitação de sincronização para o servidor a cada (min.)**.

12. Frequência de solicitações de sincronização enviadas ao servidor. Durante a sincronização, o Kaspersky Endpoint Security envia informações sobre as configurações e tarefas modificadas do aplicativo.

13. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Exclusões de telemetria do EDR Expert (on-premises)

Para melhorar o desempenho e otimizar a transmissão de dados para o servidor de coleta de telemetria, é possível adicionar exclusões de telemetria. Por exemplo, é possível optar pelo não envio de dados de comunicações de rede para aplicativos individuais.

> Usar muitas regras pode aumentar a carga no servidor de coleta de telemetria e reduzir o desempenho do computador. Recomendamos adicionar apenas as regras necessárias.

Para criar uma exclusão de telemetria no Web Console e no Cloud Console:

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Configurações de telemetria**.

5. Selecione a guia **Telemetria do EDR Expert (on-premises)**.

6. No bloco **Exclusões gerais**, clique no botão **Adicionar**.
   A janela **Adicionar regra de exclusão** é aberta.

7. Caso necessário, altere o conteúdo da regra. Por padrão, a regra está ativa.

8. Insira um nome para a regra.

9. Selecione a ação a ser executada quando a regra for acionada:

   - **Não coletar**. O evento filtrado será excluído da telemetria enviada.

   - **Excluir IOA**. O evento de acionamento da regra IOA será excluído da telemetria enviada.

10. Caso a opção **Excluir IOA** esteja selecionada, especifique as regras de IOA a serem adicionadas às exclusões:

    - **Excluir tudo**. Quando a condição especificada for atendida, o aplicativo excluirá os eventos gerados de acordo com todas as regras IOA da telemetria.

    - **Excluir por GUID**. Especifique o GUID da regra IOA. É possível especificar vários GUIDs usando `,`. Para obter mais detalhes sobre as regras IOA, consulte a Ajuda do EDR Expert (on-premises).

11. Especifique a condição de filtragem:

    a. Selecione o nome do campo a ser usado para filtragem.

    b. Selecione um operador (consulte a tabela abaixo) e especifique o valor com o qual comparar o valor do campo do evento.

Lista de operadores condicionais

Operador	Descrição
<	Caso o valor do campo seja menor que o valor especificado na condição, o evento será filtrado.
≤	Caso o valor do campo seja menor que ou igual ao valor especificado na condição, o evento será filtrado.
=	Caso o valor do campo seja igual ao valor especificado na condição, o evento será filtrado.
≥	Caso o valor do campo seja maior que ou igual ao valor especificado na condição, o evento será filtrado.
>	Caso o valor do campo seja maior que o valor especificado na condição, o evento será filtrado.
≠	Caso o valor do campo não seja igual ao valor especificado na condição, o evento será filtrado.
é como	Caso o valor do campo corresponda à máscara especificada na condição, o evento será filtrado. O aplicativo é compatível com os caracteres `*` e `?` ao inserir uma máscara:
não é como	Caso o valor do campo não corresponda à máscara especificada na condição, o evento será filtrado. O aplicativo é compatível com os caracteres `*` e `?` ao inserir uma máscara:
um de	Caso o valor do campo corresponda a um dos valores na lista especificada na condição, o evento será considerado filtrado.
nenhum de	Caso o valor do campo não corresponda a nenhum dos valores na lista especificada na condição, o evento será considerado filtrado.
é como um de	Caso o valor do campo corresponda a uma das máscaras especificadas na condição, o evento será filtrado. O aplicativo é compatível com os caracteres * e ? ao inserir uma máscara.

Operador	Descrição
não é como nenhum de	Caso o valor do campo não corresponda a nenhuma das máscaras especificadas na condição, o evento será filtrado. O aplicativo é compatível com os caracteres * e ? ao inserir uma máscara.
sair	Caso o campo especificado na condição esteja presente no evento, o evento será filtrado.
não sair	Caso o campo especificado na condição não esteja presente no evento, o evento será filtrado.
contém	Caso o valor especificado na condição esteja presente no valor do campo, o evento será filtrado.
é igual a	Caso o valor do campo seja igual ao valor especificado na condição, o evento será filtrado. A verificação não diferencia maiúsculas de minúsculas.
bitwise E	Caso o resultado da operação bitwise E (&) entre o valor do campo e o valor especificado na condição for 1, o evento será filtrado.

12. Caso necessário, é possível criar critérios de filtragem complexos adicionando várias condições de filtro e grupos de condições. Também é possível adicionar condições aninhadas e grupos de condições a um grupo de condições. É possível usar as seguintes configurações:

    - **AND** significa que o filtro seleciona eventos que atendem a todas as condições especificadas.
    - **OR** significa que o filtro seleciona eventos que atendem a uma das condições especificadas.
    - **NOT** (para usar este operador, selecione a opção **Adicionar NOT antes**) significa que o filtro seleciona eventos que não atendem a nenhuma das condições especificadas.

    As condições e os grupos de condições de primeiro nível são combinados com o operador **AND**.

13. Caso o computador esteja executando a Open Single Management Platform (OSMP), será possível verificar a regra de filtragem criada. Para executar a verificação, clique no botão **Verificar regra**.

    Na janela aberta, será exibida uma tabela de eventos filtrados pela regra criada. Para obter mais detalhes, consulte a Ajuda do EDR Expert (on-premises).

14. Caso seja necessário, em **Todos os tipos de eventos**, adicione exclusões de telemetria por tipo de evento.

    a. Clique no nome do tipo de evento.

    b. Na janela que é aberta, clique no botão **Configurar manualmente**.

    c. Caso necessário, configure a transmissão de telemetria para o tipo de evento selecionado usando o botão de alternância **Enviar evento**. Por padrão, a transmissão de telemetria é ativada para todos os tipos de eventos.

    d. No bloco **Regras de exclusões**, clique no botão **Adicionar**.

    A janela **Adicionar regra de exclusão** é aberta.

    e. Execute as ações descritas nas etapas 7 a 13 para cada regra adicionada.

15. Para alguns tipos de evento, também é possível adicionar regras de inclusão para expandir a telemetria coletada:

    a. No bloco **Regras de inclusão**, clique no botão **Adicionar**.

    A janela **Adicionar regra de inclusão** é aberta.

b. Insira um nome para a regra.

c. Abaixo de **Condição**, insira valores para os campos exibidos. O tipo de campos disponíveis depende do evento selecionado.

As regras de exclusão têm prioridade sobre as regras de inclusão.

16. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Exportar e importar filtros de eventos do EDR Expert (on-premises)

Você pode exportar a lista de exclusões para um arquivo JSON. Em seguida, será possível modificar o arquivo para, por exemplo, adicionar um grande número de IDs de eventos. Também é possível usar a função de exportação/importação para fazer backup dos filtros de eventos ou para migrar a lista para um servidor diferente.

Usar muitas regras pode aumentar a carga no servidor de coleta de telemetria e reduzir o desempenho do computador. Recomendamos adicionar apenas as regras necessárias.

Como exportar e importar os filtros de eventos no Console de Administração (MMC)

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

2. Na árvore do console, selecione **Políticas**.

3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

4. Na janela da política, selecione **Configurações gerais** → **Exclusões e tipos de objetos**.

5. No bloco **Configurações de telemetria** → **Telemetria do EDR Expert (on-premises)**, clique no botão **Configurações**.

6. Para exportar os filtros de evento:

   a. Clique **Exportar**.

   Na janela exibida, especifique o nome do arquivo JSON para o qual deseja exportar os filtros de eventos e selecione a pasta na qual deseja salvar o arquivo.

   b. Salvar o arquivo.

   O Kaspersky Endpoint Security exporta todos os filtros de eventos para o arquivo JSON.

7. Para importar os filtro de evento:

   a. Clique **Importar**.

   b. Na janela que é aberta, selecione o arquivo JSON do qual deseja importar os filtro de eventos.

c. Abra o arquivo.

Caso já existam regras de filtragem de eventos no computador, o Kaspersky Endpoint Security substituirá essas regras durante a importação.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como exportar e importar filtros de eventos no Web Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Configurações de telemetria**.

5. Selecione a guia **Telemetria do EDR Expert (on-premises)**.

6. Para exportar os filtros de evento:

a. Clique **Exportar**.

b. Na janela exibida, especifique o nome do arquivo JSON para o qual deseja exportar os filtros de eventos e selecione a pasta na qual deseja salvar o arquivo.

c. Salvar o arquivo.

O Kaspersky Endpoint Security exporta todos os filtros de eventos para o arquivo JSON.

7. Para importar os filtro de evento:

a. Clique **Importar**.

b. Na janela que é aberta, selecione o arquivo JSON do qual deseja importar os filtro de eventos.

c. Selecione como deseja que as regras de filtragem de eventos sejam importadas: adicionando às regras existentes ou descartando as regras existentes e substituindo por novas.

d. Abra o arquivo.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Também é possível exportar ou importar filtros de eventos na linha de comando.

Considerações especiais ao usar perfis da política para configurar a integração com o EDR Expert (on-premises) e EDR (KATA)

Para configurar, como parte de uma única política, a integração com EDR (KATA) para determinados grupos de administração e com EDR Expert (on-premises) para outros, será necessário usar perfis da política. Você deve definir as configurações de integração com o EDR (KATA) nas propriedades da política, e a integração com o EDR Expert (on-premises) para os grupos de administração selecionados deve ser configurada nas propriedades do perfil da política.

O uso de perfis da política para configurar a integração com o EDR Expert (on-premises) tem as seguintes limitações:

- Se você configurar a integração com o EDR Expert (on-premises) nas propriedades da política, essas configurações serão aplicadas a todos os grupos de administração; as configurações de integração dos perfis da política não serão aplicadas.

- Ao usar perfis da política para configurar a integração com o EDR Expert (on-premises), não será possível usar o Console de Administração (MMC) para gerenciar políticas. Quando você abre as propriedades da política no Console de Administração, as configurações de integração com o EDR Expert (on-premises) nos perfis da política são substituídas pelas configurações da política, fazendo com que o componente funcione incorretamente. Será necessário redefinir as configurações do componente Endpoint Detection and Response Expert (on-premises) de acordo com a instrução abaixo.

- Ao usar perfis da política para configurar a integração com o EDR Expert (on-premises), não será possível usar políticas secundárias.

Se você já tiver uma política configurada em uma versão anterior do plug-in da web, deverá redefinir as configurações do componente Endpoint Detection and Response Expert (on-premises) para aplicar as configurações de integração com o EDR Expert (on-premises) aos dispositivos gerenciados a partir dos perfis da política.

Para redefinir as configurações do componente:

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configuração de agentes integrados** → **Endpoint Detection and Response Expert (on-premises)**.

5. Altere o modo de operação de **Endpoint Detection and Response Expert (versão 7.1 ou anterior)** para **Modo Endpoint Detection and Response Expert (versão 8.0 ou posterior)**.

6. Volte para **Endpoint Detection and Response Expert (versão 7.1 ou anterior)**.

7. Salvar alterações.

Endpoint Detection and Response Expert (cloud)

A integração do Kaspersky Endpoint Security com o Kaspersky Endpoint Detection and Response Expert (cloud) está temporariamente indisponível. O suporte para essa funcionalidade está planejado para ser encerrado no final de 2026. Acompanhe nossas notas de lançamento para ficar por dentro das atualizações do aplicativo e dos novos recursos.

O Kaspersky Endpoint Security é compatível com a integração com a solução Kaspersky Endpoint Detection and Response Expert (cloud). *Kaspersky Endpoint Detection and Response Expert (cloud)* é uma solução de segurança virtual empresarial que inclui aplicativos da Kaspersky que viabilizam para uma organização a defesa contra a maioria dos tipos de riscos virtuais, além de englobar os cenários mais importantes de propagação de ameaças. Os componentes do EDR Expert (cloud) são implantados na Open Single Management Platform (OSMP). Esta plataforma executa cenários multiplataforma em uma única interface e permite a integração de aplicativos da Kaspersky com aplicativos de terceiros em um sistema de segurança abrangente.

Um dos elementos centrais da solução é o componente *SIEM*. O componente SIEM rastreia eventos provenientes de todos os componentes e correlaciona esses eventos entre si com o uso de regras definidas pelo fornecedor e pelo usuário. O EDR Expert (cloud) analisa os logs e a telemetria recebidos da infraestrutura corporativa para detectar automaticamente os ataques e permitir a investigação de incidentes com o uso de um gráfico de investigação unificado que combina todos os eventos coletados no EDR Expert (cloud), inclusive os eventos de aplicativos da Kaspersky e de produtos de segurança da informação de terceiros.

Para responder a incidentes avançados, o EDR Expert (cloud) usa cenários predefinidos e definidos pelo usuário. Também é possível usar ações de resposta de aplicativos de terceiros e cenários de resposta que envolvem vários aplicativos.

Ferramentas de inteligência contra ameaças

O Kaspersky Endpoint Detection and Response usa as seguintes ferramentas Threat Intelligence:

- Integração com o Kaspersky Threat Intelligence Portal que contém e exibe as informações sobre a reputação de arquivos e endereços da Web.
- Banco de dados de Ameaças da Kaspersky.
- A infraestrutura de serviço na nuvem da Kaspersky Security Network (doravante também chamada de "KSN"), que fornece acesso a arquivos em tempo real, ao site e às informações sobre a reputação de software da base de conhecimento da Kaspersky. A utilização de dados do Kaspersky Security Network garante respostas mais rápidas dos aplicativos da Kaspersky contra as ameaças, melhora o desempenho de alguns componentes de proteção e reduz a possibilidade de falsos positivos.

Princípio de funcionamento da solução

O Kaspersky Endpoint Security é instalado em computadores individuais na infraestrutura corporativa de TI e monitora continuamente os processos, as conexões de rede abertas e os arquivos em modificação.

As informações sobre eventos no computador são enviadas para o servidor do EDR Expert (cloud). Nesse caso, o Kaspersky Endpoint Security também envia informações sobre ameaças descobertas pelo aplicativo, além das informações sobre o processamento dos resultados dessas ameaças para os servidores de coleta de telemetria.

A integração do EDR Expert (cloud) é configurada no console do Kaspersky Security Center. Então, o agente integrado é gerenciado com o uso da Open Single Management Platform (OSMP), inclusive a execução de tarefas, gerenciamento de objetos na Quarentena, exibição de relatórios e outras ações.

Integração do agente integrado com o EDR Expert (cloud)

Para configurar a integração com a solução Kaspersky Endpoint Detection and Response (nuvem), é necessário instalar o componente Endpoint Detection and Response Expert (cloud) e configurar o Kaspersky Endpoint Security.

> Os componentes Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) e Endpoint Detection and Response Expert (on-premises) não são compatíveis entre si.

Condições de operação do EDR Expert (cloud)

Para que o EDR Expert (cloud) funcione, as seguintes condições devem ser atendidas:

- A infraestrutura do Kaspersky Endpoint Detection and Response Expert (cloud) está disponível em sua região. Para obter informações sobre a disponibilidade da infraestrutura EDR Expert (cloud) em sua região, entre em contato com o Suporte Técnico.
- A OSMP (Open Single Management Platform) deve estar instalada.
- Kaspersky Endpoint Security instalado em modo padrão.
- O aplicativo Kaspersky Endpoint Security é ativado e a funcionalidade é contemplada pela licença.
- Você aceitou os termos do Contrato de Processamento de Dados do Kaspersky Endpoint Detection and Response Expert (cloud).
- O componente Endpoint Detection and Response Expert (cloud) está ativado.
- Os componentes do aplicativo que garantem a operação do EDR Expert (cloud) estão ativados e operacionais:
  - Proteção Contra Ameaças ao Arquivo.
  - Proteção Contra Ameaças da Web.
  - Proteção Contra Ameaças ao Correio.
  - Prevenção de Exploit.
  - Detecção de Comportamento.
  - Prevenção de Intrusão do Host.

- Mecanismo de Remediação.
- Controle Adaptativo de Anomalias.

Etapas para integração com o EDR Expert (cloud)

A configuração da integração EDR Expert (cloud) envolve as seguintes etapas:

1. **Instalação do componente Endpoint Detection and Response Expert (cloud)**

   É possível selecionar o componente Endpoint Detection and Response Expert (cloud) durante a instalação ou atualização, assim como usando a tarefa *Alterar componentes do aplicativo*.

   > É necessário reiniciar o computador para concluir a atualização do aplicativo com o novo componente.

2. **Ativar o Kaspersky Endpoint Detection and Response Expert (cloud)**

   É preciso comprar uma licença separada para o Kaspersky Endpoint Detection and Response Expert (cloud).

   A funcionalidade estará disponível após a adição de uma chave separada para o Kaspersky Endpoint Detection and Response Expert (cloud). Assim, duas chaves serão instaladas no computador: uma chave para o Endpoint Security e uma para o Kaspersky Endpoint Detection and Response Expert (cloud).

   A licença para a funcionalidade independente Endpoint Detection and Response Expert (cloud) é a mesma que a licença do Kaspersky Endpoint Security.

   Verifique e confirme se a funcionalidade EDR Expert (cloud) está incluída na licença e se está sendo executada na interface local do aplicativo.

3. **Conexão com servidor de coleta de telemetria e servidor de reposta**

   O Kaspersky Endpoint Detection and Response Expert (cloud) requer uma conexão confiável entre o Kaspersky Endpoint Security e dois servidores:

   - Um *servidor de coleta de telemetria* é um servidor que faz parte de uma solução SIEM que coleta, normaliza, correlaciona, analisa e armazena informações sobre eventos que ocorrem no computador.
   - Um *servidor de resposta* é um dispositivo que recebe e verifica dados, estuda o comportamento de objetos e publica os resultados desses estudos.

   Como conectar um computador Kaspersky Endpoint Security com a EDR Expert (cloud) com o uso do Web Console

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

      A janela de propriedades da política é exibida.
   3. Selecione a guia **Configurações do aplicativo**.
   4. Selecione **Configuração de agentes integrados** → **Endpoint Detection and Response Expert (cloud)**.
   5. Ative o componente usando o botão de alternância **Endpoint Detection and Response Expert (cloud) DESATIVADO**.

6. Caso a política atual seja uma política secundária e a política principal proíba alterações nas configurações de integração do EDR Expert (cloud) ("cadeado" fechado), será possível definir a herança de configurações na seção **Herança**:

   - **Herdar configurações de conexão da política** (valor padrão) As configurações de conexão serão herdadas da política pai. Não será possível editar as configurações.

   - **Usar configurações de conexão personalizadas**. É possível configurar as configurações de conexão manualmente.

7. A guia **Servidor de reposta** exibe o nome de domínio totalmente qualificado e a porta do servidor de resposta, que são recuperados automaticamente. Caso a política de segurança em sua infraestrutura não permita a conexão direta aos servidores EDR Expert (cloud), será possível configurar uma conexão por meio de um túnel TCP:

   a. Marque a caixa de seleção **Usar um túnel TCP para resposta**.

   b. Especifique o endereço do servidor (IPv4, IPv6) e a porta para se conectar ao túnel.

8. Caso necessário, defina a frequência de envio de solicitações de sincronização ao servidor no campo **Enviar solicitação de sincronização para o servidor a cada (min.)**. Durante a sincronização, o Kaspersky Endpoint Security receberá tarefas de resposta a ameaças e enviará os resultados da tarefa.

9. Vá para a guia **Servidor de coleta de telemetria**.

10. Defina as configurações de conexão do servidor de coleta de telemetria:

    a. Clique no link **Editar**.

    b. Na janela exibida, selecione o servidor de coleta de telemetria na lista. O coletor KUMA serve como o servidor de coleta de telemetria no EDR Expert (cloud). Para mais detalhes sobre o gerenciamento de coletores, consulte a Ajuda da Kaspersky Unified Monitoring and Analysis Platform.

    Caso ocorra um erro durante a conexão com o servidor de coleta de telemetria, selecione um servidor diferente. Caso não consiga se conectar com o servidor de coleta de telemetria, basta entrar em contato com o Suporte Técnico.

    c. Se necessário, você pode configurar uma conexão com o servidor de coleta de telemetria por meio de um túnel TCP, assim como faria para o servidor de resposta.

11. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

É possível verificar o status do componente usando o *Relatório de status dos componentes do aplicativo*. Também é possível visualizar o status operacional de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente do **Endpoint Detection and Response Expert (cloud)** será adicionado na lista de componentes do Kaspersky Endpoint Security.

Definição das configurações de telemetria do EDR Expert (cloud)

Telemetria é uma lista de eventos que ocorreram no computador protegido. O Kaspersky Endpoint Security analisa os dados de telemetria para enviá-los para a Kaspersky Anti Targeted Attack Platform durante a sincronização. Os eventos de telemetria chegam ao servidor quase continuamente. O Kaspersky Endpoint Security inicia a sincronização com o servidor quando qualquer uma das seguintes condições for satisfeita:

- O intervalo de sincronização terminou.
- O número de eventos no buffer excede o limite superior.

Portanto, por padrão, o aplicativo sincroniza a cada 30 segundos ou sempre que o buffer contiver 1024 eventos. É possível configurar o comportamento de sincronização na política do Kaspersky Endpoint Security e selecionar os valores ideais para que correspondam com sua carga de rede (consulte as instruções abaixo).

Se não houver conexão entre o Kaspersky Endpoint Security e o servidor, o aplicativo enfileira novos eventos. Quando a conexão é restaurada, o Kaspersky Endpoint Security envia eventos em fila para o servidor na ordem correta. Para evitar sobrecarregar o servidor, o Kaspersky Endpoint Security pode ignorar alguns eventos. Para ativar essa opção, é possível otimizar as configurações de transmissão de eventos, por exemplo, para definir um valor máximo de eventos por hora (consulte as instruções abaixo).

Para definir as configurações de telemetria, execute as seguintes etapas:

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configuração de agentes integrados** → **Endpoint Detection and Response Expert (cloud)**.
5. Na janela que é aberta, selecione a guia **Configurações de transmissão de dados**.
6. Certifique-se de que a caixa de seleção **Envio de telemetria ATIVADO** esteja marcada.
7. Se necessário, ative a funcionalidade **Enviar apenas telemetria com IOA**. *Indicadores de ataque (IOA)* é uma regra que contém uma descrição de comportamentos suspeitos no sistema que podem indicar um ataque direcionado. O aplicativo compara o comportamento contínuo no sistema com essas regras e registra os eventos que indicam um ataque direcionado. O aplicativo usa a tecnologia *de verificação de streaming*, que permite fazer o rastreamento de eventos em tempo real. Por padrão, a funcionalidade está desativada.
8. Caso necessário, defina as configurações de sincronização do servidor:
   - **Atraso máximo na transmissão de eventos (segundos)**. O aplicativo sincroniza com o servidor para enviar eventos após expirar o intervalo de sincronização. A configuração padrão é 30 segundos.
   - **Número máximo de pacotes de eventos**. O aplicativo sincroniza com o servidor quando o buffer está cheio de eventos. A configuração padrão é 1024 eventos.
9. Vá para a guia **Limitação de solicitações**.

10. Se necessário, desative a limitação de solicitações usando o botão de alternância **Limitação de solicitações ATIVADA**.

    Esse recurso ajuda a otimizar a carga no computador. Se essa funcionalidade estiver ativada, o aplicativo restringirá a transmissão de eventos. Caso o número de eventos exceda os limites configurados, o Kaspersky Endpoint Security interromperá o envio de eventos. Esta opção está ativada por padrão.

11. Defina as configurações de otimização para enviar eventos ao servidor:

    - **Número máximo de eventos por hora**. O aplicativo analisa o fluxo de dados de telemetria e restringe o envio de eventos caso ele exceda o limite de eventos configurado por hora. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. A configuração padrão é de 3 mil eventos por hora. Caso o aplicativo esteja instalado em um servidor, o fluxo de dados de telemetria será maior. Para servidores, é recomendável aumentar o valor para 60 mil eventos por hora.

    - **Porcentagem de excesso do limite de eventos (%)**. O aplicativo ordena os eventos por tipo (por exemplo, eventos "alterações no registro") e restringe a transmissão de eventos caso a proporção de eventos do mesmo tipo para o número total de eventos exceda o limite configurado em porcentagem. O Kaspersky Endpoint Security retoma o envio de eventos quando a proporção de outros eventos para o número total de eventos torna-se volumosa o suficiente novamente. A configuração padrão é 15%.

12. Para aplicar a política aos computadores, feche os ícones de cadeado 🔒 e salve as alterações.

Exclusões de telemetria EDR Expert (cloud)

Para melhorar o desempenho e otimizar a transmissão de dados para o servidor de coleta de telemetria, é possível adicionar exclusões de telemetria. Por exemplo, é possível optar pelo não envio de dados de comunicações de rede para aplicativos individuais.

> Usar muitas regras pode aumentar a carga no servidor de coleta de telemetria e reduzir o desempenho do computador. Recomendamos adicionar apenas as regras necessárias.

Para criar uma exclusão de telemetria no Web Console e no Cloud Console:

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Configurações de telemetria**.

5. Selecione a guia **Telemetria do EDR Expert (cloud)**.

6. No bloco **Exclusões gerais**, clique no botão **Adicionar**.

   A janela **Adicionar regra de exclusão** é aberta.

7. Caso necessário, altere o conteúdo da regra. Por padrão, a regra está ativa.

8. Insira um nome para a regra.

9. Selecione a ação a ser executada quando a regra for acionada:

- **Não coletar**. O evento filtrado será excluído da telemetria enviada.
- **Excluir IOA**. O evento de acionamento da regra IOA será excluído da telemetria enviada.

10. Caso a opção **Excluir IOA** esteja selecionada, especifique as regras de IOA a serem adicionadas às exclusões:

- **Excluir tudo**. Quando a condição especificada for atendida, o aplicativo excluirá os eventos gerados de acordo com todas as regras IOA da telemetria.
- **Excluir por GUID**. Especifique o GUID da regra IOA. É possível especificar vários GUIDs usando `,`. Para obter mais detalhes sobre as regras IOA, consulte a ajuda da EDR Expert (cloud).

11. Especifique a condição de filtragem:

a. Selecione o nome do campo a ser usado para filtragem.

b. Selecione um operador (consulte a tabela abaixo) e especifique o valor com o qual comparar o valor do campo do evento.

Lista de operadores condicionais

Operador	Descrição
<	Caso o valor do campo seja menor que o valor especificado na condição, o evento será filtrado.
≤	Caso o valor do campo seja menor que ou igual ao valor especificado na condição, o evento será filtrado.
=	Caso o valor do campo seja igual ao valor especificado na condição, o evento será filtrado.
≥	Caso o valor do campo seja maior que ou igual ao valor especificado na condição, o evento será filtrado.
>	Caso o valor do campo seja maior que o valor especificado na condição, o evento será filtrado.
≠	Caso o valor do campo não seja igual ao valor especificado na condição, o evento será filtrado.
é como	Caso o valor do campo corresponda à máscara especificada na condição, o evento será filtrado. O aplicativo é compatível com os caracteres `*` e `?` ao inserir uma máscara:
não é como	Caso o valor do campo não corresponda à máscara especificada na condição, o evento será filtrado. O aplicativo é compatível com os caracteres `*` e `?` ao inserir uma máscara:
um de	Caso o valor do campo corresponda a um dos valores na lista especificada na condição, o evento será considerado filtrado.
nenhum de	Caso o valor do campo não corresponda a nenhum dos valores na lista especificada na condição, o evento será considerado filtrado.
é como um de	Caso o valor do campo corresponda a uma das máscaras especificadas na condição, o evento será filtrado. O aplicativo é compatível com os caracteres * e ? ao inserir uma máscara.
não é como nenhum de	Caso o valor do campo não corresponda a nenhuma das máscaras especificadas na condição, o evento será filtrado. O aplicativo é compatível com os caracteres * e ? ao inserir uma máscara.
sair	Caso o campo especificado na condição esteja presente no evento, o evento será filtrado.
não sair	Caso o campo especificado na condição não esteja presente no evento, o evento será filtrado.
contém	Caso o valor especificado na condição esteja presente no valor do campo, o evento será filtrado.
é igual a	Caso o valor do campo seja igual ao valor especificado na condição, o evento será filtrado. A verificação não diferencia maiúsculas de minúsculas.
bitwise E	Caso o resultado da operação bitwise E (&) entre o valor do campo e o valor especificado na condição for 1, o evento será filtrado.

12. Caso necessário, é possível criar critérios de filtragem complexos adicionando várias condições de filtro e grupos de condições. Também é possível adicionar condições aninhadas e grupos de condições a um grupo de condições. É possível usar as seguintes configurações:

    - **AND** significa que o filtro seleciona eventos que atendem a todas as condições especificadas.
    - **OR** significa que o filtro seleciona eventos que atendem a uma das condições especificadas.
    - **NOT** (para usar este operador, selecione a opção **Adicionar NOT antes**) significa que o filtro seleciona eventos que não atendem a nenhuma das condições especificadas.

    As condições e os grupos de condições de primeiro nível são combinados com o operador **AND**.

13. Para verificar a regra de filtragem criada, clique no botão **Verificar regra**.

    Na janela aberta, será exibida uma tabela de eventos filtrados pela regra criada. Para obter mais detalhes, consulte a Ajuda do EDR Expert (cloud).

14. Caso seja necessário, em **Todos os tipos de eventos**, adicione exclusões de telemetria por tipo de evento.

    a. Clique no nome do tipo de evento.

    b. Na janela que é aberta, clique no botão **Configurar manualmente**.

    c. Caso necessário, configure a transmissão de telemetria para o tipo de evento selecionado usando o botão de alternância **Enviar evento**. Por padrão, a transmissão de telemetria é ativada para todos os tipos de eventos.

    d. No bloco **Regras de exclusões**, clique no botão **Adicionar**.

    A janela **Adicionar regra de exclusão** é aberta.

    e. Execute as ações descritas nas etapas 7 a 13 para cada regra adicionada.

15. Para alguns tipos de evento, também é possível adicionar regras de inclusão para expandir a telemetria coletada:

    a. No bloco **Regras de inclusão**, clique no botão **Adicionar**.

    A janela **Adicionar regra de inclusão** é aberta.

    b. Insira um nome para a regra.

    c. Abaixo de **Condição**, insira valores para os campos exibidos. O tipo de campos disponíveis depende do evento selecionado.

    As regras de exclusão têm prioridade sobre as regras de inclusão.

16. Para aplicar a política aos computadores, certifique-se de que os cadeados estejam fechados (🔒) e salve suas alterações.

Como exportar ou importar filtros de eventos do EDR Expert (cloud)

Você pode exportar a lista de exclusões para um arquivo JSON. Em seguida, será possível modificar o arquivo para, por exemplo, adicionar um grande número de IDs de eventos. Também é possível usar a função de exportação/importação para fazer backup dos filtros de eventos ou para migrar a lista para um servidor diferente.

> Usar muitas regras pode aumentar a carga no servidor de coleta de telemetria e reduzir o desempenho do computador. Recomendamos adicionar apenas as regras necessárias.

Para exportar ou importar filtros de eventos no Web Console:

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Configurações de telemetria**.
5. Selecione a guia **Telemetria do EDR Expert (cloud)**.
6. Para exportar os filtros de evento:
   a. Clique **Exportar**.
   b. Na janela exibida, especifique o nome do arquivo JSON para o qual deseja exportar os filtros de eventos e selecione a pasta na qual deseja salvar o arquivo.
   c. Salvar o arquivo.

      O Kaspersky Endpoint Security exporta todos os filtros de eventos para o arquivo JSON.
7. Para importar os filtro de evento:
   a. Clique **Importar**.
   b. Na janela que é aberta, selecione o arquivo JSON do qual deseja importar os filtro de eventos.
   c. Selecione como deseja que as regras de filtragem de eventos sejam importadas: adicionando às regras existentes ou descartando as regras existentes e substituindo por novas.
   d. Abra o arquivo.

8. Para aplicar a política aos computadores, certifique-se de que os cadeados estejam fechados (🔒) e salve suas alterações.

    1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

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

       A janela de propriedades da política é exibida.

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

    4. Selecione **Configurações gerais** → **Configurações de telemetria**.

    5. Selecione a guia **Telemetria do EDR Expert (cloud)**.

    6. Para exportar os filtros de evento:

       a. Clique **Exportar**.

       b. Na janela exibida, especifique o nome do arquivo JSON para o qual deseja exportar os filtros de eventos e selecione a pasta na qual deseja salvar o arquivo.

       c. Salvar o arquivo.

       O Kaspersky Endpoint Security exporta todos os filtros de eventos para o arquivo JSON.

    7. Para importar os filtro de evento:

       a. Clique **Importar**.

       b. Na janela que é aberta, selecione o arquivo JSON do qual deseja importar os filtro de eventos.

       c. Selecione como deseja que as regras de filtragem de eventos sejam importadas: adicionando às regras existentes ou descartando as regras existentes e substituindo por novas.

       d. Abra o arquivo.

    8. Para aplicar a política aos computadores, certifique-se de que os cadeados estejam fechados (🔒) e salve suas alterações.

Gerenciamento da Quarentena

A *Quarentena* é um armazenamento local especial no computador. O usuário pode colocar em quarentena arquivos que considere perigosos para o computador. Os arquivos em quarentena são armazenados em um estado criptografado e não ameaçam a segurança do dispositivo. O Kaspersky Endpoint Security usa a Quarentena somente quando estiver integrado com as soluções Detection and Response da Kaspersky. Em outros casos, o Kaspersky Endpoint Security coloca o arquivo relevante no Backup. Para obter informações sobre o gerenciamento da Quarentena como parte das soluções, consulte a Ajuda do Kaspersky Sandbox, a Ajuda do Kaspersky Endpoint Detection and Response Optimum, a Ajuda do Kaspersky Endpoint Detection and Response Expert, a Ajuda da Kaspersky Anti Targeted Attack Platform e a Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises).

O Kaspersky Endpoint Security usa a conta do sistema (SISTEMA) para os arquivos da quarentena.

Só é possível definir as configurações da quarentena no console do Kaspersky Security Center. Também é possível usar o Kaspersky Security Center Console para gerenciar objetos em quarentena (restaurar, excluir, adicionar, etc). Localmente, no computador, só é possível restaurar o objeto utilizando a linha de comando.

Configuração do tamanho máximo da Quarentena

Por padrão, o tamanho da Quarentena é limitado a 1024 MB. Quando a quarentena atingir o tamanho máximo, o Kaspersky Endpoint Security interrompe o envio de arquivos e gera o evento *Não há espaço suficiente no armazenamento da Quarentena*. Para evitar que a quarentena fique sem espaço em disco, é possível definir um limite no qual o Kaspersky Endpoint Security gere o evento *O armazenamento da Quarentena está quase sem espaço*. Não é possível configurar um período de retenção para arquivos em quarentena para que sejam removidos automaticamente.

Caso a solução Kaspersky Anti Targeted Attack Platform (EDR) esteja implantada em sua organização, recomendamos aumentar o tamanho da Quarentena. Ao fazer uma verificação YARA, o aplicativo pode encontrar um grande dump de memória. Caso o tamanho do dump de memória exceda o tamanho da Quarentena, a verificação YARA será concluída com um erro e o dump de memória não será colocado na quarentena. Recomendamos definir o tamanho da Quarentena igual ao tamanho total da RAM no computador (por exemplo, 8 GB) ou desativar o limite do tamanho da Quarentena.

Como configurar o tamanho máximo da quarentena no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Relatórios e Armazenamento**.
4. No bloco **Quarentena**, configure o tamanho da Quarentena:
   - **Limitar o tamanho da Quarentena a N MB**. Caso a caixa de seleção esteja marcada, o tamanho máximo da quarentena será limitado ao valor definido. Por padrão, a dimensão máxima é 1024 MB. Quando a quarentena atingir o tamanho máximo, o Kaspersky Endpoint Security envia o evento *Não há espaço suficiente no armazenamento da Quarentena* ao Kaspersky Security Center e publica o evento no log de eventos do Windows. Enquanto isso, o aplicativo interrompe a quarentena de novos objetos. É preciso esvaziar a quarentena manualmente.

     Caso a caixa de seleção seja desmarcada, o tamanho da Quarentena será limitado pelo espaço livre disponível em disco.
   - **Notificar quando o armazenamento da Quarentena atingir N porcento**. Valor limite da quarentena. Por exemplo, é possível definir o limite da quarentena para 50%. Quando a quarentena atingir o limite, o Kaspersky Endpoint Security envia o evento correspondente ao Kaspersky Security Center e publica o evento no log de eventos do Windows. Enquanto isso, o aplicativo continua colocando novos objetos em quarentena.

     Caso a caixa de seleção seja desmarcada, o aplicativo não gerará eventos quando o limite de quarentena for atingido.
5. Salvar alterações.

Como configurar o tamanho máximo da Quarentena no Web Console e Cloud Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Relatórios e Armazenamento**.

5. No bloco **Quarentena**, configure o tamanho da Quarentena:

   - **Limitar o tamanho da Quarentena**. Caso a caixa de seleção esteja marcada, o tamanho máximo da Quarentena será limitado ao valor especificado. Caso a caixa de seleção seja desmarcada, o tamanho da Quarentena será limitado pelo espaço livre disponível em disco. Talvez isso seja necessário para a verificação YARA, pois o aplicativo pode salvar um arquivo de despejo de memória grande.

   - **Tamanho máximo para a Quarentena (MB)**. Caso a caixa de seleção esteja marcada, o tamanho máximo da quarentena será limitado ao valor definido. Por padrão, a dimensão máxima é 1024 MB. Quando a quarentena atingir o tamanho máximo, o Kaspersky Endpoint Security envia o evento *Não há espaço suficiente no armazenamento da Quarentena* ao Kaspersky Security Center e publica o evento no log de eventos do Windows. Enquanto isso, o aplicativo interrompe a quarentena de novos objetos. É preciso esvaziar a quarentena manualmente.

     Caso a caixa de seleção seja desmarcada, o tamanho da Quarentena será limitado pelo espaço livre disponível em disco.

   - **Notificar quando o armazenamento da Quarentena atingir (%)**. Valor limite da quarentena. Por exemplo, é possível definir o limite da quarentena para 50%. Quando a quarentena atingir o limite, o Kaspersky Endpoint Security envia o evento correspondente ao Kaspersky Security Center e publica o evento no log de eventos do Windows. Enquanto isso, o aplicativo continua colocando novos objetos em quarentena.

6. Salvar alterações.

Envio de dados sobre os arquivos em Quarentena para o Kaspersky Security Center

Para executar ações com objetos na Quarentena no Web Console, é preciso ativar o envio de dados de arquivos na Quarentena para o Servidor de Administração. Por exemplo, é possível baixar um arquivo a partir da quarentena para a análise no Web Console. O envio de dados de arquivos na Quarentena deve ser ativado para todas as funcionalidades do Kaspersky Sandbox e Kaspersky Endpoint Detection and Response para funcionar.

Como ativar a transferência de dados de arquivos na quarentena para o Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.

2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela da política, selecione **Configurações gerais** → **Relatórios e Armazenamento**.

4. No bloco **Transferência de dados para o Servidor de Administração**, clique no botão **Configurações**.

5. Na janela que é aberta, marque a caixa de seleção **Arquivos da Quarentena**.

6. Salvar alterações.

Para permitir a transferência de dados de arquivos na quarentena para o Web Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Integração KSC**.

5. No bloco **Transferência de dados para o Servidor de Administração**, marque a caixa de seleção **Sobre os arquivos na Quarentena**.

6. Salvar alterações.

Como resultado, é possível visualizar uma lista de arquivos colocados em quarentena no computador no console do Kaspersky Security Center. Também é possível utilizar o Kaspersky Security Center Console para gerenciar os objetos em quarentena (restaurar, excluir, adicionar, etc). Para obter mais detalhes sobre o funcionamento da Quarentena, consulte a ajuda do Kaspersky Security Center.

Restauração do arquivo da Quarentena

Por padrão, o Kaspersky Endpoint Security restaura os arquivos na pasta original. Caso a pasta de destino tenha sido excluída ou o usuário não possua direitos de acesso a essa pasta, o aplicativo coloca o arquivo na pasta `%DataRoot%\QB\Restored`. Então, é preciso mover manualmente o arquivo para a pasta de destino.

Para restaurar arquivos da Quarentena:

1. Na janela principal do Web Console, selecione **Operações** → **Repositórios** → **Quarentena**.

2. Isso abre a lista de arquivos na Quarentena; nessa lista, selecione os arquivos que deseja restaurar e clique em **Restaurar**.

O Kaspersky Endpoint Security restaura o arquivo. Caso a pasta de destino já possua um arquivo com o mesmo nome, o aplicativo cancelará a restauração do arquivo. O aplicativo salva uma cópia do arquivo na Quarentena após restaurá-lo. Para excluir o arquivo, você deve limpar manualmente a Quarentena.

Monitoramento de ações de EDR

O Kaspersky Endpoint Security for Windows 12.9 apresenta o centro de monitoramento de ações EDR. O *Centro de monitoramento de ações EDR* é um console no qual o usuário pode visualizar o histórico de resposta a ameaças para todas as soluções Detection and Response da Kaspersky. Se sua organização tiver várias Detection and Response implementadas (por exemplo, EDR Optimum e MDR), o Kaspersky Endpoint Security exibirá o histórico de resposta a ameaças para todas as soluções. Isso permite analisar o desempenho das soluções de Detection and Response em um computador separado e otimizar as configurações dessas soluções.

O centro de monitoramento fornece as seguintes informações:

- Informações sobre tarefas de resposta a ameaças (por exemplo, a tarefa *Encerrar processo*)
- Alterações das regras de Isolamento de rede e Prevenção de execução

Se a resposta a ameaças encontrar um erro relacionado ao acesso a um compartilhamento de rede, esse erro será omitido do histórico de respostas a ameaças exibido.

Para navegar até o centro de monitoramento de ações EDR:

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Ativos (dispositivos)**.
2. Selecione o computador para o qual você deseja definir as configurações locais do aplicativo.

   Isso abre as propriedades do computador.
3. Selecione a guia **Aplicativos**.
4. Clique **Kaspersky Endpoint Security for Windows 14.2**.

   Isso abre as configurações locais do aplicativo.
5. Selecione a guia **Configurações do aplicativo**.
6. Selecione **Detection and Response** → **Histórico de resposta**.

Isso abre o console do centro de monitoramento de ações EDR. É possível usar o console para exibir os status da tarefa Resposta a ameaças, incluindo a duração dela, as alterações de regra e os detalhes do iniciador.

Kaspersky Unified Monitoring and Analysis Platform (KUMA)

O Kaspersky Endpoint Security for Windows é compatível com a solução Kaspersky Unified Monitoring and Analysis Platform. A *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* é uma solução de gerenciamento de eventos e informações de segurança (SIEM) para a infraestrutura de TI das organizações. O KUMA permite detectar, analisar e mitigar as ameaças de segurança antes que elas possam causar danos.

O Kaspersky Endpoint Security é instalado em computadores individuais na infraestrutura corporativa de TI e monitora continuamente os processos, as conexões de rede abertas e os arquivos em modificação. As informações sobre os eventos no computador (telemetria) são enviadas para o servidor da Kaspersky Unified Monitoring and Analysis Platform (KUMA). Em seu console, a KUMA exibe os eventos como uma lista sem marcação, semelhante ao log de eventos do Windows.

O Kaspersky Endpoint Security não fornece todas as funcionalidades de um agente para KUMA. O aplicativo somente envia eventos à KUMA sem marcação. Para acessar todas as funcionalidades da KUMA, é necessário comprar uma licença e implementar a solução de acordo com o guia do administrador KUMA.

Integração do Kaspersky Endpoint Security com a KUMA

A configuração da integração do KES com o KUMA envolve as seguintes etapas:

1. No console do KUMA, adicione um coletor.
2. No console do KUMA, configure um conector para que o coletor receba eventos do KES.
3. No console do KUMA, ative a autenticação bidirecional (opcional).
4. Na política do Kaspersky Endpoint Security for Windows, defina as configurações de conexão do KES com o KUMA.
5. No console do KUMA, verifique se os eventos do KES são encaminhados ao locatário correto e processados pelas regras de correlação corretas.

Preparação para a integração do KES com o KUMA

Para usar a KUMA, as seguintes condições devem ser atendidas:

- Kaspersky Security Center versão 14.2 ou posterior. Em versões anteriores do Kaspersky Security Center, é impossível ativar a funcionalidade de integração KUMA.
- O aplicativo é ativado e a funcionalidade é contemplada pela licença.
- O componente integração KUMA está ativado.

A preparação para a integração do KES com o KUMA envolve as seguintes etapas:

1. **Instalação do componente de integração KUMA**

   É possível selecionar o componente integração KUMA durante a instalação ou atualização do aplicativo, assim como usar a tarefa *Alterar componentes do aplicativo*.

   É necessário reiniciar o computador para concluir a atualização do aplicativo com o novo componente.

2. **Ativação do KUMA**

   Além de uma licença do aplicativo Kaspersky Endpoint Security (por exemplo, Kaspersky Endpoint Security for Business Standard), é necessário ter uma licença separada para a integração do Kaspersky Endpoint Security com o KUMA (add-on de integração do Kaspersky Endpoint Security for Windows KUMA).

   Caso esteja instalando o aplicativo no modo EDR Agent, será necessário ter uma licença para integrar o Kaspersky Endpoint Security com o KUMA e uma licença do Kaspersky Anti Targeted Attack Platform (KATA) ou uma licença do Kaspersky Managed Detection and Response (MDR). Não é possível implementar somente o EDR Agent para KUMA.

   A funcionalidade fica disponível depois da adição da chave KUMA separada. Como resultado, haverá outra chave ativa no computador para a integração do Kaspersky Endpoint Security com o KUMA.

   A licença para a funcionalidade KUMA é a mesma que a licença do Kaspersky Endpoint Security.

   Certifique-se de que a funcionalidade KUMA esteja incluída na licença e esteja sendo executada na interface local do aplicativo.

Conectar o KES ao KUMA

Para conectar o computador com o aplicativo Kaspersky Endpoint Security com a solução KUMA:

1. No console do KUMA, adicione um coletor com conectores do tipo **tcp**, **udp** ou **http** e especifique as configurações básicas de rede da conexão. Para obter detalhes sobre o gerenciamento de conectores, consulte a ajuda da Kaspersky Unified Monitoring and Analysis Platform.

2. Na política do Kaspersky Endpoint Security, adicione os endereços dos coletores do KUMA e especifique as configurações de rede da conexão.

Como conectar um computador Kaspersky Endpoint Security com a KUMA com o uso do Console de Administração (MMC)

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

2. Na árvore do console, selecione **Políticas**.

3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

4. Na janela da política, selecione **Integração KUMA**.

5. Marque a caixa de seleção **Integração KUMA**.

6. No bloco **Configurações de integração**, marque a caixa de seleção **Ativar transmissão de eventos do Windows para um servidor KUMA**.

7. Adicione os servidores KUMA:

   a. Clique **Adicionar**.

   Isso abre o formulário no qual é possível adicionar servidores do KUMA.

   b. Selecione o protocolo para se conectar ao servidor do KUMA: **HTTP / HTTPS**, **TCP**, **UDP**.

   O protocolo para conexão com o coletor no Kaspersky Endpoint Security deve corresponder ao tipo de conector no KUMA: **http**, **tcp** ou **udp**.

   > Ao usar o protocolo UDP, os dados podem ser perdidos devido à perda de pacotes inerente ao protocolo.

   c. Insira o endereço do servidor (IPv4, IPv6, FQDN) e a porta para se conectar ao servidor (por padrão, a porta 443 é especificada).

   Ao inserir o endereço do servidor, considere o seguinte:

   - **TCP**:
     - **Sem TLS**. Você pode especificar o endereço IP ou o FQDN do servidor.
     - **Com TLS**. Você deve especificar somente o FQDN do servidor.
   - **HTTP / HTTPS**:
     - **Sem TLS**. Você deve especificar explicitamente o protocolo HTTP no endereço do servidor (por exemplo, `http://server.com` ou `http://10.10.10.100`).
     - **Com TLS**. Você não precisa especificar o protocolo (por exemplo, `https://server.com` ou `server.com`).
   - **UDP**. O protocolo UDP não é compatível com a criptografia TLS. Você pode especificar o endereço IP ou o FQDN do servidor.

   Você pode ver o endereço do servidor nas propriedades do conector no console do KUMA. Para obter mais informações sobre os conectores do KUMA, consulte a ajuda da Kaspersky Unified Monitoring and Analysis Platform.

   d. Clique **OK**.

   O Kaspersky Endpoint Security estabelecerá conexão com o primeiro servidor da KUMA na lista. Caso a conexão falhe, o Kaspersky Endpoint Security estabelecerá conexão com o segundo servidor da KUMA na lista e assim sucessivamente.

8. Caso seja necessário, defina a configuração **Atraso máximo na transmissão de eventos (segundos)** no bloco **Configurações de transmissão de dados**. Quando o tempo especificado se esgotar, o Kaspersky Endpoint Security tentará estabelecer conexão com o mesmo coletor ou com o próximo coletor da lista caso haja vários coletores. A configuração padrão é 30 segundos.

9. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como conectar um computador Kaspersky Endpoint Security com a KUMA com o uso do Web Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Configuração de agentes integrados** → **Integração KUMA**.

5. Ative o botão de alternância **Integração KUMA ATIVADA**.

6. Adicione os servidores KUMA:

   a. Clique **Adicionar**.

      Isso abre o formulário no qual é possível adicionar servidores do KUMA.

   b. Selecione o protocolo para se conectar ao servidor do KUMA: **HTTP/HTTPS**, **TCP**, **UDP**.

      O protocolo para conexão com o coletor no Kaspersky Endpoint Security deve corresponder ao tipo de conector no KUMA: **http**, **tcp** ou **udp**.

      > Ao usar o protocolo UDP, os dados podem ser perdidos devido à perda de pacotes inerente ao protocolo.

   c. Insira o endereço do servidor (IPv4, IPv6, FQDN) e a porta para se conectar ao servidor (por padrão, a porta 443 é especificada).

      Ao inserir o endereço do servidor, considere o seguinte:

      - **TCP**:
        - **Sem TLS**. Você pode especificar o endereço IP ou o FQDN do servidor.
        - **Com TLS**. Você deve especificar somente o FQDN do servidor.
      - **HTTP/HTTPS**:
        - **Sem TLS**. Você deve especificar explicitamente o protocolo HTTP no endereço do servidor (por exemplo, `http://server.com` ou `http://10.10.10.100`).
        - **Com TLS**. Você não precisa especificar o protocolo (por exemplo, `https://server.com` ou `server.com`).
      - **UDP**. O protocolo UDP não é compatível com a criptografia TLS. Você pode especificar o endereço IP ou o FQDN do servidor.

      Você pode ver o endereço do servidor nas propriedades do conector no console do KUMA. Para obter mais informações sobre os conectores do KUMA, consulte a ajuda da Kaspersky Unified Monitoring and Analysis Platform.

   d. Clique **OK**.

O Kaspersky Endpoint Security estabelecerá conexão com o primeiro servidor da KUMA na lista. Caso a conexão falhe, o Kaspersky Endpoint Security estabelecerá conexão com o segundo servidor da KUMA na lista e assim sucessivamente.

7. Caso seja necessário, defina a configuração **Atraso máximo ao enviar eventos (s)** no bloco **Configurações de conexão do servidor**. Quando o tempo especificado se esgotar, o Kaspersky Endpoint Security tentará estabelecer conexão com o mesmo coletor ou com o próximo coletor da lista caso haja vários coletores. A configuração padrão é 30 segundos.

8. Salvar alterações.

É possível verificar se a integração KUMA está configurada corretamente no console do KUMA (para obter detalhes, consulte a ajuda da Kaspersky Unified Monitoring and Analysis Platform). Verifique o status operacional do componente visualizando o *Relatório de status dos componentes do aplicativo* no console do Kaspersky Security Center. Também é possível visualizar o status operacional de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente do **Integração KUMA** será adicionado na lista de componentes do Kaspersky Endpoint Security.

Como estabelecer uma conexão confiável entre o KES e o KUMA

É possível estabelecer uma conexão confiável entre o Kaspersky Endpoint Security e um coletor do KUMA que tenha um conector do tipo tcp ou http. Não é possível estabelecer uma conexão confiável com um conector do tipo udp.

Para estabelecer uma conexão confiável, é necessário configurar um modo TLS nas configurações do conector. Os seguintes modos TLS estão disponíveis:

- **Disabled**: Não usar criptografia TLS. Esta opção está selecionada por padrão.
- **Enabled**: Usar criptografia TLS, mas sem verificação de certificado.
- **Custom PFX with client authentication**: Usar criptografia TLS com um segredo PFX. Nesse modo, o cliente é autenticado com um certificado.

O Kaspersky Endpoint Security não suporta o modo TLS **Custom PFX**. Ao integrar o KES ao KUMA usando PFX, é necessário autenticar o usuário com uma senha.

Para configurar uma conexão confiável, é necessário um certificado TLS: o *certificado da CA para o microsserviço*. Você pode obter um certificado TLS no console do KUMA. Para obter detalhes sobre como baixar certificados TLS, consulte a ajuda da Kaspersky Unified Monitoring and Analysis Platform. Em seguida, é necessário adicionar o certificado TLS ao Kaspersky Endpoint Security (consulte as instruções abaixo).

Para tornar a conexão mais segura, também é possível ativar a autenticação adicional do computador no KUMA (autenticação bidirecional). Para ativar essa autenticação, é necessário criar um contêiner criptográfico em uma autoridade de certificação externa. Um *contêiner criptográfico* é um arquivo PFX que contém um certificado e uma chave privada no formato PKCS#12. Em seguida, é necessário ativar a autenticação bidirecional nas configurações do KUMA (modo TLS **Custom PFX with client authentication**), ativar a autenticação bidirecional no Kaspersky Endpoint Security e adicionar um arquivo PFX ao console do KUMA e ao Kaspersky Endpoint Security.

Como configurar uma conexão confiável entre o KES e o KUMA no Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Integração KUMA**.
5. Marque a caixa de seleção **Integração KUMA**.
6. No bloco **Configurações de conexão com servidores KUMA**, marque a caixa de seleção **Usar criptografia TLS**.
7. Configure a conexão confiável:

   a. Clique **Configurações de conexão com servidores KUMA**.

   b. Configure a conexão do servidor:

   - **Tempo limite (seg)**. Tempo máximo de espera por uma resposta do servidor do KUMA (por padrão, o valor é de 5 segundos). Quando o tempo limite se esgotar, o Kaspersky Endpoint Security tenta estabelecer conexão com um servidor da KUMA diferente.
   - **Certificado TLS do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor da KUMA. Você pode obter um certificado TLS no console da Kaspersky Unified Monitoring and Analysis Platform (consulte as instruções na ajuda da Kaspersky Unified Monitoring and Analysis Platform).

     Para estabelecer uma conexão confiável, é necessário selecionar o modo TLS **Enabled** no console do KUMA.
   - **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o KES e a KUMA. Para usar a autenticação bidirecional, no console do KUMA, nas configurações do conector, é necessário selecionar o modo TLS **Custom PFX with client authentication** (consulte as configurações do conector na ajuda da Kaspersky Unified Monitoring and Analysis Platform). Em seguida, é necessário baixar um certificado de servidor e definir uma senha para proteger o contêiner criptográfico.

     > O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.

   c. Clique **OK**.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como configurar uma conexão confiável entre o KES e o KUMA no Web Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.

4. Selecione **Configuração de agentes integrados** → **Integração KUMA**.

5. Ative o botão de alternância **Integração KUMA ATIVADA**.

6. Em **Configurações de conexão do servidor**, ative o botão de alternância **Usar criptografia TLS**.

7. Configure a conexão confiável:

   a. Clique **Configurações de conexão**.

   b. Configure a conexão do servidor:

   - **Tempo limite (s)**. Tempo máximo de espera por uma resposta do servidor do KUMA (por padrão, o valor é de 5 segundos). Quando o tempo limite se esgotar, o Kaspersky Endpoint Security tenta estabelecer conexão com um servidor da KUMA diferente.

   - **Certificado TLS do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor da KUMA. Você pode obter um certificado TLS no console da Kaspersky Unified Monitoring and Analysis Platform (consulte as instruções na ajuda da Kaspersky Unified Monitoring and Analysis Platform).

     Para estabelecer uma conexão confiável, é necessário selecionar o modo TLS **Enabled** no console do KUMA.

   - **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o KES e a KUMA. Para usar a autenticação bidirecional, no console do KUMA, nas configurações do conector, é necessário selecionar o modo TLS **Custom PFX with client authentication** (consulte as configurações do conector na ajuda da Kaspersky Unified Monitoring and Analysis Platform). Em seguida, é necessário baixar um certificado de servidor e definir uma senha para proteger o contêiner criptográfico.

     > O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.

   c. Clique **OK**.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Ativação do envio de telemetria para o servidor KUMA

Por padrão, o envio de eventos ao servidor KUMA está desativado. Para garantir que o KUMA funcione corretamente, é necessário ativar o envio de telemetria. É possível selecionar uma fonte de evento entre os logs padrão: *Application*, *Security* ou *System*.

Como ativar o envio de telemetria para o KUMA no Console de Administração (MMC)

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

2. Na árvore do console, selecione **Políticas**.

3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

4. Na janela da política, selecione **Configurações gerais** → **Exclusões e tipos de objetos**.

5. No bloco **Configurações de telemetria** → **Telemetria KUMA**, clique no botão **Configurações**.

6. Selecione os logs de eventos que deseja usar como fontes de eventos: *Application*, *Security* ou *System*.
   Além dos logs padrão, é possível especificar um log de um aplicativo de terceiros.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como ativar o envio de telemetria para o KUMA no Web Console

1. Na janela principal do Web Console, selecione a guia **Gerenciamento de ativos** → **Políticas**.

2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é exibida.

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

4. Selecione **Configurações gerais** → **Configurações de telemetria**.

5. Selecione a guia **Telemetria KUMA**.

6. Selecione os logs de eventos que deseja usar como fontes de eventos: *Application*, *Security* ou *System*.
   Além dos logs padrão, é possível especificar um log de um aplicativo de terceiros.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Filtragem de eventos para serem enviados para a KUMA

Por padrão, o envio de eventos ao servidor KUMA está desativado. Para garantir que o KUMA funcione corretamente, é necessário ativar o envio de telemetria. É possível selecionar uma fonte de evento entre os logs padrão: *Application*, *Security* ou *System*. Para aprimorar o desempenho e otimizar a transmissão de dados para o servidor KUMA, é possível adicionar ou excluir manualmente os eventos individuais da telemetria. Por exemplo, é possível excluir os eventos Sysmon.

Como criar uma lista de eventos para serem enviados para KUMA no Console de Administração (MMC)

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

2. Na árvore do console, selecione **Políticas**.

3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

4. Na janela da política, selecione **Configurações gerais** → **Exclusões e tipos de objetos**.

5. No bloco **Configurações de telemetria** → **Telemetria KUMA**, clique no botão **Configurações**.

6. Na janela exibida, configure os filtros do evento para serem enviados para KUMA.

É possível configurar a filtragem de eventos para os logs padrão *Application*, *Security*, *System* ou adicionar manualmente outro log:

a. Abra as propriedades do log ou clique no botão **Adicionar** e insira o nome do log.

b. Selecione um modo de envio do evento:

- **Enviar todos os eventos**. Neste modo, o aplicativo envia todos os eventos do log do Windows, exceto os eventos adicionados nas regras de exclusão.
- **Enviar apenas os eventos selecionados**. Neste modo, o aplicativo envia apenas os eventos adicionados nas regras de inclusão.

c. Crie listas de regras de exclusão ou inclusão para o modo de envio dos eventos pertinentes.

Para adicionar regras, é necessário especificar a ID do evento no log de eventos do Windows. É possível listar diversas IDs de eventos em uma regra. Para especificar diversas IDs de eventos, use uma vírgula (`,`).

d. Caso necessário, ative o registro em log de eventos usando a caixa de seleção ao lado do nome do log.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como criar uma lista de eventos a serem enviados para KUMA no Web Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Configurações de telemetria**.
5. Selecione a guia **Telemetria KUMA**.
6. Na janela exibida, configure os filtros do evento para serem enviados para KUMA.

   É possível configurar a filtragem de eventos para os logs padrão *Application*, *Security*, *System* ou adicionar manualmente outro log:

   a. Abra as propriedades do log ou clique no botão **Adicionar** e insira o nome do log.

   b. Selecione um modo de envio do evento:

   - **Enviar todos os eventos**. Neste modo, o aplicativo envia todos os eventos do log do Windows, exceto os eventos adicionados nas regras de exclusão.
   - **Enviar apenas os eventos selecionados**. Neste modo, o aplicativo envia apenas os eventos adicionados nas regras de inclusão.

   c. Crie listas de regras de exclusão ou inclusão para o modo de envio dos eventos pertinentes.

   Para adicionar regras, é necessário especificar a ID do evento no log de eventos do Windows. É possível listar diversas IDs de eventos em uma regra. Para especificar diversas IDs de eventos, use uma vírgula (`,`).

   d. Caso necessário, ative o registro em log de eventos usando o botão de alternância ao lado do nome do log.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Exportar e importar filtros de eventos KUMA

Você pode exportar a lista de exclusões para um arquivo JSON. Em seguida, será possível modificar o arquivo para, por exemplo, adicionar um grande número de IDs de eventos. Também é possível usar a função de exportação/importação para fazer backup dos filtros de eventos ou para migrar a lista para um servidor diferente.

> Usar muitas regras pode aumentar a carga no servidor KUMA e reduzir o desempenho do computador. Recomendamos adicionar apenas as regras necessárias.

Como exportar e importar os filtros de eventos no Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Configurações gerais** → **Exclusões e tipos de objetos**.
5. No bloco **Configurações de telemetria** → **Telemetria KUMA**, clique no botão **Configurações**.
6. Para exportar os filtros de evento:
   a. Selecione os logs de eventos com os filtros que deseja exportar.
   b. Clique no botão → **Exportar**.
   c. Na janela exibida, especifique o nome do arquivo JSON para o qual deseja exportar os filtros de eventos e selecione a pasta na qual deseja salvar o arquivo.
   d. Salvar o arquivo.
      O Kaspersky Endpoint Security exporta todos os filtros de eventos para o arquivo JSON.
7. Para importar os filtro de evento:
   a. Clique no botão → **Importar**.
   b. Na janela que é aberta, selecione o arquivo JSON do qual deseja importar os filtro de eventos.
   c. Abra o arquivo.
      Caso já existam regras de filtragem de eventos no computador, o Kaspersky Endpoint Security substituirá essas regras durante a importação.
8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como exportar e importar filtros de eventos no Web Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Configurações de telemetria**.
5. Selecione a guia **Telemetria KUMA**.
6. Para exportar os filtros de evento:

   a. Selecione os logs de eventos com os filtros que deseja exportar.

   b. Clique no botão → **Exportar**.

   c. Na janela exibida, especifique o nome do arquivo JSON para o qual deseja exportar os filtros de eventos e selecione a pasta na qual deseja salvar o arquivo.

   d. Salvar o arquivo.

   O Kaspersky Endpoint Security exporta todos os filtros de eventos para o arquivo JSON.
7. Para importar os filtro de evento:

   a. Clique no botão → **Importar**.

   b. Na janela que é aberta, selecione o arquivo JSON do qual deseja importar os filtro de eventos.

   c. Abra o arquivo.

   Caso já existam regras de filtragem de eventos no computador, o Kaspersky Endpoint Security substituirá essas regras durante a importação.
8. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Também é possível exportar ou importar filtros de eventos na linha de comando.

Guia de Migração de KSWS para KES

A partir da versão 11.8.0, o Kaspersky Endpoint Security for Windows é compatível com a funcionalidade básica da solução Kaspersky Security for Windows Server (KSWS). O *Kaspersky Security for Windows Server* protege os servidores que executam sistemas operacionais Microsoft Windows e armazenamentos anexados na rede contra vírus e outras ameaças à segurança do computador às quais os servidores e armazenamentos anexados na rede são expostos durante a troca de arquivos. Para obter informações detalhadas sobre o funcionamento da solução, consulte a ajuda do Kaspersky Security for Windows Server. Desde o Kaspersky Endpoint Security 11.8.0, é possível migrar do Kaspersky Security for Windows Server para o Kaspersky Endpoint Security for Windows e usar a mesma solução para a proteção de estações de trabalho e servidores.

Requisitos de software

Antes de iniciar a migração de KSWS para KES, verifique e confirme se seu servidor satisfaz os requisitos de hardware e software do Kaspersky Endpoint Security for Windows. As listas de versões de sistemas operacionais compatíveis são diferentes para KES e KSWS. Por exemplo, o KES não é compatível com servidores que executam o Windows Server 2003.

Requisitos mínimos de software para migrar de KSWS para KES:

- Kaspersky Endpoint Security para Windows 12.0.
- Kaspersky Security 11.0.1 for Windows Server.

  Caso o usuário tenha uma versão anterior do Kaspersky Security for Windows Server instalada, recomendamos atualizar o aplicativo para a versão mais recente. O assistente de conversão de políticas e tarefas não é compatível com as versões anteriores do Kaspersky Security for Windows Server.
- Kaspersky Security Center 14.2

  Caso tenha uma versão anterior do Kaspersky Security Center instalada, basta atualizá-la para a versão 14.2 ou posterior. Nesta versão do Kaspersky Security Center, o assistente de conversão em lote de políticas e tarefas permite migrar as políticas para um perfil em vez de migrar para uma política. Nesta versão do Kaspersky Security Center, o assistente de conversão em lote de políticas e tarefas também permite a migração de uma gama mais ampla de configurações de política.
- Kaspersky Endpoint Agent 3.10.

  Caso tenha uma versão anterior do Kaspersky Endpoint Agent instalada, recomendamos atualizar o aplicativo para a versão mais recente. O Kaspersky Endpoint Security é compatível com a migração de uma configuração [KSWS+KEA] para [KES built-in agent] iniciando com o Kaspersky Endpoint Agent 3.10.

Recomendações de migração

Ao migrar de KSWS para KES, observe as seguintes recomendações:

- Planeje o tempo de migração de KSWS para KES com antecedência. Escolha um horário em que os servidores estejam operando com carga mais leve, por exemplo, durante o fim de semana.
- Após a migração, ative os componentes do aplicativo gradualmente. Ou seja, comece, por exemplo, ativando apenas o componente Proteção Contra Ameaças ao Arquivo, depois ative outros componentes de proteção, então ative os componentes de controle e assim por diante. Em cada etapa, é preciso verificar se o aplicativo está funcionando corretamente e monitorar o desempenho do servidor. A arquitetura do KES difere do KSWS, portanto, o sistema operacional também pode se comportar de maneira diferente.
- Realize a migração gradualmente. Primeiro, migre um único servidor, depois vários servidores e, em seguida, execute a migração em todos os servidores da organização.
- Migre diferentes tipos de servidores separadamente. Ou seja, comece, por exemplo, migrando os servidores de banco de dados, depois os servidores de correio e assim por diante.
- A migração em servidores de alta carga envolve algumas considerações especiais.

Etapas de migração

A migração de KSWS para KES é realizada de forma semiautomática. Isso é necessário devido às diferentes arquiteturas dos aplicativos. Para migrar configurações de política, é preciso executar o assistente de conversão em lote de políticas e tarefas (o assistente de migração). Depois de migrar as configurações de política, é preciso definir manualmente as configurações que o assistente de migração não pode migrar automaticamente (por exemplo, as Configurações de proteção por senha). Após a migração, também é recomendável verificar se o assistente de migração migrou corretamente todas as configurações.

Migre de KSWS para KES na seguinte ordem:

1. **Migrar as tarefas e políticas do KSWS**

   Depois de migrar as políticas e tarefas, é preciso executar as etapas de configuração adicionais. Também recomendamos garantir que o Kaspersky Endpoint Security forneça o nível de segurança necessário após a migração do KSWS.

   > O assistente de conversão em lote de políticas e tarefas do Kaspersky Security for Windows Server está disponível apenas no Console de Administração (MMC). As configurações de políticas e tarefas não podem ser migradas no Web Console e no Kaspersky Security Center Cloud Console.

2. **Instalar o Kaspersky Endpoint Security**

É possível instalar o Kaspersky Endpoint Security das seguintes maneiras:

- Instalar o KES após remover o KSWS (recomendado).

  O utilitário kavremover não é compatível com o gerenciamento de KSWS.

- Instalação do KES sobre o KSWS.

3. Ativar o KES com uma chave do KSWS

4. **Confirme se o aplicativo está funcionando corretamente após a migração**

   Depois de migrar de KSWS para KES, verifique e confirme se o aplicativo está funcionando corretamente. Verifique o status do servidor no console (deve estar *OK*). Verifique e confirme se nenhum erro foi relatado para o aplicativo, verifique também a hora da última conexão com o Servidor de Administração, a hora da última atualização do banco de dados e o status de proteção do servidor.

   Observe especialmente a migração de listas de exclusão, aplicativos confiáveis, endereços da Web confiáveis e regras de controle de aplicativos.

Correspondência dos componentes do KSWS e KES

Ao migrar de KSWS para KES, o conjunto de componentes é migrado apenas quando o aplicativo está sendo instalado localmente.

Correspondência dos componentes do Kaspersky Security for Windows Server e Kaspersky Endpoint Security for Windows

Componente do Kaspersky Security for Windows Server	Componente do Kaspersky Endpoint Security for Windows
Basic functionality	Kernel do aplicativo
Log Inspection	Inspeção de log
Device Control	Controle de dispositivos
Firewall Management	*(não compatível)* As funções do KSWS Firewall são executadas pelo Firewall no nível do sistema. No KES, um componente separado é responsável pela funcionalidade do Firewall. Após a migração, é possível configurar o Firewall do Kaspersky Endpoint Security.
File Integrity Monitor	Monitor de integridade do sistema
Exploit Prevention	Prevenção de Exploits
System Tray Icon	*(não compatível)* É possível configurar a interação do usuário nas configurações da interface do aplicativo.
Integration with Kaspersky Security Center	Conector do Agente de Rede
Endpoint Agent	*(não compatível)* No Kaspersky Endpoint Security 11.9.0, o pacote de distribuição do Kaspersky Endpoint Agent não faz mais parte do kit de distribuição do Kaspersky Endpoint Security. É necessário baixar o pacote de distribuição do Kaspersky Endpoint Agent separadamente.
Network Threat Protection	Proteção Contra Ameaças à Rede
Anti-Cryptor	Detecção de Comportamento
Anti-Cryptor for NetApp	*(não compatível)*

Componente do Kaspersky Security for Windows Server	Componente do Kaspersky Endpoint Security for Windows
Traffic Security	Proteção Contra Ameaças da Web Proteção Contra Ameaças ao Correio Controle da Web
On-Demand Scan	Kernel do aplicativo
ICAP Network Storage Protection	*(não compatível)* O Kaspersky Endpoint Security não oferece suporte a componentes de Proteção de armazenamento de rede. Caso precise desses componentes, é possível continuar usando o Kaspersky Security for Windows Server.
RPC Network Storage Protection	*(não compatível)* O Kaspersky Endpoint Security não oferece suporte a componentes de Proteção de armazenamento de rede. Caso precise desses componentes, é possível continuar usando o Kaspersky Security for Windows Server.
Real-Time File Protection	Proteção Contra Ameaças ao Arquivo
Script Monitoring	*(não compatível)* O monitoramento de scripts é tratado por outros componentes, por exemplo, pela Proteção AMSI.
KSN Usage	Kaspersky Security Network
Applications Launch Control	Controle de aplicativos
Performance counters	*(não compatível)*

Correspondência das configurações do KSWS e do KES

Ao migrar políticas e tarefas, o KES é configurado de acordo com as configurações do KSWS. As configurações dos componentes do aplicativo que o KSWS não possui são definidas com os valores padrão.

Application settings

Scalability, interface and scanning settings

As configurações do aplicativo não são compatíveis com o Kaspersky Endpoint Security for Windows.

Configurações do aplicativo

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Scalability settings	*(não migra)* O Kaspersky Endpoint Security gerencia todos os processos de trabalho.
Show System Tray Icon	*(não migra)* Em um computador cliente, a janela principal do Kaspersky Endpoint Security e o ícone na área de notificação do Windows estão disponíveis por padrão. No menu de contexto do ícone, o usuário pode executar operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security também exibe notificações acima do ícone do aplicativo. É possível configurar a interação do usuário nas configurações da interface do aplicativo.
Restore file attributes after scanning	*(não migra)* O Kaspersky Endpoint Security restaura automaticamente os atributos do arquivo após verificar um arquivo.
Limit CPU usage for scanning threads	*(não migra)* O Kaspersky Endpoint Security não limita a utilização da CPU durante a verificação. É possível configurar a tarefa para ser executada quando o computador estiver operando com carga mínima.

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Folder for temporary files created during scanning	*(não migra)* O Kaspersky Endpoint Security coloca os arquivos temporários na pasta `C:\Windows\Temp`.
HSM system settings	*(não migra)* O Kaspersky Endpoint Security não oferece suporte a sistemas HSM.

Security and reliability

As configurações de segurança do KSWS são migradas para o **Configurações gerais** seção, Configurações do aplicativo e subseções Interface.

Configurações de segurança do aplicativo

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Protect application processes from external threats	**Ativar a Autodefesa** (subseção **Configurações do aplicativo**)
Apply password protection	*(não migra)* O Kaspersky Endpoint Security possui um recurso integrado de proteção de senha (consulte a subseção **Interface**).
Perform task recovery	*(não migra)* O Kaspersky Endpoint Security restaura automaticamente apenas as tarefas de *Verificação de malware*. O Kaspersky Endpoint Security executa outras tarefas de acordo com o agendamento.
Do not start scheduled scan tasks	**Adiar tarefas agendadas quando estiver em modo de bateria** (subseção **Configurações do aplicativo**)
Stop current scan tasks	*(não migra)* Quando o computador é alimentado por um no-break, o Kaspersky Endpoint Security não interrompe as tarefas de verificação que já estão em execução.

Connection settings

As configurações de interação do Servidor de Administração são migradas para o **Configurações gerais** seção, Configurações de rede e subseções Configurações do aplicativo.

Configurações de interação do Servidor de Administração

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Proxy server settings	**Configurações do servidor proxy** (subseção **Configurações de rede**)
Do not use proxy server for local addresses	**Ignorar servidor proxy para endereços locais** (subseção **Configurações de rede**)
Proxy server authentication settings	**Usar autenticação de servidor proxy** (subseção **Configurações de rede**) A senha de autenticação do servidor proxy não é migrada. Após a migração de uma política, a senha deve ser inserida manualmente.
Use Kaspersky Security Center as a proxy server when activating the application	**Usar o Kaspersky Security Center como servidor proxy para ativação** (subseção **Configurações do aplicativo**)

Run local system tasks

O Kaspersky Endpoint Security ignora as configurações para executar as tarefas do sistema local do Kaspersky Security for Windows Server. É possível configurar o uso de tarefas locais do KES em **Tarefas locais**, Gerenciamento de tarefas. Também é possível configurar uma programação para executar as tarefas de *Verificação de malware* e *Atualização de bancos de dados e módulos do aplicativo* nas propriedades dessas tarefas.

Supplementary

Trusted zone

As configurações de zona confiável do KSWS são migradas para a seção **Configurações gerais**, subseção **Exclusões**.

Configurações da zona confiável

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Object to scan (Exclusions)	**Exclusões de verificação** (Exclusões de verificação) Os métodos utilizados pelo KSWS e KES para selecionar objetos são diferentes. Ao migrar, o KES oferece suporte a exclusões definidas como arquivos individuais ou caminhos para arquivo/pasta. Caso o KSWS tenha exclusões configuradas como uma área predefinida ou uma URL de script, tais exclusões não serão migradas. Após a migração, é necessário adicionar essas exclusões manualmente. As exclusões como áreas predefinidas devem ser definidas nas configurações da tarefa *Verificação de malware*. As exclusões como endereços da Web de scripts devem ser adicionadas aos endereços da Web confiáveis para a Proteção Contra Ameaças da Web.
Apply also to subfolders (Exclusions)	**Incluir subpastas** (Exclusões de verificação)
Objects to detect (Exclusions)	**Tipo do objeto detectado** (Exclusões de verificação)
Exclusion usage scope (Exclusions)	**Componentes de proteção** (Exclusões de verificação) Se pelo menos um componente for selecionado no KSWS, o KES aplicará as exclusões a todos os componentes do aplicativo.
Comment (Exclusions)	**Comentário** (Exclusões de verificação)
Trusted process (Trusted process)	**Aplicativos confiáveis** Os métodos confiáveis de seleção de processos/aplicativos diferem no KSWS e no KES. Ao migrar, o KES oferece suporte a aplicativos confiáveis configurados como um caminho para o arquivo executável ou máscara. Caso o KSWS tenha processos confiáveis configurados como um hash de arquivo, esses processos confiáveis não são migrados. Após a migração, é necessário adicionar esses processos confiáveis manualmente.
Do not check file backup operations (Trusted process)	**Não monitorar a atividade do aplicativo** (Aplicativos confiáveis)

Removable drives scan

As configurações de verificação de unidades removíveis são migradas para a seção **Tarefas locais**, subseção **Verificação de unidades removíveis**.

Configurações da verificação de unidades removíveis

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Scan removable drives on connection via USB	**Ação sobre a conexão de uma unidade removível**
Scan removable drives if its stored data volume does not exceed (MB)	**Tamanho máximo da unidade removível**

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Scan with security level: • **Maximum protection** • **Recommended** • **Maximum performance**	**Ação sobre a conexão de uma unidade removível**: • **Proteção máxima**. • **Recomendado**. Os níveis de segurança do KSWS correspondem aos modos de verificação do KES da seguinte forma: • Maximum protection – Proteção máxima • Recommended – Recomendado • Maximum performance – Recomendado

User permissions for application management

O Kaspersky Endpoint Security não oferece suporte para a atribuição de permissões de acesso do usuário para gerenciamento de aplicativos e gerenciamento de serviços de aplicativos. É possível definir as configurações de acesso para usuários e grupos de usuários para gerenciar o aplicativo no Kaspersky Security Center.

User access permissions for Kaspersky Security Service management

O Kaspersky Endpoint Security não oferece suporte para a atribuição de permissões de acesso do usuário para gerenciamento de aplicativos e gerenciamento de serviços de aplicativos. É possível definir as configurações de acesso para usuários e grupos de usuários para gerenciar o aplicativo no Kaspersky Security Center.

Storages

As configurações de armazenamento do KSWS são migradas para a seção **Configurações gerais**, subseção Relatórios e Armazenamento e para a seção **Proteção Essencial Contra Ameaças**, subseção Proteção Contra Ameaças à Rede.

Configurações de armazenamento

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Backup folder	*(não migra)* O Kaspersky Endpoint Security salva cópias de backup dos arquivos na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.
Maximum Backup size (MB)	**Limitar o tamanho do backup a N MB** (**Configurações gerais** → seção **Relatórios e Armazenamento**)
Threshold value for space available (MB)	*(não migra)* O Kaspersky Endpoint Security registra o evento *O armazenamento da Quarentena está quase sem espaço* quando o limite de 50% é atingido.
Target folder for restoring objects	*(não migra)* O Kaspersky Endpoint Security restaura os arquivos na pasta original.
Quarantine folder	*(não migra)* O Kaspersky Endpoint Security salva cópias de backup dos arquivos na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.
Maximum Quarantine size (MB)	*(não migra)* O Kaspersky Endpoint Security utiliza o Backup para armazenar os objetos provavelmente infectados. Durante a migração, o Kaspersky Endpoint Security ignora as configurações de Quarentena.
Threshold value for space available (MB)	*(não migra)* O Kaspersky Endpoint Security utiliza o Backup para armazenar os objetos provavelmente infectados. Durante a migração, o Kaspersky Endpoint Security ignora as configurações de Quarentena.
Target folder for restoring objects	*(não migra)* O Kaspersky Endpoint Security restaura os arquivos na pasta original.
Unblock automatically in N	**Bloquear dispositivos de ataque por N min** (seção **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças à Rede**)

Real-time server protection

Real-Time File Protection

As configurações do KSWS Real-Time File Protection são migradas para a seção **Proteção Essencial Contra Ameaças**, subseção Proteção Contra Ameaças ao Arquivo.

Configurações de Proteção de Arquivos em Tempo Real

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Objects protection mode: • Smart mode • When run • On access • On access and modification	Modo de verificação: • **Modo inteligente**. • **Ao executar**. • **Ao acessar**. • **Ao acessar e modificar**.
Deeper analysis of launching processes	*(não migra)* O Kaspersky Endpoint Security oferece apenas um modo de análise, o modo Optimal.
Heuristic analyzer: • Light • Medium • Deep	Análise heurística: • **Verificação superficial**. • **Verificação média**. • **Verificação profunda**.
Apply Trusted Zone	*(não migra)* O Kaspersky Endpoint Security aplica a zona confiável a todos os componentes. É possível configurar as exclusões em configurações de zona confiável.
Use KSN for protection	*(não migra)* O Kaspersky Endpoint Security utiliza a KSN para todos os componentes do aplicativo.
Block access to network shared resources for the hosts that show malicious activity	*(não migra)* Por padrão, o Kaspersky Endpoint Security bloqueia o acesso aos recursos compartilhados da rede para hosts que mostram atividades maliciosas.
Launch critical areas scan when active infection is detected	*(não migra)* O Kaspersky Endpoint Security não inicia a tarefa de verificação de áreas críticas quando uma infecção ativa é detectada.
Use Kaspersky Sandbox for protection	*(não migra)* Por padrão, o Kaspersky Endpoint Security envia os objetos para verificação ao Kaspersky Sandbox.
Protection scope	Escopo de proteção
Schedule settings	*(não migra)* O Kaspersky Endpoint Security utiliza o próprio agendamento para pausar a Proteção contra ameaças ao arquivo.

KSN Usage

As configurações do KSWS para o Kaspersky Security Network são migradas para a seção **Proteção Avançada Contra Ameaças**, subseção Kaspersky Security Network.

Configurações da Kaspersky Security Network

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
I confirm that I have fully read, understood, and accept the terms of participation in Kaspersky Security Network	**Declaração da Kaspersky Security Network** O Kaspersky Endpoint Security solicita o consentimento com a Declaração da Kaspersky Security Network quando o aplicativo é instalado, uma nova política é criada ou o uso da Kaspersky Security Network é ativado.
Send data about scanned files	*(não migra)* O Kaspersky Endpoint Security envia dados sobre os arquivos verificados automaticamente se a KSN estiver ativada.
Send data about requested URLs	*(não migra)* O Kaspersky Endpoint Security envia dados sobre URLs solicitadas automaticamente se a KSN estiver ativada.
Send Kaspersky Security Network statistics	**Ativar modo KSN estendido**
Accept the terms of the Kaspersky Managed Protection Statement	*(não migra)* O Kaspersky Endpoint Security não inclui o serviço KMP.
Action to perform on KSN untrusted objects	*(não migra)* É possível configurar a Ação ao detectar ameaça nas configurações do componente de proteção e nas configurações da tarefa de Verificação.
Do not calculate checksum before sending to KSN if file size exceeds N MB	*(não migra)* É possível configurar restrições de verificação de arquivos grandes nas configurações do componente de proteção e nas configurações de tarefas de Verificação.
Use Kaspersky Security Center as KSN Proxy	**Usar o Servidor de Administração como um servidor proxy da KSN**
Schedule settings	*(não migra)* Não é possível configurar um agendamento separado para o componente. O componente está sempre ativado enquanto o Kaspersky Endpoint Security está operacional.

Traffic Security

As configurações do KSWS Traffic Security são migradas para a seção **Proteção Essencial Contra Ameaças**, Proteção Contra Ameaças da Web e subseção Proteção Contra Ameaças ao Correio seção, **Controles de Segurança**, subseção Controle da Web, seção **Configurações gerais**, subseção Configurações de rede.

Configurações de segurança de tráfego

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Apply URL-based rules	**Controle da Web** (subseção **Controle da Web**) As regras baseadas em URL são migradas para regras separadas no Kaspersky Endpoint Security.
Apply certificate-based rules	*(não migra)* O Kaspersky Endpoint Security não oferece suporte a regras baseadas em certificados.
Apply rules for web traffic category control	**Controle da Web** (subseção **Controle da Web**) As regras de bloqueio para controle de categoria de tráfego da web são migradas para uma única regra de bloqueio no Kaspersky Endpoint Security. O Kaspersky Endpoint Security ignora as regras de permissão para controle de categoria. A correspondência das categorias do KSWS e do KES está listada abaixo.
Allow access if the web page can not be categorized	*(não migra)* O Kaspersky Endpoint Security permite o acesso caso a página da web não possa ser categorizada.
Allow access to legitimate web resources that can be used to damage a protected device	*(não migra)* O Kaspersky Endpoint Security permite o acesso a recursos legítimos da web que podem ser utilizados para danificar o dispositivo protegido.
Allow access to legitimate advertisement	*(não migra)* É possível gerenciar o acesso a anúncios legítimos utilizando a categoria de recursos da Web *Banners* nas configurações do controle da Web.

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Operation mode: • **Driver Interceptor** • **Redirector** • **External Proxy**	*(não migra)* O Kaspersky Endpoint Security é compatível apenas com o modo Driver Interceptor.
ICAP-service connection settings	*(não migra)* O Kaspersky Endpoint Security não oferece suporte à proteção de armazenamento de rede ICAP.
Check safe connections through the HTTPS protocol	Modo **Verificar conexões criptografadas** / **Sempre verificar conexões criptografadas** (subseção **Configurações de rede**)
Use TLS protocol version	*(não migra)* O Kaspersky Endpoint Security verifica o tráfego de rede criptografado transmitido através dos seguintes protocolos: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Também é possível bloquear as conexões SSL 2.0 em configurações de verificação de conexões criptografadas.
Do not trust web-servers with invalid certificate	**Endereço** (subseção **Configurações de rede**)
Intercept ports (Interception area)	**Portas monitoradas** (subseção **Configurações de rede**) Durante a migração, o KES limpa as caixas de seleção **Monitorar todas as portas de aplicativos na lista recomendada pela Kaspersky** e **Monitorar todas as portas dos aplicativos especificados**.
Exclude ports (Interception area)	*(não migra)*
Exclude IP addresses (Interception area)	**Configurar endereços confiáveis** (subseção **Configurações de rede**)
Exclude processes (Interception area)	**Configurar aplicativos confiáveis** (subseção **Configurações de rede**) Durante a migração, o KES define as seguintes configurações para o aplicativo confiável: • A caixa de seleção **Não verificar o tráfego de rede** é marcada. O KES não verifica o tráfego de rede em busca de nenhum endereço IP remoto e nenhuma porta. • As outras caixas de seleção nas configurações do aplicativo confiável são desmarcadas.
Security port	*(não migra)*
Use malicious URL database to scan web links	**Verificar se o endereço está no banco de dados de endereços da Web maliciosos** (subseção **Proteção Contra Ameaças da Web**)
Use anti-phishing database to scan web pages	**Verificar se o endereço está no banco de dados de endereços da Web de phishing** (subseção **Proteção Contra Ameaças da Web**)
Use KSN for protection	*(não migra)* O Kaspersky Endpoint Security utiliza a KSN para todos os componentes do aplicativo.
Use Trusted Zone	*(não migra)* O Kaspersky Endpoint Security aplica a zona confiável a todos os componentes. É possível configurar as exclusões em configurações de zona confiável.
Use heuristic analyzer	**Usar a análise heurística** (subseções **Proteção Contra Ameaças da Web** e **Proteção Contra Ameaças ao Correio**)
Security level	*(não migra)* O Kaspersky Endpoint Security tem seus próprios níveis de segurança para os componentes Proteção contra ameaças da web e Proteção contra ameaças ao correio. Por padrão, o Kaspersky Endpoint Security define o nível de segurança recomendado.
Enable mail threat protection	**Proteção Contra Ameaças ao Correio** (subseção **Proteção Contra Ameaças ao Correio**) **Conectar a extensão do Microsoft Outlook** **Apenas mensagens recebidas** (Escopo de proteção) **Verificar ao receber** (Proteção de e-mail)
Schedule settings	*(não migra)* Não é possível configurar um agendamento separado para o componente. O componente está sempre ativado enquanto o Kaspersky Endpoint Security está operacional.

Exploit Prevention

As configurações do KSWS Exploit Prevention são migradas para a seção **Proteção Avançada Contra Ameaças**, subseção **Prevenção de Exploits**.

Configurações de Prevenção de exploit

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Prevent vulnerable processes exploit: • **Terminate on exploit** • **Notify only**	**Na detecção de exploit**: • **Bloquear**. • **Informar**.
Notify about abused processes via Terminal Service	*(não migra)* O Kaspersky Endpoint Security não oferece suporte a serviços de terminal.
Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled	*(não migra)* O Kaspersky Endpoint Security evita constantemente o exploit de processos vulneráveis.
Protected processes	**Ativar a proteção da memória de processos do sistema** O Kaspersky Endpoint Security não é compatível com a seleção de processos protegidos. Só é possível ativar a proteção de memória de processos do sistema.
Exploit prevention techniques: • **Apply all available exploit prevention techniques** • **Apply selected exploit prevention techniques**	*(não migra)* O Kaspersky Endpoint Security aplica todas as técnicas de prevenção de exploit disponíveis.

Network Threat Protection

As configurações do KSWS Network Threat Protection são migradas para a seção **Proteção Essencial Contra Ameaças**, subseção **Proteção Contra Ameaças à Rede**.

Configurações de Proteção contra ameaças à rede

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Operation mode: • **Pass-through** • **Only inform about network attacks** • **Block connections when attack is detected**	**Proteção Contra Ameaças à Rede** Caso a opção **Pass-through** estiver selecionada, a Proteção Contra Ameaças à Rede será desativada. Caso o modo **Only inform about network attacks** ou o modo **Block connections when attack is detected** seja selecionado, a Proteção Contra Ameaças à Rede será ativada. O Kaspersky Endpoint Security sempre funciona no modo **Block connections when attack is detected**.
Do not stop traffic analysis when the task is not running	*(não migra)* O Kaspersky Endpoint Security analisa o tráfego continuamente se o componente estiver ativado.
Do not control excluded IP addresses	**Exclusões**
Schedule settings	*(não migra)* Não é possível configurar um agendamento separado para o componente. O componente está sempre ativado enquanto o Kaspersky Endpoint Security está operacional.

Script Monitoring

O Kaspersky Endpoint Security não oferece suporte ao componente Monitoramento de scripts. O monitoramento de scripts é tratado por outros componentes, por exemplo, pela Proteção AMSI.

Website categories

O Kaspersky Endpoint Security não oferece suporte a todas as categorias do Kaspersky Security for Windows Server. As categorias que não existem no Kaspersky Endpoint Security não são migradas. Portanto, as regras de classificação de recursos da Web com categorias não compatíveis não são migradas.

Categorias do Kaspersky Security for Windows Server	Categorias do Kaspersky Endpoint Security for Windows
Wargaming	Videogames
Abortion	*(não migra)*
Lotteries (extended)	Jogos de azar, loterias, apostas
Alcohol	Álcool, tabaco, drogas
Anonymous proxy servers	Anonimizadores
Anorexia	*(não migra)*
Rentals for real estate	*(não migra)*
Audio, video and software	Software, áudio, vídeo
Banks	Bancos
Blogs	Blogs
Military	Armas, explosivos, conteúdo militar
For children	*(não migra)*
Discrimination	Violência, intolerância
Home and family	*(não migra)*
Hosting and domain services	Comunicações via Internet
Pets and animals	*(não migra)*
Law and politics	Proibidos por leis regionais
Restricted by Roskomnadzor (RF)	Proibido segundo as leis da Federação Russa
Restricted by Federal Law 436 (RF)	Proibido segundo as leis da Federação Russa
Restricted by RF legislation	Proibido segundo as leis da Federação Russa
Restricted by global legislation	Proibidos por leis regionais
Adult dating	Conteúdo adulto
Internet services	*(não migra)*
Sex shops	Conteúdo adulto
Information technologies	*(não migra)*
Casinos, card games	Jogos de azar, loterias, apostas
Books and writing	*(não migra)*
Computer games	Videogames
Health and beauty	*(não migra)*
Culture and society	*(não migra)*
LGBT	Conteúdo adulto
Lotteries	Jogos de azar, loterias, apostas
Medicine	*(não migra)*
Fashion	*(não migra)*
Music	*(não migra)*
Drugs	Álcool, tabaco, drogas
Violence	Violência, intolerância
Discontent	*(não migra)*
Illegal drugs	Álcool, tabaco, drogas
Hate and discrimination	Violência, intolerância

Categorias do Kaspersky Security for Windows Server	Categorias do Kaspersky Endpoint Security for Windows
Obscene vocabulary	Linguagem explícita, obscenidades
Lingerie	Conteúdo adulto
News	Mídia de notícias
Nudism	Conteúdo adulto
Education	*(não migra)*
Online shopping	Lojas on-line
All communication media	Comunicações via Internet
Payment by credit cards	Sistemas de pagamento
Online shopping (own payment system)	Lojas on-line
Online encyclopedias	*(não migra)*
Online banking	Bancos
Weapons	Armas, explosivos, conteúdo militar
Fishing and hunting	*(não migra)*
Payment systems	Sistemas de pagamento
Job search	Busca de empregos
Search engines	*(não migra)*
Police decision (JP)	Proibido segundo as leis do Japão
Trusted by KPSN	*(não migra)*
Untrusted by KPSN	*(não migra)*
Porn	Conteúdo adulto
Media hosting and streaming	Mídia de notícias
Web Mail	E-mail baseado na Web
Traveling	*(não migra)*
TV and radio	Mídia de notícias
Teasers and ads services	Banners
Religion	Religiões, associações religiosas
Restaurants, cafe and food	*(não migra)*
Dating sites	Sites de namoro
Sex education	Conteúdo adulto
Social networks	Redes sociais
Sport	*(não migra)*
Betting	Jogos de azar, loterias, apostas
Suicide	Violência, intolerância
Tobacco	Álcool, tabaco, drogas
Torrents	Torrents
Mentioned in Federal list of extremists (RF)	Proibido segundo as leis da Federação Russa
File sharing	Compartilhamento de arquivos
Pharmacy	*(não migra)*
Hobby and entertainment	*(não migra)*
Chats and forums	Chats, fóruns e mensagens instantâneas
Schools and universities pages	*(não migra)*

Categorias do Kaspersky Security for Windows Server	Categorias do Kaspersky Endpoint Security for Windows
Astrology and esoterica	*(não migra)*
Extremism and racism	Violência, intolerância
E-commerce	Lojas on-line
Erotic	Conteúdo adulto
Humor	*(não migra)*

Local activity control

Applications Launch Control

As configurações de Controle de aplicativos do KSWS são migradas para a seção **Controles de Segurança**, subseção **Controle de aplicativos**.

Configurações do Controle de Inicialização de Aplicativos

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Operation mode: • **Statistics only** • **Active**	**Ação** (controle de aplicativos): • **Testar regras**. • **Aplicar regras**.
Repeat action taken for the first file launch on all the subsequent launches for this file	*(não migra)* O Kaspersky Endpoint Security verifica o aplicativo sempre que ele tenta executar.
Deny the command interpreters launch with no command to execute	*(não migra)* O Kaspersky Endpoint Security permite a execução de interpretadores de comandos caso não sejam proibidos pelo Controle de aplicativos.
Rules	**Regras de Controle de aplicativos** *(compatível com limitações)* O Kaspersky Endpoint Security 11.11.0 apresenta compatibilidade com a migração de Regras de Controle de Inicialização de Aplicativos. A funcionalidade de migração de Regra de Controle Inicialização de Aplicativos tem algumas limitações. Por padrão, o Controle de Inicialização de Aplicativos do KSWS inclui duas regras: • **Allow scripts and MSI by OS-trusted certificate** • **Allow executable by OS-trusted certificate** Se pelo menos uma regra de origem do KSWS tiver o tipo **Allow**, o KES cria uma nova regra de permissão durante a migração, **Aplicativos com certificados raiz confiáveis**. Ou seja, o Controle de Aplicativos do KES usa uma única regra para permitir a execução de scripts confiáveis, pacotes MSI e arquivos executáveis. Se ambas as regras de origem do KSWS tiverem o tipo **Deny**, o KES não adiciona regras para gerenciar aplicativos com certificados raiz confiáveis.
Apply rules to executable files	*(não migra)* O escopo de aplicação da regra não pode ser configurado nas configurações do Controle de Aplicativos do KES. O Controle de Aplicativos do KES aplica regras a todos os tipos de arquivos: arquivos executáveis, scripts e pacotes MSI. Se todos os tipos de arquivos estiverem incluídos no escopo de aplicação da regra no KSWS, o KES transferirá as regras do KSWS durante a migração. Se algum tipo de arquivo for excluído do escopo de aplicação da regra no KSWS, o KES também transferirá as regras do KSWS durante a migração, mas **Testar regras** será selecionado como a ação de Controle de Aplicativos.
Monitor loading of DLL modules	**Monitorar o carregamento de módulos DLL (aumenta significativamente a carga no sistema)**
Apply rules to scripts and MSI packages	*(não migra)* O escopo de aplicação da regra não pode ser configurado nas configurações do Controle de Aplicativos do KES. O Controle de Aplicativos do KES aplica regras a todos os tipos de arquivos: arquivos executáveis, scripts e pacotes MSI. Se todos os tipos de arquivos estiverem incluídos no escopo de aplicação da regra no KSWS, o KES transferirá as regras do KSWS durante a migração. Se algum tipo de arquivo for excluído do escopo de aplicação da regra no KSWS, o KES transferirá as regras do KSWS durante a migração, mas **Testar regras** será selecionado como a ação de Controle de Aplicativos.

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Deny applications untrusted by KSN	*(não migra)* O Kaspersky Endpoint Security não leva em consideração a reputação dos aplicativos e permite ou nega a execução de aplicativos de acordo com as regras.
Allow applications trusted by KSN	Durante a migração, o KES adiciona uma nova regra de permissão. A categoria KL **Outro software\Aplicativos, confiável de acordo com a reputação no KSN** é especificada como a condição de acionamento da regra.
Users and / or user groups allowed to run applications trusted by KSN	**Usuários e seus direitos** é uma regra de permissão do Controle de aplicativos que inclui a categoria KL **Outro software\Aplicativos, confiável de acordo com a reputação no KSN**.
Automatically allow software distribution via applications and packages listed	O Controle de Distribuição de Software funciona de forma diferente no KSWS e no KES. Durante a migração, o KES adiciona novas regras de permissão para aplicativos que possuem distribuição automática de software permitida. O hash do arquivo é especificado como a condição de acionamento da regra.
Always allow software distribution via Windows Installer	O Controle de Distribuição de Software funciona de forma diferente no KSWS e no KES. Durante a migração, o KES adiciona novas regras de permissão para aplicativos que têm a distribuição automática de software permitida (**Software distribution applications and packages allowed**). O hash do arquivo é especificado como a condição de acionamento da regra. Nas propriedades da conta, a caixa de seleção **Atualizadores confiáveis** estará marcada.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(não migra)*
Software distribution applications and packages allowed	O Controle de Distribuição de Software funciona de forma diferente no KSWS e no KES. Durante a migração, o KES adiciona novas regras de permissão para aplicativos que possuem distribuição automática de software permitida. O hash do arquivo é especificado como a condição de acionamento da regra. Nas propriedades da conta, a caixa de seleção **Atualizadores confiáveis** estará marcada.
Schedule settings	*(não migra)* Caso uma programação seja configurada para o componente nas configurações do KSWS, o componente Controle de Aplicativos será ativado na migração. Caso uma programação não seja configurada para o componente nas configurações do KSWS, o Controle de Aplicativos será desabilitado na migração. Não é possível configurar um agendamento separado para o componente. O componente está sempre ativado enquanto o Kaspersky Endpoint Security está operacional.

Device Control

As configurações de Controle de dispositivos do KSWS são migradas para a seção **Controles de Segurança**, subseção **Controle de dispositivos**.

Configurações do Controle de dispositivos

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Operation mode: • **Active** • **Statistics only**	*(não migra)* O Controle de Aplicativos opera no modo *Active*. As estatísticas de conexão de dispositivos são fornecidas continuamente pela Auditoria.
Allow using all external devices when the Device Control task is not running	*(não migra)* O Controle de dispositivos está sempre ativado durante a execução do Kaspersky Endpoint Security.
Device Control rules	**Dispositivos confiáveis** Durante a migração, o Kaspersky Endpoint Security ignora as regras do KSWS desabilitadas.
Schedule settings	*(não migra)* O Kaspersky Endpoint Security utiliza o próprio agendamento para obter acesso a certos tipos de dispositivos.

Network-Attached Storages Protection

RPC Network Storage Protection

O Kaspersky Endpoint Security não oferece suporte a componentes de Proteção de armazenamento de rede. Caso precise desses componentes, é possível continuar usando o Kaspersky Security for Windows Server.

ICAP Network Storage Protection

O Kaspersky Endpoint Security não oferece suporte a componentes de Proteção de armazenamento de rede. Caso precise desses componentes, é possível continuar usando o Kaspersky Security for Windows Server.

Anti-Cryptor for NetApp

O Kaspersky Endpoint Security não oferece suporte ao Anti-Cryptor for NetApp. A funcionalidade do Anti-Cryptor é fornecida por outros componentes do aplicativo, como a Detecção de comportamento.

Network activity control

Firewall Management

O Kaspersky Endpoint Security não oferece suporte ao Gerenciamento de Firewall KSWS. As funções do KSWS Firewall são executadas pelo Firewall no nível do sistema. Após a migração, é possível configurar o firewall do Kaspersky Endpoint Security.

Anti-Cryptor

As configurações do Network Anti-Cryptor são migradas para a seção **Proteção Avançada Contra Ameaças**, subseção **Detecção de Comportamento**.

Configurações do Anticryptor

Configurações do KSWS	Configurações do KES
Operation mode: • **Statistics only** • **Active**	**Na detecção de criptografia externa de pastas compartilhadas**: • **Informar**. • **Bloquear**.
Heuristic analyzer	*(não migra)* O Kaspersky Endpoint Security não utiliza a Análise Heurística para a Detecção de comportamento.
Configuration of protection scope: • **All shared network folders on the protected device** • **Only specified shared folders**	*(não migra)* O Kaspersky Endpoint Security impede a criptografia de todas as pastas de rede compartilhadas do computador protegido.
Exclusions	*(não migra)* O Kaspersky Endpoint Security tem suas próprias exclusões para o componente Detecção de Comportamento. É possível adicionar as exclusões manualmente após a migração.
Schedule settings	*(não migra)* Não é possível configurar um agendamento separado para o componente. O componente está sempre ativado enquanto o Kaspersky Endpoint Security está operacional.

System Inspection

File Integrity Monitor

As configurações do Monitor de integridade de arquivos do KSWS são migradas para a seção **Controles de Segurança**, subseção **Monitor de integridade do sistema**.

Configurações do Monitor de Integridade de Arquivos

Configurações do KSWS	Configurações do KES
Log information about file operations that appear during the monitor interruption period	*(não migra)* O Kaspersky Endpoint Security não registra eventos para operações de arquivo realizadas durante o período de interrupção do monitor.
Block attempts to compromise the USN log	*(não migra)* O Kaspersky Endpoint Security não bloqueia tentativas de comprometer o log USN.
Monitoring scope	**Escopo de monitoramento** → **Arquivo** *(compatível com limitações)* Os registros de escopo de monitoramento desativados não são migrados para o KES. O Kaspersky Endpoint Security adiciona apenas registros ativos ao escopo de monitoramento.
Trusted users	**Usuários e/ou grupos de usuários confiáveis**
File operation markers	**Marcadores de operação de arquivo**
Calculate checksum for the file if possible	**Hashing**
Exclusions	**Exclusões** → **Arquivo**

Log Inspection

As configurações de inspeção de log do KSWS são migradas para a seção **Controles de Segurança**, subseção **Inspeção de log**.

Configurações de Inspeção de Log

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Apply custom rules for log inspection	*(não migra)* O Kaspersky Endpoint Security aplica todas as regras personalizadas ativas.
Custom rules	**Regras personalizadas** A regra predefinida **A service was installed in the system (for Server 2003 OS)** não é migrada para o KES.
Apply predefined rules for log inspection	*(não migra)* O Kaspersky Endpoint Security aplica todas as regras predefinidas ativas.
Predefined rules	**Regras predefinidas**
Password brute-force detection	**Detecção de ataque de força bruta**
Network logon detection	**Detecção de logon na rede**
Exclusions (IP addresses)	**Exclusões** (Endereço IP)
Exclusions (users)	**Exclusões** (Usuários)
Schedule settings	*(não migra)* Não é possível configurar um agendamento separado para o componente. O componente está sempre ativado enquanto o Kaspersky Endpoint Security está operacional.

Logs and notifications

Task logs

As configurações de logs do KSWS são migradas para a seção **Configurações gerais**, subseções **Interface** e **Relatórios e armazenamento**.

Configurações de logs

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Event logging	**Notificações** (subseção **Interface**)
Logs folder	*(não migra)* O Kaspersky Endpoint Security salva os relatórios na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\Report`.
Remove task logs older than N day(s)	*(não migra)* É possível configurar o período de armazenamento para relatórios KES em **Configurações gerais**, **Relatórios e armazenamento**.
Remove from the audit log events N day(s)	*(não migra)* O Kaspersky Endpoint Security aplica limitações de armazenamento de relatórios a todos os relatórios, incluindo relatórios de auditoria do sistema.
SIEM Integration	*(não migra)* É possível configurar a integração SIEM no Kaspersky Security Center.

Event notifications

As configurações de notificações do KSWS são migradas para a seção **Configurações gerais**, subseção **Interface**.

Configurações de notificações

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Notifications	**Notificações**
Notify users: • **By using terminal service** • **By using Windows Messenger Service command**	*(não migra)* O Kaspersky Endpoint Security não oferece suporte à modificação do texto de notificações. O Kaspersky Endpoint Security exibe notificações padrão.
Notify administrators: • **By using Windows Messenger Service command** • **By running executable file** • **By sending email**	Apenas as configurações de notificação por e-mail são migradas para o Kaspersky Endpoint Security – **Configurações de notificação por e-mail** (bloco **Notificações**). Não há suporte para outros métodos de notificação de administradores.
Application database is out of date	**Envie a notificação "Bancos de dados desatualizados" se os bancos de dados não tiverem sido atualizados**
Application database is extremely out of date	**Envie a notificação "Bancos de dados muito desatualizados" se os bancos de dados não tiverem sido atualizados**
Critical areas scan has not been performed for a long time	*(não migra)* O Kaspersky Endpoint Security gera um evento perdido de Verificação de áreas críticas após três dias.

Interaction with Administration Server

As configurações de interação do KSWS Administration Server são migradas para a seção **Configurações gerais**, subseção **Relatórios e armazenamento**.

Configurações de interação do Servidor de Administração

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Quarantined files	**Arquivos da Quarentena**
Backed up files	**Arquivos de Backup**
Blocked hosts	*(não migra)* O Kaspersky Endpoint Security envia automaticamente dados sobre hosts bloqueados.

Tasks

Activating the application

O Kaspersky Endpoint Security não é compatível com a tarefa (KSWS) *Application activation*. É possível criar uma tarefa (KES) *Adicionar chave*, adicionar uma chave de licença ao Pacote de instalação, ou ativar a distribuição automática de chave da licença.

Copying Updates

As configurações da tarefa *Copying Updates* (KSWS) são migradas para a tarefa *Atualização de bancos de dados e módulos do aplicativo* (KES).

Configurações da tarefa Copiar atualizações

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Fonte de atualização**: • **Kaspersky Security Center**. • **Servidores de atualização Kaspersky**. • **Especificado pelo usuário**.
Use Kaspersky update servers if specified servers are not available	*(não migra)* O Kaspersky Endpoint Security permite selecionar várias fontes de atualização, incluindo os servidores de atualização da Kaspersky. Caso a primeira fonte de atualização não esteja disponível, o Kaspersky Endpoint Security permite obter as atualizações a partir de outra fonte da lista.
Use proxy server settings to connect to Kaspersky update servers	*(não migra)* O Kaspersky Endpoint Security utiliza o servidor proxy para todos os componentes. Também é possível configurar a conexão do servidor proxy nas opções de rede do aplicativo.
Use proxy server settings to connect to other servers	*(não migra)* O Kaspersky Endpoint Security utiliza o servidor proxy para todos os componentes. Também é possível configurar a conexão do servidor proxy nas opções de rede do aplicativo.
Copying updates settings: • **Copy database updates** • **Copy critical software modules updates** • **Copy database updates and critical updates of application modules**	*(não migra)* O Kaspersky Endpoint Security copia atualizações de banco de dados e atualizações críticas de módulos de aplicativos como um único pacote.
Folder for local storage of copied updates	**Copiar atualizações para a pasta**

Baseline File Integrity Monitor

As configurações da tarefa *Baseline File Integrity Monitor* (KSWS) são migradas para a tarefa *Verificação de integridade do sistema* e para a seção de política de **Controles de Segurança**, subseção **Monitor de integridade do sistema**.

Configurações da tarefa do Monitor de integridade de arquivos de linha de base

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Hash calculation algorithm: • **MD5** • **SHA256**.	*(não migra)* O Kaspersky Endpoint Security usa o algoritmo SHA256 para o cálculo da soma de verificação.
Scan scope	**Escopo de monitoramento** (subseção **Monitor de integridade do sistema**)

Database Update

As configurações da tarefa *Database Update* (KSWS) são migradas para a tarefa *Atualização de bancos de dados e módulos do aplicativo* (KES).

Configurações da tarefa Atualização do banco de dados

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Fonte de atualização**: • **Kaspersky Security Center**. • **Servidores de atualização Kaspersky**. • **Especificado pelo usuário**.
Use Kaspersky update servers if specified servers are not available	*(não migra)* O Kaspersky Endpoint Security permite selecionar várias fontes de atualização, incluindo os servidores de atualização da Kaspersky. Caso a primeira fonte de atualização não esteja disponível, o Kaspersky Endpoint Security permite obter as atualizações a partir de outra fonte da lista.
Use proxy server settings to connect to Kaspersky update servers	*(não migra)* O Kaspersky Endpoint Security utiliza o servidor proxy para todos os componentes. Também é possível configurar a conexão do servidor proxy nas opções de rede do aplicativo.
Use proxy server settings to connect to other servers	*(não migra)* O Kaspersky Endpoint Security utiliza o servidor proxy para todos os componentes. Também é possível configurar a conexão do servidor proxy nas opções de rede do aplicativo.
Lower the load on the disk I/O	*(não migra)*

Software modules updates

As configurações da tarefa *Software Modules Update* (KSWS) são migradas para a tarefa *Atualização de bancos de dados e módulos do aplicativo* (KES).

As configurações da tarefa de atualização dos módulos de software

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Fonte de atualização**: • **Kaspersky Security Center**. • **Servidores de atualização Kaspersky**. • **Especificado pelo usuário**.
Use Kaspersky update servers if specified servers are not available	*(não migra)* O Kaspersky Endpoint Security permite selecionar várias fontes de atualização, incluindo os servidores de atualização da Kaspersky. Caso a primeira fonte de atualização não esteja disponível, o Kaspersky Endpoint Security permite obter as atualizações a partir de outra fonte da lista.
Use proxy server settings to connect to Kaspersky update servers	*(não migra)* O Kaspersky Endpoint Security utiliza o servidor proxy para todos os componentes. Também é possível configurar a conexão do servidor proxy nas opções de rede do aplicativo.

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Use proxy server settings to connect to other servers	*(não migra)* O Kaspersky Endpoint Security utiliza o servidor proxy para todos os componentes. Também é possível configurar a conexão do servidor proxy nas opções de rede do aplicativo.
Copy and install critical software modules updates	**Instalar atualizações críticas e aprovadas**
Only check for critical software updates available	*(não migra)* O Kaspersky Endpoint Security verifica continuamente a disponibilidade de atualizações críticas para os módulos de aplicativos.
Allow operating system restart	*(não migra)* O Kaspersky Endpoint Security solicita ao usuário a permissão para reiniciar o computador.
Receive information about available scheduled software modules updates	*(não migra)* O Kaspersky Endpoint Security exibe notificações sobre atualizações de módulos de software.

Rollback of Application Database Update

As configurações da tarefa *Rollback of Application Database Update* (KSWS) são migradas para a tarefa *Reversão de atualização* (KES). A nova tarefa (KES) *Reversão de atualização* tem um agendamento de início de tarefa – *Manualmente*.

On-Demand Scan

As configurações da tarefa *On-Demand Scan* (KSWS) são migradas para a tarefa *Verificação de malware* (KES).

Configurações da tarefa de Verificação de vírus

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Scan scope	**Escopo da verificação**
Protection level: • **Maximum protection** • **Recommended** • **Maximum performance**	**Nível de segurança**: • **Alto**. • **Recomendado**. • **Baixo**. As configurações de nível de segurança são diferentes no KSWS e no KES.
Objects to scan: • **All objects** • **Objects scanned by format** • **Objects scanned according to list of extensions specified in anti-virus database** • **Objects scanned by specified list of extensions**	**Tipos de arquivos**: • **Todos os arquivos**. • **Arquivos verificados por formato**. • **Arquivos verificados por extensão**. O Kaspersky Endpoint Security não permite a criação de listas de extensão personalizadas. O Kaspersky Endpoint Security substitui o valor **Objects scanned by specified list of extensions** pelo valor **Arquivos verificados por extensão**.
Subfolders	**Incluir subpastas**
Subfiles	*(não migra)*
Scan disk boot sectors and MBR	*(não migra)*
Scan alternate NTFS streams	*(não migra)*
Scan only new and modified files	**Verificar somente arquivos novos e alterados**
Scan of compound objects: • **All archives** • **All SFX archives** • **All email databases** • **All packed objects** • **All plain email** • **All embedded OLE objects**	**Verificação de arquivos compostos**: • **Verificar arquivos compactados**. • **Verificar arquivos compactados protegidos por senha**. • **Verificar pacotes de distribuição**. • **Verificar arquivos de formato de e-mail**. • **Verificar arquivos de formatos do Microsoft Office**.

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Action to perform on infected and other objects: • Disinfect • Disinfect. Remove if disinfection fails • Remove • Perform recommended action • Notify only	Ação ao detectar ameaça: • Desinfectar e excluir se a desinfecção falhar. • Desinfectar e informar se a desinfecção falhar. • Informar.
Action to perform on probably infected objects: • Quarantine • Remove • Perform recommended action • Notify only	*(não migra)* O Kaspersky Endpoint Security aplica a ação caso alguma ameaça seja detectada.
Perform actions depending on the type of object detected	*(não migra)*
Entirely remove compound file that cannot be modified by the application in case of embedded object detection	*(não migra)*
Exclude files	*(não migra)* O Kaspersky Endpoint Security aplica a zona confiável a todos os componentes. É possível configurar as exclusões em configurações de zona confiável.
Do not detect	*(não migra)*
Stop scanning if it takes longer than N sec	Ignorar arquivos verificados por mais de N seg
Do not scan compound objects larger than N MB	Não descompactar arquivos compostos grandes
Use iSwift technology	Tecnologia iSwift
Use iChecker technology	Tecnologia iChecker
Action on the offline files: • Do not scan • Scan resident part of file only • Scan entire file • Only if the file has been accessed within the specified period (days) • Do not copy file to a local hard drive, if possible	*(não migra)* O Kaspersky Endpoint Security verifica os arquivos autônomos em sua totalidade.

Application Integrity Check

As configurações da tarefa *Application Integrity Control* (KSWS) são migradas para a tarefa *Verificação de integridade do aplicativo* (KES).

Rule Generator for Applications Launch Control

O Kaspersky Endpoint Security não oferece suporte à tarefa do *Applications Launch Control Generator*. É possível gerar regras nas configurações do Controle de aplicativos.

Rule Generator for Device Control

O Kaspersky Endpoint Security não oferece suporte à tarefa do *Rule Generator for Device Control*. É possível gerar regras de acesso nas configurações do Controle de dispositivos.

Migração de componentes do KSWS

Antes da instalação, o Kaspersky Endpoint Security verifica o computador para confirmar se há algum aplicativo da Kaspersky. Caso o Kaspersky Security for Windows Server esteja instalado no computador, o KES detecta o conjunto de componentes do KSWS instalados e seleciona os mesmos componentes para instalação.

Os componentes do KES que o KSWS não possui são instalados da seguinte forma:

- A Proteção AMSI, a Prevenção de Intrusão do Host e o Mecanismo de Remediação são instalados com as configurações padrão.
- Os componentes de Prevenção contra ataque BadUSB, Controle Adaptativo de Anomalias, Criptografia de dados e Detection and Response são ignorados.

Quando instalado remotamente, o aplicativo KES ignora o conjunto de componentes KSWS instalados. O instalador instala os componentes selecionados nas propriedades do pacote de instalação. Depois da instalação do Kaspersky Endpoint Security e migração das políticas e tarefas, as configurações do KES são definidas de acordo com as configurações do KSWS.

Migrando tarefas e políticas do KSWS

É possível migrar as configurações da política e da tarefa de KSWS das seguintes maneiras:

- Utilização do Assistente de Conversão de Políticas e Tarefas em Lotes (ou "Assistente de migração").

  O Assistente de Migração para KSWS está disponível apenas no Console de Administração (MMC). As configurações de política e tarefa não podem ser migradas no Web Console e Cloud Console.

  O assistente de conversão em lote funciona de forma diferente para diferentes versões do Kaspersky Security Center. Recomendamos atualizar a solução para a versão 14.2 ou superior. Nesta versão do Kaspersky Security Center, o assistente de conversão em lote de políticas e tarefas permite migrar as políticas para um perfil em vez de migrar para uma política. Nesta versão do Kaspersky Security Center, o assistente de conversão em lote de políticas e tarefas também permite a migração de uma gama mais ampla de configurações de política.

- Uso do Assistente de Nova Política do Kaspersky Endpoint Security for Windows.

  O Assistente de Nova Política permite criar uma política do KES de acordo com uma política do KSWS.

Os procedimentos de migração de política KSWS são diferentes ao usar o assistente de migração e o assistente de nova política.

Assistente de conversão de políticas e tarefas em lotes

O assistente de migração transfere as configurações de política KSWS para o perfil da política em vez das configurações de política KES. O *perfil da política* é um conjunto de configurações de política ativado em um computador caso o computador atenda às regras de ativação configuradas. A tag do dispositivo `UpgradedFromKSWS` é selecionada como o critério de acionamento do perfil da política. O Kaspersky Security Center adiciona automaticamente a tag `UpgradedFromKSWS` para todos os computadores nos quais o KES é instalado sobre o KSWS usando a tarefa de instalação remota. Caso tenha escolhido um método de instalação diferente, será possível atribuir a tag aos dispositivos manualmente.

Para adicionar uma tag em um dispositivo:

1. Criar uma nova tag para servidores – `UpgradedFromKSWS`.

   Para obter mais detalhes sobre a criação de tags para dispositivos, consulte a ajuda do Kaspersky Security Center.

2. Criar um novo grupo de administração no console do Kaspersky Security Center e adicionar os servidores aos quais deseja atribuir a tag nesse grupo.

   É possível agrupar servidores usando a ferramenta de seleção. Para obter mais detalhes sobre o funcionamento com seleções, consulte a ajuda do Kaspersky Security Center.

3. Selecionar todos os servidores do grupo de administração no console do Kaspersky Security Center, abrir as propriedades dos servidores selecionados e atribuir a tag.

Caso esteja migrando diversas políticas KSWS, cada política será convertida em um perfil dentro de uma política abrangente. Caso a política KSWS já contenha perfis, esses perfis também serão migrados como perfis. Como resultado, uma única política que inclui perfis correspondentes a todas as políticas KSWS será obtida.

Como usar o assistente de conversão de políticas e tarefas em lotes para migrar as configurações de tarefa e política do KSWS

1. No Console de administração, 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**.

O Assistente de Conversão de Políticas e Tarefas em Lotes será iniciado. Siga as instruções do Assistente.

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

Nesta etapa, é preciso selecionar o Kaspersky Endpoint Security for Windows. Vá para a próxima etapa.

Etapa 2. Conversão de políticas

O assistente de migração cria perfis da política KSWS dentro de uma política KES. Selecionar as políticas do Kaspersky Security for Windows Server que deseja converter para perfis da política. Vá para a próxima etapa.

O Assistente de Migração começará a converter as políticas. Os nomes dos novos perfis da política corresponderão às políticas KSWS originais.

Etapa 3. Relatório de migração de política

O assistente de migração cria um relatório de migração de política. O relatório de migração de política contém a data e a hora em que as políticas foram convertidas, o nome da política KSWS original, o nome da política KES de destino e o nome do novo perfil da política.

Etapa 4. Conversão de tarefas

O Assistente de migração cria novas tarefas para o Kaspersky Endpoint Security for Windows. Na lista de tarefas, selecione as tarefas do KSWS que deseja criar para o Kaspersky Endpoint Security. Novas tarefas serão nomeadas *<nome da tarefa do KSWS> (convertido)*. Vá para a próxima etapa.

Etapa 5. Conclusão do Assistente

Conclua o assistente. Como resultado, o assistente faz o seguinte:

- Novos perfis da política são adicionados na política do Kaspersky Endpoint Security.

  A política inclui perfis com as configurações do Kaspersky Security for Windows Server. A nova política possui o status *Ativo*. O Assistente deixa as políticas do KSWS inalteradas.

- Cria novas tarefas do Kaspersky Endpoint Security.

  As novas tarefas são cópias das tarefas do KSWS. O assistente deixa as tarefas do KSWS inalteradas.

O novo perfil da política com as configurações KSWS será nomeado *UpgradedFromKSWS <Nome da política do Kaspersky Security for Windows Server>*. Nas propriedades do perfil, o assistente de migração seleciona automaticamente a tag do dispositivo `UpgradedFromKSWS` como critério de acionamento. Assim, as configurações do perfil da política são aplicadas nos servidores automaticamente.

Assistente para criar uma política de acordo com uma política KSWS

Quando uma política KES é criada de acordo com uma política KSWS, o assistente transfere adequadamente as configurações para a nova política. Ou seja, uma política KES corresponderá a uma política KSWS. O assistente não converte a política em um perfil.

Como usar o Assistente de Nova Política para migrar as configurações de política do KSWS

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos gerenciados** da árvore do Console de Administração, selecione a pasta com o nome do grupo de administração a que pertence o computador cliente desejado.
3. No espaço de trabalho, selecione a guia **Políticas**.
4. Clique **Nova política**.

   O Assistente de Políticas é iniciado.
5. Siga as instruções do Assistente de Políticas.

Etapa 1. Selecionar o aplicativo para criar a política de grupo

Selecione o aplicativo **Kaspersky Endpoint Security for Windows (14.2)**.

Etapa 2. Nomear a política de grupo

Insira um nome para a política de grupo, por exemplo, *Política para o escritório*.

Marque a caixa de seleção **Usar as configurações de política para uma versão anterior do aplicativo**. Clique em **Procurar** e selecione a política do KSWS.

Etapa 3. Participação na Kaspersky Security Network

Leia e aceite os termos da Declaração da Kaspersky Security Network (KSN).

Etapa 4. Selecionar o modo de uso do aplicativo em computadores

Selecione **Modo Standard para proteger hosts**. O Kaspersky Endpoint Security fornece uma política comum para todos os modos de aplicativo e tipos de SO.

> Recomendamos usar políticas diferentes para diferentes modos e tipos de sistema operacional.

Etapa 5. Importando configurações

> Esta etapa estará disponível caso a configuração manual da política na etapa 4 seja selecionada.

É possível criar uma política de acordo com as configurações do Kaspersky Endpoint Security por meio de um arquivo de configuração CFG. O Assistente de nova política não oferece suporte a arquivos de configuração criptografados. Ao exportar o arquivo de configuração, ignore a etapa de criptografia do arquivo.

Ao importar um arquivo de configuração CFG do aplicativo, nem todas as configurações de política ficam disponíveis para o assistente. Por exemplo, os perfis de política estão ausentes nas configurações do aplicativo. Caso queira transferir todas as configurações e perfis para a política, é possível importar outra política de um arquivo KLP.

Ao importar um arquivo de configuração, o Kaspersky Endpoint Security não transfere as senha do contêiner de criptografia. Caso use a autenticação bidirecional ao se conectar aos servidores, será necessário especificar as senhas do contêiner de criptografia do zero.

Etapa 6 - 10. Definição das configurações da política

Esta etapa estará disponível caso a configuração manual da política na etapa 4 seja selecionada.

Siga as etapas para gerenciar as configurações de política.

Etapa 11. Configuração da zona confiável

Configure a zona confiável. É possível adicionar exclusões de verificação e aplicativos confiáveis predefinidos. As exclusões predefinidas de verificação e aplicativos confiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, Microsoft Exchange e System Center Configuration Manager. Isso significa que não será necessário configurar manualmente uma zona confiável para o aplicativo nos servidores. Exclusões de verificação e aplicativos confiáveis predefinidos também podem ajudar a configurar rapidamente o Kaspersky Endpoint Security no modo Light Agent em ambientes virtuais Citrix e VMware.

Etapa 12. Selecionar o status da política

- **Ativo**. Depois da sincronização seguinte, a política será usada como a política ativa no computador.

  As configurações de uma política ativa são salvas nos computadores clientes durante a sincronização. Você não pode aplicar simultaneamente várias políticas a um computador, portanto, apenas uma política pode estar ativa em cada grupo.

- **Inativo**. Política de reserva. Se necessário, uma política inativa pode ser trocada para o status ativo.

  Você pode criar um número ilimitado de políticas inativas. Uma política inativa não afeta as configurações do aplicativo em computadores na rede. As políticas inativas funcionam como preparativos para situações de emergência, como um ataque de vírus. Se ocorrer um ataque por meio de pen drives, você poderá ativar uma política que bloqueie o acesso aos pen drives. Nesse caso, a política ativa torna-se automaticamente inativa.

- **Fora do escritório**. A política é ativada quando um computador sai do perímetro da rede da organização.

Conclua o assistente.

Configuração adicional de políticas e tarefas após a migração

KSWS e KES possuem diferentes conjuntos de componentes e configurações de política, portanto, após a migração, é necessário verificar se as configurações de política atendem aos seus requisitos de segurança corporativa.

Verifique as seguintes configurações básicas da política:

- Proteção por senha. As configurações de proteção por senha do KSWS não são migradas. O Kaspersky Endpoint Security possui um recurso integrado de proteção por senha. Caso seja necessário, ativar a proteção por senha e definir uma senha.

- Zona confiável. Os métodos utilizados pelo KSWS e KES para selecionar objetos são diferentes. Ao migrar, o KES oferece suporte a exclusões definidas como arquivos individuais ou caminhos para arquivo/pasta. Caso o KSWS tenha exclusões configuradas como uma área predefinida ou uma URL de script, tais exclusões não serão migradas. Após a migração, é necessário adicionar essas exclusões manualmente.

  Para garantir que o Kaspersky Endpoint Security funcione corretamente nos servidores, é recomendável adicionar arquivos importantes para o funcionamento do servidor na zona confiável. Para servidores SQL, é necessário adicionar arquivos de banco de dados MDF e LDF. Para servidores Microsoft Exchange, é necessário incluir arquivos CHK, EDB, JRS, LOG e JSL. É possível usar as máscaras, por exemplo, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

  A partir do Kaspersky Endpoint Security 12.6 for Windows, as exclusões de verificação e aplicativos confiáveis são adicionadas na zona confiável. As exclusões predefinidas de verificação e aplicativos confiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, Microsoft Exchange e System Center Configuration Manager. Isso significa que não será necessário configurar manualmente uma zona confiável para o aplicativo nos servidores.

- Firewall. As funções do KSWS Firewall são executadas pelo Firewall no nível do sistema. No KES, um componente separado é responsável pela funcionalidade do Firewall. Após a migração, é possível configurar o Firewall do Kaspersky Endpoint Security.

- Kaspersky Security Network. O Kaspersky Endpoint Security não é compatível com a configuração da KSN para componentes individuais. O Kaspersky Endpoint Security utiliza a KSN para todos os componentes do aplicativo. Para usar a KSN, é necessário aceitar os novos termos e condições da Declaração da Kaspersky Security Network.

- Controle da Web. As regras de bloqueio para controle de categoria de tráfego da web são migradas para uma única regra de bloqueio no Kaspersky Endpoint Security. O Kaspersky Endpoint Security ignora as regras de permissão para controle de categoria. O Kaspersky Endpoint Security não oferece suporte a todas as categorias do Kaspersky Security for Windows Server. As categorias que não existem no Kaspersky Endpoint Security não são migradas. Portanto, as regras de classificação de recursos da Web com categorias não compatíveis não são migradas. Caso seja necessário, adicionar as regras de Controle da Web.

- Servidor proxy. A senha de conexão do servidor proxy não é migrada. Inserir a senha a ser usada para conexão com o servidor proxy manualmente.

- Agendamentos de componentes individuais. O Kaspersky Endpoint Security não é compatível com a configuração de agendamentos para componentes individuais. O componente está sempre ativado enquanto o Kaspersky Endpoint Security estiver em operação.

- Conjunto de componentes. O conjunto de recursos disponíveis do Kaspersky Endpoint Security depende do tipo do sistema operacional: estação de trabalho ou servidor (veja a tabela a seguir). Por exemplo, fora das ferramentas de criptografia, apenas a Criptografia de Unidade de Disco BitLocker está disponível nos servidores.

- Atributo . O estado do atributo não é migrado. O atributo terá o valor padrão. Por padrão, quase todas as configurações na nova política têm uma proibição aplicada na modificação de configurações nas políticas secundárias e na interface do aplicativo local. O atributo possui o valor para configurações de política na seção **Managed Detection and Response (Industrial CyberSecurity)** e no grupo de configurações **Suporte ao usuário** (seção **Interface**). Caso seja necessário, configurar a herança de configurações da política principal.

- Trabalhando com ameaças ativas. A Desinfecção Avançada funciona de maneira diferente para estações de trabalho e servidores. É possível configurar a desinfecção avançada nas configurações da tarefa de *Verificação de malware* e nas configurações do aplicativo.

- Atualização do aplicativo. Para instalar as principais atualizações e patches sem reiniciar, é necessário alterar o modo de atualização do aplicativo. Por padrão, o recurso Instalar atualizações do aplicativo sem reinicialização está desativado.

- Kaspersky Endpoint Agent. O Kaspersky Endpoint Security possui um agente integrado para trabalhar com as soluções de Detection and Response. Caso seja necessário, transferir as configurações da política do Kaspersky Endpoint Agent para a política do Kaspersky Endpoint Security.

- Tarefas de *Atualização de bancos de dados e módulos do aplicativo*. Verifique e confirme se as configurações da tarefa *Atualização de bancos de dados e módulos do aplicativo* foram migradas corretamente. Em vez das três tarefas do KSWS, o KES usa uma única tarefa do KES. É possível otimizar as tarefas *Atualização de bancos de dados e módulos do aplicativo* e remover tarefas supérfluas.

- Outras tarefas. Os componentes do Controle de Aplicativos, Controle de Dispositivos e Monitor de Integridade de Arquivos funcionam de maneira diferente no KSWS e no KES. O KES não usa as tarefas *Baseline File Integrity Monitor*, *Applications Launch Control Generator*, *Rule Generator for Device Control*. Portanto, essas tarefas não são migradas. Após a migração, é possível configurar os componentes do Monitor de Integridade de Arquivos, Controle de Aplicativos e Controle de Dispositivos.

Migração da zona confiável do KSWS

Uma *zona confiável* é uma lista de objetos e aplicativos configuradas pelo administrador de sistema que o Kaspersky Endpoint Security não monitora quando ativado. É possível migrar os objetos da zona confiável do KSWS para o KES usando o *Assistente de Conversão de Políticas e Tarefas em Lote* ou pelo *assistente de criação de nova política do KES de acordo com a política do KSWS*. O KSWS e o KES têm diferentes conjuntos de componentes e recursos, portanto, após a migração, é necessário verificar se as exclusões atendem aos seus requisitos de segurança corporativa. Os métodos de adição de exclusões para a zona confiável também são diferentes para o KES e o KSWS. O Assistente de Migração não tem ferramentas para migrar todas as exclusões do KSWS. Isso significa que, após a migração, é necessário adicionar algumas das exclusões do KSWS manualmente.

Para garantir que o Kaspersky Endpoint Security funcione corretamente nos servidores, é recomendável adicionar arquivos importantes para o funcionamento do servidor na zona confiável. Para servidores SQL, é necessário adicionar arquivos de banco de dados MDF e LDF. Para servidores Microsoft Exchange, é necessário incluir arquivos CHK, EDB, JRS, LOG e JSL. É possível usar as máscaras, por exemplo, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

A partir do Kaspersky Endpoint Security 12.6 for Windows, as exclusões de verificação e aplicativos confiáveis são adicionadas na zona confiável. As exclusões predefinidas de verificação e aplicativos confiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, Microsoft Exchange e System Center Configuration Manager. Isso significa que não será necessário configurar manualmente uma zona confiável para o aplicativo nos servidores.

Métodos de criação da zona confiável no KES e no KSWS.

KSWS		KES
Object to scan		
• Predefined scope	*(não migra)*	
• Disk, folder or network location	→	**Arquivo ou pasta**
• File	→	**Arquivo ou pasta**
• Script file or web address	*(não migra)*	
Detected object	→	**Tipo do objeto detectado**
Trusted processes	→	**Aplicativos confiáveis**

Migração de objetos verificados

As exclusões do KSWS que tenham o método **Object to scan** selecionado em suas propriedades são migradas para as exclusões do KES que tenham o método **Arquivo ou pasta** selecionado em suas propriedades, com algumas limitações. A migração de uma exclusão depende do método de seleção do objeto:

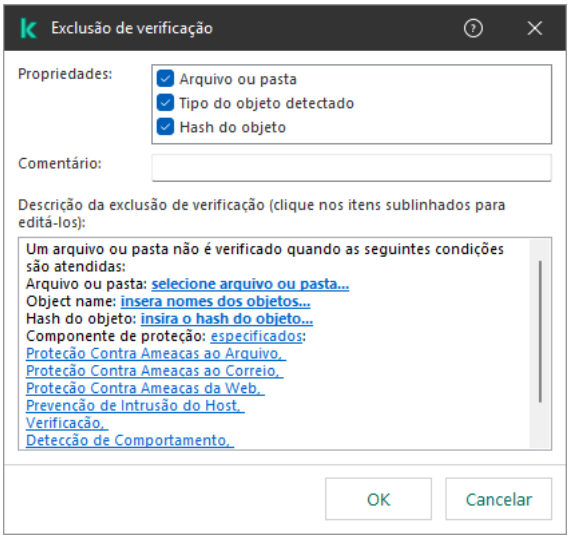
- Predefined scope – *não migra*.

  Após a migração, é necessário adicionar essas exclusões manualmente. As exclusões como áreas predefinidas devem ser definidas nas configurações da tarefa *Verificação de malware*.

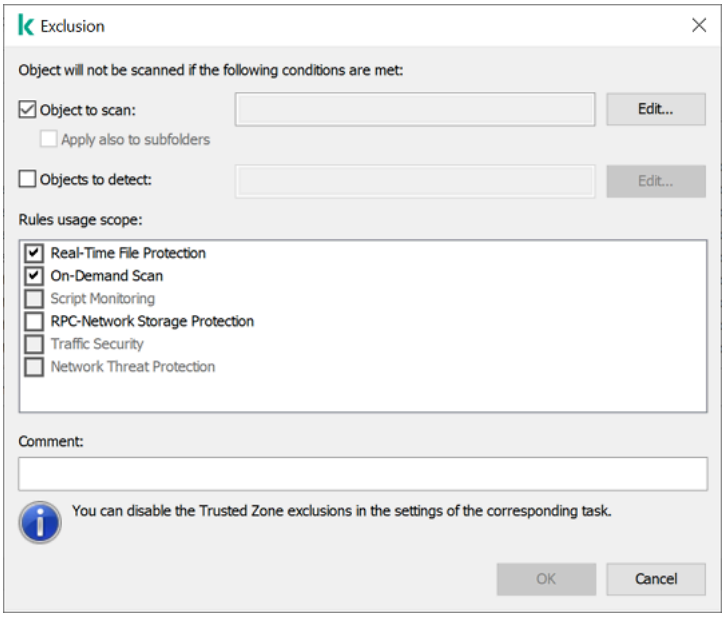
- Disk, folder or network location – migram para as exclusões do KES que tenham o método "Arquivo ou pasta" selecionado nas propriedades.
- File – migram para as exclusões do KES que tenham o método "Arquivo ou pasta" selecionado nas propriedades.
- Script file or web address – *não migra*.

  Após a migração, é necessário adicionar essas exclusões manualmente. As exclusões como endereços da Web de scripts devem ser adicionadas aos endereços da Web confiáveis para a Proteção Contra Ameaças da Web.

Caso a caixa de seleção **Apply also to subfolders** esteja marcada para o objeto verificado, essa configuração será migrada para as exclusões do KES (a caixa de seleção **Incluir subpastas**).



Configurações de exclusão do KES



Configurações de exclusão do KSWS

Migração de objetos detectados

As exclusões do KSWS que tenham o método **Detected object** selecionado em suas propriedades são migradas para as exclusões do KES que tenham o método **Tipo do objeto detectado** selecionado em suas propriedades. O nome do objeto detectado corresponde à classificação da Enciclopédia da Kaspersky (por exemplo, `Email-Worm`, `Rootkit` ou `RemoteAdmin`). O Kaspersky Endpoint Security é compatível com as máscaras com o ponto de interrogação `?` (corresponde a qualquer caractere único) e o asterisco `*` (corresponde a qualquer sequência de caracteres).

Migração do escopo de uso da exclusão

O escopo de uso de uma exclusão é um conjunto de componentes aos quais a exclusão se aplica. O KES e o KSWS têm diferentes conjuntos de componentes, portanto, o Assistente de Migração não pode migrar o escopo de uso de uma exclusão. Assim, se pelo menos um componente for selecionado no escopo de uso do KSWS, o KES aplicará a exclusão a todos os componentes do aplicativo.

É possível configurar o escopo de uso do KSWS nas configurações da zona confiável e nas configurações dos componentes de proteção do KSWS. Para fazer isso, é possível marcar ou desmarcar a caixa de seleção **Apply Trusted Zone** na seção correspondente da política. As configurações dos componentes de proteção do KES não incluem essa caixa de seleção. Isso significa que o status da zona confiável nas configurações de componentes individuais é perdido no momento da migração. Após concluir a migração, selecione os componentes aos quais a exclusão se aplica nas configurações da zona confiável na política do KES.

Comentários de migração

Os comentários da zona confiável do KSWS são migrados para os comentários de exclusão do KES sem modificação.

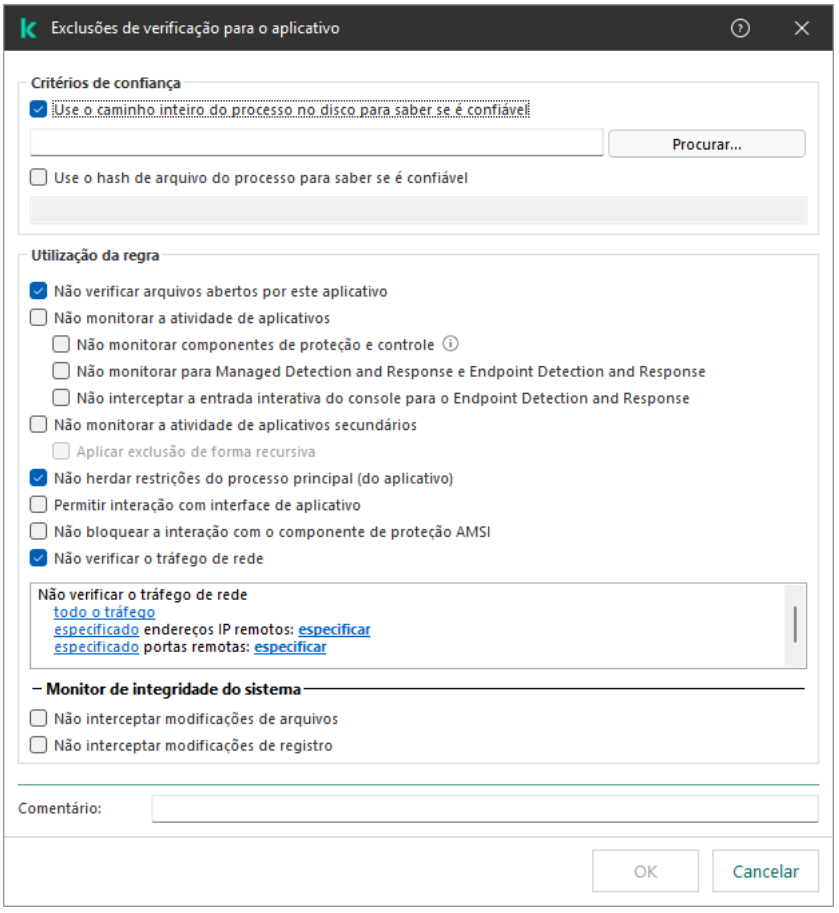
Migração de processos confiáveis

Os processos confiáveis do KSWS são migrados para os processos confiáveis do KES com algumas limitações. A migração de processos confiáveis depende do método de seleção do objeto:

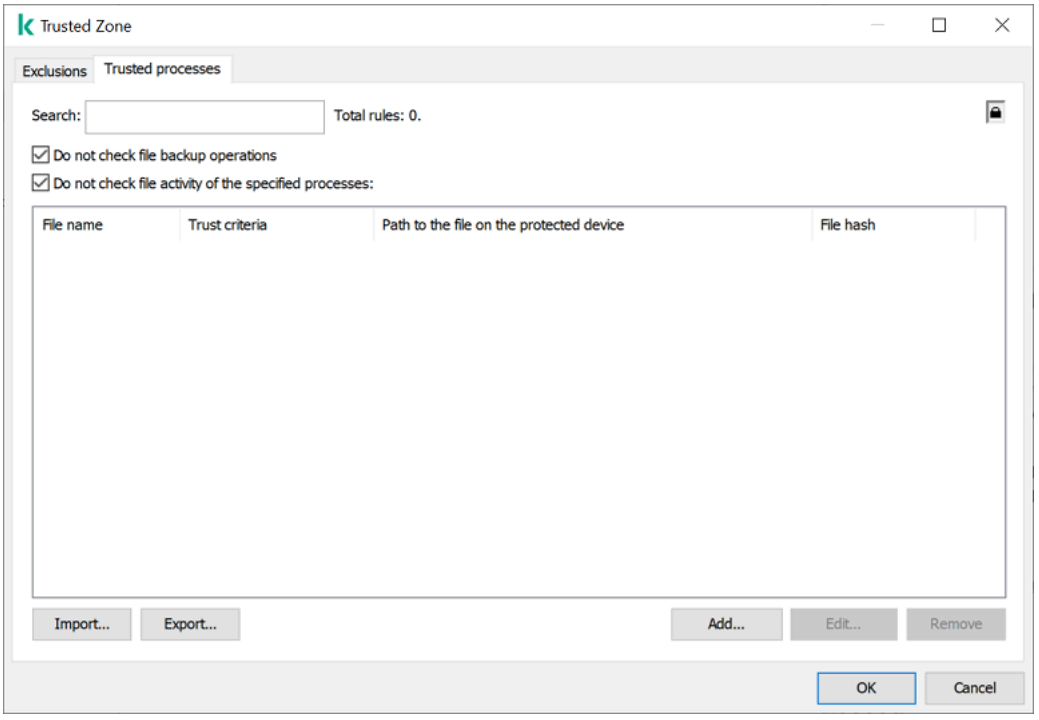
- Path to the file on the protected device – migra para os aplicativos confiáveis do KES.
- File hash – *não migra*.

Caso o KSWS tenha processos confiáveis configurados como um hash de arquivo, esses processos confiáveis não são migrados. Após a migração, é necessário adicionar esses processos confiáveis manualmente.

Caso a caixa de seleção **Do not check file backup operations** esteja marcada nas configurações do processo confiável, essa configuração será migrada para os aplicativos confiáveis do KES (a caixa de seleção **Não monitorar a atividade do aplicativo**).



Configurações de aplicativo confiável do KES



Configurações de processo confiável do KSWS

Migrar regras de Controle de Inicialização de Aplicativos do KSWS

O Controle de Inicialização de Aplicativos do KSWS fica bloqueado por padrão. Ou seja, o Controle de Inicialização de Aplicativos bloqueia automaticamente todos os aplicativos não especificados nas regras como aplicativos permitidos. Portanto, o assistente de migração para o Controle de aplicativos do KES define automaticamente o modo de controle **Lista de permissão**, que corresponde ao princípio de bloqueio por padrão.

É possível migrar regras do KSWS para o KES usando o *Assistente de Conversão de Políticas e Tarefas em Lote* ou pelo *assistente de criação de nova política do KES de acordo com a política do KSWS*.

Migrar o modo do Controle de Inicialização de Aplicativos

O modo do Controle de Inicialização de Aplicativos do KSWS migra para o Controle de Aplicativos do KES da seguinte forma:

- **Statistics only** → **Testar regras**;
- **Active** → **Aplicar regras**.

Migrar regras predefinidas do Controle de Inicialização de Aplicativos do KSWS

Por padrão, o Controle de Inicialização de Aplicativos do KSWS inclui duas regras:

- **Allow scripts and MSI by OS-trusted certificate**
- **Allow executable by OS-trusted certificate**

As regras predefinidas permitem a execução de *scripts*, *Pacotes MSI* e *arquivos executáveis* assinados por um certificado raiz confiável. Se pelo menos uma regra predefinida do KSWS tiver o tipo **Allow**, o assistente de migração cria uma regra de permissão **Aplicativos com certificados raiz confiáveis**. Ou seja, o Controle de Aplicativos do KES usa uma única regra para permitir a execução de scripts confiáveis, pacotes MSI e arquivos executáveis.

Se ambas as regras predefinidas do KSWS forem do tipo **Deny**, o KES ignorará as regras predefinidas.

Migrar regras personalizadas do Controle de Inicialização de Aplicativos do KSWS

As regras de Controle de Inicialização de Aplicativos do KSWS regulam a execução de arquivos de acordo com os seguintes critérios:

- assinatura com certificado digital;
- hash SHA256;
- caminho do arquivo.

As regras são criadas de forma diferente no KSWS e no KES, portanto, o assistente de migração cria *categorias de aplicativos*, que incluem condições e exclusões das regras do KSWS, e adiciona essas categorias de aplicativos às regras do KES. O assistente usa as condições **Certificado**, **Caminho da pasta** e **Hash do arquivo** nas categorias de aplicativos. Novas categorias de aplicativos estão disponíveis no Console de Administração do Kaspersky Security Center, na seção **Gerenciamento de aplicativos** → **Categorias de aplicativos**.

O assistente de migração agrupa as regras do KSWS por tipo e por usuário. Em seguida, o assistente cria categorias de aplicativos que incluem condições e exclusões das regras do KSWS e adiciona as categorias de aplicativos às novas regras do KES. O assistente especifica os nomes das regras do KSWS no campo **Descrição** das regras do KES.

Migrar configurações avançadas do Controle de Inicialização de Aplicativos do KSWS

O princípio de operação do Controle de Inicialização de Aplicativos do KSWS e do Controle de Aplicativos do KES é diferente, portanto, o assistente de migração pode migrar um subconjunto de configurações.

Configurações do Controle de Inicialização de Aplicativos

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Repeat action taken for the first file launch on all the subsequent launches for this file	*(não migra)* O Kaspersky Endpoint Security verifica o aplicativo sempre que ele tenta executar.
Deny the command interpreters launch with no command to execute	*(não migra)* O Kaspersky Endpoint Security permite a execução de interpretadores de comandos caso não sejam proibidos pelo Controle de aplicativos.
Apply rules to executable files	*(não migra)* O escopo de aplicação da regra não pode ser configurado nas configurações do Controle de Aplicativos do KES. O Controle de Aplicativos do KES aplica regras a todos os tipos de arquivos: arquivos executáveis, scripts e pacotes MSI. Se todos os tipos de arquivos estiverem incluídos no escopo de aplicação da regra no KSWS, o KES transferirá as regras do KSWS durante a migração. Se algum tipo de arquivo for excluído do escopo de aplicação da regra no KSWS, o KES também transferirá as regras do KSWS durante a migração, mas **Testar regras** será selecionado como a ação de Controle de Aplicativos.
Monitor loading of DLL modules	**Monitorar o carregamento de módulos DLL (aumenta significativamente a carga no sistema)**
Apply rules to scripts and MSI packages	*(não migra)* O escopo de aplicação da regra não pode ser configurado nas configurações do Controle de Aplicativos do KES. O Controle de Aplicativos do KES aplica regras a todos os tipos de arquivos: arquivos executáveis, scripts e pacotes MSI. Se todos os tipos de arquivos estiverem incluídos no escopo de aplicação da regra no KSWS, o KES transferirá as regras do KSWS durante a migração. Se algum tipo de arquivo for excluído do escopo de aplicação da regra no KSWS, o KES transferirá as regras do KSWS durante a migração, mas **Testar regras** será selecionado como a ação de Controle de Aplicativos.

Configurações do Kaspersky Security for Windows Server	Configurações do Kaspersky Endpoint Security for Windows
Deny applications untrusted by KSN	*(não migra)* O Kaspersky Endpoint Security não leva em consideração a reputação dos aplicativos e permite ou nega a execução de aplicativos de acordo com as regras.
Allow applications trusted by KSN	Durante a migração, o KES adiciona uma nova regra de permissão. A categoria KL **Outro software\Aplicativos, confiável de acordo com a reputação no KSN** é especificada como a condição de acionamento da regra.
Users and / or user groups allowed to run applications trusted by KSN	**Usuários e seus direitos** é uma regra de permissão do Controle de aplicativos que inclui a categoria KL **Outro software\Aplicativos, confiável de acordo com a reputação no KSN**.
Automatically allow software distribution via applications and packages listed	O Controle de Distribuição de Software funciona de forma diferente no KSWS e no KES. Durante a migração, o KES adiciona novas regras de permissão para aplicativos que possuem distribuição automática de software permitida. O hash do arquivo é especificado como a condição de acionamento da regra.
Always allow software distribution via Windows Installer	O Controle de Distribuição de Software funciona de forma diferente no KSWS e no KES. Durante a migração, o KES adiciona novas regras de permissão para aplicativos que têm a distribuição automática de software permitida (**Software distribution applications and packages allowed**). O hash do arquivo é especificado como a condição de acionamento da regra. Nas propriedades da conta, a caixa de seleção **Atualizadores confiáveis** estará marcada.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(não migra)*
Software distribution applications and packages allowed	O Controle de Distribuição de Software funciona de forma diferente no KSWS e no KES. Durante a migração, o KES adiciona novas regras de permissão para aplicativos que possuem distribuição automática de software permitida. O hash do arquivo é especificado como a condição de acionamento da regra. Nas propriedades da conta, a caixa de seleção **Atualizadores confiáveis** estará marcada.
Schedule settings	*(não migra)* Caso uma programação seja configurada para o componente nas configurações do KSWS, o componente Controle de Aplicativos será ativado na migração. Caso uma programação não seja configurada para o componente nas configurações do KSWS, o Controle de Aplicativos será desabilitado na migração. Não é possível configurar um agendamento separado para o componente. O componente está sempre ativado enquanto o Kaspersky Endpoint Security está operacional.

Instalação do KES sobre o KSWS

É possível instalar o Kaspersky Endpoint Security das seguintes maneiras:

- Instalar o KES após remover o KSWS (recomendado).
- Instalação do KES sobre o KSWS.

Remoção do Kaspersky Security for Windows Server

É possível remover o aplicativo remotamente usando a tarefa *Desinstalar aplicativo remotamente* ou localmente no servidor. Pode ser necessário reiniciar o servidor após remover o KSWS. Caso queira instalar o Kaspersky Endpoint Security sem reiniciar, verifique e confirme se o Kaspersky Security for Windows Server foi completamente removido. Caso o aplicativo não seja completamente removido, a instalação do Kaspersky Endpoint Security pode causar falha na operação do servidor. Ter a certeza de que o aplicativo foi completamente removido também é recomendável caso o usuário tenha usado o utilitário kavremover. O utilitário kavremover não é compatível com o gerenciamento de KSWS.

> Caso a proteção por senha esteja ativada para restringir o acesso ao KSWS, insira a senha de desinstalação nas configurações do pacote de instalação do KES.

Depois de remover o KSWS, instalar o Kaspersky Endpoint Security for Windows usando qualquer método disponível.

Instalando o Kaspersky Endpoint Security

Ao instalar o KES remotamente, os componentes selecionados nas propriedades do pacote de instalação serão instalados no servidor. Recomendamos a seleção de componentes padrão nas propriedades do pacote de instalação. Uma reinicialização não é necessária ao instalar o KES sobre o KSWS.

Antes da instalação, o Kaspersky Endpoint Security verifica o computador para confirmar se há algum aplicativo da Kaspersky. Caso o Kaspersky Security for Windows Server esteja instalado no computador, o KES detecta o conjunto de componentes do KSWS instalados e seleciona os mesmos componentes para instalação. Uma reinicialização não é necessária ao instalar o KES sobre o KSWS.

> Caso a instalação do KES sobre o KSWS falhar, será possível reverter a instalação. Depois de reverter a instalação, é recomendável reiniciar o servidor e tentar novamente.

As configurações e tarefas do KSWS não são migradas quando o Kaspersky Endpoint Security for Windows é instalado. Para migrar as configurações e tarefas, execute o assistente de conversão de políticas e tarefas em lote.

É possível verificar a lista de componentes instalados na seção **Segurança** da interface do aplicativo, basta utilizar o comando `status` ou acessar o console do Kaspersky Security Center nas propriedades do computador. É possível alterar o conjunto de componentes após a instalação usando *Alterar componentes do aplicativo*.

Migração da configuração [KSWS+KEA] para [KES+built-in agent]

> Para oferecer suporte ao uso do Kaspersky Endpoint Security for Windows como parte do EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA e MDR, um agente integrado foi adicionado ao aplicativo. Não é mais preciso um aplicativo separado do Kaspersky Endpoint Agent para trabalhar com estas soluções.

Ao migrar do KSWS para o KES, as soluções EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA e MDR continuam funcionando com os agentes integrados do Kaspersky Endpoint Security. Além disso, o Kaspersky Endpoint Agent será removido do computador.

A migração da configuração [KSWS+KEA] para [KES+agente integrado] envolve as seguintes etapas:

1. **Migração de KSWS para KES**

   A migração de KSWS para KES envolve a instalação do Kaspersky Endpoint Security em vez do Kaspersky Security for Windows Server.

   Geralmente, os administradores ativam a Proteção por senha para restringir o acesso ao KSWS e KEA. A partir do Kaspersky Security Center Linux 15.1, é possível inserir a senha de desinstalação do aplicativo nas configurações da tarefa *Instalar o aplicativo remotamente*. A tarefa permite inserir apenas uma senha de desinstalação. Ou seja, caso a mesma senha seja definida para KSWS e KEA, os aplicativos KSWS e KEA serão removidos com êxito. Caso as senhas sejam diferentes, a remoção de um dos aplicativos falhará com um erro de acesso. Para concluir a migração, é necessário desativar a Proteção por senha do aplicativo cuja senha não pôde ser inserida nas configurações da tarefa *Instalar o aplicativo remotamente*.

   Para realizar a migração, é necessário selecionar os componentes necessários de suporte às soluções de Detection and Response como parte do Kaspersky Endpoint Security. Após instalação do aplicativo, o Kaspersky Endpoint Security alterna o uso do agente integrado e remove o Kaspersky Endpoint Agent.

2. **Migração das políticas e tarefas**

   A migração das políticas e tarefas [KSWS+KEA] para [KES+agente integrado] envolve as seguintes etapas:

   1. Migração de políticas e tarefas de KSWS para KES usando o Assistente de Conversão de Políticas e Tarefas em Lotes (disponível apenas no Console de Administração (MMC)).

      Como resultado, um perfil da política com o nome *UpgradedFromKSWS <Nome da política do Kaspersky Security for Windows Server>* é adicionado na política KES. Novas tarefas KES também são criadas com os nomes *<nome de tarefa KSWS> (convertido)*.

   2. Migração de políticas e tarefas de KEA para KES usando o assistente para migração do Kaspersky Endpoint Agent (disponível apenas no Web Console e no Cloud Console).

      Como resultado, uma nova política é criada com o nome *<Nome da política do Kaspersky Endpoint Security> & <Nome da política do Kaspersky Endpoint Agent>*. Novas tarefas e tarefas KES também são criadas.

3. **Licenciamento da funcionalidade**

   Caso utilize uma licença comum do Kaspersky Endpoint Detection and Response Optimum ou do Kaspersky Optimum Security para ativar o Kaspersky Endpoint Security for Windows e Kaspersky Endpoint Agent, a funcionalidade do EDR Optimum será ativada automaticamente após a atualização do aplicativo para a versão 11.7.0. Não é necessário fazer mais nada.

   Caso utilize uma licença autônoma do add-on do Kaspersky Endpoint Detection and Response Optimum para ativar a funcionalidade do EDR Optimum, é necessário garantir que a chave do add-on do EDR Optimum seja adicionada ao repositório do Kaspersky Security Center e que a funcionalidade de distribuição automática da chave de licença seja ativada. Após a atualização do aplicativo para a versão 11.7.0, a funcionalidade do EDR Optimum é ativada automaticamente.

   Caso utilize uma licença do Kaspersky Endpoint Detection and Response Optimum ou do Kaspersky Optimum Security para ativar o Kaspersky Endpoint Agent e uma licença diferente para ativar o Kaspersky Endpoint Security for Windows, é necessário substituir a chave do Kaspersky Endpoint Security for Windows pela chave comum do Kaspersky Endpoint Detection and Response Optimum ou da chave Kaspersky Optimum Security. É possível substituir a chave utilizando a tarefa *Adicionar chave*.

Não é necessário ativar a funcionalidade do Kaspersky Sandbox. A funcionalidade do Kaspersky Sandbox estará disponível imediatamente após a atualização e ativação do Kaspersky Endpoint Security for Windows.

Somente a licença da Kaspersky Anti Targeted Attack Platform pode ser usada para ativar o Kaspersky Endpoint Security como parte da solução Kaspersky Anti Targeted Attack Platform. Após a atualização do aplicativo para a versão 12.1, a funcionalidade do EDR (KATA) é ativada automaticamente. Não é necessário fazer mais nada.

4. **Verificação da saúde do Kaspersky Endpoint Detection and Response Optimum e Kaspersky Sandbox**

   Se, após a atualização, o computador estiver com o status *Crítico* no console do Kaspersky Security Center:

   - Certifique-se de que o computador possui o Agente de Rede versão 13.2 ou posterior instalado.
   - Verifique o status operacional do agente integrado visualizando o *Relatório de status dos componentes do aplicativo*. Caso o componente tenha o status *Não instalado*, instale o componente usando a tarefa *Alterar componentes do aplicativo*.
   - Certifique-se de aceitar a Declaração da Kaspersky Security Network na nova política do Kaspersky Endpoint Security for Windows.

   Assegure-se de que a funcionalidade EDR Optimum esteja ativada usando o *Relatório de status dos componentes do aplicativo*. Caso um componente tenha o status *Não coberto pela licença*, certifique-se de que funcionalidade de distribuição automática da chave de licença do EDR Optimum esteja ligada.

Verifique e confirme se o Kaspersky Security for Windows Server foi removido com êxito

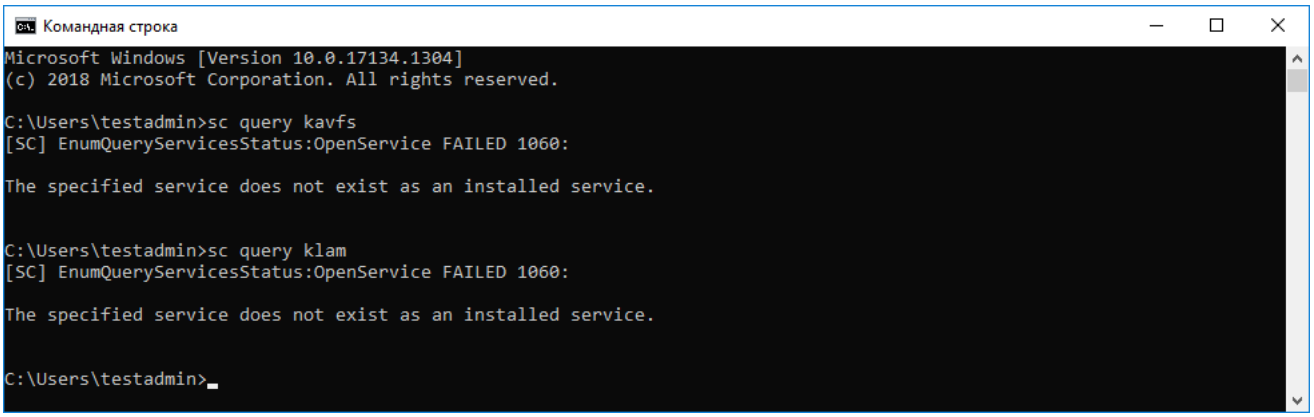
Verifique e confirme se o Kaspersky Security for Windows Server foi removido completamente:

- A pasta `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` não existe.
- Os seguintes serviços não estão presentes:
  - Kaspersky Security Service (KAVFS)
  - Serviço Kaspersky Security Management (KAVFSGT)
  - Serviço Kaspersky Security Exploit Prevention (KAVFSSLP)
  - Serviço Kaspersky Security Script Checker (KAVFSSCS)

  É possível verificar os serviços em execução no Gerenciador de Tarefas ou usar o comando de `sc query` (veja a figura abaixo).
- Os seguintes drivers não estão presentes:
  - klam.sys
  - klflt.sys
  - klramdisk.sys
  - klelaml.sys

- klfltdev.sys
- klips.sys
- klids.sys
- klwtpee

É possível verificar os drivers instalados na pasta `C:\Windows\System32\drivers` ou usar o comando `sc query`. Caso um serviço ou driver esteja faltando, o usuário receberá a seguinte resposta:



Verifique e confirme se os serviços e drivers do Kaspersky Security for Windows Server foram removidos com êxito

Caso os arquivos do aplicativo ou do driver permaneçam no servidor, exclua os arquivos pertinentes manualmente. Caso os serviços do Kaspersky Security for Windows Server ainda estejam em execução no servidor, interrompa os serviços com (`sc stop`) e exclua com (`sc delete`) manualmente. Para interromper o driver klam.sys, use o `fltmc unload klam` comando.

Ativação do KES com uma chave do KSWS

Depois de instalar o aplicativo, é possível ativar o Kaspersky Endpoint Security for Windows (KES) utilizando uma chave de licença do Kaspersky Security for Windows Server (KSWS). O processo de ativação após a migração depende do método de ativação do KSWS (consulte a tabela abaixo).

O Kaspersky Endpoint Security não é compatível com a *licença do Kaspersky Security for Storage*. Para funcionar com essa licença, use o Kaspersky Security for Windows Server.

Para ativar o KES com a chave KSWS, é possível apenas usar o código de ativação. Se você estiver usando um arquivo de chave para ativar o aplicativo, entre em contato com o Suporte Técnico para obter um arquivo de chave do Kaspersky Endpoint Security.

Ativação do Kaspersky Endpoint Security for Windows com uma chave do Kaspersky Security for Windows Server

Método de ativação do Kaspersky Security for Windows Server	Migração da chave para o Kaspersky Endpoint Security for Windows.
Distribuição automática da chave de licença do KSWS para computadores.	Caso a distribuição automática de chaves esteja ativada nas propriedades da chave de licença do KSWS, o KES será automaticamente ativado com a chave do KSWS.
A chave do KSWS é adicionada por uma tarefa.	Caso o KSWS seja ativado utilizando a tarefa, a chave de licença do KSWS será excluída durante a migração do KSWS. É necessário ativar o aplicativo novamente. Por exemplo, é possível adicionar uma chave de licença ao pacote de instalação do Kaspersky Endpoint Security for Windows.

Método de ativação do Kaspersky Security for Windows Server	Migração da chave para o Kaspersky Endpoint Security for Windows.
A chave do KSWS é adicionada localmente na interface do aplicativo.	Caso o KSWS seja ativado localmente utilizando o Assistente de ativação do aplicativo, a chave de licença do KSWS será excluída durante a migração do KSWS. É necessário ativar o aplicativo novamente. Por exemplo, é possível adicionar uma chave de licença ao pacote de instalação do Kaspersky Endpoint Security for Windows.
A chave do KSWS é adicionada ao pacote de instalação.	Caso o KSWS seja ativado utilizando a chave do pacote de instalação, a chave de licença do KSWS será excluída durante a migração do KSWS. É necessário ativar o aplicativo novamente. Por exemplo, é possível adicionar uma chave de licença ao pacote de instalação do Kaspersky Endpoint Security for Windows.
Imagem de máquina virtual paga (Amazon Machine Image – AMI) na Amazon Web Services (AWS).	Caso tenha comprado o Kaspersky Security Center como uma imagem de máquina virtual paga (Amazon Machine Image – AMI) na Amazon Web Services (AWS), não é necessário ativar o KES. Nesse caso, o Kaspersky Security Center usa a assinatura da AWS que já está adicionada ao aplicativo.
Imagem gratuita e pronta do Kaspersky Security Center com sua própria licença (o modelo Bring Your Own License – BYOL).	Caso esteja usando uma imagem gratuita e pronta do Kaspersky Security Center com sua própria licença em um ambiente na nuvem (o modelo Bring Your Own License – BYOL), é necessário ativar o aplicativo usando qualquer método disponível. Será necessário possuir uma licença do Kaspersky Hybrid Cloud Security.

Considerações especiais para migrar servidores de alta carga

Em servidores de alta carga, é importante monitorar o desempenho e evitar as falhas. Após a migração para o Kaspersky Endpoint Security for Windows, recomendamos desativar temporariamente os componentes do aplicativo que usam recursos consideráveis do servidor em relação a outros componentes. Depois de verificar se o servidor está funcionando normalmente, é possível reativar os componentes do aplicativo.

Recomendamos a migração de servidores de alta carga da seguinte forma:

1. Crie uma política do Kaspersky Endpoint Security com as configurações padrão.

   As configurações padrão são consideradas ideais. Elas são recomendadas pelos peritos da Kaspersky. As configurações padrão fornecem o nível de proteção recomendado e o uso ideal de recursos.

2. Nas configurações de política, desative os seguintes componentes: Proteção Contra Ameaças à Rede, Detecção de Comportamento, Prevenção de Exploit, Mecanismo de Remediação, Controle de Aplicativos.

   Caso sua organização tenha a solução Kaspersky Managed Detection and Response (MDR) implantada, carregue o arquivo de configuração BLOB para a política do Kaspersky Endpoint Security.

3. Remova o Kaspersky Security for Windows Server do servidor.

4. Instale o Kaspersky Endpoint Security for Windows com o conjunto padrão de componentes.

   Caso sua organização tenha as soluções de Detection and Response implantadas, selecione os componentes relevantes nas propriedades do pacote de instalação.

5. Verificar as configurações do aplicativo:

   - O aplicativo é ativado com a chave de licença KSWS.
   - A nova política é aplicada. Os componentes selecionados anteriormente são desativados.

6. Verifique e confirme se o servidor está funcionando. Verifique e confirme se o Kaspersky Endpoint Security for Windows não está usando mais de 1% dos recursos do servidor.

7. Caso seja necessário, criar exclusões de verificação, adicionar aplicativos confiáveis, criar uma lista de endereços da Web confiáveis.

8. Ative os componentes de Detecção de Comportamento, Prevenção de Exploit e Mecanismo de Remediação. Verifique e confirme se o Kaspersky Endpoint Security for Windows não está usando mais de 1% dos recursos do servidor.

9. Ative o componente Proteção Contra Ameaças à Rede. Verifique e confirme se o Kaspersky Endpoint Security for Windows não está usando mais de 2% dos recursos do servidor.

10. Ative o componente Controle de Aplicativos em modo de teste de regras.

11. Verifique e confirme se o Controle de Aplicativos está funcionando. Caso seja necessário, adicionar novas regras de Controle de Aplicativos e desativar o modo de teste de regras após confirmar que o Controle de Aplicativos está funcionando.

Depois de migrar de KSWS para KES, verifique e confirme se o aplicativo está funcionando corretamente. Verifique o status do servidor no console (deve estar *OK*). Verifique e confirme se nenhum erro foi relatado para o aplicativo, verifique também a hora da última conexão com o Servidor de Administração, a hora da última atualização do banco de dados e o status de proteção do servidor.

Gerenciamento do aplicativo em um servidor no modo Server Core

Um servidor no modo de Server Core não possui uma GUI. Portanto, só é possível gerenciar o aplicativo remotamente usando o console do Kaspersky Security Center ou localmente na linha de comando.

Gerenciar o aplicativo usando o console do Kaspersky Security Center

Instalar o aplicativo usando o console do Kaspersky Security Center não é diferente de instalá-lo da maneira normal. Ao criar um pacote de instalação, é possível adicionar uma chave de licença para ativar o aplicativo. É possível usar uma chave do Kaspersky Endpoint Security for Windows ou do Kaspersky Security for Windows Server.

> Em um servidor no modo Server Core, os seguintes componentes do aplicativo não estão disponíveis: Proteção Contra Ameaças da Web, Proteção Contra Ameaças ao Correio, Controle da Web, Prevenção contra ataque BadUSB, Criptografia em Nível de Arquivo (FLE), Kaspersky Disk Encryption (FDE).

Não é necessário reiniciar ao instalar o Kaspersky Endpoint Security. A reinicialização será necessária apenas se você precisar remover aplicativos incompatíveis antes da instalação. A reinicialização também poderá ser necessária quando a versão do aplicativo for atualizada. O aplicativo não pode exibir uma janela para solicitar que o usuário reinicie o servidor. É possível saber mais sobre a necessidade de reiniciar o servidor nos relatórios no console do Kaspersky Security Center.

O gerenciamento do aplicativo em um servidor no modo Server Core não é diferente do gerenciamento em um computador. É possível usar políticas e tarefas para configurar o aplicativo.

O gerenciamento do aplicativo em servidores no modo Server Core envolve as seguintes considerações especiais:

- O servidor do modo Server Core não possui uma GUI, portanto o Kaspersky Endpoint Security não exibe um aviso informando ao usuário que a desinfecção avançada é necessária. Para desinfetar uma ameaça, é necessário ativar a tecnologia de desinfecção avançada nas configurações do aplicativo e ativar a desinfecção avançada imediatamente nas configurações de tarefa de *Verificação de malware*. Em seguida, será necessário iniciar a tarefa de *Verificação de malware*.

- A Criptografia de Unidade de Disco BitLocker está disponível apenas com o módulo de plataforma confiável (TPM). Um PIN/senha não pode ser utilizado para criptografia porque o aplicativo não é capaz de exibir a janela de solicitação de senha para autenticação pré-inicialização. Caso o sistema operacional tenha o modo de compatibilidade do Federal Information Processing Standard (FIPS) ativado, conecte uma unidade removível para salvar a chave de criptografia antes de começar a criptografar a unidade.

Gerenciar o aplicativo a partir da linha de comando

Quando não é possível usar uma GUI, você pode gerenciar o Kaspersky Endpoint Security a partir da linha de comando.

Para instalar o aplicativo em um servidor no modo Server Core, execute o seguinte comando:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

Para ativar o aplicativo, execute o seguinte comando:

```
avp.com license /add <activation code or key file>
```

Para verificar os status do perfil do aplicativo, execute o seguinte comando:

```
avp.com status
```

Para visualizar a lista de comandos de gerenciamento de aplicativos, execute o seguinte comando:

```
avp.com help
```

Migração de [KSWS+KEA] para [KES+agente integrado]

Ao migrar de Kaspersky Security for Windows Server (KSWS) para Kaspersky Endpoint Security (KES), é possível usar as seguintes recomendações para configurar a proteção do servidor e otimizar o desempenho. Aqui, veremos um exemplo de migração para uma única organização.

Infraestrutura da organização

A empresa possui os seguintes equipamentos instalados:

- Kaspersky Security Center 14.2

  O administrador gerencia as soluções Kaspersky usando o Console de Administração (MMC). Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) também foi implantado

  No Kaspersky Security Center, três grupos de administração são criados, contendo os servidores da organização: dois grupos de administração para servidores SQL e um grupo de administração para servidores Microsoft Exchange. Cada grupo de administração é gerenciado por sua própria política. As tarefas *Database Update* e *On-demand scan* são criadas para todos os servidores da organização.

  A chave de ativação KSWS é adicionada ao Kaspersky Security Center. A distribuição automática de chaves está ativada.

- Servidores SQL com Kaspersky Security for Windows Server 11.0.1 e Kaspersky Endpoint Agent 3.11 instalados. Os servidores SQL são combinados em dois clusters.

  O KSWS é gerenciado por políticas *SQL_Policy(1)* e *SQL_Policy(2)*. As tarefas *Database Update*, *On-demand scan* também são criadas.

- Um servidor Microsoft Exchange com Kaspersky Security for Windows Server 11.0.1 e Kaspersky Endpoint Agent 3.11 instalados.

  O KSWS é gerenciado por política *Exchange_Policy*. As tarefas *Database Update*, *On-demand scan* também são criadas.

Planejamento da migração

A migração envolve as seguintes etapas:

1. Migração das tarefas e políticas do KSWS usando o assistente de conversão de políticas e tarefas em lotes.
2. Migração da política do Kaspersky Endpoint Agent usando o assistente de conversão em lote de políticas e tarefas.
3. Uso de tags para ativar perfis da política nas propriedades da nova política.
4. Instalação do KES em vez do KSWS.
5. Ativação do EDR Optimum.
6. Confirmação de que o KES está funcionando.

O cenário de migração é executado inicialmente em um dos clusters de servidores SQL. Em seguida, o cenário de migração é executado no outro cluster de servidores SQL. Em seguida, o cenário de migração é executado no Microsoft Exchange.

Migração das tarefas e políticas do KSWS usando o assistente de conversão de políticas e tarefas em lotes

Para migrar as tarefas do KSWS, é possível usar o assistente de conversão de políticas e tarefas em lotes (o assistente de migração). Como resultado, em vez das políticas *SQL_Policy(1)*, *SQL_Policy(2)*, e *Exchange_Policy*, uma única política com três perfis para servidores SQL e Microsoft Exchange será obtida, respectivamente. O novo perfil da política com as configurações KSWS será nomeado *UpgradedFromKSWS <Nome da política do Kaspersky Security for Windows Server>*. Nas propriedades do perfil, o assistente de migração seleciona automaticamente a tag do dispositivo `UpgradedFromKSWS` como critério de acionamento. Assim, as configurações do perfil da política são aplicadas nos servidores automaticamente.

Migração da política do Kaspersky Endpoint Agent usando o assistente de conversão em lote de políticas e tarefas

Para migrar as políticas do Kaspersky Endpoint Agent, é possível usar o assistente de conversão de políticas e tarefas em lotes. O assistente de migração de tarefas e políticas para Kaspersky Endpoint Agent está disponível apenas no Web Console.

Uso de tags para ativar perfis da política nas propriedades da nova política

Selecionar a tag do dispositivo que foi atribuída anteriormente como condição de ativação do perfil. Abrir as propriedades da política e selecionar *Regras gerais para a ativação do perfil de política* como condição de ativação do perfil.

Instalação do KES sobre o KSWS

Antes de instalar o KES, é preciso desativar a proteção por senha nas propriedades da política KSWS.

A instalação do KES envolve as seguintes etapas:

1. Prepare o pacote de instalação. Nas propriedades do pacote de instalação, selecione o kit de distribuição Kaspersky Endpoint Security for Windows 12.0 e selecione o conjunto padrão de componentes.

2. Crie uma tarefa *Instalar o aplicativo remotamente* para um dos grupos de administração do servidor SQL.

3. Nas propriedades da tarefa, selecionar o pacote de instalação e o arquivo de chave da licença.

4. Aguarde até que a tarefa seja concluída com êxito.

5. Repita a instalação do KES para os grupos de administração restantes.

O Kaspersky Security Center adiciona automaticamente a tag `UpgradedFromKSWS` aos nomes dos computadores no console após a conclusão da instalação do KES.

Para verificar a instalação do KES, é possível usar o *Relatório de implementação de proteção*. Também é possível verificar o status do dispositivo. Para confirmar a ativação do aplicativo, é possível usar o *Relatório de uso das chaves de licença*.

Ativação do EDR Optimum

É possível ativar a funcionalidade EDR Optimum usando uma licença independente do Kaspersky Endpoint Detection and Response Optimum Add-on. É preciso confirmar se a chave EDR Optimum foi adicionada ao repositório do Kaspersky Security Center e se a funcionalidade de distribuição automática da chave da licença está ativada.

Para verificar a ativação do EDR Optimum, é possível usar o *Relatório de status dos componentes do aplicativo*.

Confirmação de que o KES está funcionando

Para confirmar se o KES está funcionando, é possível verificar se nenhum erro foi relatado. O estado do dispositivo deve estar *OK*. Tarefas de verificação de malware e atualização concluídas com êxito.

Modo Light Agent para proteger máquinas virtuais

A partir da versão 12.8, é possível usar o Kaspersky Endpoint Security for Windows como parte do Kaspersky Security for Virtualization Light Agent. O *Kaspersky Security for Virtualization Light Agent* é uma solução integrada que fornece proteção abrangente de máquinas virtuais contra vários tipos de ameaças à segurança da informação, ataques de rede e ataques de phishing. Para usar essa solução, é necessário instalar o aplicativo no modo Light Agent.

A instalação do Kaspersky Endpoint Security no Modo Light Agent em máquinas virtuais baseadas em Arm não é compatível.

É possível usar o Kaspersky Endpoint Security no modo Light Agent como parte do Kaspersky Security for Virtualization Light Agent a partir da versão 6.2.

Ao iniciar o Light Agent, ele estabelece e mantém uma conexão com a máquina virtual SVM (Secure Virtual Machine). Um Servidor de proteção é implementado no SVM. O *Servidor de proteção* é o componente da solução Kaspersky Security for Virtualization Light Agent que verifica arquivos em busca de vírus e outros malwares, atualiza bancos de dados do antivírus e gerencia chaves da licença. O Light Agent envia arquivos ou seus fragmentos que precisam ser verificados para a SVM. Os resultados da verificação estão disponíveis para todas as máquinas virtuais com o Light Agent instalado (a tecnologia SharedCache). Esta tecnologia aumenta a eficiência da solução e proporciona uma resposta mais rápida às ameaças.

A infraestrutura da organização pode conter muitas máquinas virtuais com o Light Agent instalado e muitos SVMs. O Servidor de integração gerencia a interação entre máquinas virtuais e SVMs. O *Servidor de integração* é um componente da solução Kaspersky Security for Virtualization Light Agent que gera uma lista de SVMs disponíveis e transfere esses dados para os Light Agents, participa da descoberta de SVMs pelos Light Agents, protege a conexão entre Light Agents e SVMs e executa outras funções.

Considerações especiais para o modo Light Agent

É possível gerenciar o Kaspersky Endpoint Security no modo Standard e no modo Light Agent usando as políticas e tarefas do Kaspersky Endpoint Security. No modo Light Agent, alguns componentes e recursos do aplicativo não estão disponíveis.

Atualizar bancos de dados e módulos do software aplicativo

O Kaspersky Endpoint Security no modo Light Agent usa bancos de dados de malware especiais de que o aplicativo precisa ao trabalhar como parte da solução Kaspersky Security for Virtualization Light Agent. O Kaspersky Endpoint Security obtém atualizações de bancos de dados e do módulo do aplicativo do Servidor de proteção.

Os bancos de dados e módulos em máquinas virtuais protegidas são atualizados usando uma tarefa especial *Atualização de bancos de dados e módulos do aplicativo*, em que uma pasta no SVM é especificada como fonte de atualização. O Light Agent executa a tarefa *Atualização de bancos de dados e módulos do aplicativo* automaticamente. Não é possível selecionar uma fonte de atualização diferente, configurar o agendamento da tarefa nem remover a tarefa.

Uma reversão da atualização mais recente do banco de dados de malware também é tratada no Servidor de proteção. Após a reversão de uma atualização de bancos de dados e módulos do aplicativo no SVM, uma tarefa especial *Atualização de bancos de dados e módulos do aplicativo* local é iniciada na máquina virtual protegida. Essa tarefa faz com que o Light Agent volte a usar o conjunto anterior de bancos de dados de malware.

O Kaspersky Endpoint Security no modo Light Agent não é compatível com a tarefa *Reversão de atualização*.

Ativar o Light Agent

Para ativar o aplicativo, é necessário adicionar uma chave de licença no SVM a que o Light Agent está conectado. Não há necessidade de ativar o aplicativo separadamente.

Outras considerações especiais para o modo Light Agent

- Ao criar uma política para o aplicativo, recomendamos selecionar o modo Light Agent. Nesse modo, o assistente de Nova Política solicita que o usuário configure a conexão com o SVM. Essas configurações são necessárias para que o aplicativo funcione no modo Light Agent.
- Não é possível instalar os componentes de criptografia de dados e o Controle Adaptativo de Anomalias no modo Light Agent. O conjunto de componentes também depende do tipo de sistema operacional convidado: estação de trabalho ou servidor.
- O Light Agent não é compatível com a integração com as soluções Kaspersky Endpoint Detection and Response Expert e Kaspersky Endpoint Detection and Response Expert (cloud).
- É possível gerenciar o Light Agent no Console de Administração (MMC) e no Kaspersky Security Center Web Console. Não é possível gerenciar o Light Agent no Kaspersky Security Center Cloud Console.
- Não há suporte para a alteração do conjunto de componentes do aplicativo em máquinas virtuais VDI.
- O Kaspersky Endpoint Security se comunica com os servidores da KSN por meio de um servidor proxy da KSN. Não suporte para a comunicação direta com a KSN.
- Não há suporte para o modo na nuvem da Kaspersky Security Network.
- Não há suporte para o uso do servidor proxy do aplicativo ao se conectar com o Servidor de integração (VIIS), o Servidor de proteção (SVM) e os servidores da KSN.

Configuração preliminar da máquina virtual

É possível instalar o Kaspersky Endpoint Security em uma máquina virtual que usa a tecnologia de plataforma virtual. O Kaspersky Endpoint Security é compatível com as plataformas virtuais VMware, Microsoft Hyper-V e Citrix. Antes da instalação, é necessário executar a configuração preliminar das máquinas virtuais.

Compatibilidade com a tecnologia Citrix App Layering

Caso pretenda usar o Full User Layer para salvar o estado das máquinas virtuais temporárias, é necessário fazer o seguinte procedimento antes de instalar no modelo de máquina virtual:

1. Crie o arquivo C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt e adicione as seguintes exclusões nele:

   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`

2. No registro do sistema operacional na chave HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr, crie um novo valor DWORD denominado MiniFilterBypass e defina-o como 1.

3. No registro do sistema operacional, na camada de aplicativo, na chave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd, crie um novo valor MULTI_SZ denominado ExcludeKey e defina-o como \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab.

4. Reinicie a máquina virtual.

Para a instalação em máquinas virtuais em uma infraestrutura que usa Citrix App Layering, é necessário fazer o seguinte:

1. Instale o Agente de Administração do Kaspersky Security Center e o Kaspersky Endpoint Security for Windows no modelo de máquina virtual na camada de aplicativo.

2. Crie uma imagem de máquina virtual que consiste em várias camadas.

3. Implemente a imagem criada em hipervisores compatíveis com a solução Citrix App Layering.

4. Configure a criação de máquinas virtuais temporárias pela imagem criada.

Para obter detalhes sobre a instalação do software antivírus junto com o Citrix App Layering, consulte a documentação do Citrix App Layering.

Compatibilidade com a tecnologia Citrix Provisioning (Citrix Provisioning Services)

Para garantir que o aplicativo seja compatível com a tecnologia Citrix Provisioning (Citrix Provisioning Services):

- Caso o software Citrix Provisioning Target Device esteja instalado na máquina virtual, será necessário removê-lo antes de instalar o aplicativo Kaspersky Endpoint Security (para obter detalhes, acesse o site de suporte técnico da Citrix). Depois de instalar o aplicativo, é necessário reinstalar o Citrix Provisioning Target Device. Também é necessário reinstalar o Citrix Provisioning Target Device ao restaurar o aplicativo, inclusive ao atualizar o sistema operacional.

  A atualização do sistema operacional envolve as seguintes etapas:

  1. Exclua o Citrix Provisioning Target Device.
  2. Atualize o sistema operacional.
  3. Depois de iniciar a máquina virtual, certifique-se de que o aplicativo Kaspersky Endpoint Security esteja em execução e funcionando corretamente.
  4. Reinstale o Citrix Provisioning Target Device.

- Ao instalar o aplicativo usando o assistente de instalação ou remotamente usando o Kaspersky Security Center, é necessário marcar a caixa de seleção **Garantir a compatibilidade com Citrix PVS**.

Compatibilidade com a tecnologia Omnissa App Volumes

Antes de instalar no modelo da máquina virtual, é necessário criar o arquivo %SVAgent%\Config\Custom\snapvol.cfg e adicionar as seguintes exclusões nele:

- `exclude_path=\ProgramData\Kaspersky Lab`
- `exclude_path=\ProgramData\KasperskyLab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Common Files\Kaspersky Lab`

- `exclude_process_path=\Program Files\Kaspersky Lab`
- `exclude_process_name=avp.exe`
- `exclude_process_name=klnagent.exe`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon`

Para mais detalhes, consulte a documentação da Omnissa.

Instalando o Light Agent

A instalação do Kaspersky Endpoint Security no Modo Light Agent em máquinas virtuais baseadas em Arm não é compatível.

A instalação do aplicativo no modo Light Agent é igual à do modo Standard. Antes de instalar o Light Agent em uma máquina virtual, é necessário certificar-se de que o Agente de Rede do Kaspersky Security Center esteja instalado. O *Agente de Rede* facilita a interação entre o Servidor de Administração e uma máquina virtual.

O Light Agent pode ser instalado em uma máquina virtual de uma das seguintes maneiras:

- Uso remoto do Kaspersky Security Center.
- Localmente, usando o assistente de instalação.
- Localmente, usando a linha de comando.

Para instalar o Light Agent, é necessário selecionar a configuração apropriada em configurações do pacote de instalação ou no assistente de instalação.

Ao instalar o Light Agent em um servidor, os componentes de proteção avançados (Detecção de Comportamento, Prevenção de Exploits, Mecanismo de Remediação) serão excluídos da configuração padrão do aplicativo. As configurações padrão do aplicativo fornecem o nível de proteção recomendado e o uso ideal dos recursos do servidor. Ao instalar o Light Agent em uma estação de trabalho, os componentes de proteção avançados serão incluídos na configuração padrão do aplicativo.

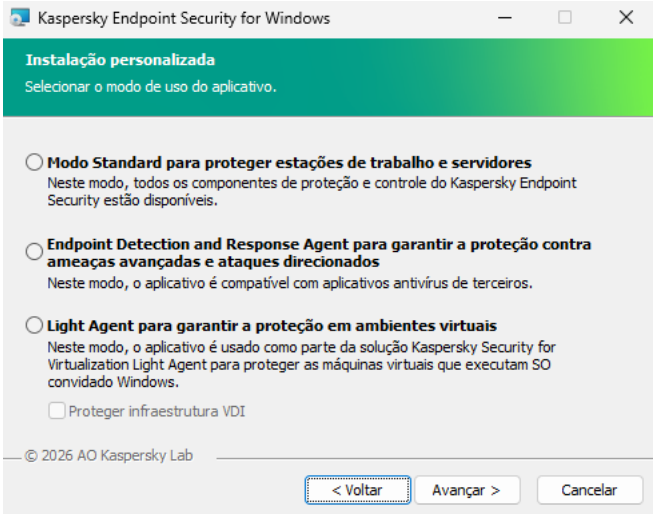
Ao instalar o Light Agent, recomendamos selecionar exclusões predefinidas e aplicativos confiáveis para o ambiente virtual relevante. As predefinições de exclusões de verificação e aplicativos confiáveis ajudam a configurar rapidamente o aplicativo e evitam problemas de compatibilidade do ambiente virtual. Na política, também é possível configurar predefinições de exclusões de verificação e aplicativos confiáveis após a instalação.

Como instalar o Light Agent usando o assistente de instalação

1. Copie a pasta do kit de distribuição para a máquina virtual.
2. Execute setup_kes.exe.

   O assistente de Instalação é iniciado.

Configuração do Kaspersky Endpoint Security



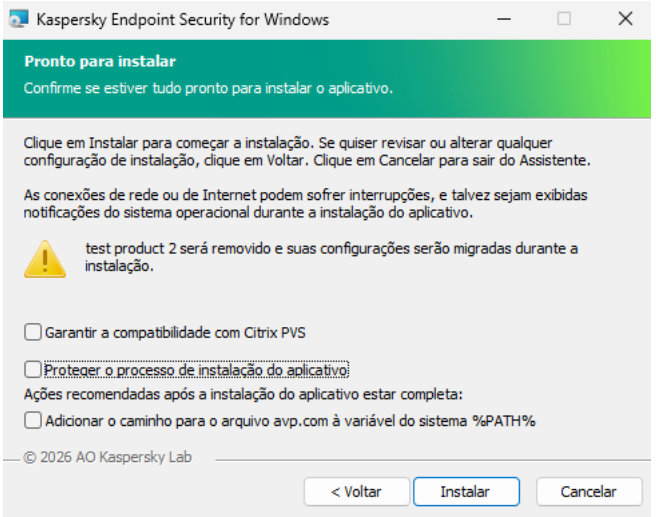
Escolhendo a configuração do aplicativo

Selecione a configuração **Light Agent para garantir a proteção em ambientes virtuais**. Essa configuração destina-se ao aplicativo usado como parte da solução do Kaspersky Security for Virtualization Light Agent. O Light Agent deve ser instalado em cada máquina virtual que precisa ser protegida pela solução. Nessa configuração, não é possível usar componentes de criptografia de dados ou o Controle Adaptativo de Anomalias. Se estiver instalando o Light Agent em um modelo de máquina virtual que será usado para criar *máquinas virtuais não persistentes*, marque a caixa de seleção **Proteger infraestrutura VDI** (VDI significa Virtual Desktop Infrastructure). O modo de proteção VDI ajuda a otimizar o desempenho do Kaspersky Endpoint Security em máquinas virtuais não persistentes. Nesse modo, o Light Agent recusa as atualizações do aplicativo que exigem a reinicialização da máquina virtual. Ao receber atualizações do aplicativo que exijam uma reinicialização, o Light Agent gerará um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas.

Componentes do Kaspersky Endpoint Security

Selecione os componentes que deseja instalar (veja a figura abaixo). Você pode alterar os componentes disponíveis do aplicativo depois de concluir a instalação do aplicativo. Para isso, você precisa executar o Assistente de instalação novamente e optar por alterar os componentes disponíveis.

Configurações avançadas



Configurações avançadas de instalação do aplicativo

Proteger o processo de instalação do aplicativo. 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 Endpoint Security e bloqueio do acesso à seção de registro do sistema que contém chaves do aplicativo. Contudo, 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.

Garantir a compatibilidade com Citrix PVS. É possível ativar o suporte ao Citrix Provisioning Services para instalar o Kaspersky Endpoint Security em uma máquina virtual.

Adicionar o caminho para o arquivo avp.com à variável do sistema %PATH%. É possível adicionar o caminho de instalação à variável %PATH% para uso adequado da interface da linha de comando.

Como instalar o Light Agent usando a linha de comando

1. Execute o interpretador da linha de comando (cmd.exe) como um administrador.

2. Vá até a pasta onde o pacote de distribuição do Kaspersky Endpoint Security está localizado.

3. Execute o seguinte comando:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
   ```

   ou

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]
   ```

   A opção `VDI` ativa o modo de proteção VDI (Virtual Desktop Infrastructure). O modo de proteção VDI ajuda a otimizar o desempenho do Kaspersky Endpoint Security em máquinas virtuais não persistentes. Nesse modo, o Light Agent recusa as atualizações do aplicativo que exigem a reinicialização da máquina virtual. Ao receber atualizações do aplicativo que exijam uma reinicialização, o Light Agent gerará um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas. Por padrão, o modo de proteção VDI está desativado.

Como resultado, o Light Agent é instalado na máquina virtual com o conjunto padrão de componentes. É possível editar o conjunto de componentes e especificar configurações avançadas usando o arquivo setup.ini. Também é possível especificar as configurações de instalação na linha de comando.

Como instalar o Light Agent no Console de Administração (MMC)

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

2. Na árvore do console, selecione a pasta **Avançado** → **Instalação remota** → **Pacotes de instalação**.

   Isso abre uma lista de pacotes de instalação que foram baixados no Kaspersky Security Center.

3. Abra as propriedades do pacote de instalação do Kaspersky Endpoint Security for Windows.

   Caso seja necessário, crie um novo pacote de instalação.

4. Ir para a seção **Configurações**.

5. Selecione a configuração **Light Agent para garantir a proteção em ambientes virtuais**. Essa configuração destina-se ao aplicativo usado como parte da solução do Kaspersky Security for Virtualization Light Agent. O Light Agent deve ser instalado em cada máquina virtual que precisa ser protegida pela solução. Nessa configuração, não é possível usar componentes de criptografia de dados ou o Controle Adaptativo de Anomalias. Se estiver instalando o Light Agent em um modelo de máquina virtual que será usado para criar *máquinas virtuais não persistentes*, marque a caixa de seleção **Proteger infraestrutura VDI** (VDI significa Virtual Desktop Infrastructure). O modo de proteção VDI ajuda a otimizar o desempenho do Kaspersky Endpoint Security em máquinas virtuais não persistentes. Nesse modo, o Light Agent recusa as atualizações do aplicativo que exigem a reinicialização da máquina virtual. Ao receber atualizações do aplicativo que exijam uma reinicialização, o Light Agent gerará um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas.

6. Selecione os componentes que deseja instalar.

   Você pode alterar os componentes disponíveis do aplicativo depois de concluir a instalação do aplicativo.

7. Configure a zona confiável. Selecione exclusões de verificação predefinidas e aplicativos confiáveis para o ambiente virtual no qual você está instalando o aplicativo.

   As predefinições de exclusões de verificação e aplicativos confiáveis ajudam a configurar rapidamente o aplicativo e evitam problemas de compatibilidade do ambiente virtual.

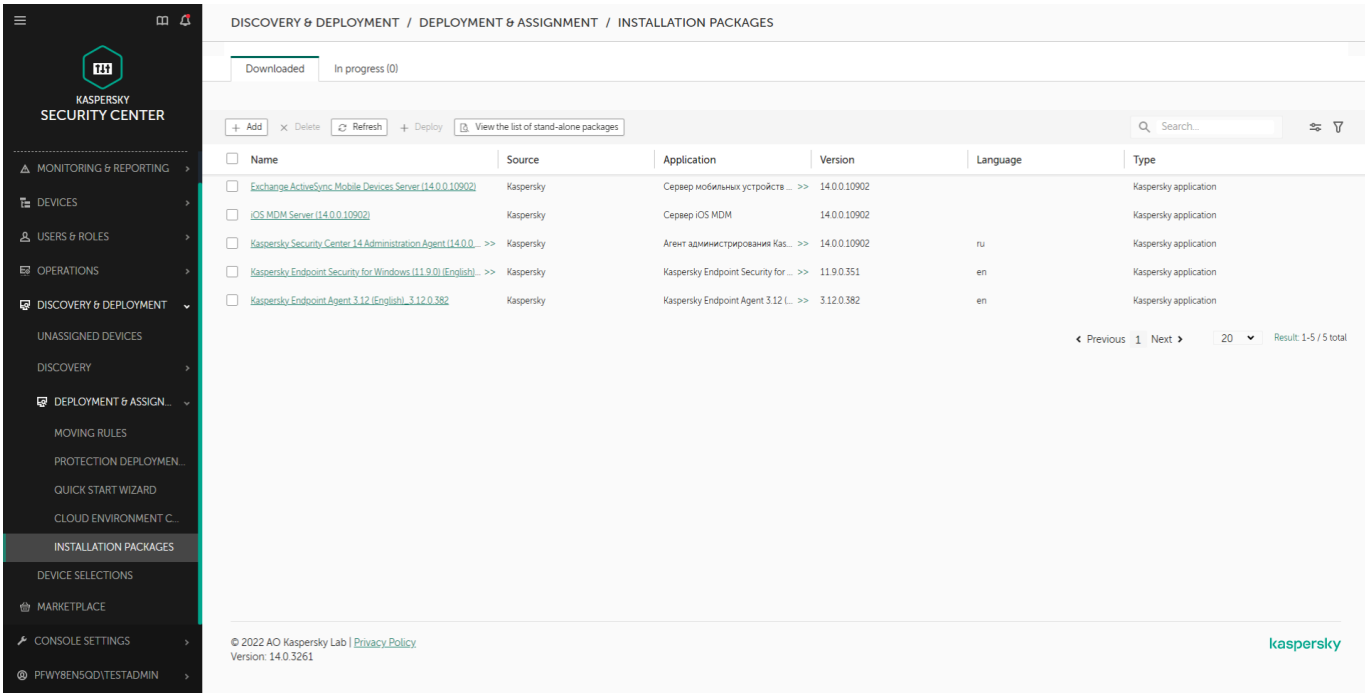
8. Salvar alterações.

9. Crie uma tarefa de instalação remota. Nas propriedades da tarefa, selecione o pacote de instalação criado.

Como instalar o Light Agent usando o Web Console

1. Na janela principal do Web Console, selecione **Descoberta e implementação** → **Implementação e atribuição** → **Pacotes de instalação**.

Isso abre uma lista de pacotes de instalação que foram baixados no Kaspersky Security Center.



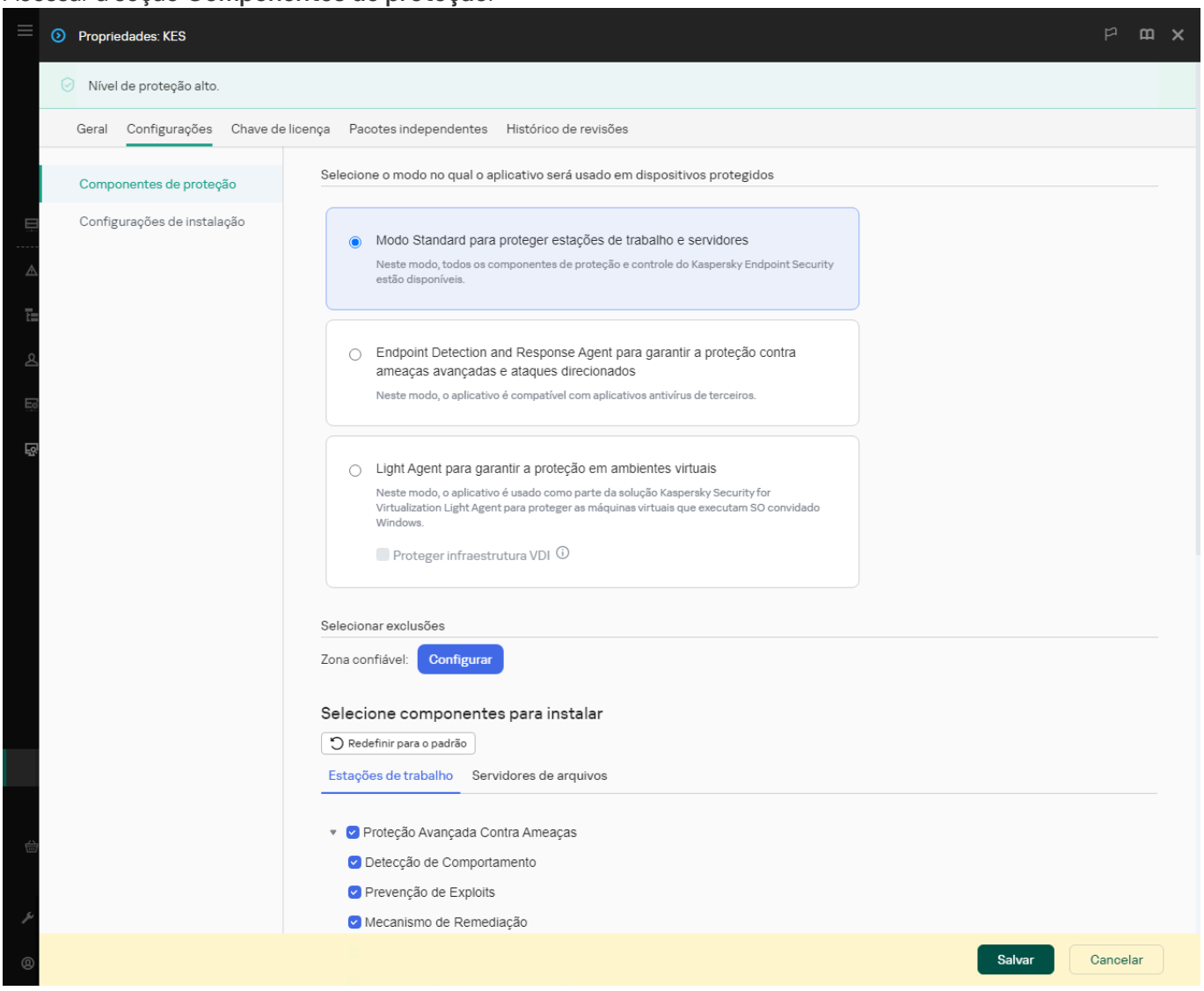
Lista de pacotes de instalação

2. Abra as propriedades do pacote de instalação do Kaspersky Endpoint Security for Windows.

   Caso seja necessário, crie um novo pacote de instalação.

3. Selecione a guia **Configurações**.

4. Acessar a seção **Componentes de proteção**.



Componentes incluídos no pacote de instalação

5. Selecione a configuração **Light Agent para garantir a proteção em ambientes virtuais**. Essa configuração destina-se ao aplicativo usado como parte da solução do Kaspersky Security for Virtualization Light Agent. O Light Agent deve ser instalado em cada máquina virtual que precisa ser protegida pela solução. Nessa configuração, não é possível usar componentes de criptografia de dados ou o Controle Adaptativo de Anomalias. Se estiver instalando o Light Agent em um modelo de máquina virtual que será usado para criar *máquinas virtuais não persistentes*, marque a caixa de seleção **Proteger infraestrutura VDI** (VDI significa Virtual Desktop Infrastructure). O modo de proteção VDI ajuda a otimizar o desempenho do Kaspersky Endpoint Security em máquinas virtuais não persistentes. Nesse modo, o Light Agent recusa as atualizações do aplicativo que exigem a reinicialização da máquina virtual. Ao receber atualizações do aplicativo que exijam uma reinicialização, o Light Agent gerará um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas.

6. Selecione os componentes que deseja instalar.

   Você pode alterar os componentes disponíveis do aplicativo depois de concluir a instalação do aplicativo.

7. Configure a zona confiável. Selecione exclusões de verificação predefinidas e aplicativos confiáveis para o ambiente virtual no qual você está instalando o aplicativo.

   As predefinições de exclusões de verificação e aplicativos confiáveis ajudam a configurar rapidamente o aplicativo e evitam problemas de compatibilidade do ambiente virtual.

8. Salvar alterações.

9. Crie uma tarefa de instalação remota. Nas propriedades da tarefa, selecione o pacote de instalação criado.

Assim, o Light Agent será instalado na máquina virtual. É possível usar a interface do aplicativo. Um um ícone do aplicativo será exibido na área de notificação . Agora é necessário configurar a conexão do Light Agent ao SVM.

Janela principal do Light Agent

Conectar o Light Agent ao SVM

A solução Kaspersky Security for Virtualization Light Agent requer a comunicação contínua do Light Agent e do SVM. Isso é necessário para verificar arquivos enviados pelo Light Agent quanto à presença de vírus e outros malwares. Sem uma conexão de SVM, o Light Agent não pode enviar arquivos para verificação. Se a conexão não puder ser estabelecida por mais de cinco minutos, a verificação é concluída com erro.

A conexão de um Light Agent a um SVM envolve as seguintes etapas:

1. O Light Agent obtém a lista de SVMs disponíveis.

2. O Light Agent determina um Servidor de proteção (SVM) disponível que seja ideal para conexão de acordo com o algoritmo de seleção de SVMs.

3. O Light Agent verifica as configurações de conexão de SVM adicionais: tags, status de proteção da conexão, funcionalidade do aplicativo coberta pela licença.

4. Conectar o Light Agent ao SVM.

É possível obter informações sobre o status da conexão do Light Agent ao SVM no Kaspersky Endpoint Security ou usando o comando do aplicativo. O aplicativo gera eventos sempre que a conexão do Light Agent com o SVM for perdida ou estabelecida e os envia para o Kaspersky Security Center. Ao usar um Servidor de integração para descoberta de SVM, é possível obter informações sobre o status do SVM e o número de Light Agents conectados no Console do Servidor de integração. Para obter detalhes sobre o monitoramento de status de SVM, consulte a Ajuda do Kaspersky Security for Virtualization Light Agent.

Descoberta de SVM

É possível selecionar um dos métodos de descoberta de SVM para o Light Agent:

- Usando o Servidor de integração (VIIS).

  O *Servidor de integração* é o componente da solução que permite a interação do Kaspersky Security for Virtualization Light Agent com a infraestrutura virtual e gera uma lista de SVMs disponíveis para conexão. O Light Agent estabelece uma conexão com o Servidor de integração e obtém a lista de endereços de SVM.

  O Servidor de integração é mais útil em infraestruturas virtuais de grande porte, pois equilibra automaticamente a carga entre as SVMs, obtém informações sobre as SVMs disponíveis, analisa essas informações e fornece aos Light Agents uma lista de Servidores de Proteção (SVMs) ideais para conexão.

  Para que o Light Agent possa obter uma lista de SVMs, basta inserir o endereço do Servidor de integração.

- Uso de um cluster de alta disponibilidade de Servidores de integração.

  A implementação de um cluster de alta disponibilidade de Servidores de integração está disponível no Kaspersky Security for Virtualization Light Agent a partir da versão 6.4. Um cluster de alta disponibilidade de Servidores de integração fornece proteção ininterrupta ao ambiente virtual graças ao failover das SVMs e dos Light Agents para um Servidor de integração de backup sempre que o Servidor de integração principal falha. Um componente especial do cluster, o *balanceador de carga*, é responsável pelo failover do servidor. Para obter detalhes sobre um cluster de alta disponibilidade de Servidores de integração, consulte a Ajuda do Kaspersky Security for Virtualization Light Agent.

  Para que o Light Agent obtenha uma lista de SVMs, é necessário inserir o endereço do dispositivo no qual o balanceador de carga está instalado.

- Usando a lista de endereços de SVM.

  Caso precise especificar SVMs individuais aos quais deseja que o Light Agent se conecte, é possível preparar uma lista manualmente.

  É necessário listar os endereços de SVMs disponíveis aos quais o Light Agent poderá se conectar.

Como configurar a descoberta de SVM pelo Light Agent no Console de Administração (MMC)

1. Abra o Console de Administração do Kaspersky Security Center.
2. Na árvore do console, selecione **Políticas**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela da política, selecione **Modo Light Agent** → **Configurações de descoberta de SVM**.

5. Selecione um método de descoberta de SVM.

- **Usar Servidor de integração**. Insira as configurações de conexão com o Servidor de integração de acordo com sua infraestrutura:

  - **Servidor de integração único**. Insira as configurações de conexão do Servidor de integração: Endereço IPv4 ou nome de domínio totalmente qualificado (FQDN) do dispositivo.

  - **Cluster de alta disponibilidade de Servidores de integração**. Insira o endereço IP e a porta do balanceador de carga que faz parte do cluster.

- **Usar lista personalizada de endereços de SVM**. Crie uma lista de SVMs aos quais o Light Agent poderá se conectar. Especifique o endereço IP no formato IPv4 ou o nome de domínio totalmente qualificado (FQDN) do SVM. Cada item da lista deve ser inserido em uma nova linha ou separado do item anterior com um caractere de ponto e vírgula (`;`).

  > Na lista de endereços de SVM, especifique somente nomes de domínio completos (FQDN) que correspondam a um único endereço IP. Usar um nome de domínio totalmente qualificado que corresponda a vários endereços IP pode levar a erros na solução.

6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como configurar a descoberta de SVM pelo Light Agent no Web Console

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

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

   A janela de propriedades da política é exibida.

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

4. Selecione **Modo Light Agent** → **Configurações de descoberta de SVM**.

5. Selecione um método de descoberta de SVM.

- **Usar Servidor de integração**. Insira as configurações de conexão com o Servidor de integração de acordo com sua infraestrutura:

  - **Servidor de integração único**. Insira as configurações de conexão do Servidor de integração: Endereço IPv4 ou nome de domínio totalmente qualificado (FQDN) do dispositivo.

  - **Cluster de alta disponibilidade de Servidores de integração**. Insira o endereço IP e a porta do balanceador de carga que faz parte do cluster.

- **Usar lista personalizada de endereços de SVM**. Crie uma lista de SVMs aos quais o Light Agent poderá se conectar. Especifique o endereço IP no formato IPv4 ou o nome de domínio totalmente qualificado (FQDN) do SVM. Cada item da lista deve ser inserido em uma nova linha ou separado do item anterior com um caractere de ponto e vírgula (`;`).

  > Na lista de endereços de SVM, especifique somente nomes de domínio completos (FQDN) que correspondam a um único endereço IP. Usar um nome de domínio totalmente qualificado que corresponda a vários endereços IP pode levar a erros na solução.

6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como configurar a descoberta de SVM pelo Light Agent na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .

2. Na janela de configurações do aplicativo, em **Modo Light Agent**, clique no bloco **Configurações de descoberta de SVM**.

3. Selecione um método de descoberta de SVM.

   - **Usar Servidor de integração**. Insira as configurações de conexão com o Servidor de integração de acordo com sua infraestrutura:

     - **Servidor de integração único**. Insira as configurações de conexão do Servidor de integração: Endereço IPv4 ou nome de domínio totalmente qualificado (FQDN) do dispositivo.

     - **Cluster de alta disponibilidade de Servidores de integração**. Insira o endereço IP e a porta do balanceador de carga que faz parte do cluster.

   - **Usar lista personalizada de endereços de SVM**. Crie uma lista de SVMs aos quais o Light Agent poderá se conectar. Especifique o endereço IP no formato IPv4 ou o nome de domínio totalmente qualificado (FQDN) do SVM. Cada item da lista deve ser inserido em uma nova linha ou separado do item anterior com um caractere de ponto e vírgula (`;`).

     > Na lista de endereços de SVM, especifique somente nomes de domínio completos (FQDN) que correspondam a um único endereço IP. Usar um nome de domínio totalmente qualificado que corresponda a vários endereços IP pode levar a erros na solução.

4. Salvar alterações.

Configurar o algoritmo de seleção de SVMs para o Light Agent

A infraestrutura da organização pode ter vários SVMs implementados aos quais os Light Agents podem se conectar. Para equilibrar a carga na rede e os recursos da infraestrutura virtual, é necessário distribuir os Light Agents entre os SVMs.

Algoritmos de seleção de SVMs

Os Light Agents podem aplicar os seguintes algoritmos de seleção de SVMs para conexão: Algoritmo padrão (por padrão) e algoritmo estendido.

Algoritmos de seleção de SVMs

Algoritmo padrão	Algoritmo estendido
Caso esse algoritmo seja usado, após a instalação e inicialização, o Light Agent na máquina virtual escolherá se conectar com um SVM *local* em relação ao Light Agent. Caso nenhum SVM local adequado para conexão seja encontrado, o Light Agent selecionará um SVM ao qual o menor número de Light Agents esteja conectado, independentemente da posição do SVM na infraestrutura virtual. O aplicativo não determina se a SVM é local em relação ao Light Agent se o modo de proteção de grandes infraestruturas estiver ativado para o Servidor de proteção na SVM. Nesse caso, é recomendável usar o algoritmo de seleção de SVM estendido e selecionar o Servidor de integração como o método de descoberta de SVM. O fato de uma SVM ser considerada local para um Light Agent depende do tipo de infraestrutura virtual.	Se esse algoritmo for aplicado, você poderá definir as seguintes configurações de seleção de SVM: • se deve considerar ou ignorar a localização das SVMs na infraestrutura ao escolher SVMs para conexão • se a localização da SVM for considerada, o método para determinar a localidade da SVM em relação ao Light Agent Se os Light Agents ignorarem a localização das SVMs na infraestrutura, eles poderão se conectar a quaisquer SVMs disponíveis para conexão. Se os Light Agents precisarem considerar a localização das SVMs na infraestrutura, você precisará selecionar o tipo de caminho da SVM que será considerado ao determinar se uma SVM é local em relação ao Light Agent. O fato de uma SVM ser considerada local para o Light Agent depende do tipo de infraestrutura virtual. Se os Light Agents considerarem a localização das SVMs na infraestrutura ao escolher a qual SVM se conectar, eles só poderão se conectar a SVMs locais. Por exemplo, se você especificar cluster do hipervisor como o tipo de caminho da SVM, todas as SVMs implementadas nesse cluster do hipervisor serão consideradas locais em relação ao Light Agent, e o Light Agent poderá se conectar somente a uma dessas SVMs. Se não houver SVMs disponíveis para conexão no mesmo cluster em que o Light Agent estiver em execução, o Light Agent não se conectará a uma SVM. Ao selecionar SVMs, os Light Agents também consideram o número de Light Agents conectados para garantir que os Light Agents sejam distribuídos uniformemente entre as SVMs disponíveis para conexão. Se um Light Agent usar o algoritmo de seleção de SVM estendido, uma lista de endereços de SVM for selecionada como método de descoberta de SVM e o modo de proteção de infraestrutura de grande porte estiver ativado em uma SVM, a conexão de um Light Agent a essa SVM só será possível se o caminho da SVM for ignorado.
Basis Dynamix Enterprise	
Em uma infraestrutura virtual baseada no Basis Dynamix Enterprise, a SVM considerada local em relação a um Light Agent é a SVM implementada no mesmo nó que a máquina virtual com o Light Agent instalado.	Em uma infraestrutura virtual baseada no Basis Dynamix Enterprise, uma SVM pode ser considerada local em relação ao Light Agent em qualquer um dos seguintes casos: • Uma SVM está implementada no mesmo nó que a máquina virtual com o Light Agent instalado. • Uma SVM está localizada na mesma zona que a máquina virtual com o Light Agent instalado. • Uma SVM está implementada no mesmo data center que a máquina virtual com o Light Agent instalado.
Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer e Basis Dynamix Standard	

Algoritmo padrão	Algoritmo estendido
Em uma infraestrutura virtual baseada no Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, FusionSphere da HUAWEI, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard, a SVM considerada local em relação a um Light Agent é a SVM implementada no mesmo hipervisor que a máquina virtual com o Light Agent instalado.	Em uma infraestrutura virtual baseada em Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, FusionSphere da HUAWEI, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard, uma SVM pode ser considerada local em relação ao Light Agent em qualquer um dos seguintes casos: • Uma SVM está implementada no mesmo hipervisor que a máquina virtual com o Light Agent instalado. • Uma SVM está implementada no mesmo cluster de hipervisor que a máquina virtual com o Light Agent instalado. • Uma SVM está implementada no mesmo data center que a máquina virtual com o Light Agent instalado.
SVM do OpenStack e da VK Private Cloud	
Em uma infraestrutura virtual em execução na Plataforma OpenStack ou no VK Private Cloud, você pode especificar como a localidade da SVM em relação ao Light Agent é determinada usando o parâmetro `StandardAlgorithmSvmLocality` na seção `HypervisorSpecificSettings:Openstack` do arquivo de configuração appsettings.json do Servidor de integração. Dependendo da versão do Servidor de integração, o arquivo está localizado em um dos seguintes caminhos: • /var/opt/kaspersky/viis/common/ para o Servidor de integração baseado em Linux • %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ para o Servidor de integração baseado em Windows O parâmetro `StandardAlgorithmSvmLocality` pode assumir os seguintes valores: • `ServerGroup` – se esse valor for selecionado, a SVM será considerada local em relação ao Light Agent se estiver localizada no mesmo grupo de servidores que a máquina virtual em que o Light Agent está instalado. Esse valor é usado por padrão. • `Project` – se esse valor for selecionado, a SVM será considerada local em relação ao Light Agent se estiver implementada no mesmo projeto do OpenStack que a máquina virtual com o Light Agent instalado. • `AvailabilityZone` – se esse valor for selecionado, a SVM será considerada local em relação ao Light Agent se estiver localizada na mesma zona de disponibilidade que a máquina virtual com o Light Agent instalado.	Em uma infraestrutura virtual em execução na plataforma OpenStack ou no VK Private Cloud, uma SVM pode ser considerada local em relação ao Light Agent em qualquer um dos seguintes casos: • Uma SVM está localizada no mesmo grupo de servidores que a máquina virtual com o Light Agent instalado. • Uma SVM está implementada no mesmo projeto do OpenStack que a máquina virtual com o Light Agent instalado. • Uma SVM está localizada na mesma zona de disponibilidade que a máquina virtual com o Light Agent instalado.

Além dos algoritmos de conexão de SVM, é possível regular a conexão de Light Agents com SVMs usando tags.

Configuração do algoritmo de seleção de SVMs

Como configurar o algoritmo de seleção de SVMs para o Light Agent no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Modo Light Agent** → **Algoritmo de seleção de SVMs**.
4. Selecione o algoritmo:
   - **Usar o algoritmo de seleção de SVM padrão**. O Light Agent seleciona SVMs implementados no mesmo hipervisor.
   - **Usar o algoritmo de seleção de SVM estendido**. O Light Agent seleciona SVMs implementados no tipo de caminho do SVM selecionado (por padrão, **Hipervisor**).

5. Se necessário, selecione caminho do SVM para o algoritmo de seleção de SVMs estendido:

- **Hipervisor**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

  - As SVMs são implementados no mesmo hipervisor que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual baseada em Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - A SVM está localizada no mesmo grupo de servidores que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual em execução na plataforma OpenStack ou no VK Private Cloud).

  - A SVM está localizada no mesmo nó que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual do Basis Dynamix Enterprise).

  Se não houver SVMs disponíveis para conexão no mesmo hipervisor ou no mesmo Grupo de servidores em que a máquina virtual com o Light Agent está localizada, o Light Agent não se conectará à SVM.

- **Cluster**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

  - As SVMs são implementados no mesmo cluster do hipervisor que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual baseada em Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - As SVMs são implementados no mesmo projeto do OpenStack que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual em execução na plataforma OpenStack ou no VK Private Cloud).

  - A SVM está localizada na mesma zona que a máquina virtual com o Light Agent instalado (na infraestrutura virtual do Basis Dynamix Enterprise).

  Se não houver SVMs disponíveis para conexão no mesmo cluster de hipervisor ou no mesmo projeto OpenStack em que a máquina virtual com o Light Agent está localizada, o Light Agent não se conectará à SVM.

- **Datacenter**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

  - As SVMs são implementados no mesmo data center que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual baseada em Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - As SVMs são localizadas na mesma zona de disponibilidade que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual em execução na plataforma OpenStack ou no VK Private Cloud).

  - A SVM está localizada no mesmo data center que a máquina virtual com o Light Agent instalado (na infraestrutura virtual do Basis Dynamix Enterprise).

Se não houver nenhum SVM disponível para conexão no mesmo datacenter ou zona de disponibilidade em que a máquina virtual com o Light Agent está localizada, o Light Agent não se conecta ao SVM.

- **Ignorar**. O Light Agent ignora o caminho do SVM para se conectar ao Servidor de proteção. Os Light Agents levam em consideração outros critérios: tags, o número de Light Agents conectados a um SVM e assim por diante.

6. Salvar alterações.

Como configurar o algoritmo de seleção de SVMs para o Light Agent no Web Console

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

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Modo Light Agent** → **Algoritmo de seleção de SVMs**.
5. Selecione o algoritmo:

   - **Usar o algoritmo de seleção de SVM padrão**. O Light Agent seleciona SVMs implementados no mesmo hipervisor.
   - **Usar o algoritmo de seleção de SVM estendido**. O Light Agent seleciona SVMs implementados no tipo de caminho do SVM selecionado (por padrão, **Hipervisor**).
6. Se necessário, selecione caminho do SVM para o algoritmo de seleção de SVMs estendido:

   - **Hipervisor**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

     - As SVMs são implementados no mesmo hipervisor que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual baseada em Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).
     - A SVM está localizada no mesmo grupo de servidores que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual em execução na plataforma OpenStack ou no VK Private Cloud).
     - A SVM está localizada no mesmo nó que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual do Basis Dynamix Enterprise).

     Se não houver SVMs disponíveis para conexão no mesmo hipervisor ou no mesmo Grupo de servidores em que a máquina virtual com o Light Agent está localizada, o Light Agent não se conectará à SVM.

- **Cluster**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

  - As SVMs são implementados no mesmo cluster do hipervisor que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual baseada em Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - As SVMs são implementados no mesmo projeto do OpenStack que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual em execução na plataforma OpenStack ou no VK Private Cloud).

  - A SVM está localizada na mesma zona que a máquina virtual com o Light Agent instalado (na infraestrutura virtual do Basis Dynamix Enterprise).

  Se não houver SVMs disponíveis para conexão no mesmo cluster de hipervisor ou no mesmo projeto OpenStack em que a máquina virtual com o Light Agent está localizada, o Light Agent não se conectará à SVM.

- **Datacenter**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

  - As SVMs são implementados no mesmo data center que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual baseada em Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - As SVMs são localizadas na mesma zona de disponibilidade que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual em execução na plataforma OpenStack ou no VK Private Cloud).

  - A SVM está localizada no mesmo data center que a máquina virtual com o Light Agent instalado (na infraestrutura virtual do Basis Dynamix Enterprise).

  Se não houver nenhum SVM disponível para conexão no mesmo datacenter ou zona de disponibilidade em que a máquina virtual com o Light Agent está localizada, o Light Agent não se conecta ao SVM.

- **Ignorar**. O Light Agent ignora o caminho do SVM para se conectar ao Servidor de proteção. Os Light Agents levam em consideração outros critérios: tags, o número de Light Agents conectados a um SVM e assim por diante.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como configurar o algoritmo de seleção de SVMs para o Light Agent na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .

2. Na janela de configurações do aplicativo, em **Modo Light Agent**, clique no bloco **Configurações de descoberta de SVM**.

3. Selecione o algoritmo:

   - **Usar o algoritmo de seleção de SVM padrão**. O Light Agent seleciona SVMs implementados no mesmo hipervisor.

   - **Usar o algoritmo de seleção de SVM estendido**. O Light Agent seleciona SVMs implementados no tipo de caminho do SVM selecionado (por padrão, **Hipervisor**).

4. Se necessário, selecione caminho do SVM para o algoritmo de seleção de SVMs estendido:

- **Hipervisor**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

  - As SVMs são implementados no mesmo hipervisor que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual baseada em Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - A SVM está localizada no mesmo grupo de servidores que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual em execução na plataforma OpenStack ou no VK Private Cloud).

  - A SVM está localizada no mesmo nó que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual do Basis Dynamix Enterprise).

  Se não houver SVMs disponíveis para conexão no mesmo hipervisor ou no mesmo Grupo de servidores em que a máquina virtual com o Light Agent está localizada, o Light Agent não se conectará à SVM.

- **Cluster**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

  - As SVMs são implementados no mesmo cluster do hipervisor que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual baseada em Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - As SVMs são implementados no mesmo projeto do OpenStack que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual em execução na plataforma OpenStack ou no VK Private Cloud).

  - A SVM está localizada na mesma zona que a máquina virtual com o Light Agent instalado (na infraestrutura virtual do Basis Dynamix Enterprise).

  Se não houver SVMs disponíveis para conexão no mesmo cluster de hipervisor ou no mesmo projeto OpenStack em que a máquina virtual com o Light Agent está localizada, o Light Agent não se conectará à SVM.

- **Datacenter**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

  - As SVMs são implementados no mesmo data center que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual baseada em Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer ou Basis Dynamix Standard).

  - As SVMs são localizadas na mesma zona de disponibilidade que a máquina virtual com o Light Agent instalado (em uma infraestrutura virtual em execução na plataforma OpenStack ou no VK Private Cloud).

  - A SVM está localizada no mesmo data center que a máquina virtual com o Light Agent instalado (na infraestrutura virtual do Basis Dynamix Enterprise).

Se não houver nenhum SVM disponível para conexão no mesmo datacenter ou zona de disponibilidade em que a máquina virtual com o Light Agent está localizada, o Light Agent não se conecta ao SVM.

- **Ignorar**. O Light Agent ignora o caminho do SVM para se conectar ao Servidor de proteção. Os Light Agents levam em consideração outros critérios: tags, o número de Light Agents conectados a um SVM e assim por diante.

5. Salvar alterações.

Distribuição das conexões de Light Agents com SVMs (tags)

Vários Light Agents podem se conectar a um SVM. Para equilibrar as conexões do Light Agent, é possível especificar uma lista separada de SVMs. Ao usar um Servidor de integração para a descoberta de SVM, é possível usar *tags* para equilibrar as conexões do Light Agent a SVMs. Ou seja, para um Light Agent, é possível atribuir uma lista de SVMs para conexão usando uma tag. Para fazer isso, é necessário atribuir uma tag ao Light Agent e especificá-la nas configurações de SVM. Para obter detalhes sobre como especificar tags nas configurações de SVM, consulte a Ajuda do Kaspersky Security for Virtualization Light Agent.

Exemplo: A solução Kaspersky Endpoint Detection and Response Optimum é implementada em sua infraestrutura para hosts de máquina virtual designados. Nesse caso, é possível atribuir a tag do `[EDROptimum]` ao Light Agent para fazer com que ele se conecte aos SVMs que tenham a chave da licença do EDR Optimum (add-on do EDR Optimum) adicionada. Como resultado, será possível usar a funcionalidade EDR Optimum na máquina virtual com o Light Agent. Ao conectar o Light Agent a um SVM sem uma chave de licença do EDR Optimum, a funcionalidade do Kaspersky Endpoint Detection and Response Optimum ficará indisponível.

Como atribuir uma tag de conexão SVM a um Light Agent no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Modo Light Agent** → **Tag de conexão SVM**.
4. Marque a caixa de seleção **Usar tag de conexão** e insira uma tag de conexão ao SVM.

   Para cada tag, é possível inserir uma cadeia de texto de até 255 caracteres. É possível usar qualquer caractere, exceto `;`.

5. Salvar alterações.

Como atribuir uma tag de conexão SVM a um Light Agent no Web Console

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

   A janela de propriedades da política é exibida.

3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Modo Light Agent** → **Tag de conexão SVM**.

5. Marque a caixa de seleção **Usar tag de conexão** e insira uma tag de conexão ao SVM.

   Para cada tag, é possível inserir uma cadeia de texto de até 255 caracteres. É possível usar qualquer caractere, exceto `;`.

6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como atribuir uma tag de conexão SVM a um Light Agent na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .
2. Na janela de configurações do aplicativo, em **Modo Light Agent**, clique no bloco **Tag de conexão SVM**.
3. Marque a caixa de seleção **Usar tag de conexão** e insira uma tag de conexão ao SVM.

   Para cada tag, é possível inserir uma cadeia de texto de até 255 caracteres. É possível usar qualquer caractere, exceto `;`.

4. Salvar alterações.

Proteger a conexão entre Light Agent e SVM

É possível configurar a criptografia da conexão entre os Light Agents e o Servidor de proteção. Para fazer isso, é necessário ativar a criptografia do canal de dados entre o Light Agent e o Servidor de proteção nas configurações do Servidor de proteção no SVM e nas configurações do Light Agent.

Um Light Agent para o qual a proteção de conexão está ativada só pode se conectar a SVMs para os quais a criptografia do canal de dados entre o Light Agent e o Servidor de proteção está ativada. Um Light Agent para o qual a proteção de conexão está desativada só pode se conectar a SVMs para os quais a criptografia de canal está desativada ou uma conexão não segura entre o Servidor de proteção e o Light Agent é permitida.

Para obter detalhes sobre como configurar a proteção de conexão no Servidor de proteção, consulte a Ajuda do Kaspersky Security for Virtualization Light Agent.

> Proteger a conexão usando criptografia pode reduzir o desempenho do Kaspersky Security for Virtualization Light Agent.

Como configurar a proteção da conexão em um Light Agent no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Modo Light Agent** → **Proteção de conexão**.
4. Marque a caixa de seleção **Criptografar o canal de dados entre o Light Agent e o Servidor de Proteção**.
5. Salvar alterações.

Como configurar a proteção da conexão em um Light Agent no Web Console

1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Modo Light Agent** → **Proteção de conexão**.
5. Marque a caixa de seleção **Criptografar o canal de dados entre o Light Agent e o Servidor de Proteção**.
6. Para aplicar a política aos computadores, feche os ícones de cadeado e salve as alterações.

Como configurar a proteção da conexão em um Light Agent na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão .
2. Na janela de configurações do aplicativo, em **Modo Light Agent**, clique no bloco **Proteção de conexão**.
3. Marque a caixa de seleção **Criptografar o canal de dados entre o Light Agent e o Servidor de Proteção**.
4. Salvar alterações.

Ativar o Light Agent

Se o Kaspersky Endpoint Security estiver sendo usado no modo Light Agent para proteger ambientes virtuais, não há necessidade de ativar o aplicativo separadamente. Para ativar o aplicativo, é necessário adicionar uma chave de licença ao SVM. É possível adicionar uma chave da licença ao SVM usando a tarefa especial no console do Kaspersky Security Center. Não é possível gerenciar chaves da licença na interface do Light Agent, no entanto, o usuário pode visualizar as informações da licença (veja a figura abaixo). Também é possível visualizar as informações de licenciamento do Light Agent na linha de comando (consulte as instruções abaixo). O Light Agent obtém essas informações do SVM. Para obter detalhes sobre como ativar a solução e gerenciar chaves de licença, consulte a Ajuda do Kaspersky Security for Virtualization Light Agent.

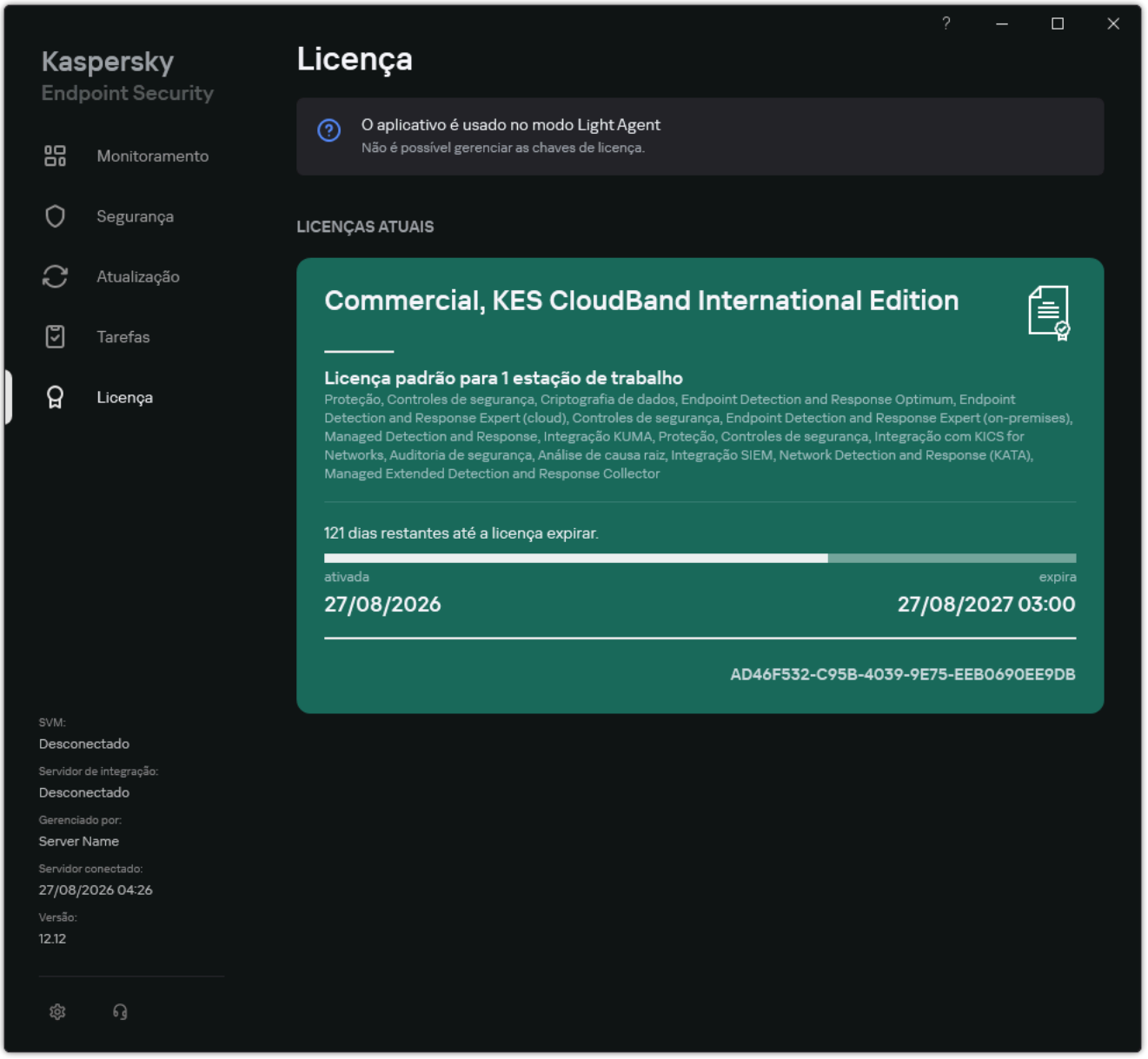
Para ver as informações de licenciamento do Light Agent:

1. Execute o interpretador da linha de comando (cmd) como um administrador.
2. Vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

3. Execute o seguinte comando:

```
avp.com LICENSE /CHECK
```

Como resultado, o Kaspersky Endpoint Security exibe as informações da licença: endereço do SVM a que o Light Agent está conectado, o número de dias até a expiração da licença e outras informações. Caso encontre algum problema ao ativar o Light Agent, consulte a Base de Dados de Conhecimento do Suporte Técnico.



A janela Licença

Guia de migração do KSVLA Light Agent para o KES Light Agent

O Kaspersky Security for Virtualization 5.2 Light Agent inclui o componente Light Agent for Windows 5.2 (aqui também referido como "KSVLA Light Agent"). No Kaspersky Security for Virtualization Light Agent 6.2, o Kaspersky Endpoint Security no modo Light Agent é usado como o componente Light Agent. Para atualizar a solução para a versão 6.2, é necessário migrar do KSVLA Light Agent 5.2 para o Kaspersky Endpoint Security no modo Light Agent (aqui também referido como "KES Light Agent"). Para obter detalhes sobre como atualizar a versão da solução Kaspersky Security for Virtualization Light Agent, consulte a Ajuda do Kaspersky Security for Virtualization Light Agent.

Requisitos de software

Antes de iniciar a migração do KSVLA Light Agent para o KES Light Agent, verifique se sua máquina virtual atende aos requisitos de hardware e software do Kaspersky Endpoint Security for Windows. As listas de versões de sistemas operacionais compatíveis são diferentes para KES e KSWS. Por exemplo, o KES não é compatível com servidores que executam o Windows Server 2003.

Requisitos mínimos de software para migrar do KSVLA Light Agent para o KES Light Agent:

- Kaspersky Endpoint Security para Windows 12.8.
- Kaspersky Security for Virtualization Light Agent 6.2 (incluindo os componentes do Servidor de Proteção e do Servidor de Integração).
- Kaspersky Security Center 14.2

  Caso tenha uma versão anterior do Kaspersky Security Center instalada, basta atualizá-la para a versão 14.2 ou posterior. Nesta versão do Kaspersky Security Center, o assistente de conversão em lote de políticas e tarefas permite migrar as políticas para um perfil em vez de migrar para uma política. Nesta versão do Kaspersky Security Center, o assistente de conversão em lote de políticas e tarefas também permite a migração de uma gama mais ampla de configurações de política.

Etapas de migração

A migração do KSVLA Light Agent para o KES Light Agent é realizada de forma semiautomática. Isso é necessário devido às diferentes arquiteturas dos aplicativos.

Migre do KSVLA Light Agent para o KES Light Agent na seguinte ordem:

1. **Migre as tarefas e as políticas do KSVLA Light Agent**

   Para migrar configurações de política, é preciso executar o assistente de conversão em lote de políticas e tarefas (o assistente de migração). Depois de migrar as configurações de política, é preciso definir manualmente as configurações que o assistente de migração não pode migrar automaticamente (por exemplo, as Configurações de atualização do banco de dados). Após a migração, também é recomendável verificar se o assistente de migração migrou corretamente todas as configurações.

   > Se a Proteção por senha estiver ativada para restringir o acesso ao KSVLA Light Agent, antes de instalar o KES Light Agent, será necessário desativar a Proteção por senha na política do KSVLA Light Agent. Não é possível inserir a senha de desinstalação nas configurações do pacote de instalação do KES Light Agent. Depois de concluir a instalação do KES Light Agent sobre o KSVLA Light Agent, será necessário ativar a Proteção por senha na política do KES.

2. **Instale o Kaspersky Endpoint Security no modo Light Agent**

   É possível instalar o KES Light Agent das seguintes maneiras:

   - Instalando o KES Light Agent após remover o KSVLA Light Agent (recomendado)
   - Instalando o KES Light Agent sobre o KSVLA Light Agent

3. **Confirme se o aplicativo está funcionando corretamente após a migração**

   Depois de migrar do KSVLA Light Agent para o KES Light Agent, verifique se o aplicativo está funcionando corretamente. Ative a política convertida. Verifique o status da máquina virtual no console do Kaspersky Security Center (deve ser *OK*). Certifique-se de que nenhum erro esteja relatado para o aplicativo, além de verificar a hora da última conexão ao SVM e o status de proteção da máquina virtual. Não é necessário ativar o Light Agent porque a chave da licença é adicionada ao SVM.

Instalação do KES Light Agent em vez do KSVLA Light Agent

É possível instalar o KES Light Agent das seguintes maneiras:

- Instalando o KES Light Agent após remover o KSVLA Light Agent (recomendado)
- Instalando o KES Light Agent sobre o KSVLA Light Agent

Removendo o KSVLA Light Agent

É possível remover o aplicativo remotamente usando a tarefa *Instalar o aplicativo remotamente*, localmente na máquina virtual ou no modelo de máquina virtual. Depois de remover o KSVLA Light Agent, pode ser necessário reiniciar a máquina virtual.

Depois de remover o KSVLA Light Agent, instale o KES Light Agent usando qualquer método disponível.

Se a Proteção por senha estiver ativada para restringir o acesso ao KSVLA Light Agent, antes de instalar o KES Light Agent, será necessário desativar a Proteção por senha na política do KSVLA Light Agent. Não é possível inserir a senha de desinstalação nas configurações do pacote de instalação do KES Light Agent. Depois de concluir a instalação do KES Light Agent sobre o KSVLA Light Agent, será necessário ativar a Proteção por senha na política do KES.

Ao instalar o Kaspersky Endpoint Security, é necessário selecionar o modo **Light Agent para garantir a proteção em ambientes virtuais**. Antes de instalar o KES Light Agent em uma máquina virtual, o instalador detecta o KSVLA Light Agent como um software incompatível e o remove. A migração da configuração do KSVLA Light Agent não é compatível. Ou seja, ao instalar o KES Light Agent, o conjunto de componentes a instalar será determinado por sua seleção nas propriedades do pacote de instalação ou no assistente de instalação. Depois de remover o KSVLA Light Agent, é preciso reiniciar a máquina virtual.

Configurações e tarefas do KSVLA Light Agent não são migradas quando instalamos o KES Light Agent. Para migrar as configurações e tarefas, execute o assistente de conversão de políticas e tarefas em lote.

É possível verificar a lista de componentes instalados na seção **Segurança** da interface do aplicativo, basta utilizar o comando `status` ou acessar o console do Kaspersky Security Center nas propriedades do computador. É possível alterar o conjunto de componentes após a instalação usando *Alterar componentes do aplicativo*.

Correspondência entre os componentes do KSVLA Light Agent e do KES Light Agent

Os conjuntos de componentes do KSVLA Light Agent e do KES Light Agent são praticamente os mesmos. O KES Light Agent tem mais configurações que o KSVLA Light Agent. Após a migração, as novas configurações terão valores padrão.

Correspondência entre os componentes do KSVLA Light Agent e do KES Light Agent

Light Agent 5.2	KES Light Agent
Scan kernel	Kernel do aplicativo
File Anti-Virus	Proteção Contra Ameaças ao Arquivo
Mail Anti-Virus	Proteção Contra Ameaças ao Correio
Web Anti-Virus	Proteção Contra Ameaças da Web
Firewall	Firewall
Network Attack Blocker	Proteção Contra Ameaças à Rede
Application Privilege Control	Prevenção de Intrusão do Host
Applications Launch Control	Controle de aplicativos
Web Control	Controle da Web
Device Control	Controle de dispositivos
System Watcher	No Kaspersky Endpoint Security, esse componente é dividido nos seguintes componentes: • Prevenção de Exploits • Detecção de Comportamento • Mecanismo de Remediação
System Integrity Monitoring	Monitor de integridade do sistema

Light Agent 5.2	KES Light Agent
Integration with Kaspersky Endpoint Agent	*(não compatível)* A partir do Kaspersky Endpoint Security for Windows 11.9.0, o pacote de distribuição do Kaspersky Endpoint Agent não faz mais parte do kit de distribuição.
AMSI Protection	Proteção AMSI

Migração de tarefas e políticas do KSVLA Light Agent

É possível migrar as configurações das políticas e das tarefas do KSVLA Light Agent usando o Assistente de conversão em lote de políticas e tarefas (aqui também referido como o "Assistente de migração").

O Assistente de Migração para KSVLA Light Agent está disponível apenas no Console de Administração (MMC). As configurações de política e tarefa não podem ser migradas no Web Console e Cloud Console.

As seguintes considerações especiais estão envolvidas na migração de políticas e tarefas:

- Uma nova política tem o nome *<Política> (convertido)*.
- A nova política possui o status *Política inativa*.
- A proibição de modificar configurações ("cadeado") não é migrada. O Assistente de Migração define valores padrão.
- Os perfis da política não são migrados. É preciso adicionar manualmente os perfis da política.
- Gerenciamento aprimorado da zona confiável. No KSVLA Light Agent, é possível adicionar exclusões predefinidas somente ao criar uma política. Posteriormente, nas propriedades da política, é possível configurar exclusões predefinidas adicionadas anteriormente ou adicionar exclusões manualmente. Não é possível adicionar exclusões predefinidas nas propriedades da política. No KES Light Agent, as exclusões predefinidas ficam disponíveis durante a criação da política e nas propriedades da política criada. Também é possível selecionar exclusões predefinidas no pacote de instalação.
- A configuração da interface do usuário do aplicativo no Kaspersky Endpoint Security foi movida do instalador para a política. Se for necessário, por exemplo, ocultar a interface do usuário do aplicativo, gerencie as configurações da política.
- Os conjuntos de funcionalidades para configurar o controle de acesso baseado em direitos (RBAC) são diferentes no Kaspersky Endpoint Security e no KSVLA Light Agent. É necessário configurar os direitos de acesso do usuário às áreas funcionais do zero.

Como usar o assistente de Conversão de políticas e tarefas em lotes para migrar as configurações de política do KSVLA Light Agent

1. No Console de administração, 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**.

O Assistente de Conversão de Políticas e Tarefas em Lotes será iniciado. Siga as instruções do Assistente.

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

Nesta etapa, é preciso selecionar o Kaspersky Endpoint Security for Windows. Vá para a próxima etapa.

Etapa 2. Conversão de políticas

Selecione a política do Kaspersky Security for Virtualization 5.2 Light Agent for Windows que deseja converter. Vá para a próxima etapa.

O Assistente de Migração começará a converter as políticas. Durante a conversão, o Assistente de migração solicita que o usuário aceite as condições da Declaração da KSN. Uma nova política tem o nome *<Política> (convertido)*.

Etapa 3. Conversão de tarefas

O Assistente de migração cria novas tarefas para o Kaspersky Endpoint Security for Windows. Na lista, selecione as tarefas do KSVLA Light Agent que deseja criar para o Kaspersky Endpoint Security. Novas tarefas serão nomeadas *<Nome da tarefa> (convertido)*. Vá para a próxima etapa.

Etapa 4. Conclusão do Assistente

Conclua o assistente.

Depois de migrar uma política, é necessário abrir as propriedades dela, verificar suas configurações e salvá-la. Caso não conclua essas etapas, o KES Light Agent poderá ignorar a política convertida.

Observe especialmente a migração de configurações de conexão de SVM do Light Agent, listas de exclusão, aplicativos confiáveis, endereços da Web confiáveis e regras de controle de aplicativos.

Migração da configuração [KSVLA Light Agent+KEA] para a configuração [KES Light Agent+agente integrado]

Para oferecer suporte ao uso do Kaspersky Endpoint Security for Windows como parte do EDR (KATA), EDR Optimum e Kaspersky Sandbox, um agente integrado foi adicionado ao aplicativo. Não é mais preciso um aplicativo separado do Kaspersky Endpoint Agent para trabalhar com estas soluções.

Ao migrar do KSVLA Light Agent para o KES Light Agent, as soluções EDR (KATA), EDR Optimum e Kaspersky Sandbox continuam funcionando com os agentes integrados do Kaspersky Endpoint Security. Além disso, o Kaspersky Endpoint Agent será removido do computador.

Antes de migrar do KSVLA Light Agent para o KES Light Agent, é necessário atualizar todos os componentes do Kaspersky Security for Virtualization para a versão 6.2, incluindo o Servidor de proteção e o Servidor de integração. Para obter detalhes sobre como atualizar a versão da solução Kaspersky Security for Virtualization Light Agent, consulte a Ajuda do Kaspersky Security for Virtualization Light Agent.

A migração da configuração [KSVLA Light Agent+KEA] para a configuração [KES Light Agent+agente integrado] envolve as seguintes etapas:

1. **Migração das políticas e tarefas**

   A migração de políticas e tarefas [KSVLA Light Agent+KEA] para [KES Light Agent+agente integrado] envolve as seguintes etapas:

   1. Migração de políticas e tarefas do KSVLA Light Agent para o KES Light Agent usando o assistente de Conversão de políticas e tarefas em lote (disponível apenas no Console de Administração [MMC]).

      Como resultado, uma nova política é criada com o nome *<Política> (convertida)*. Novas tarefas do KES também são criadas com os nomes *<nome de tarefa> (convertida)*.

   2. Migração de políticas e tarefas de KEA para KES usando o assistente para migração do Kaspersky Endpoint Agent (disponível apenas no Web Console e no Cloud Console).

      Como resultado, uma nova política é criada com o nome *<Nome da política do Kaspersky Endpoint Security> & <Nome da política do Kaspersky Endpoint Agent>*. Novas tarefas e tarefas KES também são criadas.

2. **Migração do KSVLA Light Agent para o KES Light Agent**

   A migração do KSVLA Light Agent para o KES Light Agent envolve a instalação do KES Light Agent em vez do KSVLA Light Agent.

   Geralmente, os administradores ativam a Proteção por senha para restringir o acesso ao KSVLA Light Agent e ao KEA. É possível inserir a senha de desinstalação do KEA somente nas propriedades da tarefa *Instalar o aplicativo remotamente*. Para a migração, é necessário desativar a Proteção por senha para o KSVLA Light Agent.

   Para realizar a migração, é necessário selecionar os componentes necessários de suporte às soluções de Detection and Response como parte do Kaspersky Endpoint Security. Após instalação do aplicativo, o Kaspersky Endpoint Security alterna o uso do agente integrado e remove o Kaspersky Endpoint Agent.

3. **Licenciamento da funcionalidade**

   Se o aplicativo estiver sendo usado no modo Light Agent, não há necessidade de ativar o aplicativo. Para ativar o aplicativo, é necessário adicionar uma chave de licença ao SVM. Também é necessário adicionar a chave de licença para ativar a funcionalidade adicional (por exemplo, EDR Optimum) ao SVM. Ou seja, como parte da migração, o licenciamento da funcionalidade ocorre automaticamente.

4. **Verificação da saúde do Kaspersky Endpoint Detection and Response Optimum e Kaspersky Sandbox**

Se, após a atualização, o computador estiver com o status *Crítico* no console do Kaspersky Security Center:

- Certifique-se de que o computador possui o Agente de Rede versão 13.2 ou posterior instalado.
- Verifique o status operacional do agente integrado visualizando o *Relatório de status dos componentes do aplicativo*. Caso o componente tenha o status *Não instalado*, instale o componente usando a tarefa *Alterar componentes do aplicativo*.
- Certifique-se de aceitar a Declaração da Kaspersky Security Network na nova política do Kaspersky Endpoint Security for Windows.
- Assegure-se de que a funcionalidade EDR Optimum esteja ativada usando o *Relatório de status dos componentes do aplicativo*. Caso um componente tenha o status *Não coberto pela licença*, certifique-se de que funcionalidade de distribuição automática da chave de licença do EDR Optimum esteja ligada.
- Verifique o status da conexão da máquina virtual com o SVM. É possível obter informações sobre o status da conexão do Light Agent ao SVM no Kaspersky Endpoint Security ou usando o comando do aplicativo.

Gerenciar o aplicativo a partir da linha de comando

Você pode gerenciar o Kaspersky Endpoint Security a partir da linha de comando. Você pode visualizar a lista de comandos para gerenciar o aplicativo, executando o comando `avp.com HELP` (AJUDA). Para ler sobre a sintaxe de um comando específico, digite `avp.com HELP <command>`.

Caracteres especiais no comando devem ser escapados. Para ignorar os caracteres `&`, `|`, `(`, `)`, `<`, `>`, `^`, use o caractere `^` (por exemplo, para usar o caractere `&`, digite `^&`). Para escapar o caractere `%`, digite `%%`.

Em alternativa ao valor `1`, é possível usar os valores `yes`, `on`, `enable`, `enabled` e `true`. Em alternativa ao valor `0`, é possível usar os valores `no`, `off`, `disable`, `disabled` e `false`.

Setup. Instalar o aplicativo

A instalação do aplicativo pela linha de comando envolve as seguintes etapas:

1. **Escolha de um pacote de distribuição**

   A Kaspersky fornece pacotes de distribuição para diferentes localizações, compatíveis com diferentes arquiteturas de CPU e que incluem diversos módulos de criptografia.

   O kit de distribuição inclui os seguintes pacotes de distribuição:

   - **AES256**

     Esse pacote de distribuição se destina à instalação em computadores com arquitetura x86/x64. Esse pacote de distribuição contém ferramentas criptográficas que implementam o algoritmo de criptografia AES (Advanced Encryption Standard), com um comprimento de chave efetivo de 256 bits.

   - **AES56**

     Esse pacote de distribuição se destina à instalação em computadores com arquitetura x86/x64. Esse pacote de distribuição contém ferramentas criptográficas que implementam o algoritmo de criptografia AES, com um comprimento de chave efetivo de 56 bits.

   - **Arm64**

     Este pacote de distribuição está destinado à instalação em computadores baseados em Arm. Esse pacote de distribuição não se destina à instalação em servidores.

2. **Transferência do pacote de distribuição do aplicativo para o armazenamento do computador**

   O pacote de distribuição é um arquivo compactado de extração automática no formato EXE. Para visualizar o conteúdo do pacote de distribuição, é necessário extrair o arquivo compactado para uma pasta separada. Para instalar o aplicativo, são necessários todos os arquivos do pacote de distribuição, incluindo o arquivo bases.cab.

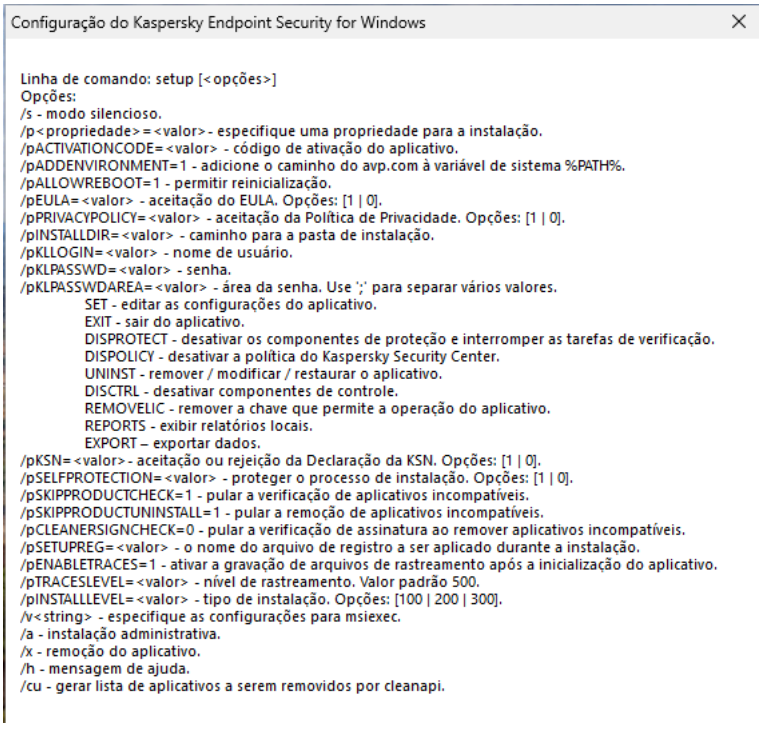
3. **Execução do comando de instalação**

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

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

> Antes de instalar o aplicativo no modo silencioso, abra e leia o Contrato de Licença de Usuário Final e o texto da Política de Privacidade. O Contrato de Licença de Usuário Final e o texto da Política de Privacidade estão incluídos no kit de distribuição do Kaspersky Endpoint Security. Você só pode continuar com a instalação do aplicativo se tiver lido, compreendido e aceitado integralmente as disposições e termos do Contrato de Licença de Usuário Final; se entender e concordar que seus dados serão processados e transmitidos (inclusive para países terceiros) de acordo com a Política de Privacidade; e se tiver lido e compreendido integralmente a Política de Privacidade. Se você não aceitar as provisões e termos do Contrato de Licença de Usuário Final e da Política de Privacidade, não instale nem use o Kaspersky Endpoint Security.

Você pode visualizar a lista de comandos para instalar o aplicativo executando o comando `/h`. Para obter ajuda sobre a sintaxe do comando de instalação, digite `setup_kes.exe /h`. Como resultado, o instalador exibe uma janela com uma descrição das opções de comando (veja a figura abaixo).



Descrição das opções de comando de instalação

Para instalar o aplicativo ou fazer um upgrade de uma versão anterior do aplicativo:

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

3. Execute o seguinte comando:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pCONFIGPATH=<path to the configuration file>]
[/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=
<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>]
[/pSKIPKB5007186CHECK=1] [/s]
```

ou

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration
file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password
scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/qn]
```

Assim, o aplicativo será instalado no computador. É possível confirmar se o aplicativo está instalado e verificar as suas configurações ao enviar o comando `status`.

Configurações de instalação do aplicativo

`EULA=1`	A aceitação dos termos do Contrato de Licença do Usuário Final. O texto do Contrato de Licença está incluído no kit de distribuição do Kaspersky Endpoint Security. A aceitação dos termos do Contrato de Licença de Usuário Final é necessária para instalar o aplicativo ou para atualizar uma versão do aplicativo.
`PRIVACYPOLICY=1`	Aceitação da Política de Privacidade. O texto da Política de Privacidade está incluído no kit de distribuição do Kaspersky Endpoint Security. Para instalar o aplicativo ou atualizar a versão do aplicativo, aceite a Política de Privacidade.
`KSN`	Acordo ou recusa em participar da Kaspersky Security Network (KSN). Se nenhum valor for definido para este parâmetro, o Kaspersky Endpoint Security solicitará a confirmação do seu consentimento ou recusa em participar da KSN quando o Kaspersky Endpoint Security for iniciado pela primeira vez. Valores disponíveis: • `1` – concordo em participar da KSN. • `0` – não aceito participar da KSN (valor padrão). O pacote de distribuição do Kaspersky Endpoint Security é otimizado para uso com a Kaspersky Security Network. Se você optar por não participar da Kaspersky Security Network, atualize o Kaspersky Endpoint Security assim que a instalação for concluída.
`CONFIGPATH=<path to the configuration file>`	Instalação do aplicativo com configurações predefinidas. Para fazer isso, você precisa carregar um arquivo que define as configurações do Kaspersky Endpoint Security. Você pode criar um arquivo de configuração na interface local do aplicativo.
`ALLOWREBOOT=1`	Reinício automático do computador, se necessário após a instalação ou atualização do aplicativo. Se nenhum valor for definido para esse parâmetro, a reinicialização automática do computador é bloqueada. Não é necessário reiniciar ao instalar o Kaspersky Endpoint Security. A reinicialização será necessária apenas se você precisar remover aplicativos incompatíveis antes da instalação. A reinicialização também poderá ser necessária quando a versão do aplicativo for atualizada.
`SKIPPRODUCTCHECK=1`	Desative a verificação de software instalado. A lista de softwares que podem causar problemas de compatibilidade está disponível no arquivo incompatible.txt do kit de distribuição. Se nenhum valor for definido para este parâmetro e um software da lista for detectado, a instalação do Kaspersky Endpoint Security será interrompida.
`SKIPPRODUCTUNINSTALL=1`	Desative a remoção automática do software detectado da lista incompatible.txt. Se nenhum valor for definido para este parâmetro, o Kaspersky Endpoint Security tentará remover o software que pode causar problemas de compatibilidade. A remoção automática de software não pode ser ativada ao instalar o Kaspersky Endpoint Security com o uso do instalador msiexec. Para remover automaticamente o software que pode causar problemas de compatibilidade, use o arquivo setup_kes.exe.

`CLEANERSIGNCHECK=0|1`	Verificação das assinaturas digitais dos arquivos de software detectados na lista incompatible.txt. Para remover o software, o Kaspersky Endpoint Security executa o arquivo do instalador do software. Se o arquivo do instalador não tiver assinatura digital, o Kaspersky Endpoint Security considera o arquivo não confiável e interrompe a remoção do software para evitar a execução de um possível código malicioso. Se o aplicativo não puder verificar a assinatura digital do arquivo de software detectado, a instalação do Kaspersky Endpoint Security é interrompida com um erro. O valor padrão é diferente dependendo do método de instalação do software: • `0` significa que a verificação de assinatura digital está desativada (valor padrão caso tenha sido implantado pelo Kaspersky Security Center). • `1` significa que a verificação de assinatura digital está ativada (valor padrão caso o aplicativo seja instalado localmente).
`STANDALONEMODE=1`	Instalação do aplicativo na configuração do Endpoint Detection and Response Agent (EDR Agent) para integração com as soluções Kaspersky Endpoint Detection and Response (KATA) ou Kaspersky Endpoint Detection and Response Expert (on-premises). Esta configuração é necessária caso uma Endpoint Protection Platform (EPP) de terceiros seja implantada na sua organização juntamente com a solução de primeira linha Kaspersky Endpoint Detection and Response. Isso torna o Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent compatível com os aplicativos EPP de terceiros.
`KLLOGIN`	Defina o nome de usuário para acessar os recursos e configurações do Kaspersky Endpoint Security (o componente Proteção por senha). O nome de usuário é definido junto com as configurações `KLPASSWD` e `KLPASSWDAREA`. O nome de usuário KLAdmin é usado por padrão.
`KLPASSWD`	Especifique uma senha para acessar os recursos e as configurações do Kaspersky Endpoint Security (a senha é especificada em conjunto com os parâmetros de `KLLOGIN` e `KLPASSWDAREA`). Se você especificou uma senha mas não especificou um nome de usuário com o parâmetro `KLLOGIN`, o nome de usuário KLAdmin é usado por padrão.
`KLPASSWDAREA`	Especifique o escopo da senha para acessar os recursos e as configurações do Kaspersky Endpoint Security. Quando um usuário tenta executar uma ação incluída nesse escopo, o Kaspersky Endpoint Security solicita as credenciais da conta do usuário (os parâmetros `KLLOGIN` e `KLPASSWD`). Use o caractere `;` para especificar vários valores. Valores disponíveis: • `SET` – modificar as configurações do aplicativo. • `EXIT` – sair do aplicativo. • `DISPROTECT` – desativar componentes de proteção e interromper tarefas de verificação. • `DISPOLICY` – desativar a política do Kaspersky Security Center. • `UNINST` – remover o aplicativo do computador. • `DISCTRL` – desativar componentes de controle. • `REMOVELIC` – remover a chave. • `REPORTS` – visualizar relatórios. • `EXPORT` – exportar as configurações do aplicativo. Por exemplo, `KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT`. A conta KLAdmin tem o direito de executar qualquer ação protegida por senha. Portanto, é impossível configurar o escopo da senha para a conta KLAdmin. Se o usuário tentar configurar o escopo da senha para a conta KLAdmin, o aplicativo proíbe as ações especificadas para o grupo "Todos".
`PROTECTOSSERVICES`	Proteção da funcionalidade dos serviços do sistema operacional. A proteção dos serviços do sistema operacional impede que aplicativos de terceiros interfiram no funcionamento desses serviços. Esses serviços incluem, por exemplo, o serviço de inicialização automática de aplicativos. • `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.
`ENABLETRACES`	Ativar ou desativar rastreamentos de aplicativos. Após o Kaspersky Endpoint Security ser iniciado, os arquivos de rastreamento serão salvos na pasta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. Valores disponíveis: • `1` – rastreamentos ativados. • `0` – rastreamentos desativados (valor padrão).
`TRACESLEVEL`	Nível de detalhe dos rastreamentos. Valores disponíveis: • `100` (crítico). Apenas mensagens sobre erros fatais. • `200` (alto). Mensagens sobre todos os erros, incluindo erros fatais. • `300` (diagnóstico). Mensagens sobre todos os erros, bem como avisos. • `400` (importante). Todas as mensagens de erro, avisos e informações adicionais. • `500` (normal). Mensagens sobre todos os erros e avisos, bem como informações detalhadas sobre a operação do aplicativo no modo normal (padrão). • `600` (baixo). Todas as mensagens.

`ENABLEAZURESUPPORT`	Ativação ou desativação do modo de compatibilidade Azure WVD. Valores disponíveis: • `1`: o modo de compatibilidade do Azure WVD está ativado. • `0`: o modo de compatibilidade do Azure WVD está desativado (valor padrão). Esse recurso garante a exibição correta do estado das máquinas virtuais Azure no console do Kaspersky Anti Targeted Attack Platform. Para monitorar o desempenho do computador, o Kaspersky Endpoint Security envia telemetria aos servidores da KATA. A telemetria inclui um ID do computador (Sensor ID). O modo de compatibilidade do Azure WVD permite atribuir um Sensor ID exclusivo e permanente para essas máquinas virtuais. Caso o modo de compatibilidade esteja desativado, o Sensor ID poderá mudar depois que o computador for reiniciado devido ao funcionamento das máquinas virtuais do Azure. Isso pode fazer com que máquinas virtuais duplicadas apareçam no console.
`AMPPL`	Ativa ou desativa a proteção do serviço Kaspersky Endpoint Security usando a tecnologia AM-PPL (Antimalware Protected Process Light). Para obter mais detalhes sobre a tecnologia AM-PPL, visite o site da Microsoft. A tecnologia AM-PPL está disponível para os sistemas operacionais Windows 10 versão 1703 (RS2) ou posterior e Windows Server 2019. Valores disponíveis: • `1` – Proteção do serviço Kaspersky Endpoint Security usando a tecnologia AM-PPL ativada. • `0` – Proteção do serviço Kaspersky Endpoint Security usando a tecnologia AM-PPL desativada.
`UPGRADEMODE`	Modo de atualização do aplicativo: • `Seamless` atualização do aplicativo com a reinicialização do computador (padrão). • `Force` atualização do aplicativo sem a reinicialização do computador. É possível atualizar o aplicativo sem reiniciar a partir da versão 11.10.0. Para atualizar uma versão anterior do aplicativo, é necessário reiniciar o computador. Também é possível instalar patches sem reiniciar a partir da versão 11.11.0. Não é necessário reiniciar ao instalar o Kaspersky Endpoint Security. Portanto, o modo de atualização do aplicativo será especificado nas configurações do aplicativo. É possível alterar este parâmetro nas configurações ou na política do aplicativo. Ao atualizar um aplicativo já instalado, a prioridade do parâmetro da linha de comando será menor do que aquela do parâmetro especificado nas configurações do aplicativo ou no arquivo setup.ini. Por exemplo, se o modo de atualização `Force` estiver especificado na linha de comando e o modo `Seamless` estiver especificado nas configurações do aplicativo, a atualização será instalada com a reinicialização do computador (`Seamless`).
`RESTAPI`	Gerenciamento do aplicativo por meio da API REST. Para gerenciar o aplicativo por meio da API REST, você deve especificar o nome do usuário (parâmetro `RESTAPI_User`). Valores disponíveis: • `1` – Gerenciamento via API REST permitido. • `0` – Gerenciamento via API REST bloqueado (valor padrão). Para gerenciar o aplicativo por meio da API REST, o gerenciamento usando sistemas administrativos deve ser permitido. Para fazer isso, defina o parâmetro `AdminKitConnector=1`. Se você gerencia o aplicativo por meio da API REST, é impossível gerenciar o aplicativo usando os sistemas de administração da Kaspersky.
`RESTAPI_User`	Nome de usuário da conta de domínio do Windows usada para gerenciar o aplicativo por meio da API REST. O gerenciamento do aplicativo por meio da API REST está disponível apenas para este usuário. Digite o nome do usuário no formato `<DOMAIN>\<UserName>` (por exemplo, `RESTAPI_User=COMPANY\Administrator`). Você pode selecionar apenas um usuário para trabalhar com a API REST. Adicionar um nome de usuário é um pré-requisito para gerenciar o aplicativo por meio da API REST.
`RESTAPI_Port`	Porta usada para gerenciar o aplicativo por meio da API REST. A porta 6782 é usada por padrão. Certifique-se de que a porta está livre.
`RESTAPI_Certificate`	Certificado de identificação de solicitações (por exemplo, `RESTAPI_Certificate=C:\cert.pem`). A interação segura do Kaspersky Endpoint Security com o cliente REST requer a configuração da identificação da solicitação. Para fazer isso, é necessário instalar um certificado e, posteriormente, assinar a carga útil de cada solicitação.
`ADMINKITCONNECTOR`	Gerenciamento de aplicativos usando sistemas de administração. Os sistemas de administração incluem, por exemplo, o Kaspersky Security Center. Além dos sistemas de administração da Kaspersky, você pode usar soluções de terceiros. O Kaspersky Endpoint Security fornece uma API para essa finalidade. Valores disponíveis: • `1` – Gerenciamento de aplicativos com a ajuda de sistemas de administração permitido (valor padrão). • `0` – Gerenciamento de aplicativos permitido apenas pela interface local.

`EnableUniqueSensorID`	Criar um identificador exclusivo do computador (Sensor ID) durante a instalação ou a atualização do aplicativo. O Sensor ID é usado na solução Kaspersky Anti Targeted Attack Platform para identificar computadores que enviam telemetria ao servidor. Ao criar o Sensor ID, o aplicativo usa um algoritmo que leva em consideração a configuração do computador, como o número de série da placa-mãe. Em alguns casos, por exemplo, ao usar o aplicativo em um ambiente virtual, o Sensor ID pode ser duplicado. Como resultado, a Kaspersky Anti Targeted Attack Platform não consegue identificar o computador do qual a telemetria é enviada. Para criar um Sensor ID exclusivo, é necessário definir o parâmetro `EnableUniqueSensorID=1`. Como resultado, o aplicativo usará um algoritmo diferente para criar o Sensor ID, que leva em consideração outros dados sobre o computador. Isso garante um Sensor ID exclusivo. Por padrão, o parâmetro não é definido. O aplicativo herda o Sensor ID nos seguintes casos: • Atualizar a versão do aplicativo; • migração da configuração [KES+KEA] para [KES+built-in agent]. Como parte do seu reparo, o instalador tenta herdar o Sensor ID. Se o Sensor ID não puder ser restaurado, o aplicativo criará um novo Sensor ID.
`SKIPKB5007186CHECK=1`	Desativar a verificação de atualização do sistema operacional instalado KB5007186. Antes de instalar o aplicativo, o instalador verifica as atualizações já feitas no sistema operacional. A atualização KB5007186 está na lista de atualizações do sistema operacional que podem causar problemas para o aplicativo. Para obter informações detalhadas, consulte a Base de Conhecimento do Suporte Técnico. Portanto, o instalador cancela a instalação se essa atualização for descoberta. Para prosseguir com a instalação, defina `SKIPKB5007186CHECK=1`.

Exemplo

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
```

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

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

Após instalar o Kaspersky Endpoint Security, a licença de avaliação é ativada, a menos que você tenha fornecido um código de ativação no arquivo setup.ini. Uma licença de avaliação geralmente tem um termo curto. Quando a licença de avaliação expira, todos os recursos do aplicativo do Kaspersky Endpoint Security são desativados. Para continuar usando o aplicativo, é necessário ativá-lo com uma licença comercial usando o Assistente de Ativação do Aplicativo ou um comando especial.

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

- setup.ini – configurações gerais da instalação do aplicativo.

  Para aplicar as configurações do arquivo setup.ini, coloque esse arquivo na pasta que contém o pacote de distribuição do Kaspersky Endpoint Security.

- install.cfg – configurações da operação do Kaspersky Endpoint Security

  Para aplicar as configurações do arquivo de configuração install.cfg, você precisa especificar o caminho para o arquivo no seguinte comando de instalação do aplicativo: `CONFIGPATH=<path to the configuration file>`.

- setup.reg – chaves de registro.

  As chaves de registro do arquivo setup.reg serão gravadas no registro apenas se o valor `setup.reg` estiver definido para o parâmetro `SetupReg` no arquivo setup.ini. O arquivo setup.reg é gerado pelos especialistas da Kaspersky. Não é recomendado modificar os conteúdos desse arquivo. Para aplicar as configurações do arquivo setup.reg, coloque esse arquivo na pasta que contém o pacote de distribuição do Kaspersky Endpoint Security. Você também pode colocar o arquivo setup.reg em uma pasta diferente. Se fizer isso, será necessário especificar o caminho para o arquivo no seguinte comando de instalação do aplicativo: `SETUPREG=<path to the setup.reg file>`.

Setup /x. Remoção do aplicativo

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

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

- No modo silencioso. Depois que a desinstalação tiver iniciado no modo silencioso, o seu envolvimento no processo de remoção não é necessário (desinstalação silenciosa). Para desinstalar o aplicativo no modo silencioso, use as opções `/s` e `/qn`.

Para desinstalar o aplicativo no modo silencioso:

1. Execute o interpretador da linha de comando (cmd.exe) como um administrador.

2. Vá até a pasta onde o pacote de distribuição do Kaspersky Endpoint Security está localizado.

3. Execute o seguinte comando:

   - Se o processo de remoção não estiver protegido por senha:

     ```
     setup_kes.exe /s /x
     ```

     ou

     ```
     msiexec.exe /x <GUID> /qn
     ```

     `<GUID>` é o identificador exclusivo do aplicativo. É possível descobrir o GUID do aplicativo na Base de Dados de Conhecimento do Suporte Técnico ou por meio do uso do seguinte comando:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - Se o processo de remoção for protegido por senha:

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

     ou

     ```
     msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Também é possível usar o parâmetro `SAVEQB` para salvar arquivos verificados pelo aplicativo e colocados no backup. As cópias de backup dos arquivos são armazenadas na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`. Por padrão, o salvamento de arquivos no backup está desativado (`SAVEQB=0`).

Exemplo

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

msiexec /i. Recuperação do aplicativo

Durante a recuperação, o aplicativo verifica e restaura a integridade de todos os módulos do aplicativo e chaves de registro do sistema danificados criados como parte do processo de instalação do aplicativo.

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

- Em modo interativo usando o Assistente de instalação de aplicativo.
- No modo silencioso. Depois de iniciar a recuperação no modo silencioso, o seu envolvimento no processo não é necessário.

Se o instalador do Kaspersky Endpoint Security estiver sendo executado no modo de recuperação e o aplicativo não precisar de recuperação, o instalador não fará nenhuma alteração.

Se o instalador do Kaspersky Endpoint Security estiver sendo executado no modo de recuperação e o aplicativo não estiver instalado, o instalador iniciará o processo de instalação.

Para recuperar o aplicativo no modo silencioso:

1. Execute o interpretador da linha de comando (cmd.exe) como um administrador.
2. Vá até a pasta onde o pacote de distribuição do Kaspersky Endpoint Security está localizado.
3. Execute o seguinte comando:
   - Se o processo de recuperação não for protegido por senha:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     `<GUID>` é o identificador exclusivo do aplicativo. É possível descobrir o GUID do aplicativo na Base de Dados de Conhecimento do Suporte Técnico ou por meio do uso do seguinte comando:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - Se o processo de recuperação for protegido por senha:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Exemplo

```
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

Comandos AVP

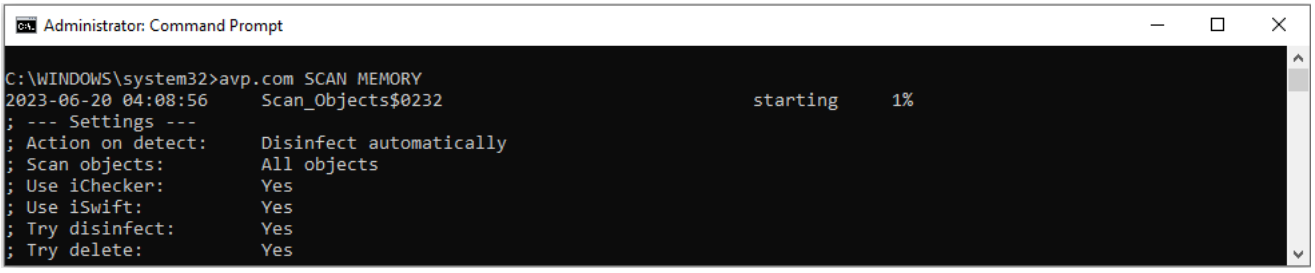
Para gerenciar o Kaspersky Endpoint Security a partir da linha de comando:

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

   É possível adicionar o caminho para o arquivo executável à variável de sistema %PATH% durante a instalação do aplicativo.
3. Use o seguinte modelo para executar o comando:

   ```
   avp.com <command> [options]
   ```

Como resultado, o Kaspersky Endpoint Security executará o comando (veja a figura abaixo).



Gerenciar o aplicativo a partir da linha de comando

SCAN. Verificação de malware

Execução da tarefa de *Verificação de malware*.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report
file>] [<scan technologies>] [/C:<file with scan settings>]
```

Escopo da verificação	
`<files to scan>`	Uma lista separada por espaços de arquivos e pastas. Caminhos longos devem ser colocados entre aspas. Caminhos abreviados (formato MS-DOS) não precisam ser colocados entre aspas. Por exemplo: • `"C:\Program Files (x86)\Example Folder"` - caminho longo. • `C:\PROGRA~2\EXAMPL~1` – caminho curto.
`/ALL`	Execute a tarefa de *Verificação de malware* Kaspersky Endpoint Security verifica os seguintes objetos: • Memória Kernel • Os objetos que são carregados quando o sistema operacional é iniciado • Setores de inicialização • Backup do sistema operacional • Todos os discos rígidos e unidades removíveis No Kaspersky Endpoint Security for Windows 12.12, o e-mail está excluído do escopo da verificação de aplicativos. A verificação de mensagens de e-mail recebidas e enviadas é realizada pelo componente Proteção Contra Ameaças ao Correio. Caso esteja usando uma versão anterior do plug-in de gerenciamento, o aplicativo excluirá o e-mail do escopo da verificação, mesmo que a política o inclua.
`/MEMORY`	Verifique a memória Kernel
`/STARTUP`	Verifique os Objetos carregados durante a inicialização do sistema operacional
`/REMDRIVES`	Todas as unidades removíveis.
`/FIXDRIVES`	Verifique os discos rígidos.
`/NETDRIVES`	Verifique as unidades de rede.
`/QUARANTINE`	Verifique os arquivos no Backup do Kaspersky Endpoint Security.
`/@:<file list.lst>`	Verifique os arquivos e pastas de uma lista. Cada arquivo na lista deve estar em uma nova linha. Caminhos longos devem ser colocados entre aspas. Caminhos abreviados (formato MS-DOS) não precisam ser colocados entre aspas. Por exemplo: • `"C:\Program Files (x86)\Example Folder"` - caminho longo. • `C:\PROGRA~2\EXAMPL~1` – caminho curto.

Ação ao detectar ameaças	
`/i0`	**Informar**. Caso esta opção seja selecionada, o Kaspersky Endpoint Security adiciona as informações sobre arquivos infectados à lista de ameaças ativas na detecção destes arquivos.
`/i1`	**Desinfectar e informar se a desinfecção falhar**. Caso esta opção seja selecionada, o Kaspersky Endpoint Security tentará desinfectar automaticamente todos os arquivos infectados que são detectados. Caso a desinfeção não seja possível, o Kaspersky Endpoint Security adicionará as informações sobre os arquivos infectados e detectados na lista de ameaças ativas.
`/i2`	**Desinfectar e excluir se a desinfecção falhar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Caso a desinfecção falhe, o aplicativo excluirá o arquivo. Esta ação é selecionada por padrão.
`/i3`	**Excluir, se a desinfecção falhar**. Exclua também os arquivos compostos (por exemplo, arquivos mortos) se o arquivo infectado não puder ser desinfectado ou excluído.
`/i4`	**Excluir**. Exclua também os arquivos compostos (por exemplo, arquivos mortos) se o arquivo infectado não puder ser excluído.

Tipos de arquivos	
`/fe`	**Arquivos verificados por extensão**. Se esta configuração for ativada, o aplicativo verificará apenas arquivos infetáveis. O formato do arquivo é determinado com base na extensão do arquivo.

`/fi`	**Arquivos verificados por formato**. Se esta configuração for ativada, o aplicativo verificará apenas arquivos infetáveis. Antes de verificar um arquivo quanto a código malicioso, o cabeçalho interno do arquivo é analisado para determinar o formato do arquivo (por exemplo, .txt, .doc ou .exe). A verificação também procura arquivos com extensões específicas.
`/fa`	**Todos os arquivos**. Se essa configuração estiver ativada, o aplicativo verifica todos os arquivos sem exceção (todos os formatos e extensões). Esta é a configuração padrão.

Exclusões de verificação	
`-e:a`	Arquivos do tipo RAR, ARJ, ZIP, CAB, LHA, JAR e ICE são excluídos do escopo da verificação.
`-e:<file mask>`	Arquivos que correspondem à máscara do arquivo são excluídos do escopo de verificação. Por exemplo: • A máscara `*.exe` incluirá todos os caminhos para os arquivos que têm a extensão exe. • A máscara `example*` incluirá todos os caminhos para arquivos nomeados EXAMPLE.
`-e:<seconds>`	Arquivos que demoram mais para serem verificados do que o limite de tempo especificado (em segundos) são excluídos do escopo da verificação.
`-es:<megabytes>`	Arquivos maiores do que o limite de tamanho especificado (em megabytes) são excluídos do escopo da verificação.

Salvar eventos em um modo de arquivo de relatório (somente para perfis de Verificação, Atualizador e Reversão)	
`/R:<report file>`	Salve apenas eventos críticos no arquivo de relatório.
`/RA:<report file>`	Salve todos os eventos em um arquivo de relatório.

Tecnologias de verificação	
`/iChecker=on|off`	Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iChecker tem algumas limitações: ela não funciona com arquivos grandes e se aplica somente a objetos com uma estrutura reconhecida pelo aplicativo (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).
`/iSwift=on|off`	Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iSwift é um avanço da tecnologia iChecker do sistema de arquivos NTFS.

Configurações avançadas	
`/C:<file with scan settings>`	Arquivo com configurações da tarefa de *Verificação de malware* O arquivo deve ser criado manualmente e salvo no formato TXT. O arquivo pode ter o seguinte conteúdo: `[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]`.

Exemplo

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Atualizar bancos de dados e módulos do software aplicativo

Execução da tarefa de *Atualização de bancos de dados e módulos do aplicativo*.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Esse comando não pode ser executado se o aplicativo estiver instalado em Modo Light Agent.

Sintaxe de comando

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

Configurações da tarefa da atualização	
`local`	Início da tarefa de *Atualização de bancos de dados e módulos do aplicativo* que foi criada automaticamente após a instalação do aplicativo. Você pode alterar as configurações da tarefa de *Atualização de bancos de dados e módulos do aplicativo* na interface do aplicativo local ou no console do Kaspersky Security Center. Se esta configuração não for definida, o Kaspersky Endpoint Security iniciará a tarefa de *Atualização de bancos de dados e módulos do aplicativo* com as configurações padrão ou com as configurações especificadas no comando. É possível definir as configurações da tarefa de *Atualização de bancos de dados e módulos do aplicativo* da seguinte maneira: • `UPDATE` inicia a tarefa de *Atualização de bancos de dados e módulos do aplicativo* com as configurações padrão: a fonte de atualização são os servidores de atualização da Kaspersky, a conta é Sistema e outras configurações padrão. • `UPDATE local` inicia a tarefa de *Atualização de bancos de dados e módulos do aplicativo* criada automaticamente após a instalação (tarefa predefinida). • `UPDATE <update settings>` inicia a tarefa de *Atualização de bancos de dados e módulos do aplicativo* com configurações definidas manualmente (veja abaixo).

Fonte de atualização	
`"<update source>"`	Endereço de um servidor HTTP ou FTP ou de uma pasta compartilhada com o pacote de atualização. Você pode especificar apenas uma fonte de atualização. Se a fonte de atualização não for especificada, o Kaspersky Endpoint Security usa a fonte padrão: Servidores de atualização da Kaspersky.

Salvar eventos em um modo de arquivo de relatório (somente para perfis de Verificação, Atualizador e Reversão)	
`/R:<report file>`	Salve apenas eventos críticos no arquivo de relatório.
`/RA:<report file>`	Salve todos os eventos em um arquivo de relatório.

Configurações avançadas	
`/C:<file with update settings>`	Arquivo com configurações da tarefa de *Atualização de bancos de dados e módulos do aplicativo* O arquivo deve ser criado manualmente e salvo no formato TXT. O arquivo pode ter o seguinte conteúdo: `["<update source>"] [/R[A]:<report file>]`.

Exemplo

```
avp.com UPDATE local
```

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Reversão da última atualização

Reversão da última atualização do banco de dados de antivírus. Isso permite reverter os bancos de dados e os módulos do aplicativo para a versão anterior quando necessário, por exemplo, quando a nova versão do banco de dados contém uma assinatura inválida que faz com que o Kaspersky Endpoint Security bloqueie um aplicativo seguro.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Esse comando não pode ser executado se o aplicativo estiver instalado em Modo Light Agent.

Sintaxe de comando

```
avp.com ROLLBACK [/R[A]:<report file>]
```

Salvar eventos em um modo de arquivo de relatório (somente para perfis de Verificação, Atualizador e Reversão)	
`/R:<report file>`	Salve apenas eventos críticos no arquivo de relatório.
`/RA:<report file>`	Salve todos os eventos em um arquivo de relatório.

Exemplo

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Tracing

Os arquivos de rastreamento são armazenados no computador enquanto o aplicativo estiver em uso, e excluídos permanentemente quando o aplicativo for removido. Os arquivos de rastreamento, exceto aqueles do Agente de Autenticação, são armazenados na pasta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. Por padrão, o rastreamento está desabilitado.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

Nível de rastreamento	
`<tracing level>`	Nível de detalhe dos rastreamentos. Valores disponíveis: • `100` (crítico). Apenas mensagens sobre erros fatais. • `200` (alto). Mensagens sobre todos os erros, incluindo erros fatais. • `300` (diagnóstico). Mensagens sobre todos os erros, bem como avisos. • `400` (importante). Todas as mensagens de erro, avisos e informações adicionais. • `500` (normal). Mensagens sobre todos os erros e avisos, bem como informações detalhadas sobre a operação do aplicativo no modo normal (padrão). • `600` (baixo). Todas as mensagens.

Configurações avançadas	
`all`	Execute um comando com os parâmetros `file` e `mem`.
`file`	Salve um arquivo de rastreamento (sem limite de tamanho).
`rot`	Salve os rastreamentos em um número limitado de conjunto de arquivos de tamanho limitado e substitua os arquivos mais antigos quando o tamanho máximo for atingido.
`mem`	Salvar rastreamentos para arquivos de despejo.

Exemplo

```
avp.com TRACES on 500
```

```
avp.com TRACES off
```

```
avp.com TRACES on 500 mem
```

```
avp.com TRACES off file
```

START. Iniciação de um perfil

Iniciação de um perfil (por exemplo, para atualizar bancos de dados ou ativar um componente de proteção).

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com START <profile> [/R[A]:<report file>]
```

Perfil	
`<profile>`	Nome do perfil. Um *Perfil* é um componente, tarefa ou recurso do Kaspersky Endpoint Security. É possível visualizar a lista de perfis disponíveis executando o comando `HELP START`.

Salvar eventos em um modo de arquivo de relatório (somente para perfis de Verificação, Atualizador e Reversão)	
`/R:<report file>`	Salve apenas eventos críticos no arquivo de relatório.
`/RA:<report file>`	Salve todos os eventos em um arquivo de relatório.

Exemplo

```
avp.com START Scan_Objects
```

STOP. Parar um perfil

Interrupção da execução do perfil (por exemplo, interrupção de uma verificação de unidades removíveis ou desativação de um componente de proteção).

Para executar este comando a Proteção por senha deve estar ativada. O usuário deve ter as permissões **Desativar componentes de proteção** e **Desativar componentes de controle**

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

Perfil	
`<profile>`	Nome do perfil. Um *Perfil* é um componente, tarefa ou recurso do Kaspersky Endpoint Security. É possível visualizar a lista de perfis disponíveis executando o comando `HELP STOP`.

Autenticação	
`/login=<user name> /password=<password>`	Credenciais da conta de usuário com as permissões de Proteção por senha necessárias.

STATUS. Status do perfil

Visualização das informações de status para perfis de aplicação (por exemplo, `running` ou `completed`). É possível visualizar a lista de perfis disponíveis executando o comando `HELP STATUS`.

O Kaspersky Endpoint Security também exibe informações sobre o status dos perfis de serviço. Informações sobre o status dos perfis de serviço podem ser necessárias quando entrar em contato com o Suporte Técnico da Kaspersky.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com STATUS [<profile>]
```

Caso o comando seja inserido sem um perfil, o Kaspersky Endpoint Security exibe o status para todos os perfis do aplicativo.

STATISTICS. Estatísticas de operação de perfil

Visualização das estatísticas para um perfil da aplicação (por exemplo, a duração da verificação ou o número de ameaças detectadas.) É possível visualizar a lista de perfis disponíveis executando o comando `HELP STATISTICS`.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com STATISTICS <profile>
```

RESTORE. Restaurar arquivos do Backup

Restauração de um arquivo do backup para a pasta de origem. Se já existir um arquivo com o mesmo nome no caminho especificado, o aplicativo solicitará confirmação para substituir o arquivo. O arquivo que está sendo restaurado é copiado mantendo seu nome original.

> Para executar este comando a Proteção por senha deve estar ativada. O usuário deve ter a permissão **Restaurar do backup**.

O *Backup* armazena cópias de backup de arquivos que foram excluídos ou modificados durante a desinfecção. Uma *cópia backup* é uma cópia de arquivo criada antes que o arquivo seja desinfectado ou excluído. As cópias de backup de arquivos são armazenadas em um formato especial e não representam uma ameaça.

As cópias de backup dos arquivos são armazenadas na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

Os usuários no grupo de Administradores têm permissão para acessar essa pasta. Direitos de acesso limitados a essa pasta são concedidos ao usuário cuja conta foi usada para instalar o Kaspersky Endpoint Security.

> O Kaspersky Endpoint Security não fornece a capacidade de configurar permissões de acesso de usuário a cópias backup de arquivos.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Configurações avançadas	
/REPLACE	Substituir um arquivo existente.
<file name>	O nome do arquivo a ser restaurado.

Autenticação	
/login=<user name> /password=<password>	Credenciais da conta de usuário com as permissões de Proteção por senha necessárias.

Exemplo

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

EXPORT. Exportar configurações do aplicativo

Exportar as configurações do Kaspersky Endpoint Security para um arquivo. Se o comando contiver apenas o nome do arquivo para o qual você deseja exportar as configurações, o aplicativo colocará o arquivo da seguinte forma:

- Caso o caminho para avp.com seja adicionado na variável de sistema %PATH%, o aplicativo colocará o arquivo na pasta `C:\Windows\SysWOW64`.
- Se você executar o comando na pasta de instalação do aplicativo, a exportação falhará porque a autoproteção do aplicativo bloqueia a criação de um novo arquivo na pasta do aplicativo. Para exportar as configurações do aplicativo para um arquivo, insira o caminho do arquivo.

Para executar este comando a Proteção por senha deve estar ativada. O usuário deve ter a permissão **Exportar configurações**.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

Perfil	
<profile>	Nome do perfil. Um *Perfil* é um componente, tarefa ou recurso do Kaspersky Endpoint Security. É possível visualizar a lista de perfis disponíveis executando o comando `HELP EXPORT`.

Arquivo para exportar	
`<file name>`	O nome do arquivo para o qual as configurações do aplicativo serão exportadas. Também é possível inserir o caminho do arquivo. Você pode exportar as configurações do Kaspersky Endpoint Security para um arquivo de configuração DAT ou CFG para um arquivo de texto TXT ou para um documento XML.

Autenticação	
`/login=<user name> /password=<password>`	Credenciais da conta de usuário com as permissões de Proteção por senha necessárias.

Exemplo

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT. Importar configurações do aplicativo

Importação das configurações do Kaspersky Endpoint Security de um arquivo criado com o comando `EXPORT`.

Para executar este comando a Proteção por senha deve estar ativada. O usuário deve ter a permissão **Configurar o aplicativo**.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

Arquivo para importar	
`<file name>`	O nome do arquivo do qual as configurações do aplicativo serão importadas. Você pode importar as configurações do Kaspersky Endpoint Security a partir de um arquivo de configuração DAT ou CFG, um arquivo de texto TXT ou um documento XML.

Autenticação	
`/login=<user name> /password=<password>`	Credenciais da conta de usuário com as permissões de Proteção por senha necessárias.

Exemplo

```
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword
```

ADDKEY. Aplicar arquivo de chave

Ativação do Kaspersky Endpoint Security usando um arquivo de chave. Se o aplicativo já estiver ativado, a chave será adicionada como reserva.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Esse comando não pode ser executado se o aplicativo estiver instalado em Modo Light Agent.

Sintaxe de comando

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

Arquivo de chave	
`<file name>`	Nome do arquivo de chave.

Autenticação	
`/login=<user name> /password=<password>`	Credenciais da conta do usuário. Essas credenciais precisam ser inseridas somente se Proteção de senha estiver ativada.

Exemplo

```
avp.com ADDKEY file.key
```

LICENSE. Licença

Gerenciamento das chaves de licença do Kaspersky Endpoint Security, EDR Optimum ou EDR Expert (add-on do Kaspersky Endpoint Detection and Response).

Para executar este comando e remover uma chave de licença, a Proteção por senha deve estar ativada. O usuário deve ter a permissão **Remover a chave**.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Esse comando não pode ser executado se o aplicativo estiver instalado em Modo Light Agent.

Sintaxe de comando

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

Operação	
`/ADD <file name>`	Ativação do Kaspersky Endpoint Security usando um arquivo de chave. Se o aplicativo já estiver ativado, a chave será adicionada como reserva.
`/ADD <activation code>`	Ative o Kaspersky Endpoint Security usando um código de ativação. Se o aplicativo já estiver ativado, a chave será adicionada como reserva.
`/REFRESH`	Atualize o status da licença do Kaspersky Endpoint Security. Como resultado, o aplicativo recebe as informações atualizadas sobre o status da licença dos servidores de ativação da Kaspersky.

`/REFRESH <license ID>`	Atualize o status das licenças usando o ID da licença. Usando este comando, é possível atualizar o status do Add-on EDR, Add-on MDR, Add-on KUMA ou outras licenças. Você pode obter o ID da licença no certificado de licença. Como resultado, o aplicativo recebe as informações atualizadas sobre o status da licença dos servidores de ativação da Kaspersky.
`/CHECK`	Obter informações da licença O Kaspersky Endpoint Security exibe informações sobre todas as chaves de licença adicionadas, incluindo chaves reservas, add-on do EDR, add-on do MDR, chaves do add-on do KUMA e outras. O Kaspersky Endpoint Security exibe as seguintes informações da licença: • nome da licença; • identificador da licença; • endereço do Servidor de proteção (SVM) ao qual a máquina virtual está conectada e em que o aplicativo está instalado no modo Light Agent; • tipo de licença: avaliação, comercial, beta, assinatura; • data e hora da ativação do aplicativo; • data e hora de expiração da licença; • número de dias até a expiração da licença.
`/CHECK <license ID>`	Obter informações da licença por ID. É possível usar esse comando para obter informações da licença. Você pode obter o ID da licença no certificado de licença.
`/DEL /login=<user name> /password=<password>`	Remover a chave de licença do aplicativo. A chave reserva também será removida.
`/DEL <license ID> /login=<user name> /password=<password>`	Exclua a chave usando o ID da licença. Usando este comando, é possível excluir uma chave do Add-on EDR, Add-on MDR, Add-on KUMA ou outras licenças. Você pode obter o ID da licença no certificado de licença.

Autenticação	
`/login=<user name> /password=<password>`	Credenciais da conta de usuário com as permissões de Proteção por senha necessárias.

Exemplo

```
avp.com LICENSE /ADD file.key
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

Exemplo

```
avp.com LICENSE /ADD file.key
```

```
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
```

```
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

RENEW. Comprar uma licença

Abertura do site da Kaspersky para compra ou renovação da licença.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Esse comando não pode ser executado se o aplicativo estiver instalado em Modo Light Agent.

PBATESTRESET. Redefinição dos resultados da verificação do disco antes de criptografar o disco

Redefinição dos resultados da verificação de compatibilidade para Criptografia Completa do Disco (FDE), incluindo as tecnologias Kaspersky Disk Encryption e criptografia de unidade de disco da BitLocker.

Antes de executar a Criptografia Completa do Disco, o aplicativo executa diversas verificações para verificar se o computador pode ser criptografado. Se o computador não for compatível com a Criptografia completa do disco, o Kaspersky Endpoint Security registra informações sobre a incompatibilidade. Na próxima vez que você tentar criptografar, o aplicativo não executará essa verificação e avisará que a criptografia não é possível. Se a configuração de hardware do computador tiver sido alterada, os resultados da verificação de compatibilidade registrados anteriormente pelo aplicativo deverão ser redefinidos para verificar novamente o disco rígido do sistema quanto à compatibilidade com as tecnologias de Criptografia de disco da Kaspersky ou Criptografia de unidade de disco da BitLocker.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

EXIT. Sair do aplicativo

Saindo do Kaspersky Endpoint Security. O aplicativo será removido da memória RAM do computador.

Para executar este comando a Proteção por senha deve estar ativada. O usuário deve ter a permissão **Sair do aplicativo**.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. Desativar política

Desativação da política do Kaspersky Security Center no computador. Todas as configurações do Kaspersky Endpoint Security estão disponíveis para configuração, incluindo configurações que possuem um cadeado fechado na política (🔒).

Para executar este comando a Proteção por senha deve estar ativada. O usuário deve ter a permissão **Desativar política do Kaspersky Security Center**.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Ativar política

Ativação de uma política do Kaspersky Security Center no computador. As configurações do aplicativo serão configuradas de acordo com a política.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

DISABLE. Desativar proteção

Desativação da Proteção Contra Ameaças ao Arquivo em um computador com uma licença expirada do Kaspersky Endpoint Security. Não é possível executar este comando em um computador que tenha um aplicativo desativado que a licença não seja válida.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

SPYWARE. Detectar spyware

Gerenciamento da detecção de spyware. Por padrão, a detecção de spyware está ativa.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com SPYWARE on|off
```

KSN. Alternância entre KSN / KPSN

Seleção de uma solução da Kaspersky para determinar a reputação de arquivos ou sites. O Kaspersky Endpoint 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 Endpoint 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 LAN corporativa é proibida por lei ou restrita pelas políticas de segurança corporativa.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Esse comando não pode ser executado se o aplicativo estiver instalado em Modo Light Agent.

Sintaxe de comando

```
avp.com KSN /global | /private <file name>
```

Arquivo de configuração da Kaspersky Security Network	
`<file name>`	Nome do arquivo de configuração que contém as configurações da Kaspersky Private Security Network. Esse arquivo tem a extensão PKCS7 ou PEM.

Exemplo

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

Exemplo

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE. Desativação da proteção da conexão do servidor

Execução da tarefa *Proteção da conexão do Servidor de Administração* que remove a senha da conexão do computador com o Servidor de Administração. Desta forma, a tarefa desativa a proteção da conexão do Servidor de Administração.

Para executar este comando a Proteção por senha deve estar ativada.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

Senha	
`/password= <password>`	A senha da KLAdmin user account ou a senha da tarefa *Proteção da conexão do Servidor de Administração* task. Se o parâmetro não for especificado, o Kaspersky Endpoint Security solicitará que você insira uma senha na próxima linha.

Comandos KESCLI

Os comandos KESCLI permitem receber informações sobre o estado de proteção do computador usando o componente OPSWAT, além de realizar tarefas comuns, como tarefas de *Verificação de malware* e *Atualização de bancos de dados e módulos do aplicativo*.

É possível ver a lista de comandos KESCLI usando o comando `kescli --help` ou usando o comando abreviado `kescli -h`.

Para gerenciar o Kaspersky Endpoint Security a partir da linha de comando:

1. Execute o interpretador da linha de comando (cmd.exe) como um administrador.

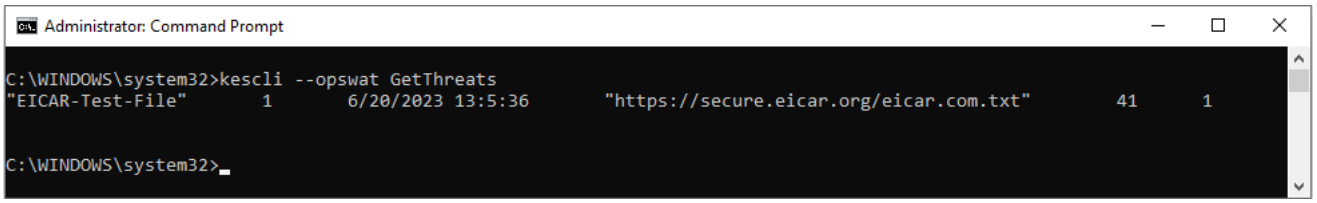
2. Vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

   É possível adicionar o caminho para o arquivo executável à variável de sistema %PATH% durante a instalação do aplicativo.

3. Use o seguinte modelo para executar o comando:

```
kescli <comando> [opções]
```

Como resultado, o Kaspersky Endpoint Security executará o comando (veja a figura abaixo).



Gerenciar o aplicativo a partir da linha de comando

Scan. Verificação de malware

Execute a tarefa de *Verificação de malware* (Verificação completa).

Para executar a tarefa, o administrador deve Permitir o uso de tarefas locais na política.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

Sintaxe de comando

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

É possível verificar o status de conclusão de uma tarefa de *Verificação de malware* usando o comando `GetScanState` e visualizar a data e hora de conclusão da última verificação usando o comando `GetLastScanTime`.

Escopo da verificação	
`<scan scope>`	`;`-lista separada de arquivos e pastas. Por exemplo, `"C:\Program Files (x86)\Example Folder"`.

Ação ao detectar ameaças	
`0`	**Informar**. Caso esta opção seja selecionada, o Kaspersky Endpoint Security adiciona as informações sobre arquivos infectados à lista de ameaças ativas na detecção destes arquivos.
`1`	**Desinfectar e excluir se a desinfecção falhar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Caso a desinfecção falhe, o aplicativo excluirá o arquivo. Esta ação é selecionada por padrão.

Exemplo

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

GetScanState. Status de conclusão da verificação

Exibição das informações sobre o status de conclusão da tarefa *Verificação de malware* (*Verificação completa*):

- `1` – a verificação está em execução.
- `0` – a verificação não está em execução.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

Sintaxe de comando

```
kescli --opswat GetScanState
```

GetLastScanTime. Determinar a hora da conclusão da verificação

Exibição das informações sobre a data e a hora de conclusão da última tarefa *Verificação de malware* (*Verificação completa*).

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

Sintaxe de comando

```
kescli --opswat GetLastScanTime
```

GetThreats. Obter dados sobre as ameaças detectadas

Exibição de uma lista de ameaças detectadas (*Relatório de ameaças*). O relatório contém informações sobre ameaças e atividades de vírus durante os últimos 30 dias antes de sua criação.

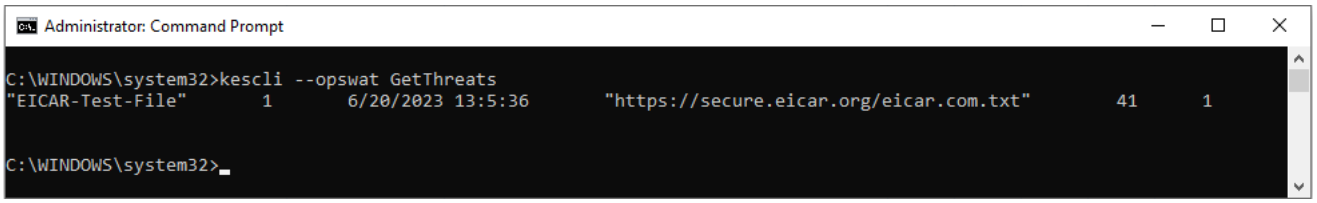
Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

Sintaxe de comando

```
kescli --opswat GetThreats
```

Quando esse comando é executado, o Kaspersky Endpoint Security enviará uma resposta no formato a seguir:

```
<name of detected object> <type of object> <detection date and time> <path to file> <action on threat detection> <threat danger level>
```



Gerenciar o aplicativo a partir da linha de comando

Tipo de objeto	
0	Desconhecido (Unknown).
1	Vírus (Virware).
2	Programas de trojan (Trojware).
3	Programas maliciosos (Malware).
4	Programas com propagandas (Adware).
5	Discadores automáticos (Pornware).
6	Aplicativos que podem ser usados por um cibercriminoso para danificar o computador ou os dados do usuário (Riskware).
7	Objetos compactados cujo método de compactação pode ser usado para proteger códigos maliciosos (Packed).
20	Objetos desconhecidos (Xfiles).
21	Aplicativos conhecidos (Software).
22	Arquivos ocultos (Hidden).
23	Aplicativos que requerem atenção (Pupware).
24	Comportamentos anômalos (Anomaly).
30	Não determinado (Undetect).
40	Banners de propaganda (Banner).
50	Ataques à rede (Attack).
51	Acesso ao registro (Registry).
52	Atividades suspeitas (Suspicion).
60	Vulnerabilidades (Vulnerability).
70	Phishing (Phishing).
80	Anexos de e-mail indesejados (Attachment).
90	Malwares detectados pelo Kaspersky Security Network (Urgent).
100	Link desconhecido (Suspic URL).
110	Outros malwares (Behavioral).

Ação ao detectar ameaças	
0	Desconhecido (unknown).
1	Ameaça remediada (ok).
2	O objeto estava infectado e não foi desinfectado (infected).
5	O objeto está em um arquivo comprimido e não foi desinfectado (archive).
9	O objeto foi desinfectado (disinfected).
10	O objeto não foi desinfectado (not disinfected).

11	O objeto foi excluído (`deleted`).
13	Foi criada uma cópia backup do objeto (`backupped`).
15	O objeto foi movido para o Backup (`quarantined`).
23	O objeto foi excluído na reinicialização do computador (`delete on reboot`).
25	O objeto foi desinfectado na reinicialização do computador (`disinfect on reboot`).
29	O objeto foi movido para o Backup por um usuário (`added by user`).
30	O objeto foi adicionado às exclusões (`added to exclude`).
31	O objeto foi movido para o Backup na reinicialização do computador (`quarantine on reboot`).
36	Falso positivo (`false alarm`).
38	O processo foi finalizado (`terminated`).
40	O objeto não foi detectado (`not found`).
41	Não é possível resolver a ameaça (`untreatable`).
42	O objeto foi restaurado (`rolled back`).
43	O objeto foi criado como resultado de atividade da ameaça (`produced by threat`).
44	O objeto foi restaurado na reinicialização do computador (`roll back on reboot`).
`0xffffffff`	O objeto não foi processado (`discarded`).

Nível de perigo da ameaça	
`0`	Desconhecido
`1`	Alto
`2`	Verificação média
`4`	Baixo
`8`	Informações (menos que *Baixo*)

UpdateDefinitions. Atualizar bancos de dados e módulos do software aplicativo

Execução da tarefa de *Atualização de bancos de dados e módulos do aplicativo*. O Kaspersky Endpoint Security usa a fonte padrão: Servidores de atualização da Kaspersky.

Para executar a tarefa, o administrador deve Permitir o uso de tarefas locais na política.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

Esse comando não pode ser executado se o aplicativo estiver instalado em Modo Light Agent.

Sintaxe de comando

```
kescli --opswat UpdateDefinitions
```

É possível visualizar a data e hora de lançamento dos bancos de dados de antivírus atuais usando o comando `GetDefinitionsetState`.

GetDefinitionState. Determinação da data e hora da última atualização dos bancos de dados

Exibição das informações sobre a data e hora da última atualização dos bancos de dados de antivírus em uso.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

Sintaxe de comando

```
kescli --opswat GetDefinitionState
```

EnableRTP. Habilitar a proteção

Ativação dos componentes de proteção do Kaspersky Endpoint Security no computador: Proteção Contra Ameaças ao Arquivo, Proteção Contra Ameaças da Web, Proteção Contra Ameaças ao Correio, Proteção contra Ameaças à Rede, Prevenção de Intrusão do Host.

> Para ativar os componentes de proteção, o administrador deve certificar-se de que as configurações de política relevantes possam ser modificadas (atributos estão abertos).

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

Sintaxe de comando

```
kescli --opswat EnableRTP
```

Como resultado, os componentes de proteção são ativados mesmo que você tenha proibido a modificação das configurações do aplicativo com a Proteção por senha.

É possível verificar o status operacional da Proteção Contra Ameaças ao Arquivo usando o comando `GetRealTimeProtectionState`.

GetRealTimeProtectionState. Status da Proteção Contra Ameaças ao Arquivo

Exibição das informações sobre o status do componente Proteção Contra Ameaças ao Arquivo:

- `1` – o componente foi ativado.
- `0` – o componente foi desativado.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

```
Sintaxe de comando

kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. Status da criptografia do disco

Exibição das informações sobre o status da criptografia de disco:

- `1` significa que o disco está protegido pela tecnologia de criptografia da Kaspersky ou BitLocker.
- `0` significa que o disco não está criptografado.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

```
Sintaxe de comando

kescli --opswat GetEncryptionState
```

Version. Identificar a versão do aplicativo

Exibição da versão do Kaspersky Endpoint Security for Windows.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.

```
Sintaxe de comando

kescli --Version
```

Também é possível usar o comando abreviado `-v`.

Comandos de gerenciamento do Detection and Response

É possível usar a linha de comando para gerenciar a funcionalidade integrada das soluções de Detection and Response (por exemplo, Kaspersky Sandbox ou Kaspersky Endpoint Detection and Response Optimum). É possível gerenciar as soluções de Detection and Response caso o gerenciamento usando o console do Kaspersky Security Center não seja possível. Você pode visualizar a lista de comandos para gerenciar o aplicativo, executando o comando `HELP` (AJUDA). Para ler sobre a sintaxe de um comando específico, digite `HELP <command>`.

Para gerenciar recursos integrados de soluções de Detection and Response utilizando a linha de comando:

1. Execute o interpretador da linha de comando (cmd.exe) como um administrador.
2. Vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.
3. Use o seguinte modelo para executar o comando:

```
avp.com <command> [options]
```

Como resultado, o Kaspersky Endpoint Security executará o comando.

SANDBOX. Gerenciamento do Sandbox

Comandos para gerenciar o componente Sandbox:

- Ativação ou desativação do componente Sandbox.

  Os componentes Sandbox fornecem interação com a solução Kaspersky Sandbox e o componente KATA Sandbox, que faz parte da Kaspersky Anti Targeted Attack Platform.

- Configuração do componente Kaspersky Sandbox:

  - Conexão do computador com os servidores Sandbox.

    Os servidores usam imagens virtuais implantadas de sistemas operacionais Microsoft Windows para executar os objetos que precisam ser verificados. É possível inserir um endereço IP (IPv4 ou IPv6) ou um nome de domínio totalmente qualificado. Para obter detalhes sobre como implantar imagens virtuais e configurar servidores Sandbox, consulte a ajuda do Kaspersky Sandbox e a ajuda da Kaspersky Anti Targeted Attack Platform.

  - Configuração do tempo esgotado da conexão para o servidor.

    Tempo de conexão esgotado para o Sandbox (para Kaspersky Sandbox) ou servidor do Central Node (para KATA). Depois de decorrido o tempo limite configurado, o Kaspersky Endpoint Security envia uma solicitação ao próximo servidor. É possível aumentar o tempo de conexão esgotado para o servidor caso a velocidade da sua conexão seja baixa ou instável. O tempo limite de solicitação recomendado é de 0.5 segundo ou menos.

  - Configuração de uma conexão confiável entre o computador e os servidores.

    Para configurar uma conexão confiável com o servidor do Sandbox (para o Kaspersky Sandbox) ou o servidor do Central Node (para o KATA), é necessário preparar um certificado TLS. Em seguida, é necessário adicionar o certificado ao computador com o uso de uma política. Também é preciso adicionar o certificado ao servidor do Sandbox (para o Kaspersky Sandbox) ou ao servidor do Central Node (para o KATA).

  - Configuração do modo de integração.

É preciso selecionar uma solução da qual o Sandbox faça parte, ou seja, Kaspersky Sandbox ou KATA Sandbox. O *Kaspersky Sandbox* é uma solução independente de Detection and Response da Kaspersky. O *KATA Sandbox* é um componente da solução Kaspersky Anti Targeted Attack Platform. Quando integrado ao KATA Sandbox, o componente pode funcionar nos seguintes modos:

- **Manualmente**. O usuário envia manualmente o arquivo para verificação pelo menu de contexto (**Enviar para o Sandbox**).
- **Automaticamente**. O aplicativo detecta os objetos automaticamente para enviá-los ao Sandbox para verificação.
- **Combinado**.

- Exibição das configurações atuais do componente.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com stop sandbox [/login=<user name> /password=<password>]
```

```
avp.com start sandbox
```

```
avp.com sandbox /set [--servers=<address:port>] [--pinned-certificate=<path to the TLS certificate>] [--client-certificate=<path to the PFX archive>] [--client-certificate-password=<password>] [--timeout=<Sandbox server connection timeout (ms)>] [--mode=<KSB|KATAManual|KATAAuto|KATAFull>] [/login=<user name> /password=<password>]
```

Operação	
`stop`	Desative o componente Sandbox.
`start`	Ative o componente Sandbox.

`set`	Configure o componente Sandbox. É possível configurar as seguintes:
	• Adicionar servidores Sandbox (`--servers`)
	• Adicionar um certificado TLS (`--pinned-certificate`)
	• Adicionar um contêiner de criptografia (`--client-certificate`)
	• Especifique uma senha para o contêiner de criptografia(`--client-certificate-password`);
	• Definir o tempo esgotado da conexão do servidor (`--timeout`)
	• Selecionar um modo de integração (`--mode`):
	  • `KSB` – integração com o Kaspersky Sandbox;
	  • `KATAManual` – integração manual com o KATA Sandbox;
	  • `KATAAuto` – integração automática com o KATA Sandbox;
	  • `KATAFull` – integração combinada com o KATA Sandbox.

`show`	Exibe as configurações atuais do componente. A seguinte resposta é obtida:
	`sandbox.timeout=<Sandbox server connection timeout (ms)>`
	`sandbox.servers=<list of Sandbox servers>`
	`sanbox.mode=<integration mode>`
	`sandbox.tls=<trusted connection status>`

Autenticação	
`/login=<user name> /password=<password>`	Credenciais da conta de usuário com as permissões de Proteção por senha necessárias.

Exemplo

```
avp.com SANDBOX /SET --servers=127.0.0.1:8080;127.0.0.2:8080 --pinned-certificate=c:\my_certs\my.cer --mode=KSB
/login=login /password=password
```

PREVENTION. Gerenciamento da prevenção de execução

Desativação do componente Prevenção de execução ou exibição das configurações atuais do componente, incluindo a lista de regras de prevenção de execução.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com prevention disable
```

```
avp.com prevention /show
```

Durante a execução do comando `prevention /show`, o usuário receberá a seguinte resposta:

```
prevention.enable=true|false

prevention.mode=audit|prevent

prevention.rules

id: <rule ID>
target: script|process|document
md5: <MD5 hash of the file>
sha256: <SHA256 hash of the file>
pattern: <path to the object>
case-sensitive: true|false
```

Valores de retorno do comando:

- `-1` significa que o comando não é compatível com a versão do aplicativo instalado no computador.
- `0` significa que o comando foi executado com sucesso.
- `1` significa que um argumento obrigatório não foi passado para o comando.
- `2` significa que ocorreu um erro geral.

- 4 significa que houve um erro de sintaxe.
- 9 – operação errada (por exemplo, uma tentativa de desativar o componente quando ele já está desativado).

ISOLATION. Gerenciando o isolamento de rede

Desativação do isolamento de rede do computador ou exibição das configurações atuais do componente. As configurações de componentes também incluem uma lista de conexões de rede adicionadas às exclusões.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com isolation /OFF /login=<user name> /password=<password>
```

```
avp.com isolation /STAT
```

Como resultado da execução do comando `stat`, o usuário recebe a seguinte resposta: `Network isolation on|off`.

RESTORE. Restauração do arquivo da Quarentena

Restauração de um arquivo da quarentena para a pasta de origem. A *Quarentena* é um armazenamento local especial no computador. O usuário pode colocar em quarentena arquivos que considere perigosos para o computador. Os arquivos em quarentena são armazenados em um estado criptografado e não ameaçam a segurança do dispositivo. O Kaspersky Endpoint Security usa a Quarentena somente quando estiver integrado com as soluções Detection and Response da Kaspersky. Em outros casos, o Kaspersky Endpoint Security coloca o arquivo relevante no Backup. Para obter informações sobre o gerenciamento da Quarentena como parte das soluções, consulte a Ajuda do Kaspersky Sandbox, a Ajuda do Kaspersky Endpoint Detection and Response Optimum, a Ajuda do Kaspersky Endpoint Detection and Response Expert, a Ajuda da Kaspersky Anti Targeted Attack Platform e a Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises).

Para executar este comando a Proteção por senha deve estar ativada. O usuário deve ter a permissão **Restaurar do backup**.

O objeto é colocado em quarentena na conta do sistema (SISTEMA).

A restauração de arquivos da Quarentena envolve as seguintes considerações especiais:

- Caso a pasta de destino tenha sido excluída ou o usuário não possua direitos de acesso a essa pasta, o aplicativo coloca o arquivo na pasta `%DataRoot%\QB\Restored`. Então, é preciso mover manualmente o arquivo para a pasta de destino.
- O aplicativo trata o nome do arquivo que está sendo restaurado com distinção entre maiúsculas e minúsculas. Se a distinção entre maiúsculas e minúsculas não foi considerada ao inserir o nome do arquivo, o aplicativo não o restaurará.

- Caso a pasta de destino já possua um arquivo com o mesmo nome, o aplicativo cancelará a restauração do arquivo.
- Se você estiver usando a solução KATA (EDR), o aplicativo salva uma cópia do arquivo na Quarentena após restaurar o arquivo. É possível esvaziar a Quarentena manualmente. Para as soluções EDR Optimum e EDR Expert, o aplicativo exclui o arquivo após a restauração.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Configurações avançadas	
`/REPLACE`	Substituir um arquivo existente.
`<file name>`	O nome do arquivo a ser restaurado.

Autenticação	
`/login=<user name> /password=<password>`	Credenciais da conta de usuário com as permissões de Proteção por senha necessárias.

Exemplo

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

Valores de retorno do comando:

- `-1` significa que o comando não é compatível com a versão do aplicativo instalado no computador.
- `0` significa que o comando foi executado com sucesso.
- `1` significa que um argumento obrigatório não foi passado para o comando.
- `2` significa que ocorreu um erro geral.
- `4` significa que houve um erro de sintaxe.

IOCSCAN. Verifica os indicadores de comprometimento (IOC)

Execução da tarefa de *Verificação de IOC*. Um *Indicador de compromisso (IOC)* é um conjunto de dados sobre um objeto ou atividade que indica acesso não autorizado ao computador (comprometimento de dados). Por exemplo, muitas tentativas malsucedidas de entrar no sistema podem constituir um indicador de compromisso. A *Verificação de IOC* tarefa permite localizar indicadores de comprometimento no computador e tomar as medidas de resposta a ameaças.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

A verificação de IOC é interrompida após 128 correspondências com indicadores de comprometimento descritos nos arquivos do IOC. Isso é necessário para limitar o número de entradas no relatório da tarefa de Verificação de IOC, o que facilita a análise e evita sobrecarregamentos causados por indicadores de comprometimento imprecisos que podem gerar muitas correspondências.

Sintaxe de comando

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder> [/process=on|off] [/hint=<full
path to executable file of a process|full file path>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off]
[/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/eventlog=on|off]
[/datetime=<event publication date>] [/channels=<list of channels>] [/files=on|off] [/drives=
<all|system|critical|custom>] [/excludes=<list of exclusions>][/scope=<list of folders to scan>]
```

Arquivos IOC	
`<full path to the IOC file>`	Caminho completo para o arquivo IOC que você deseja usar para verificação. É possível especificar vários arquivos IOC separados por espaços. O caminho completo para o arquivo IOC deve ser inserido sem o argumento `/path`. Por exemplo, `C:\Users\Admin\Desktop\IOC\file1.ioc`
`/path=<path to the folder with IOC files>`	Caminho para a pasta com os arquivos IOC que deseja usar para verificação. *Arquivos IOC* são arquivos contendo os conjuntos de indicadores que o aplicativo tenta combinar para contar uma detecção. Os arquivos IOC devem estar em conformidade com o padrão OpenIOC. Por exemplo, `C:\Users\Admin\Desktop\IOC`

Tipo de dados para a verificação IOC	
`/process=on|off`	Análise de dados do processo ao executar a verificação de IOC (termo ProcessItem). Caso o valor do argumento seja `off`, o Kaspersky Endpoint Security não analisa os processos em execução no computador durante a verificação. Caso o arquivo IOC contenha os termos do documento ProcessItem IOC, eles serão ignorados (detectados como nenhuma correspondência). Caso o argumento não seja especificado, o Kaspersky Endpoint Security analisa os dados do processo apenas se o documento ProcessItem IOC estiver descrito no arquivo IOC fornecido para a verificação.
`/hint=<full path to the executable file of the process|full path to the file>`	Analisar dados de arquivos ao executar a verificação de IOC (termos ProcessItem e FileItem). É possível selecionar um arquivo em uma das seguintes formas: • `<full path to the executable file of the process>` – termo ProcessItem; • `<full path to the file>` – termo FileItem.
`/registry=on|off`	Análise de dados de registro do Windows ao executar uma verificação de IOC (termo RegistryItem). Caso o valor do argumento seja `off`, o Kaspersky Endpoint Security não verifica o registro do Windows. Caso o arquivo IOC contenha termos do documento RegistryItem IOC, eles serão ignorados (detectados como nenhuma correspondência). Caso o argumento não seja especificado, o Kaspersky Endpoint Security analisa o registro do Windows apenas se o documento RegistryItem IOC estiver descrito no arquivo IOC fornecido para a verificação. Para o tipo de dados RegistryItem, o Kaspersky Endpoint Security verifica um conjunto de chaves do registro.
`/dnsentry=on|off`	Análise de dados sobre os registros no cache DNS local ao executar a verificação de IOC (termo DnsEntryItem). Caso o valor do argumento seja `off`, o Kaspersky Endpoint Security não verifica o cache do DNS local. Caso o arquivo IOC contenha termos do documento DnsEntryItem IOC, eles serão ignorados (detectados como nenhuma correspondência). Caso o argumento não seja especificado, o Kaspersky Endpoint Security analisa o cache DNS local apenas se o documento DnsEntryItem IOC estiver descrito no arquivo IOC fornecido para a verificação.

`/arpentry=on|off`	Análise de dados sobre os registros na tabela ARP ao realizar a verificação de IOC (termo ArpEntryItem). Caso o valor do argumento seja `off`, o Kaspersky Endpoint Security não verifica a tabela ARP. Caso o arquivo IOC contenha termos do documento ArpEntryItem IOC, eles serão ignorados (detectados como nenhuma correspondência). Caso o argumento não seja especificado, o Kaspersky Endpoint Security analisa a tabela ARP apenas se o documento ArpEntryItem IOC estiver descrito no arquivo IOC fornecido para a verificação.
`/ports=on|off`	Análise de dados sobre as portas abertas para escuta ao executar a verificação de IOC (termo PortItem). Caso o valor do argumento seja `off`, o Kaspersky Endpoint Security não verifica a tabela de conexões ativas no dispositivo. Caso o arquivo IOC contenha termos do documento PortItem IOC, eles serão ignorados (detectados como nenhuma correspondência). Caso o argumento não seja especificado, o Kaspersky Endpoint Security analisa a tabela de conexões ativas apenas se o documento PortItem IOC estiver descrito no arquivo IOC fornecido para a verificação.
`/services=on|off`	Análise de dados sobre os serviços instalados no dispositivo ao executar a verificação de IOC (termo ServiceItem). Caso o valor do argumento seja `off`, o Kaspersky Endpoint Security não verifica os dados sobre os serviços instalados no dispositivo. Caso o arquivo IOC contenha termos do documento ServiceItem IOC, eles serão ignorados (detectados como nenhuma correspondência). Caso o argumento não seja especificado, o Kaspersky Endpoint Security analisa os dados do serviço apenas se o documento ServiceItem IOC estiver descrito no arquivo IOC fornecido para a verificação.
`/system=on|off`	Análise de dados do ambiente ao executar a verificação de IOC (termo SystemInfoItem). Caso o valor do argumento seja `off`, o Kaspersky Endpoint Security não analisa os dados do ambiente. Caso o arquivo IOC contenha termos do documento SystemInfoItem IOC, eles serão ignorados (detectados como nenhuma correspondência). Caso o argumento não seja especificado, o Kaspersky Endpoint Security analisa os dados do ambiente apenas se o documento SystemInfoItem IOC estiver descrito no arquivo IOC fornecido para a verificação.
`/users=on|off`	Análise de dados sobre os usuários ao realizar a verificação de IOC (termo UserItem). Caso o valor do argumento seja `off`, o Kaspersky Endpoint Security não analisa os dados sobre os usuários criados no sistema. Caso o arquivo IOC contenha termos do documento UserItem IOC, eles serão ignorados (detectados como nenhuma correspondência). Caso o argumento não seja especificado, o Kaspersky Endpoint Security analisa os dados sobre os usuários criados no sistema apenas se o documento UserItem IOC estiver descrito no arquivo IOC fornecido para a verificação.
`/volumes=on|off`	Análise de dados sobre os volumes ao realizar a verificação de IOC (termo VolumeItem). Caso o valor do argumento seja `off`, o Kaspersky Endpoint Security não verifica os dados sobre os volumes do dispositivo. Caso o arquivo IOC contenha termos do documento VolumeItem IOC, eles serão ignorados (detectados como nenhuma correspondência). Caso o argumento não seja especificado, o Kaspersky Endpoint Security analisa os dados do volume apenas se o documento VolumeItem IOC estiver descrito no arquivo IOC fornecido para a verificação.
`/eventlog=on|off`	Análise de dados sobre os registros no log de eventos do Windows ao executar a verificação de IOC (termo EventLogItem). Caso o valor do argumento seja `off`, o Kaspersky Endpoint Security não verifica os registros no log de eventos do Windows. Caso o arquivo IOC contenha termos do documento EventLogItem IOC, eles serão ignorados (detectados como nenhuma correspondência). Caso o argumento não seja especificado, o Kaspersky Endpoint Security analisa o log de eventos do Windows se o documento EventLogItem IOC estiver descrito no arquivo IOC fornecido para a verificação. Para o termo IOC EventLogItem\source, use o valor **Nome do provedor** do esquema XML do evento.

`/datetime=<event publication date>`	Leva em consideração a data em que o evento foi publicado no log de eventos do Windows ao determinar o escopo da verificação de IOC para o documento IOC correspondente. Ao executar uma verificação de IOC, o Kaspersky Endpoint Security verifica as entradas do log de eventos do Windows publicadas durante o período da hora e data especificadas até o momento em que a tarefa é executada. O Kaspersky Endpoint Security permite especificar a data de publicação do evento como o valor do argumento. A verificação é executada apenas para os eventos publicados no log de eventos do Windows após a data especificada e antes da verificação ser executada. Caso o argumento não seja especificado, o Kaspersky Endpoint Security verifica os eventos com qualquer data de publicação. A configuração `TaskSettings::BaseSettings::EventLogItem::datetime` não pode ser editada. A configuração é usada apenas se o documento IOC EventLogItem for descrito no arquivo IOC fornecido para a verificação.
`/channel=<list of channels>`	Lista de nomes de canais (log) para os quais deseja realizar uma verificação de IOC. Caso o argumento seja especificado, o Kaspersky Endpoint Security verifica os registros publicados nos logs especificados. O documento IOC deve ter o termo EventLogItem descrito. O nome do log é especificado como uma string de acordo com o nome do log (canal) especificado nas propriedades do log (o parâmetro Full Name) ou nas propriedades do evento (o parâmetro `<Channel></Channel>` no esquema xml do evento). É possível especificar vários canais separados por espaços. Caso o argumento não seja especificado, o Kaspersky Endpoint Security verifica os registros dos canais `Application`, `System`, `Security`.
`/files=on|off`	Análise de dados do arquivo ao executar a verificação de IOC (termo FileItem). Caso o valor do argumento seja `off`, o Kaspersky Endpoint Security não analisa os dados do arquivo. Caso o arquivo IOC contenha termos do documento FileItem IOC, eles serão ignorados (detectados como nenhuma correspondência). Caso o argumento não seja especificado, o Kaspersky Endpoint Security analisa os dados do arquivo apenas se o documento IOC FileItem estiver descrito no arquivo IOC fornecido para a verificação.
`/drives=<all|system|critical|custom>`	Define o escopo da verificação de IOC ao analisar os dados para o documento FileItem IOC. Não é possível definir os seguintes valores para o escopo da verificação: • `<all>` para todos os escopos de arquivo disponíveis. • `<system>` para arquivos em pastas onde o sistema operacional está instalado. • `<critical>` para arquivos temporários nas pastas do usuário e do sistema. • `<custom>` para arquivos em escopos definidos pelo usuário (`/scope=<list of folders to scan>`). Caso o argumento não seja especificado, a verificação será executada nas áreas críticas.
`/excludes=<list of exclusions>`	Define o escopo de exclusão ao analisar dados para o documento FileItem IOC. É possível especificar vários caminhos separados por espaços.
`/scope=<list of folders to scan>`	Escopo da verificação de IOC definido pelo usuário ao analisar os dados para o documento IOC FileItem (`/drives=custom`). É possível especificar vários caminhos separados por espaços.
`/retro /<number of days>`	A *Verificação retrospectiva IOC* é um modo de tarefa de *Verificação de IOC* no qual o Kaspersky Endpoint Security verifica os indicadores de comprometimento com o uso de dados de um determinado período de tempo. Este modo é destinado à pesquisa de indicadores de comprometimento pela telemetria do computador protegido, como atividade de rede, processos, arquivos e outras telemetrias. É possível definir um período de 1 a 14 dias. Por padrão, o aplicativo verifica os indicadores de comprometimento por um dia.
`/network=on|off`	Análise de dados de rede (o termo NetworkItem).
`/url=on|off`	Análise de dados nos logs do navegador (o termo UrlHistoryItem). A Verificação retrospectiva IOC analisa os logs dos seguintes navegadores: Google Chrome, Mozilla Firefox, Microsoft Edge (versão 79 ou posterior).
`/email`	Análise de objetos de e-mail (o termo EmailItem).
`/route`	Análise de tabelas de roteamento e encaminhamento (o termo RouteEntryItem).

Valores de retorno do comando:

- `-1` significa que o comando não é compatível com a versão do aplicativo instalado no computador.
- `0` significa que o comando foi executado com sucesso.

- 1 significa que um argumento obrigatório não foi passado para o comando.
- 2 significa que ocorreu um erro geral.
- 4 significa que houve um erro de sintaxe.

Caso o comando seja executado com sucesso (valor de retorno `0`) e os indicadores de comprometimento sejam detectados ao longo do caminho, o Kaspersky Endpoint Security envia as seguintes informações de resultado da tarefa para a linha de comando:

`Uuid`	ID do arquivo IOC do cabeçalho da estrutura do arquivo IOC (a tag `<ioc id="">`)
`Name`	Descrição do arquivo IOC a partir do cabeçalho da estrutura do arquivo IOC (a tag `<description> </description>`)
`Matched Indicator Items`	Lista de IDs de todos os indicadores correspondentes.
`Matched objects`	Dados para cada documento IOC para o qual houve uma correspondência.

MDRLICENSE. Ativação do MDR

Adição do arquivo de configuração BLOB para ativar o Managed Detection and Response. O arquivo BLOB contém o ID do cliente e informações sobre a licença do Kaspersky Managed Detection and Response. O arquivo BLOB está localizado dentro do arquivo comprimido ZIP do arquivo de configuração do MDR. É possível obter o arquivo ZIP no Console do Kaspersky Managed Detection and Response. Para saber informações detalhadas sobre o arquivo BLOB, consulte a Ajuda do Kaspersky Managed Detection and Response.

São necessários privilégios de administrador para realizar operações com um arquivo BLOB. As configurações do Managed Detection and Response na política também devem estar disponíveis para edição ( ).

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

Operação	
`/ADD <file name>`	Aplique o arquivo de configuração BLOB para integração com o Kaspersky Managed Detection and Response (formato de arquivo P7). É possível aplicar apenas um arquivo BLOB. Se um arquivo BLOB já tiver sido adicionado ao computador, ele será substituído.
`/DEL`	Excluir o arquivo de configuração BLOB.

Autenticação	
`/login=<user name> /password=<password>`	Credenciais da conta de usuário com as permissões de Proteção por senha necessárias.

```
Exemplo
avp.com MDRLICENSE /ADD file.key
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

```
Exemplo
avp.com MDRLICENSE /ADD file.key
```

```
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

EDRKATA. Integração com o EDR (KATA)

Comandos para gerenciar o componente Endpoint Detection and Response (KATA):

- Ativação ou desativação do componente EDR (KATA).

  O componente EDR (KATA) fornece interoperabilidade com a solução Kaspersky Anti Targeted Attack Platform.

- Configuração da conexão com os servidores da Kaspersky Anti Targeted Attack Platform.

- Exibição das configurações atuais do componente.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

```
Sintaxe de comando
avp.com START EDRKATA
```

```
avp.com STOP EDRKATA
```

```
avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
```

```
avp.com edrkata /show
```

Operação	
`stop`	Desativar o componente EDR (KATA).
`start`	Ativar o componente EDR (KATA).
`set`	Configurar o componente EDR (KATA). É possível configurar as seguintes: • Adicionar servidores do Central Node (`servers=<server address>:<port>`) • Adicionar um certificado TLS (`server-certificate=<path to the TLS certificate>`) • Definição do tempo limite de conexão do servidor do Central Node (`/timeout=<Central Node server connection timeout (s)>`) • Defina o período para a sincronização com o servidor do Central Node (`/sync-period=<Central Node server synchronization period (min)>`)
`show`	Exibe as configurações atuais do componente.

EDRExpertOnPrem. Integração com o EDR Expert (on-premises)

Comandos para gerenciar o agente integrado a fim de configurar a integração do Kaspersky Endpoint Detection and Response Expert (on-premises):

- Ativação ou desativação do agente integrado do EDR Expert (on-premises).
- Configuração dos parâmetros de conexão dos servidores do EDR Expert (on-premises).
- Exibição das configurações atuais do agente integrado.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com START EDRExpertOnPrem
```

```
avp.com STOP EDRExpertOnPrem
```

```
avp.com EDRExpertOnPrem /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate>
[/client-certificate=<path to the PFX archive> /client-certificate-password=<password to the PFX archive>]
[/timeout=<server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
/telemetry-servers=<server address:port> /telemetry-server-certificate=<path to the TLS certificat> [telemetry-
client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>]
[/telemetry-timeout=<server connection timeout (s)>] [/events-send-period=<seconds>] [/events-limit=<0|1>]
[/events-per-hour=<number of events>] [/max-packet-length=<number of packets>] [/telemetry-only-tagged-events=
<0|1>] login=<user name> password=<password>
```

```
avp.com EDRExpertOnPrem /show
```

Operação	Descrição
`stop`	Desative o agente integrado do EDR Expert (on-premises).
`start`	Ative o agente integrado do EDR Expert (on-premises).

`set`	Configure o agente integrado do EDR Expert (on-premises).
	Você pode definir as seguintes configurações de conexão para os *servidores de resposta*:
	• `servers=<server address>:<port>`. Endereço do servidor de resposta (FQDN, IPv4, IPv6).
	• `server-certificate=<path to the TLS certificate>`. Certificado TLS para estabelecer uma conexão confiável com o servidor. É possível obter um certificado TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)).
	• `client-certificate=<path to the PFX archive> client-certificate-password=<password to the PFX archive>`. Use um contêiner criptográfico para autenticação bidirecional. Um *contêiner criptográfico* é um arquivo PFX que contém um certificado e uma chave privada no formato PKCS#12. Para ativar essa autenticação, é necessário criar um contêiner criptográfico em uma autoridade de certificação externa.
	• `timeout=<server connection timeout (s)>`. Tempo limite máximo de resposta do servidor. Quando o tempo limite se esgotar, o Kaspersky Endpoint Security tentará estabelecer conexão com um servidor diferente.
	• `sync-period=<server synchronization period (min)>`. Frequência de solicitações de sincronização enviadas ao servidor. Durante a sincronização, o Kaspersky Endpoint Security receberá tarefas de resposta a ameaças e enviará os resultados da tarefa.
	Você pode definir as seguintes configurações de conexão para os *servidores de coleta de telemetria*:
	• `telemetry-servers=<server address:port>`. Endereço do servidor de coleta de telemetria (FQDN, IPv4, IPv6).
	• `telemetry-server-certificate=<path to the TLS certificat>`. Certificado TLS para estabelecer uma conexão confiável com o servidor. É possível obter um certificado TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)).
	• `telemetry-client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>`. Use um contêiner criptográfico para autenticação bidirecional. Um *contêiner criptográfico* é um arquivo PFX que contém um certificado e uma chave privada no formato PKCS#12. Para ativar essa autenticação, é necessário criar um contêiner criptográfico em uma autoridade de certificação externa.
	• `telemetry-timeout=<server connection timeout (s)>`. Tempo limite máximo de resposta do servidor. Quando o tempo limite se esgotar, o Kaspersky Endpoint Security tentará estabelecer conexão com um servidor diferente.
	• `events-send-period=<seconds>`. Atraso máximo ao enviar eventos. O aplicativo sincroniza com o servidor para enviar eventos após expirar o intervalo de sincronização. A configuração padrão é 30 segundos.
	• `events-limit=<0|1>`. Limite o número de solicitações. Esse recurso ajuda a otimizar a carga no computador. Se essa funcionalidade estiver ativada, o aplicativo restringirá a transmissão de eventos. Caso o número de eventos exceda os limites configurados, o Kaspersky Endpoint Security interromperá o envio de eventos.
	• `events-per-hour=<number of events>`. Número máximo de eventos por hora. O aplicativo analisa o fluxo de dados de telemetria e restringe o envio de eventos caso o fluxo de eventos exceda o limite de eventos configurado por hora. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. A configuração padrão é de 3 mil eventos por hora. Caso o aplicativo esteja instalado em um servidor, o fluxo de dados de telemetria será maior. Para servidores, é recomendável aumentar o valor para 60 mil eventos por hora.
	• `max-packet-length=<number of packets>`. Comprimento máximo do pacote. O aplicativo sincroniza com o servidor quando o buffer está cheio de eventos. A configuração padrão é 1024 eventos.
	• `telemetry-only-tagged-events=<0|1>`. Envio de telemetria somente com IOA. *Indicadores de ataque (IOA)* é uma regra que contém uma descrição de comportamentos suspeitos no sistema que podem indicar um ataque direcionado. O aplicativo compara o comportamento contínuo no sistema com essas regras e registra os eventos que indicam um ataque direcionado. O aplicativo usa a tecnologia *de verificação de streaming*, que permite fazer o rastreamento de eventos em tempo real.
	É possível definir as seguintes configurações gerais:
	• `mode=EDRKATA | EDRExpertOnPrem`. Alternância entre soluções:
	  • `EDRKATA`. Endpoint Detection and Response Expert (versão 7.1 ou anterior).
	  • `EDRExpertOnPrem`. Endpoint Detection and Response Expert (versão 8.0 ou posterior). Valor padrão.
	• `login=<user name> password=<password>`. Credenciais da conta de usuário com as permissões de Proteção por senha necessárias.

`show`	Exibe as configurações atuais do componente.

KUMA. Integração KUMA

Comandos para gerenciar o agente KUMA integrado:

- Ativação ou desativação da integração KUMA.

  O agente KUMA integrado fornece interoperabilidade com a solução Kaspersky Unified Monitoring and Analysis Platform.

- Configuração da conexão com os servidores da Kaspersky Unified Monitoring and Analysis Platform.

- Exibição das configurações atuais do componente.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com START KUMA
```

```
avp.com STOP KUMA [/login=<user name> /password=<password>]
```

```
avp.com KUMA /SET /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<KUMA server connection timeout (s)>] [/client-certificate=<path to the crypto-container>] [ /client-certificate-
password=<password>] [/maximum-data-transfer-time=<maximum events transmission delay (sec)>]
```

```
avp.com KUMA /SHOW
```

Operação	
`stop`	Desativar integração KUMA.
`start`	Ativar integração KUMA.
`set`	Configurar o agente KUMA integrado. É possível configurar as seguintes: • Adicione os servidores KUMA (`/servers=<protocol>://<server address>:<port>`) O aplicativo é compatível com os seguintes protocolos de conexão do servidor: `tcp`, `udp`, `http`, `https`. • Adicionar um certificado TLS (`/server-certificate=<path to the TLS certificate>`) • Definir o tempo esgotado da conexão do servidor (`/timeout=<KUMA server connection timeout (s)>`) • Adicionar um contêiner de criptografia (`/client-certificate=<path to the crypto-container> /client-certificate-password=<password>`) • Configurar o atraso de transmissão do evento (`/maximum-data-transfer-time=<maximum events transmission delay (sec)`)
`show`	Exibe as configurações atuais do componente.

Autenticação	
`/login=<user name> /password=<password>`	Credenciais da conta de usuário com as permissões de Proteção por senha necessárias.

Exemplo

```
avp.com start kuma
```

```
avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15
/login=login /password=password
```

```
avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer
/login=login /password=password
```

YARA. Execução da Verificação YARA

Execução da tarefa *Executar Verificação YARA*. O aplicativo verifica arquivos e objetos em busca de indicadores de ataques direcionados à infraestrutura de TI corporativa com o uso de bancos de dados de regras YARA. *Regras YARA* são descrições de assinaturas de ataques e intrusões direcionados para a infraestrutura de TI corporativa que o Kaspersky Endpoint Security usa para verificar objetos.

Para executar uma verificação YARA, é necessário preparar os arquivos YARA que descrevam regras. Ao criar os arquivos YARA, considere os seguintes requisitos:

- O Kaspersky Endpoint Security é compatível com arquivos YARA com as extensões YARA e YAR que aderem ao padrão aberto YARA 4.2.3 para descrever indicadores de comprometimento.
- Apenas arquivos com regras YARA podem ser especificados para a tarefa. A tarefa *Executar Verificação YARA* não é compatível com outros tipos de regra.
- Caso tenha adicionado arquivos YARA não compatíveis com o Kaspersky Endpoint Security ou caso as regras contenham erros de sintaxe, a tarefa será interrompida com a mensagem de erro correspondente.
- Os identificadores de todos os arquivos YARA usados em uma única tarefa devem ser únicos. Se houver arquivos YARA com o mesmo identificador, isso poderá afetar os resultados da execução da tarefa.
- Uma verificação YARA é interrompida após 128 correspondências com indicadores descritos nas regras YARA. Isso é necessário para limitar o número de entradas no relatório de verificação YARA, facilitando a análise e evitando o transbordamento do relatório causado por regras YARA imprecisas que podem gerar um número excessivo de correspondências.

A Kaspersky recomenda criar uma regra por arquivo YARA. Isso torna os resultados da verificação mais legíveis.

Uma verificação YARA pode levar um tempo considerável. Dependendo do tamanho da unidade, das configurações da tarefa e do número de objetos no disco, uma verificação YARA pode durar vários minutos ou várias horas. O aplicativo não exibe um indicador de progresso. Não é possível parar ou cancelar uma verificação YARA. É aconselhável esperar até que os resultados de uma verificação YARA estejam disponíveis.

Sintaxe de comando

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

Arquivos YARA	
`<full path to the YARA file>`	Caminho completo para o arquivo YARA que você deseja usar para verificação. É possível especificar os caminhos para vários arquivos YARA separados por espaços. Argumento necessário se o valor `/path=<path to the folder with YARA files>` não for especificado. Exemplo: `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`
`/path=<path to the folder with YARA files>`	Caminho completo para a pasta com os arquivos YARA que deseja usar para verificação. Argumento necessário se o valor `<full path to the YARA file>` não for especificado. Exemplo: `/path=C:\Users\Admin\Desktop\YARA`

Configurações avançadas	
`/fastScan=<on|off>`	Verificação Rápida YARA. Para cada objeto, o aplicativo registra em log uma ocorrência do indicador detectado. O aplicativo também oculta indicadores duplicados detectados no log. A Verificação Rápida YARA permite verificar arquivos grandes mais rapidamente. Caso esta configuração não seja especificada, o aplicativo executará uma verificação YARA padrão. Nesse modo, o aplicativo registra em log os indicadores duplicados detectados.
`/maxRules=<maximum number of scan rules>`	O limite do número de regras únicas acionadas que faz com que o aplicativo interrompa a verificação YARA quando o limite for atingido. Caso o valor desta configuração não seja especificado ou caso `0` seja especificado, o aplicativo executará a verificação YARA sem limitações.
`/timeOut=<stop scan after the specified time in seconds>`	Quanto tempo uma verificação YARA pode levar, em segundos. Quando esse tempo se esgotar, o aplicativo interromperá a verificação YARA. Caso o valor desta configuração não seja especificado ou caso `0` seja especificado, o aplicativo executará a verificação YARA sem limitações.
`/recursive=<on|off>`	Este argumento inicia uma verificação recursiva de subpastas dentro de Verificação Personalizada `/scanFolders`.
`/scanFolders=<list of folders to be scanned>`	Este argumento inicia uma verificação YARA de arquivos na lista de pastas especificada. É possível especificar diversos valores separados por espaços. O Kaspersky Endpoint Security é compatível com os caracteres `*` e `?` ao inserir uma máscara para o caminho da pasta. Caso essa configuração não seja especificada, o aplicativo executará uma verificação YARA em todos os discos locais, exceto os compartilhamentos de rede, unidades na nuvem e mídia removível.
`/scanMemory=<on|off>`	Verificação da memória de todos os processos em execução.
`/scanProcess=<process name>`	Verifica a memória para os processos especificados apenas. Especifique caminhos completos separados por espaço para arquivos executáveis de processos. Também é possível usar os caracteres `*` e `?` para inserir uma máscara.
`/maxSize=<file size in bytes>`	Limita o tamanho do arquivo para a verificação YARA. O aplicativo ignora arquivos maiores.
`/includes=<list of objects to be scanned>>`	Edição do escopo da verificação. É possível especificar diversos valores separados por espaços. Os seguintes valores estão disponíveis: • Nome do arquivo • Extensão do arquivo O escopo da verificação deve ser especificado com o parâmetro `/scanFolders`. Exemplo: `/scanFolders C:\*.* /includes=*.exe *.dll`: o aplicativo verifica todos os arquivos com as extensões EXE e DLL no disco C.
`/excludes=<list of objects to be scanned>`	Exclusão de arquivos da verificação YARA. É possível especificar diversos valores separados por espaços. Os seguintes valores estão disponíveis: • Caminho do arquivo • Máscara do caminho do arquivo As exclusões devem ser especificadas com o parâmetro `/scanFolders`. Exemplo: `/scanFolders C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` – o aplicativo ignora o arquivo readme.txt, todos os arquivos da pasta C:\trusted e todos os arquivos com a extensão .xml na pasta raiz no disco C.
`/scanAutoruns=<on|off>`	Verificação YARA de objetos de ponto de autorun.
`/excludeAutoruns=<list of autorun point areas to skip>`	Exclusão de objetos de ponto de autorun do escopo da verificação. Especifique caminhos completos separados por espaço para arquivos executáveis de processos. Também é possível usar os caracteres `*` e `?` para inserir uma máscara.
`/logFolder=<path to the folder for saving the scan results in a TXT file>`	Caso um caminho para uma pasta seja especificado, o aplicativo salvará os resultados da verificação no caminho especificado em um arquivo nomeado yara_<nome do computador>_<hora de conclusão da verificação>.txt. Caso um caminho para um arquivo TXT específico seja especificado, o aplicativo salvará os resultados da verificação nesse arquivo. Por exemplo: `/logFolder=C:\test` ou `/logFolder=C:\test\abc.txt`. Os resultados da verificação são exibidos na linha de comando, independentemente da opção `/logFolder` ter sido especificada.

Valores de retorno do comando:

- `-1` significa que o comando não é compatível com a versão do aplicativo instalado no computador.
- `0` significa que o comando foi executado com sucesso.
- `1` significa que um argumento obrigatório não foi passado para o comando.
- `2` significa que ocorreu um erro geral.
- `4` significa que houve um erro de sintaxe.
- `5` significa que um ou mais arquivos com regras YARA especificadas no parâmetro não foram encontrados.

Caso o comando seja executado com sucesso (valor de retorno `0`) e os indicadores de comprometimento sejam detectados ao longo do caminho, o Kaspersky Endpoint Security envia as seguintes informações de resultado da tarefa para a linha de comando:

`Started at <time>` `Finished at <time>`	Hora de início e hora de conclusão de uma verificação.
`Host name: <computer name>`	O nome do computador no qual o objeto foi detectado.
`Result: <error>`	Código de erro para o erro ocorrido durante a execução da tarefa. Caso não haja erros, o aplicativo exibirá `0x00000000`.
`Comment: <comment text>`	Descrição do erro para o erro ocorrido durante a execução da tarefa. Por exemplo, `Operation timeout`.
`Object Name:` ou `Process:` (durante a verificação da memória do processo)	O nome do objeto ou processo no qual a regra YARA foi acionada.
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	Hashes do objeto no qual a regra YARA foi acionada.
`Rule Name`	O nome da regra YARA acionada.

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	Metadados especificados na regra YARA.

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	Correspondências encontradas no objeto que atendem às condições da regra YARA:
	• Deslocamento na memória do processo ou no arquivo onde uma correspondência foi detectada (`Offset`).
	• O nome da cadeia correspondente na regra YARA (`String name`).
	• A cadeia correspondente na memória do processo ou arquivo (`String data`).

TELEMETRYFILTERS. Filtragem de eventos para serem enviados para a KUMA

Por padrão, o envio de eventos ao servidor KUMA está desativado. Para garantir que o KUMA funcione corretamente, é necessário ativar o envio de telemetria. É possível selecionar uma fonte de evento entre os logs padrão: *Application*, *Security* ou *System*. Para aprimorar o desempenho e otimizar a transmissão de dados para o servidor KUMA, é possível adicionar ou excluir manualmente os eventos individuais da telemetria. Por exemplo, é possível excluir os eventos Sysmon.

Também é possível exportar a lista de exclusões para um arquivo JSON pela linha de comando.

Se o comando contiver apenas o nome do arquivo para o qual você deseja exportar as configurações, o aplicativo colocará o arquivo da seguinte forma:

- Caso o caminho para avp.com seja adicionado na variável de sistema %PATH%, o aplicativo colocará o arquivo na pasta `C:\Windows\SysWOW64`.
- Se você executar o comando na pasta de instalação do aplicativo, a exportação falhará porque a autoproteção do aplicativo bloqueia a criação de um novo arquivo na pasta do aplicativo. Para exportar as configurações do aplicativo para um arquivo, insira o caminho do arquivo.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com TELEMETRYFILTERS /export <file name>
```

```
avp.com TELEMETRYFILTERS /import <file name>
```

Operação	
`export`	Exportação de filtros de eventos para serem enviados para KUMA.
`import`	Importação de filtros de eventos para serem enviados para KUMA. Caso já existam regras de filtragem de eventos no computador, o Kaspersky Endpoint Security substituirá essas regras durante a importação.

Arquivo para exportação ou importação	
`<file name>`	Nome do arquivo com os filtros de eventos para serem enviados para KUMA. Também é possível inserir o caminho do arquivo. É possível exportar filtros para envio para KUMA em um arquivo JSON.

Comandos de gerenciamento do Light Agent

É possível gerenciar o aplicativo no modo Light Agent para garantir a proteção em ambientes virtuais na linha de comando. É possível gerenciar o aplicativo no modo Light Agent caso o gerenciamento usando o console do Kaspersky Security Center não seja possível. Você pode visualizar a lista de comandos para gerenciar o aplicativo, executando o comando `HELP` (AJUDA). Para ler sobre a sintaxe de um comando específico, digite `HELP <command>`.

Para gerenciar o aplicativo no modo Light Agent a partir da linha de comando:

1. Execute o interpretador da linha de comando (cmd.exe) como um administrador.
2. Vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado.
3. Use o seguinte modelo para executar o comando:

   ```
   avp.com <command> [options]
   ```

   Como resultado, o Kaspersky Endpoint Security executará o comando.

O aplicativo instalado no modo Light Agent é compatível com quase todos os comandos AVP do aplicativo instalado no modo Standard. No modo Light Agent, as tarefas de atualização de banco de dados do antivírus e de gerenciamento de chaves de licença são limitadas.

KSVLAINFO. Determinar o modo Light Agent

Determinar o modo Light Agent.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com KSVLAINFO
```

O comando gera as seguintes informações para o console:

- Modo Light Agent para proteger ambientes virtuais: ativado ou desativado.

  Se o modo Light Agent estiver ativado, o aplicativo será usado como parte da solução do Kaspersky Security for Virtualization Light Agent.

- Modo de proteção VDI: ativado ou desativado.

  O modo de proteção VDI ajuda a otimizar o desempenho do Kaspersky Endpoint Security em máquinas virtuais não persistentes. Se o modo de proteção VDI estiver ativado, as atualizações que exigem a reinicialização da máquina virtual protegida não serão instaladas em máquinas virtuais não persistentes. Ao receber atualizações que exijam reinicialização, o Light Agent instalado em uma máquina virtual não persistente envia uma mensagem ao Kaspersky Security Center informando que o modelo de máquina virtual protegida precisa ser atualizado.

- Tipo da máquina virtual protegida: persistente ou não persistente.

- Função da máquina virtual protegida na infraestrutura virtual: servidor ou estação de trabalho.

- Identificador: UUID.

VIISINFO. Status da conexão do Light Agent com o Servidor de integração

Visualizar informações sobre a conexão do Light Agent com o Servidor de integração.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com VIISINFO
```

O comando gera as seguintes informações para o console:

- Endereço e porta do Servidor de integração a que o Light Agent está conectado.
- Status da conexão do Servidor de integração.
- Data e hora da última conexão do Light Agent com o Servidor de integração.

SVMINFO. Status da conexão do Light Agent com o Servidor de proteção

Visualizar informações sobre a conexão do Light Agent com o Servidor de proteção.

Para executar o comando, vá até a pasta onde o arquivo executável do Kaspersky Endpoint Security está localizado. Você também pode adicionar o caminho do arquivo executável à variável de sistema %PATH% e executar o comando sem navegar até a pasta do aplicativo.

Sintaxe de comando

```
avp.com SVMINFO
```

O comando gera as seguintes informações para o console:

- Endereço do SVM a que o Light Agent está conectado e a localização do SVM na infraestrutura virtual em relação ao Light Agent: local ou não local.
- Método de descoberta de SVM que o Light Agent usa: por meio de um Servidor de integração ou uma lista personalizada de endereços de SVM.
- Lista de endereços de SVM, se a lista de endereços de SVM estiver selecionada como o método de descoberta de SVM.
- Tag para conectar o Light Agent ao SVM.
- Algoritmo de seleção de SVMs: standard ou estendido. Se o algoritmo de seleção de SVM estendido estiver sendo usado, o tipo de caminho do SVM na infraestrutura virtual também é exibido.
- Status de proteção da conexão entre o Light Agent e o Servidor de proteção.

Códigos de erro

Podem ocorrer erros ao trabalhar com o aplicativo através da linha de comando. Quando ocorrem erros, o Kaspersky Endpoint Security mostra uma mensagem de erro, por exemplo, `Error: Cannot start task 'EntAppControl'`. O Kaspersky Endpoint Security também pode mostrar informações adicionais na forma de um código, por exemplo, `error=8947906D` (consulte a tabela a seguir).

Código do erro	Descrição
09479001	Esta chave já está em uso
0947901D	Licença expirada. Atualização do banco de dados não disponível
89479002	Chave não encontrada
89479003	Assinatura digital ausente ou corrompida
89479004	Os dados estão corrompidos
89479005	O arquivo de chave está corrompido
89479006	Licença expirada
89479007	O arquivo de chave não foi especificado
89479008	Arquivo de chave inválido
89479009	Falha ao salvar dados
8947900A	Falha ao ler dados
8947900B	Erro de E/S
8947900C	Bancos de dados não encontrados
8947900E	Biblioteca de licenciamento não carregada
8947900F	Bancos de dados corrompidos ou atualizados manualmente
89479010	Os bancos de dados estão corrompidos
89479011	Não é possível usar um arquivo de chave inválido para adicionar uma chave reserva
89479012	Erro do sistema
89479013	Lista de bloqueio de chaves corrompida
89479014	A assinatura do arquivo não é correspondente à assinatura digital da Kaspersky
89479015	Não é possível usar uma chave de licença de avaliação como uma chave de licença comercial
89479016	É necessária uma licença beta de teste para utilizar a versão beta do aplicativo
89479017	O arquivo de chave não é compatível com este aplicativo. Não é possível ativar o Kaspersky Endpoint Security for Windows com um arquivo de chave de outro aplicativo. Verifique o aplicativo instalado
89479018	Chave de licença bloqueada pela Kaspersky
89479019	Este aplicativo já foi usado com uma licença de Avaliação. Não é possível usar a chave de licença de Avaliação novamente
8947901A	O arquivo de chave está corrompido
8947901B	A assinatura digital está ausente, corrompida ou não corresponde à assinatura digital da Kaspersky
8947901C	Não é possível adicionar uma chave se a licença não comercial correspondente tiver expirado
8947901E	A data de criação ou uso do arquivo de chave é inválida. Verifique a data do sistema
8947901F	Não é possível adicionar um arquivo de chave para a licença de Avaliação: outra licença de Avaliação já está ativa
89479020	Lista de bloqueio de chaves corrompida ou ausente
89479021	Descrição da atualização ausente ou corrompida
89479022	A chave não é adequada para este aplicativo
89479023	Não é possível usar um arquivo de chave inválido para adicionar uma chave reserva
89479025	Erro ao enviar o pedido do servidor de ativação. Motivos possíveis: erro de conexão com a Internet ou problemas temporários no servidor de ativação. Tente ativar o aplicativo mais tarde (em 1-2 horas) com o código de ativação. Se o problema persistir, entre em contato com o seu provedor de Internet
89479026	A solicitação contém um código de ativação incorreto
89479027	Não é possível obter o status da resposta

Código do erro	Descrição
89479028	Ocorreu um erro ao salvar arquivo temporário
89479029	O código de ativação foi inserido incorretamente ou a data do sistema é inválida. Verifique a data do sistema no seu computador
8947902A	A chave não é compatível com este aplicativo ou a licença expirou
8947902B	Falha ao receber um arquivo de chave. Foi inserido um código de ativação incorreto
8947902C	O servidor de ativação retornou o erro 400
8947902D	O servidor de ativação retornou o erro 401
8947902E	O servidor de ativação retornou o erro 403
8947902F	O recurso necessário está indisponível no servidor de ativação. O servidor de ativação retornou o erro 404. Verifique suas configurações de conexão com a internet
89479030	O servidor de ativação retornou o erro 405
89479031	O servidor de ativação retornou o erro 406
89479032	Autenticação de proxy necessária. Verifique as configurações de rede
89479033	Tempo limite da solicitação esgotado
89479034	O servidor de ativação retornou o erro 409
89479035	O recurso necessário está indisponível no servidor de ativação. O servidor de ativação retornou o erro 410. Verifique suas configurações de conexão com a internet
89479036	O servidor de ativação retornou o erro 411
89479037	O servidor de ativação retornou o erro 412
89479038	O servidor de ativação retornou o erro 413
89479039	O servidor de ativação retornou o erro 414
8947903A	O servidor de ativação retornou o erro 415
8947903C	Erro interno do servidor
8947903D	Funcionalidade sem suporte
8947903E	Resposta de gateway inválida. Verifique as suas configurações de rede
8947903F	Recurso temporariamente indisponível
89479040	Tempo excedido de resposta do gateway. Verifique suas configurações de conexão com a Internet
89479041	Não há suporte para o protocolo no servidor
89479043	Erro de HTTP desconhecido
89479044	ID de recursos inválido
89479046	URL incorreto
89479047	Pasta de destino inválida
89479048	Erro de alocação de memória
89479049	Ocorreu um erro ao converter parâmetros para sequência de caracteres ANSI (URL, pasta, agente)
8947904A	Ocorreu um erro ao criar o thread de trabalho
8947904B	Thread de trabalho já em execução
8947904C	Thread de trabalho fora de execução
8947904D	Arquivo de chave não encontrado no servidor de ativação
8947904E	Chave bloqueada
8947904F	Erro interno do servidor de ativação
89479050	Dados insuficientes na solicitação de ativação

Código do erro	Descrição
89479053	A licença que corresponde à chave adicionada já expirou
89479054	Uma data inválida do sistema está definida no computador. Verifique a data do sistema
89479055	A licença de avaliação expirou
89479056	O período de ativação do aplicativo expirou
89479057	O limite de ativações do aplicativo foi excedido para o código especificado
89479058	Procedimento de ativação concluído com erro do sistema
89479059	Não é possível usar uma chave de licença de avaliação como uma chave de licença comercial
8947905C	O código de ativação é necessário
89479062	Não foi possível conectar ao servidor de ativação
89479064	O servidor de ativação está indisponível. Verifique suas configurações de conexão com a Internet e tente a ativação novamente
89479065	Licença expirada
89479066	Não é possível substituir a chave ativa por uma chave expirada
89479067	Não é possível adicionar uma chave reserva se a licença correspondente expirar antes da licença atual
89479068	Chave de assinatura atualizada ausente
8947906A	Código de ativação inválido
8947906B	Chave já ativa
8947906C	Os tipos de licenças correspondentes às chaves ativas e de reserva não correspondem
8947906D	Componente não compatível com a licença
8947906E	Não foi possível adicionar chave de assinatura como chave reserva
89479213	Transportar erro genérico de camada
89479214	Falha ao conectar ao servidor de ativação
89479215	Formato de endereço da Web inválido
89479216	Falha ao converter endereço do servidor proxy
89479217	Falha ao converter o endereço do servidor. Verifique as configurações da conexão com a Internet
89479218	Falha na tentativa de conexão com o servidor
89479219	Acesso negado remotamente
8947921A	Tempo limite da operação esgotado
8947921B	Erro ao enviar solicitação de HTTP
8947921C	Erro de conexão SSL
8947921D	Operação interrompida por chamada de retorno
8947921E	Muitos redirecionamentos
8947921F	Falha na verificação de destinatário
89479220	Resposta vazia do servidor
89479221	Erro ao enviar dados
89479222	Erro ao receber dados
89479223	Problema relativo ao certificado SSL
89479224	Problema relativo à criptografia SSL
89479225	Problema relativo ao centro de certificação SSL
89479226	Conteúdo inválido do pacote de rede

Código do erro	Descrição
89479227	Acesso à conta negado
89479228	Arquivo do certificado SSL inválido
89479229	Não é possível desativar a conexão SSL
8947922A	Erro recorrente
8947922B	Arquivo inválido com certificados revogados
8947922C	Erro de solicitação de certificado SSL
89479401	Erro desconhecido do servidor
89479402	Erro interno do servidor
89479403	Nenhuma chave disponível para o código de ativação inserido
89479404	Chave ativa bloqueada
89479405	Os parâmetros necessários da solicitação de ativação estão ausentes
89479406	Número de cliente ou senha inválidos
89479407	Código de ativação inválido
89479408	O código de ativação é incompatível com este aplicativo. Não é possível ativar o Kaspersky Endpoint Security for Windows com um código de ativação de outro aplicativo. Verifique o aplicativo instalado
89479409	O código de ativação é necessário
8947940B	O período de ativação expirou
8947940C	O número de ativações permitidas com este código foi excedido
8947940D	Formato inválido do ID de solicitação
8947940E	Código de ativação já em uso
8947940F	Falha ao renovar o código de ativação
89479410	Código de ativação inválido para esta região
89479411	Este código de ativação não pode ser usado para esta localização do aplicativo
89479412	O código de ativação se destina à nova versão deste aplicativo. Pegue um código de ativação diferente para ativar a versão instalada do aplicativo
89479413	O servidor de ativação retornou o erro 643
89479414	O servidor de ativação retornou o erro 644
89479415	O servidor de ativação retornou o erro 645
89479416	O servidor de ativação retornou o erro 646
89479417	É necessária a versão 1.0 do servidor de ativação
89479418	Formato de código de ativação incorreto
89479419	A hora do computador está fora de sincronia com a hora do servidor de ativação
8947941A	Versão incorreta do aplicativo
8947941B	A assinatura expirou
8947941C	Número de ativações excedido
8947941D	Assinatura de ticket inválida
8947941E	São necessários dados adicionais
8947941F	Falha na verificação de dados
89479420	Assinatura inativa
89479421	O servidor de ativação está em manutenção

Código do erro	Descrição
89479501	Erro inesperado
89479502	Parâmetro inválido transferido. Por exemplo, uma lista vazia de endereços de servidor de ativação
89479503	Código de ativação inválido (hash inválido)
89479504	ID de usuário inválida
89479505	Senha de usuário inválida
89479506	Resposta inválida do servidor de ativação
89479507	O pedido de ativação foi interrompido
89479509	O servidor de ativação retornou uma lista de encaminhamento vazia

Apêndice. Perfis de aplicação

Um *Perfil* é um componente, tarefa ou recurso do Kaspersky Endpoint Security. Os perfis são usados para gerenciar o aplicativo na linha de comando. Você pode usar perfis para executar os comandos `START`, `STOP`, `STATUS`, `STATISTICS` e `EXPORT`. Usando perfis, você pode definir as configurações dos aplicativos (por exemplo, `STOP DeviceControl`) ou executar tarefas (por exemplo, `START Scan_My_Computer`).

As seguintes perfis estão disponíveis:

- `AdaptiveAnomaliesControl` – Controle Adaptativo de Anomalias.
- `AMSI` – Proteção AMSI.
- `AntiCryptor`
- `BehaviorDetection` – Detecção de Comportamento.
- `DeviceControl` – Controle de Dispositivo.
- `EntAppControl` – Controle de Aplicativos.
- `File_Monitoring` ou `FM` – Proteção Contra Ameaças ao Arquivo.
- `Firewall` ou `FW` – Firewall.
- `HIPS` – Prevenção de Intrusão do Host.
- `IDS` – Proteção Contra Ameaças à Rede.
- `IntegrityCheck` – Verificação de integridade.
- `LogInspector` – inspeção de log.
- `Mail_Monitoring` ou `EM` – Proteção Contra Ameaças ao Correio.
- `Rollback` – Reversão de atualizações (o perfil não pode ser aplicado se o aplicativo estiver instalado em Modo Light Agent).
- `Scan_ContextScan` – Verificar pelo menu de contexto.

- `Scan_IdleScan` – Verificação em segundo plano.
- `Scan_Memory` – Verificação da memória kernel.
- `Scan_My_Computer` – Verificação Completa.
- `Scan_Objects` – Verificação Personalizada.
- `Scan_Qscan` – Verificação de objetos carregados na inicialização do sistema operacional.
- `Scan_Removable_Drive` – Verificação de unidades removíveis.
- `Scan_Startup` ou `STARTUP` – Verificação de Áreas Críticas.
- `Updater` – Atualização (o perfil não pode ser aplicado se o aplicativo estiver instalado em Modo Light Agent).
- `Web_Monitoring` ou `WM` – Proteção Contra Ameaças da Web.
- `WebControl` – Controle da Web.

Kaspersky Endpoint Security também é compatível com perfis de serviço. Perfis de serviço podem ser necessários quando você entrar em contato com o Suporte Técnico da Kaspersky.

Gerenciar aplicativo usando a API REST

O Kaspersky Endpoint Security permite o uso de soluções de terceiros para definir as configurações do aplicativo, executar uma verificação, atualizar os bancos de dados antivírus e executar outras tarefas. O Kaspersky Endpoint Security fornece uma API para essa finalidade. A API REST do Kaspersky Endpoint Security funciona por HTTP e consiste de um conjunto de métodos de solicitação/resposta. Em outras palavras, você pode gerenciar o Kaspersky Endpoint Security através de uma solução de terceiros, não a interface do aplicativo local ou o Console de Administração do Kaspersky Security Center.

Para começar a usar a API REST é necessário instalar o Kaspersky Endpoint Security com suporte para a API REST. O cliente REST e o Kaspersky Endpoint Security devem estar instalados no mesmo computador.

Para garantir a interação segura entre o Kaspersky Endpoint Security e o cliente REST:

- Configure a proteção do cliente REST contra o acesso não autorizado de acordo com as recomendações do desenvolvedor do cliente REST. Configure a proteção contra gravação na pasta do cliente REST com ajuda da Discretionary Access Control List – DACL.
- Para executar o cliente REST, use uma conta separada com direitos de administrador. Negue a entrada interativa no sistema para essa conta.

O aplicativo é gerenciado através da API REST em http://127.0.0.1 ou http://localhost. Não é possível gerenciar remotamente o Kaspersky Endpoint Security por meio da API REST.

ABRA A DOCUMENTAÇÃO DA API REST

Instalação do aplicativo com a API REST

Para gerenciar o aplicativo através da API REST é necessário instalar o Kaspersky Endpoint Security com suporte para a API REST. Se você gerenciar o Kaspersky Endpoint Security através da API REST, não poderá gerenciar o aplicativo usando o Kaspersky Security Center.

Preparando para instalar o aplicativo com suporte REST API

A interação segura do Kaspersky Endpoint Security com o cliente REST requer a configuração da identificação da solicitação. Para fazer isso, é necessário instalar um certificado e, posteriormente, assinar a carga útil de cada solicitação.

Para criar um certificado, é possível usar, por exemplo, OpenSSL.

Exemplo:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Use o algoritmo de criptografia RSA com um comprimento de chave de 2048 bits ou mais.

Como resultado, será obtido um certificado `cert.pem` e uma chave privada `key.pem`.

Instalando o aplicativo com o suporte REST API

Para instalar o Kaspersky Endpoint Security com suporte à API REST:

1. Execute o interpretador da linha de comando (cmd.exe) como um administrador.

2. Vá para a pasta que contém o pacote de distribuição do Kaspersky Endpoint Security versão 11.2.0 ou posterior.

3. Instale o Kaspersky Endpoint Security com as seguintes configurações:

   - `RESTAPI=1`

   - `RESTAPI_User=<user name>`

     Nome de usuário para gerenciar o aplicativo por meio da API REST. Digite o nome do usuário no formato `<DOMAIN>\<UserName>` (por exemplo, `RESTAPI_User=COMPANY\Administrator`). Você pode gerenciar o aplicativo por meio da API REST apenas nesta conta. Você pode selecionar apenas um usuário para trabalhar com a API REST.

   - `RESTAPI_Port=<port>`

     Porta usada para gerenciar o aplicativo por meio da API REST. A porta 6782 é usada por padrão. Certifique-se de que a porta está livre. Parâmetro opcional.

   - `RESTAPI_Certificate=<path to certificate>`

     Certificado de identificação de solicitações (por exemplo, `RESTAPI_Certificate=C:\cert.pem`).

     É possível instalar o certificado após instalar o aplicativo ou atualizar o certificado após a expiração do certificado.

     Como instalar um certificado para identificação de solicitação REST API

     1. Desativar a autodefesa do Kaspersky Endpoint Security

        A autodefesa impede que haja alteração ou exclusão de arquivos de aplicativo no disco rígido, de processos na memória e de entradas no registro do sistema.

     2. Acesse a chave de registro que contém as configurações da REST API:
        `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestAp`

     3. Insira o caminho para o certificado, por exemplo, `Certificate = C:\Folder\cert.pem`.

     4. Ativar a autodefesa do Kaspersky Endpoint Security.

     5. Reiniciar o aplicativo.

   - `AdminKitConnector=1`

     Gerenciamento de aplicativos usando sistemas de administração. O gerenciamento é permitido por padrão.

   Você também pode usar o arquivo setup.ini para definir as configurações de trabalho com a API REST.

   Exemplo:
   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /pAdminKitConnector=1 /pRESTAPI=1
   /pRESTAPI_User=COMPANY\Administrator /pRESTAPI_Certificate=C:\cert.pem /s
   ```

Como resultado, você poderá gerenciar o aplicativo por meio da API REST. Para verificar sua operação, abra a documentação da API REST usando uma solicitação GET.

Exemplo:
```
GET http://localhost:6782/kes/v1/api-docs
```

Se tiver instalado o aplicativo com suporte REST API, o Kaspersky Endpoint Security cria automaticamente uma regra de permissão nas configurações do Controle da Web para acessar recursos Web (*Regra de serviço REST API*). Esta regra é necessária para permitir que o cliente REST acesse o Kaspersky Endpoint Security em todos os momentos. Por exemplo, se tiver acesso restrito de usuário a recursos Web, isso não afetará o gerenciamento do aplicativo por meio da REST API. Recomendamos não excluir a regra ou alterar as configurações da *Regra de serviço para REST API*. Se a regra for excluída, o Kaspersky Endpoint Security a restaurará após reiniciar o aplicativo.

Trabalhar com a API

Não é possível restringir o acesso ao aplicativo por meio da API REST usando a Proteção por senha. Por exemplo, não é possível impedir que um usuário desative a proteção por meio da API REST. Você pode configurar a proteção por senha por meio da API REST e restringir o acesso do usuário ao aplicativo por meio da interface local.

Para gerenciar o aplicativo por meio da API REST, é necessário executar o cliente REST na conta especificada durante a instalação do aplicativo com suporte à API REST. Você pode selecionar apenas um usuário para trabalhar com a API REST.

ABRA A DOCUMENTAÇÃO DA API REST

O gerenciamento do aplicativo por meio da API REST consiste nas seguintes etapas:

1. Obtenha os valores atuais das configurações do aplicativo. Para fazer isso, envie uma solicitação GET.

   Exemplo:
   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```

2. O aplicativo enviará uma resposta com a estrutura e os valores das configurações. O Kaspersky Endpoint Security suporta os formatos XML e JSON.

   Exemplo:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   "enabled": true
   }
   ```

3. Editar as configurações do aplicativo. Use a estrutura de configurações recebida em resposta à solicitação GET.

   Exemplo:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": false,
   "enabled": true
   }
   ```

4. Salve as configurações do aplicativo (a carga útil) em um JSON (payload.json).

5. Assine o JSON no formato PKCS7.

   Exemplo:
   ```
   $ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out signed_payload.pem
   ```

   Como resultado, um arquivo assinado com a carga útil da solicitação será obtido (`signed_payload.pem`).

6. Editar as configurações do aplicativo. Para fazer isso, envie uma solicitação POST e anexe o arquivo assinado com a carga útil da solicitação (`signed_payload.pem`).

O aplicativo aplica as novas configurações e envia uma resposta contendo os resultados da configuração do aplicativo (a resposta pode estar vazia). É possível verificar se as configurações estão atualizadas usando uma solicitação GET.

Fontes de informação sobre o aplicativo

Esta seção descreve as fontes de informação sobre o aplicativo.

É possível selecionar a fonte de informação mais conveniente, dependendo da importância e urgência do problema.

Página do Kaspersky Endpoint Security no site da Kaspersky

Na página do Kaspersky Endpoint Security, é possível visualizar informações gerais sobre o aplicativo, suas funções e recursos.

A página do Kaspersky Endpoint Security contém um link para a loja on-line. Na loja é possível comprar ou renovar o aplicativo.

Página do Kaspersky Endpoint Security na Base de Conhecimento

A *Base de Conhecimento* é uma seção no site de Suporte técnico.

Na Base de Conhecimento da página do Kaspersky Endpoint Security, é possível ler artigos que fornecem informações úteis, recomendações e respostas a perguntas frequentes sobre como comprar, instalar e usar o aplicativo.

Os artigos da Base de Conhecimento podem responder a perguntas relacionadas não apenas ao Kaspersky Endpoint Security, mas também a outros aplicativos da Kaspersky. Os artigos da Base de Conhecimento também podem conter novidades do Suporte técnico.

Discussão sobre 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.

Entrar em contato com o 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 Endpoint 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 aplicativo.

O Kaspersky oferece suporte ao Kaspersky Endpoint 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

Após informar o problema encontrado aos especialistas do Suporte Técnico da Kaspersky, eles talvez solicitem que você crie um *arquivo de rastreamento*. O arquivo de rastreamento permite rastrear o processo de realizar comandos do aplicativo, passo a passo, e determinar a etapa da operação do aplicativo em que o erro ocorre.

Os especialistas do Suporte técnico podem solicitar informações adicionais sobre o sistema operacional, os processos executados no computador e relatórios detalhados sobre a operação dos componentes do aplicativo.

Enquanto executa o diagnóstico, os especialistas do Suporte Técnico podem lhe pedir para alterar as configurações do aplicativo, da seguinte forma:

- Ativar a funcionalidade que recebe informações de diagnóstico adicionais.
- Configurar componentes individuais do aplicativo ao alterar configurações especiais que não estão disponíveis através da interface padrão do usuário.
- Alterar as configurações de armazenamento de informações de diagnóstico.
- Configurar a intercepção e registro de tráfego de rede.

Os especialistas do Suporte Técnico irão fornecer todas as informações necessárias para executar essas operações (descrição da sequência de etapas, configurações a modificar, arquivos de configuração, scripts, funcionalidades adicionais da linha de comando, módulos de depuração, utilitários de finalidades especiais, etc.) e irão informá-lo sobre o escopo dos usados coletados para efeitos de depuração. As informações de diagnóstico adicionais são salvas no computador do usuário. Os dados não são transmitidos automaticamente para a Kaspersky.

As operações listadas em cima devem ser executadas sob a supervisão de especialistas do Suporte Técnico, seguindo suas instruções. Alterar por conta própria as configurações do aplicativo em formas não descritas na ajuda on-line ou não recomendas pelos especialistas do suporte técnico, pode provocar lentidões e erros fatais do sistema operacional, reduzir o nível de proteção do computador e danificar a disponibilidade e integridade das informações processadas.

Conteúdo e armazenamento de arquivos de rastreio

Você é pessoalmente responsável pela segurança dos dados armazenados em seu computador, especialmente por monitorar e restringir acesso aos dados até que eles sejam enviados para a Kaspersky.

Os arquivos de rastreamento são armazenados no computador enquanto o aplicativo estiver em uso, e excluídos permanentemente quando o aplicativo for removido.

Os arquivos de rastreamento, exceto aqueles do Agente de Autenticação, são armazenados na pasta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`.

Os arquivos de rastreamento são nomeados da seguinte forma: `KES<14.2_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.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.

Conteúdo dos arquivos de rastreamento SRV.log, GUI.log e ALL.log

Os arquivos de rastreamento `SRV.log`, `GUI.log` e `ALL.log` podem armazenar as seguintes informações, além dos dados gerais:

- Dados pessoais, incluindo o nome próprio, sobrenome e nome do meio, caso esses dados sejam incluídos no caminho de arquivos em um computador local.
- Dados no hardware instalado no computador (como dados de firmware BIOS / UEFI). Esses dados são gravados em arquivos de rastreamento durante a execução do Kaspersky Disk Encryption.
- O nome de usuário e a senha, caso tenha sido transmitidos abertamente. Esses dados podem ser registrados em arquivos de rastreamento durante a verificação de tráfego da Internet.
- O nome de usuário e a senha, caso sejam incluídos em cabeçalhos HTTP.

- O nome da conta do Microsoft Windows, caso seja incluído em um nome de arquivo.
- O seu endereço de e-mail ou um endereço web com o nome da sua conta e senha, caso sejam ambos incluídos no nome do objeto detectado.
- Os sites que você visita e os redirecionamentos a partir desses sites. Esses dados são gravados em arquivos de rastreamento quando o aplicativo verifica sites.
- O endereço do servidor proxy, nome do computador, porta, endereço IP e nome de usuário usado para fazer login no servidor proxy. Esses dados são registrados em arquivos de rastreamento caso o aplicativo use um servidor proxy.
- Os endereços de IP remotos aos quais o computador estabeleceu conexões.
- Assunto da mensagem, ID, nome do remetente e endereço da página da Web do remetente da mensagem em uma rede social. Estes dados são escritos para rastrear os arquivos se o componente Controle da Web for ativado.
- Dados de tráfego de rede. Esses dados são gravados em um arquivo de rastreamento se os componentes de monitoramento de tráfego estiverem ativados (como o Controle da Web).
- Dados recebidos dos servidores da Kaspersky (como a versão dos bancos de dados antivírus).
- Status dos componentes do Kaspersky Endpoint Security e seus dados operacionais.
- Dados sobre a atividade do usuário no aplicativo.
- Eventos do sistema operacional.

Conteúdos de arquivos de rastreamento HST.log, BL.log, Dumpwriter.log, WD.log e AVPCon.dll.log

Além dos dados gerais, o arquivo de rastreamento `HST.log` contém informações sobre a execução de uma tarefa de atualização do banco de dados e módulos do aplicativo.

Além de incluir dados gerais, o arquivo de rastreamento `BL.log` contém informações sobre eventos que ocorrem durante a operação do aplicativo, bem como os dados requeridos para corrigir erros do aplicativo. Esse arquivo é criado se o aplicativo for iniciado com o parâmetro avp.exe –bl.

Além de incluir dados gerais, o arquivo de rastreamento `Dumpwriter.log` contém informações de serviço requeridas para corrigir erros que ocorrem quando o arquivo de dump do aplicativo é gravado.

Além dos dados gerais, o arquivo de rastreamento `WD.log` contém informações sobre eventos que ocorrem durante a operação do serviço avpsus, incluindo eventos de atualização do módulo do aplicativo.

Além dos dados gerais, o arquivo de rastreamento `AVPCon.dll.log` contém informações sobre eventos que ocorrem durante a operação do módulo de conectividade do Kaspersky Security Center.

Conteúdo dos arquivos de rastreamento de desempenho

Os arquivos de rastreamento de desempenho são nomeados da seguinte forma: `KES<14.2_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl`.

Além dos dados gerais, os arquivos de rastreamento de desempenho contêm informações sobre a carga no processador, informações sobre o tempo de carregamento do sistema operacional e aplicativos; e informações sobre processos em execução.

Conteúdo do arquivo de rastreamento do componente de Proteção AMSI

Além dos dados gerais, o arquivo de `AMSI.log` contém informações sobre os resultados das verificações realizadas segundo as solicitações de aplicativos de terceiros.

Conteúdo dos arquivos de rastreamento do componente de Proteção Contra Ameaças ao Correio

O arquivo de rastreamento `mcou.OUTLOOK.EXE.log` pode conter partes de mensagens de e-mail, inclusive endereços de e-mail, além de dados gerais.

Conteúdo dos arquivos de rastreamento do componente Verificar pelo menu de contexto

O arquivo de rastreamento `shellex.dll.log` contém informações sobre a conclusão da tarefa de verificação e os dados necessários para depurar o aplicativo, além de informações gerais.

Conteúdo dos arquivos de rastreamento do plug-in da web do aplicativo

Os arquivos de rastreamento do plug-in da web do aplicativo são armazenados no computador onde o Kaspersky Security Center Web Console está implantado, na pasta `Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs`.

Arquivos de rastreamento do plug-in da Web do aplicativo são nomeados da seguinte maneira: `logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log`. O Web Console começa a escrever dados depois da instalação e exclui os arquivos de rastreamento depois que o Web Console for removido.

Os arquivos de rastreamento do plug-in da web do aplicativo contêm as seguintes informações, além de dados gerais:

- Senha de usuário do KLAdmin para desbloquear a interface do Kaspersky Endpoint Security (Proteção por senha).
- Senha temporária para desbloquear a interface do Kaspersky Endpoint Security (Proteção por senha).

- Nome de usuário e senha do servidor de e-mail SMTP (Notificações de e-mail).
- Nome de usuário e senha do servidor proxy de Internet (Servidor proxy).
- Nome de usuário e senha para a tarefa *Alterar componentes do aplicativo*.
- Credenciais da conta e caminhos especificados nas tarefas do Kaspersky Endpoint Security e nas propriedades da política.

Conteúdo do arquivo de rastreamento do Agente de Autenticação

O arquivo de rastreamento do Agente de Autenticação é armazenado na pasta System Volume Information com o seguinte nome: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Além dos dados gerais, o arquivo de rastreamento do Agente de Autenticação contém informações sobre a operação do Agente de Autenticação e as ações realizadas pelo usuário com o Agente de Autenticação.

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 (por exemplo, SRV.log, WD.log e outros).

Os rastreamentos de aplicativos devem ser executados sob a supervisão do Suporte Técnico da Kaspersky.

Para criar um arquivo de rastreamento do aplicativo:

1. Na janela principal do aplicativo, clique no botão .
2. Na janela que é aberta, clique no botão **Ferramentas de suporte**.
3. Use o botão de alternância **Ativar rastreamento do aplicativo** para ativar ou desativar o rastreamento de funcionamento do aplicativo.
4. Na lista suspensa **Rastreamento**, selecione um modo de rastreamento de aplicativo:
   - **Com limitação de tamanho**. Salve os rastreamentos em um número limitado de conjunto de arquivos de tamanho limitado e substitua os arquivos mais antigos quando o tamanho máximo for atingido. Caso este modo seja selecionado, será possível definir o número máximo de conjunto de arquivos para rotação e o tamanho máximo para cada conjunto de arquivos.

     Por padrão, o aplicativo salva cinco conjuntos de arquivos de rastreamento. Conjunto de arquivos tem 3072 MB. Dessa forma, será preciso 15 GB de espaço livre em disco para salvar os arquivos de rastreamento.
   - **Sem limitações**. Salve um arquivo de rastreamento (sem limite de tamanho).

5. Selecione o nível de rastreamento na lista suspensa **Nível**:

   - **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.

   Níveis de rastreamento adicionais estão disponíveis se as configurações de rastreamento do aplicativo forem gerenciadas na linha de comando. É recomendável obter mais informações sobre o nível de rastreamento junto de um especialista do Suporte Técnico. Caso não exista orientação do Suporte técnico, defina o nível de rastreamento para **Normal**.

   Caso o rastreamento do aplicativo tenha sido ativado na linha de comando e um nível de rastreamento tenha sido definido de forma diferente de **Normal** ou **Detalhado**, a lista suspensa **Nível** estará definida como **Normal**.

6. Para interromper o processo de rastreamento, retorne à janela **Ferramentas de suporte** e desative o rastreamento.

Você também pode criar arquivos de rastreamento ao instalar o aplicativo a partir da linha de comando, inclusive usando o arquivo setup.ini.

Como resultado, os arquivos de rastreamento de funcionamento do aplicativo são criados na pasta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. Após a criação dos arquivos de rastreamento, basta enviá-los para o Suporte Técnico da Kaspersky.

O Kaspersky Endpoint Security exclui automaticamente os rastros de arquivos quando o aplicativo é removido. Também é possível excluir os arquivos manualmente. Para fazer isso, é preciso desativar o rastreamento e interromper o aplicativo.

Rastreamento de desempenho do aplicativo

O Kaspersky Endpoint Security permite que você receba informações sobre problemas operacionais do computador durante o uso do aplicativo. Por exemplo, você pode receber informações sobre atrasos no carregamento do sistema operacional após a instalação do aplicativo. Para isso, o Kaspersky Endpoint Security cria arquivos de rastreamento de desempenho *Rastreamentos de desempenho* referem-se ao registro de ações executadas pelo aplicativo com o objetivo de diagnosticar os problemas de desempenho do Kaspersky Endpoint Security. Para receber informações, o Kaspersky Endpoint Security usa o serviço Rastreamento de Eventos para Windows (ETW). O Suporte Técnico da Kaspersky é responsável por diagnosticar problemas do Kaspersky Endpoint Security e estabelecer os motivos desses problemas.

Os rastreamentos de aplicativos devem ser executados sob a supervisão do Suporte Técnico da Kaspersky.

Para criar um arquivo de rastreamento de desempenho:

1. Na janela principal do aplicativo, clique no botão .

2. Na janela que é aberta, clique no botão **Ferramentas de suporte**.

3. Use o botão de alternância **Ativar rastros de desempenho** para ativar ou desativar o rastreamento de desempenho.

4. Na lista suspensa **Rastreamento**, selecione um modo de rastreamento de aplicativo:

   - **Com limitação de tamanho**. Salve rastreamentos em um número limitado de arquivos de tamanho limitado e substitua os arquivos mais antigos quando o tamanho máximo for atingido. Se este modo for selecionado, você pode definir o tamanho máximo para cada arquivo.

   - **Sem limitações**. Salve um arquivo de rastreamento (sem limite de tamanho).

5. Selecione o nível de rastreamento na lista suspensa **Nível**:

   - **Superficial**. O Kaspersky Endpoint Security analisa os principais processos do sistema operacional relacionados ao desempenho.

   - **Detalhado**. O Kaspersky Endpoint Security analisa todos os processos do sistema operacional relacionados ao desempenho.

6. Na lista suspensa **Tipo de rastreamento**, selecione o tipo de rastreamento:

   - **Informações básicas**. O Kaspersky Endpoint Security analisa processos enquanto o sistema operacional está em execução. Use esse tipo de rastreamento se um problema persistir depois que o sistema operacional carregar, como um problema ao acessar a Internet no navegador.

   - **Ao reiniciar**. O Kaspersky Endpoint Security analisa processos apenas enquanto o sistema operacional está sendo carregado. Após o carregamento do sistema operacional, o Kaspersky Endpoint Security para de rastrear. Use esse tipo de rastreamento se o problema estiver relacionado a demora no carregamento do sistema operacional.

7. Reinicie o computador e tente reproduzir o problema.

8. Para interromper o processo de rastreamento, retorne à janela Ferramentas de suporte e desative o rastreamento.

Como resultado, um arquivo de rastreamento de desempenho é criado na pasta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. Após a criação do arquivo de rastreamento, envie-o para o Suporte técnico da Kaspersky.

Armazenar despejos

Um arquivo de dump contém todas as informações sobre a memória de trabalho de processos do Kaspersky Endpoint Security no momento em que arquivo de dump foi criado.

> Os arquivos de despejo salvos podem conter dados confidenciais. Para controlar o acesso aos dados, você deve assegurar independentemente a segurança dos arquivos de despejo.

Os arquivos de dump são armazenados no computador enquanto o aplicativo estiver em uso, e excluídos permanentemente quando o aplicativo é removido. Os arquivos de despejo são armazenados na pasta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`.

Como ativar a gravação do dump no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Configurações de aplicativos**.
4. No bloco **Informações de depuração**, clique no botão **Configurações**.
5. Na janela aberta, use a caixa de seleção **Ativar gravação do dump** para ativar ou desativar a gravação do dump do aplicativo.
6. Salvar alterações.

Como ativar a gravação do dump no Web Console e no Cloud Console

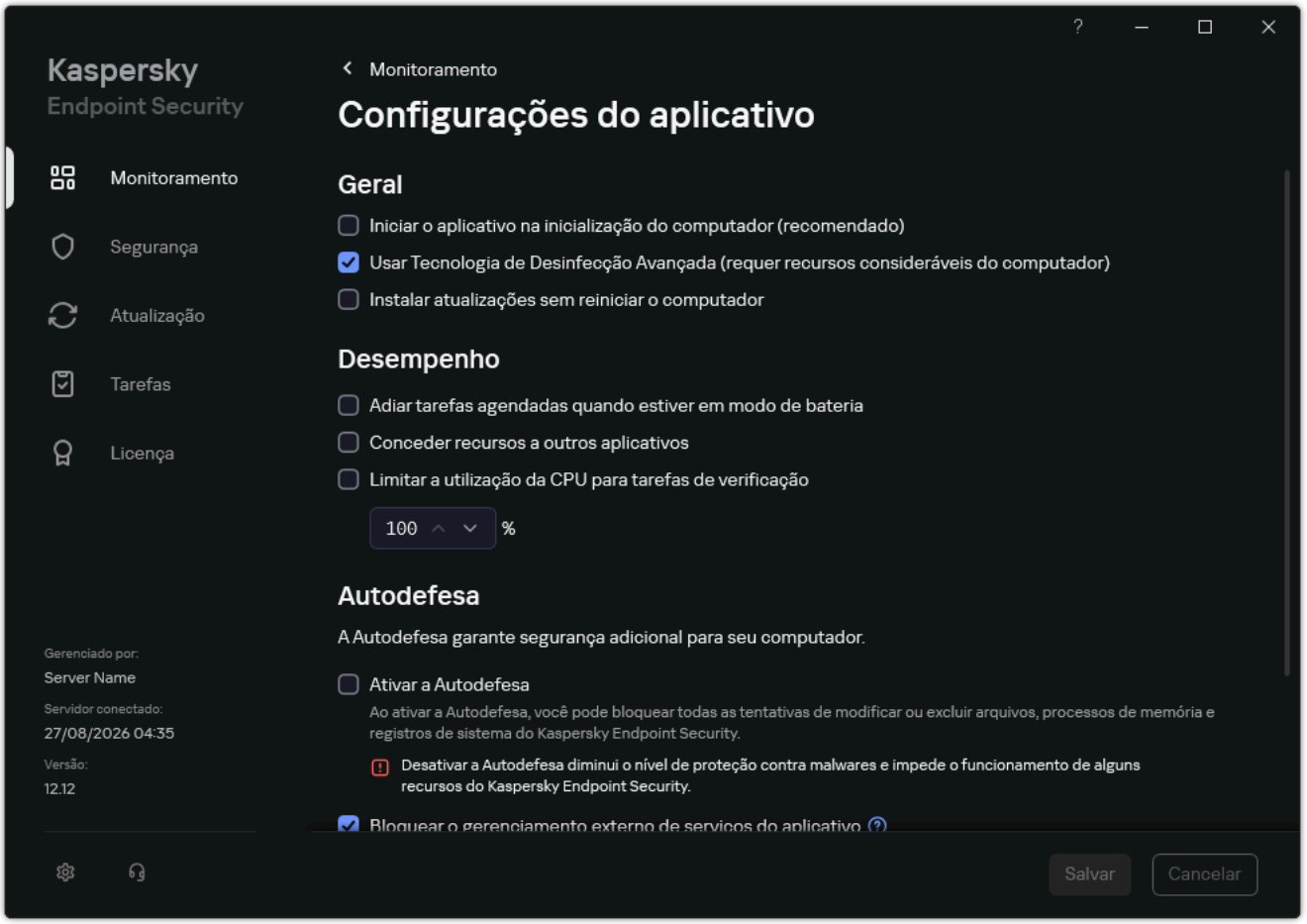
1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Suporte Técnico**.
5. No bloco **Informações de depuração**, use a caixa de seleção **Gravação do despejo ATIVADA** para ativar ou desativar a gravação do dump do aplicativo.
6. Salvar alterações.

Como ativar a gravação do dump na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações do aplicativo**.



Configurações do Kaspersky Endpoint Security for Windows

3. No bloco **Informações de depuração**, use a caixa de seleção **Ativar gravação do dump** para ativar ou desativar a gravação do dump do aplicativo.

4. Salvar alterações.

Protegendo arquivos de despejo e arquivos de rastreamento

Os arquivos de dump e rastreamento contêm informações sobre o sistema operacional e também podem conter dados de usuário. Para impedir o acesso não autorizado a tais dados, você pode ativar a proteção de arquivos de dump e arquivos de rastreamento.

Se a proteção de arquivos de dump e de rastreamento for ativada, os arquivos poderão ser acessados pelos seguintes usuários:

- Os arquivos de dump podem ser acessados pelo administrador de sistema e administrador local, e pelo usuário que ativou a escrita de arquivos de dump e arquivos de rastreamento.

- Os arquivos de rastreamento podem ser acessados somente pelo administrador do sistema e administrador local.

Como ativar a proteção de arquivos de despejo e arquivos de rastreamento no Console de Administração (MMC)

1. No Console de Administração do Kaspersky Security Center, selecione **Políticas**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela da política, selecione **Configurações gerais** → **Configurações de aplicativos**.
4. No bloco **Informações de depuração**, clique no botão **Configurações**.
5. Na janela aberta, use a caixa de seleção **Ativar proteção de arquivos de dump e de rastreamento** para ativar ou desativar a proteção de arquivos.
6. Salvar alterações.

Como ativar a proteção de arquivos de despejo e arquivos de rastreamento no Web Console e no Cloud Console

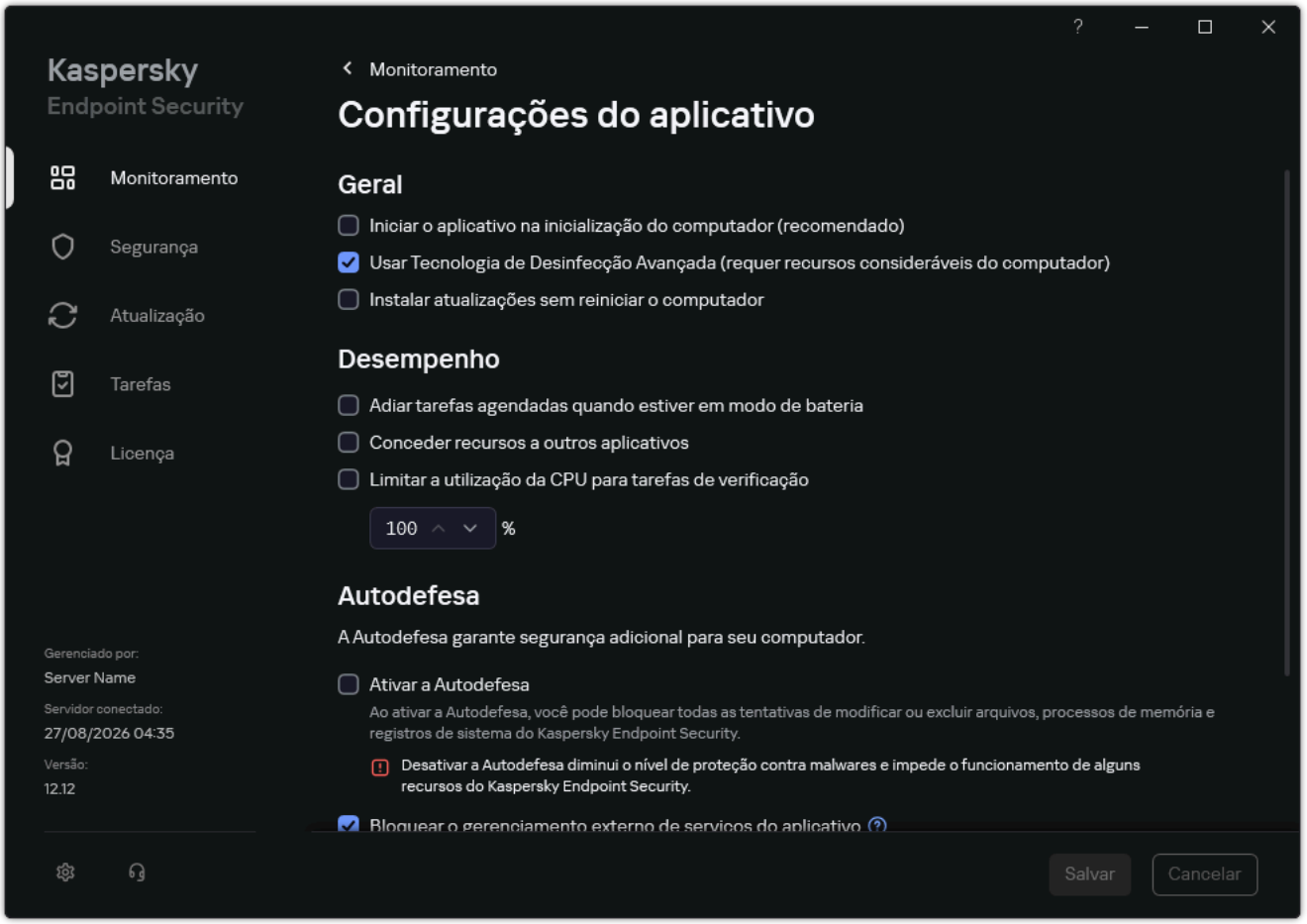
1. Na janela principal do Web Console, selecione **Gerenciamento de ativos** → **Políticas**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   A janela de propriedades da política é exibida.
3. Selecione a guia **Configurações do aplicativo**.
4. Selecione **Configurações gerais** → **Suporte Técnico**.
5. No bloco **Informações de depuração**, use a caixa de seleção **Proteção de arquivos de despejo e rastreamento ATIVADA** para ativar ou desativar a proteção de arquivos.
6. Salvar alterações.

Como ativar a proteção de arquivos de despejo e arquivos de rastreamento na interface do aplicativo

1. Na janela principal do aplicativo, clique no botão ⚙.

2. Na janela de configurações do aplicativo, selecione **Configurações gerais** → **Configurações do aplicativo**.



Configurações do Kaspersky Endpoint Security for Windows

3. No bloco **Informações de depuração**, use a caixa de seleção **Ativar proteção de arquivos de dump e de rastreamento** para ativar ou desativar a proteção de arquivos.

4. Salvar alterações.

Os arquivos de dump e os arquivos de rastreamento que foram escritos enquanto a proteção foi ativada permanecem protegidos até depois que essa função é desativada.

Obtenção de dados do SO (Kaspersky Get System Info)

Após a instalação do aplicativo Kaspersky Endpoint Security, talvez o sistema operacional ou um aplicativo não funcionem corretamente. Há um conflito entre o aplicativo e o software ou os drivers dos componentes do computador.

Para identificar a causa do problema, o Suporte Técnico da Kaspersky requer um relatório do utilitário Kaspersky Get System Info (aqui referido como GSI). Para obter informações detalhadas quanto ao uso do utilitário, consulte a Base de Dados de Conhecimento da Kaspersky.

Limitações e avisos

O Kaspersky Endpoint Security tem várias limitações que não são críticas para a operação do aplicativo.

Instalar o aplicativo

- Para obter detalhes sobre o suporte dos sistemas operacionais Microsoft Windows 10, Microsoft Windows Server 2016 e Microsoft Windows Server 2019, consulte a Base de Conhecimento do Suporte Técnico.
- Para obter detalhes sobre a compatibilidade dos sistemas operacionais Microsoft Windows 11 e Microsoft Windows Server 2022, consulte a Base de Conhecimento do Suporte Técnico.
- Depois de ser instalado em um computador infectado, o aplicativo não informa ao usuário sobre a necessidade de executar uma verificação no computador. Você pode ter problemas ao ativar o aplicativo. Para resolver esses problemas, inicie uma Verificação de Áreas Críticas.
- Se caracteres não ASCII (por exemplo, letras russas) forem usados nos arquivos setup.ini e setup.reg, é recomendável editar o arquivo usando notepad.exe e salvá-lo na codificação UTF-16LE. Não há suporte para outras codificações.
- O aplicativo não tem suporte para o uso de caracteres não ASCII ao especificar o caminho de instalação do aplicativo nas configurações do pacote de instalação.
- Quando as configurações do aplicativo são importadas de um arquivo CFG, o valor da configuração que define a participação na Kaspersky Security Network não é aplicado. Depois de importar as configurações, leia o texto da Declaração da Kaspersky Security Network e confirme o seu consentimento para participar na Kaspersky Security Network. Você pode ler o texto da Declaração na interface do aplicativo ou no arquivo ksn_*.txt localizado na pasta que contém o kit de distribuição do aplicativo.
- Se desejar remover e reinstalar a criptografia (FLE ou FDE) ou o componente de Controle de dispositivos, você deve reiniciar o sistema antes da reinstalação.
- Ao usar o sistema operacional Microsoft Windows 10, você deve reiniciar o sistema após remover o componente Criptografia em Nível de Arquivo (FLE).
- Ao remover componentes do aplicativo individuais (por exemplo, usando a tarefa *Alterar componentes do aplicativo*), pode ser necessário reiniciar o computador.
- Nas propriedades da tarefa *Alterar componentes do aplicativo*, ao alternar o modo de instalação (**Modo separado**/**Modo combinado**), a sincronização do conjunto de componentes entre os modos não é compatível. O aplicativo sincroniza o conjunto de componentes entre os modos após as propriedades da tarefa serem reabertas.
- A instalação do aplicativo pode terminar com um erro informando *Um aplicativo cujo nome está ausente ou ilegível está instalado em seu computador*. Isso significa que aplicativos incompatíveis ou fragmentos deles permanecem em seu computador. Para remover artefatos de aplicativos incompatíveis, envie uma solicitação com uma descrição detalhada da situação ao Suporte Técnico da Kaspersky pelo portal Kaspersky CompanyAccount.
- Caso tenha cancelado a remoção do Kaspersky Endpoint Security, inicie a recuperação do aplicativo após reiniciar o computador.

- O aplicativo requer Microsoft .NET Framework 4.0 ou posterior. O Microsoft .NET Framework 4.6.1 tem vulnerabilidades. Caso esteja usando o Microsoft .NET Framework 4.6.1, é preciso instalar as atualizações de segurança. Para obter detalhes sobre as atualizações de segurança do Microsoft .NET Framework, consulte o site de suporte técnico da Microsoft.

- Se o aplicativo for instalado sem sucesso com o componente Kaspersky Endpoint Agent selecionado em um sistema operacional de servidor e a janela *Erro do Coordenador do Windows Installer* aparecer, consulte as instruções no site de suporte da Microsoft.

- Se o aplicativo foi instalado localmente no modo não interativo, use o arquivo setup.ini fornecido para substituir os componentes instalados.

- Depois que o Kaspersky Endpoint Security for Windows é instalado em algumas configurações do Windows 7, o Windows Defender continua a operar. É aconselhável desativar manualmente o Windows Defender para evitar degradação do desempenho do sistema.

- Ao instalar o Kaspersky Endpoint Security for Windows em um servidor com os aplicativos Kaspersky Security for Windows Server (KSWS) e Windows Defender instalados, é necessário reiniciar o sistema. Uma reinicialização do sistema será necessária mesmo se a instalação do aplicativo sem reinicialização do sistema tiver sido habilitada. O Windows Defender para Windows Server está incluído na lista de softwares incompatíveis com o Kaspersky Endpoint Security for Windows. Antes de instalar o aplicativo, o instalador remove o Windows Defender para Windows Server. A remoção de software incompatível torna necessária uma reinicialização do sistema.

- Antes de instalar o Kaspersky Endpoint Security for Windows (KES) em um servidor com o Kaspersky Security for Windows Server (KSWS) instalado, é necessário desativar o KSWS Password Protection. Após migrar do KSWS para o KES, ative a Proteção por senha nas configurações do aplicativo.

- Para instalar o aplicativo em computadores executando Windows 7 ou Windows Server 2008 R2 com o software Veeam Backup & Replication implantado, pode ser necessário reinicializar o computador e executar o aplicativo novamente.

- A migração do Kaspersky Small Office Security (KSOS) para o Kaspersky Endpoint Security (KES) com a Proteção por senha ativada está disponível a partir do KSOS compilação 21.16. Para migrar para as versões anteriores do KSOS, é necessário desativar a Proteção por senha remover manualmente o KSOS. A migração do KSOS para o KES com a Proteção por senha desativada é executada corretamente.

- Não é possível instalar o Kaspersky Endpoint Security em uma unidade removível executável. Ao ser instalado, o Kaspersky Endpoint Security exibe uma mensagem de erro: *Você selecionou uma pasta ou unidade inválida. O aplicativo deve ser instalado em um disco rígido local.* Caso o aplicativo seja instalado em uma unidade removível usando ferramentas de terceiros, o sistema operacional pode travar (BSOD) durante o processo de inicialização. Isso significa que o Kaspersky Endpoint Security não é compatível com o Windows To Go e soluções semelhantes. Para verificar um computador a partir de uma unidade removível, use o aplicativo gratuito Kaspersky Rescue Disk.

- Instalar o Kaspersky Endpoint Security com componentes de rede em um servidor de terminal e com sessões RDP multiusuário envolve algumas considerações especiais. O sistema operacional força o encerramento de todas as sessões de usuário após o término da sessão do administrador. Para estabelecer conexão com o servidor de terminais, é necessário reiniciar o servidor ou fazer login no sistema localmente. Este comportamento é ditado por peculiaridades quanto ao funcionamento do sistema operacional Windows.

- Se os plug-ins da Web do Kaspersky Endpoint Security for Windows (versão 12.11.0.2004) e do Kaspersky Endpoint Security for Linux (versão 12.4.0.1354) estiverem instalados no Kaspersky Security Center 16.0 ou no Kaspersky Security Center 16.1, atualizar o plug-in da Web do Kaspersky Endpoint Security for Windows para a versão 12.11.0.6004 poderá causar mau funcionamento nas políticas do Kaspersky Endpoint Security for Linux.

  Solução possível: vá para a janela **Configurações** → **Plug-in da web** e remova o plug-in da Web do Kaspersky Endpoint Security for Windows, o plug-in da Web do Kaspersky Endpoint Security for Linux e o Unified Protection and Management Plug-in da lista. Instale o plug-in da Web do Kaspersky Endpoint Security for Linux e, depois, o plug-in da Web do Kaspersky Endpoint Security for Windows.

- No Web Console, a lista de componentes é exibida incorretamente nas propriedades do pacote de instalação do Kaspersky Endpoint Security 12.11 for Windows. Um componente separado, Anti-Cryptor, não está disponível nesta versão do aplicativo. A funcionalidade de proteção de pastas compartilhadas contra criptografia externa está incluída no componente Detecção de Comportamento. No Kaspersky Endpoint Security 12.12 for Windows, essa funcionalidade é um componente separado. Ao mesmo tempo, no Console de Administração (MMC), a lista de componentes é exibida corretamente.

- Ao usar o plug-in da web versão 7.0 ou posterior, a lista de componentes selecionados por padrão para instalação é exibida incorretamente nas propriedades do pacote de instalação do Kaspersky Endpoint Security 14.1 e de versões anteriores. Se essa lista não for modificada durante a criação do pacote de instalação, o aplicativo será instalado com o conjunto padrão de componentes especificado para a versão correspondente do aplicativo.

Atualização do aplicativo

- A partir da versão 11.0.0 do aplicativo, é possível sobrepor a instalação do plug-in do MMC do Kaspersky Endpoint Security for Windows com a nova versão do plug-in. Para retornar à versão anterior, exclua o plug-in atual e instale a versão anterior.

- Ao atualizar o Kaspersky Endpoint Security 11.0.0 ou 11.0.1 for Windows, as configurações de agendamento de tarefas locais para as tarefas *Atualização de bancos de dados e módulos do aplicativo*, *Verificação de áreas críticas*, *Verificação personalizada* e *Verificação de integridade do aplicativo* não são salvas.

- Em computadores que executam o Windows 10 versão 1903 e 1909, atualizações do Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 3 (compilação 10.3.3.275), Service Pack 2 Maintenance Release 4 (compilação 10.3.3.304), 11.0.0 e 11.0.1 com o componente Criptografia a nível de arquivo (FLE) instalado podem terminar com um erro. Isso ocorre porque a criptografia de arquivo não é compatível com essas versões do Kaspersky Endpoint Security for Windows no Windows 10 versão 1903 e 1909. Antes de instalar esta atualização, é recomendável remover o componente de criptografia de arquivo.

- O aplicativo requer o Microsoft .NET Framework 4.0 ou posterior. Microsoft .NET Framework 4.6.1 possui vulnerabilidades. Caso esteja usando o Microsoft .NET Framework 4.6.1, é preciso instalar as atualizações de segurança. Para obter detalhes sobre as atualizações de segurança do Microsoft .NET Framework, consulte o site de suporte técnico da Microsoft.

- Ao atualizar o Kaspersky Endpoint Security, o aplicativo desativa o uso da KSN até que a Declaração da Kaspersky Security Network seja aceita. Além disso, o status do computador pode ser alterado para *Crítico* no Kaspersky Security Center; o evento *Servidores da KSN indisponíveis* é recebido. Se estiver usando o Kaspersky Managed Detection and Response, eventos sobre violações na operação da solução serão recebidos. O uso da KSN é obrigatório para a operação do Kaspersky Managed Detection and Response. O Kaspersky Endpoint Security permite o uso da KSN após a aplicação da política na qual o administrador aceita os termos de uso da KSN. Após a Declaração da Kaspersky Security Network ser aceita, o Kaspersky Endpoint Security retoma a operação.

- Após atualizar o Kaspersky Endpoint Security para a versão 11.10.0 ou posterior sem reiniciar o computador, ele terá dois aplicativos Kaspersky Endpoint Security instalados. Não remova manualmente a versão anterior do aplicativo. A versão anterior será removida automaticamente quando o computador for reiniciado.

- Depois de atualizar o Kaspersky Endpoint Security em um computador que executa o Microsoft Windows 11, o menu de contexto do arquivo pode exibir itens para versões anteriores e novas do aplicativo. Reinicie o seu computador duas vezes para garantir o correto funcionamento do menu de contexto do arquivo.

- Caso a Autodefesa do aplicativo esteja desativada e todos os adaptadores de rede estejam parados, os componentes de rede do aplicativo não funcionarão entre o final da atualização do aplicativo e a reinicialização do computador. Os componentes de rede do aplicativo incluem Proteção Contra Ameaças da Web, Proteção Contra Ameaças ao Correio, Proteção Contra Ameaças à Rede, Firewall, Prevenção de Intrusão do Host e Controle da Web. Reinicie o computador para que o aplicativo funcione corretamente.

- O componente Prevenção contra ataque BadUSB não funciona entre o final da atualização do aplicativo e a reinicialização do computador. Reinicie o computador para que o aplicativo funcione corretamente.

- O aplicativo não pode ser atualizado se o processo de atualização anterior não tiver sido concluído. Reinicie o computador para que o aplicativo funcione corretamente.

- Após o aplicativo ser atualizado a partir de versões anteriores ao Kaspersky Endpoint Security 11 for Windows, o computador deve ser reiniciado.

- Quando o Kaspersky Endpoint Security é gerenciado pelo Kaspersky Security Center Cloud Console, não é possível atualizar o aplicativo localmente. Se o aplicativo for atualizado localmente, não será possível aceitar o Contrato de Processamento de Dados do Kaspersky Security Center Cloud Console.

Suporte para arquitetura Arm

- A instalação do Kaspersky Endpoint Security no Modo Light Agent em máquinas virtuais baseadas em Arm não é compatível.

- O Kaspersky Disk Encryption não é compatível com computadores baseados em Arm.

- A criptografia de arquivos não é compatível com computadores baseados em Arm.

- A criptografia de unidades removíveis não é compatível em computadores baseados em Arm.

- O Agente EDR não é compatível com Bitdefender Endpoint Security Tools em computadores que executam o Windows 11 para Arm64.

- A funcionalidade de proteção de sinal de áudio e a funcionalidade de proteção de acesso à webcam não são compatíveis em computadores baseados em Arm.

- Em computadores baseados em Arm, a extensão Proteção Contra Ameaças ao Correio é compatível com as versões de 32 e 64 bits do Outlook 2016, Outlook 2021, Outlook 2024 e Outlook 365 para Arm64.

- O Kaspersky Endpoint Security não envia objetos destinados à arquitetura Arm para o Kaspersky Sandbox.

- O controle de impressões não é compatível com computadores baseados em Arm.

- Em computadores baseados em Arm, a tarefa *Verificação de IOC* é compatível apenas com arquivos de e-mail dos seguintes programas de e-mail: Versões de 32 bits e 64 bits do Outlook 2016 e Outlook 2021, 2024 e 365 para Arm64.

- Em computadores com Windows 11 para Arm64, a autenticação baseada em token pode não estar disponível porque o sistema operacional não consegue detectar um certificado válido no token. Esse comportamento é causado pela forma como o sistema operacional interage com o software do token. Por exemplo, o sistema operacional pode não ter os drivers necessários para o funcionamento do token. Nesse caso, o Kaspersky Endpoint Security também não oferece suporte à autenticação baseada em token (Proteção por senha). Você pode usar outros métodos de autenticação, como credenciais de usuário.

Suporte para plataformas de servidor

- Em servidores com *desduplicação de dados* ativada, é necessário adicionar o arquivo fsdmhost.exe à lista de aplicativos confiáveis. Isso ajuda a otimizar o desempenho do aplicativo e evitar carga excessiva na CPU.

- O suporte ao sistema de arquivos de ReFS possui limitações:

  - O Kaspersky Endpoint Security pode processar os eventos de desinfecção de ameaças incorretamente. Por exemplo, caso o aplicativo exclua um arquivo malicioso, o relatório pode ter uma entrada objeto não processado. Ao mesmo tempo, o Kaspersky Endpoint Security desinfecta as ameaças de acordo com as configurações do aplicativo. O Kaspersky Endpoint Security também pode criar uma cópia do evento *O objeto será desinfectado ao reiniciar* para o mesmo objeto.

  - A Proteção contra ameaças ao arquivo pode ignorar algumas ameaças. Ao mesmo tempo, a Verificação de malware funciona corretamente.

  - Depois que a tarefa *Verificação de malware* for iniciada, as exclusões adicionadas com o iChecker são redefinidas ao reiniciar o servidor.

  - Não há suporte para a tecnologia iSwift. O Kaspersky Endpoint Security não considera exclusões de verificação adicionadas usando a tecnologia iSwift.

  - O Kaspersky Endpoint Security não detecta arquivos eicar.com e susp-eicar.com se o arquivo meicar.exe estiver presente no computador antes da instalação do Kaspersky Endpoint Security.

  - O Kaspersky Endpoint Security pode exibir incorretamente as notificações de desinfecção de ameaças. Por exemplo, o aplicativo pode exibir uma notificação de ameaça para uma ameaça desinfectada anteriormente.

- As tecnologias Criptografia em Nível de Arquivo (FLE) e Kaspersky Disk Encryption (FDE) não são compatíveis com plataformas de servidor. Ao mesmo tempo, o Kaspersky Endpoint Security pode processar incorretamente os eventos de criptografia de dados.

- Em sistemas operacionais de servidor, nenhum aviso é exibido sobre a necessidade de desinfecção avançada.

- O Microsoft Windows Server 2008 foi excluído do suporte. A instalação do aplicativo em um computador executando o sistema operacional Microsoft Windows Server 2008 não é suportada.

- Instalar o Kaspersky Endpoint Security em um servidor com o Microsoft Data Protection Manager (DPM) implementado pode prejudicar o funcionamento do DPM. Isso é causado por limitações na operação do DPM. Para evitar o funcionamento incorreto, é necessário adicionar as unidades de servidor locais às exclusões para o componente Proteção Contra Ameaças ao Arquivo e para as tarefas de *Verificação de malware*.

- Há suporte para o modo Server Core, porém com limitações:

  - A interface gráfica do usuário local não está disponível, incluindo notificações, notificações pop-up e outros controles de interface. O aplicativo não pode exibir as janelas de prompt, incluindo as seguintes janelas:

    - Prompts de versão do aplicativo e confirmação de atualização do módulo;

    - Prompt de reinicialização do computador;

    - Prompt de credenciais de autenticação do servidor proxy;

    - Perguntar para obter acesso ao dispositivo (Controle de Dispositivos).

- Os seguintes componentes não estão disponíveis: Proteção Contra Ameaças da Web, Proteção Contra Ameaças ao Correio, Controle da Web, Prevenção contra ataque BadUSB.
- O Antibridging não está disponível.
- Só é possível aceitar a Declaração da Kaspersky Security Network na política do aplicativo no console do Kaspersky Security Center.
- A Criptografia de Unidade de Disco BitLocker está disponível apenas com o módulo de plataforma confiável (TPM). Um PIN/senha não pode ser utilizado para criptografia porque o aplicativo não é capaz de exibir a janela de solicitação de senha para autenticação pré-inicialização. Caso o sistema operacional tenha o modo de compatibilidade do Federal Information Processing Standard (FIPS) ativado, conecte uma unidade removível para salvar a chave de criptografia antes de começar a criptografar a unidade.

Suporte para plataformas virtuais

- Não há suporte para criptografia completa do disco (FDE) em máquinas virtuais Hyper-V.
- Não há suporte para a Criptografia Completa do Disco (FDE) em plataformas virtuais Citrix.
- Os sistemas operacionais Windows 10 Enterprise multissessão e Windows 11 Enterprise multissessão são compatíveis com limitações:
  - O Kaspersky Endpoint Security desinfecta as ameaças ativas sem notificar o usuário, apenas ao desinfectar ameaças ativas nos servidores. Outros usuários ativos podem perder os dados caso a ameaça não seja imediatamente resolvida, pois o sistema operacional continua a funcionar em modo multissessão.
  - A Criptografia Completa do Disco (FDE) não é compatível.
  - O gerenciamento do BitLocker não é compatível.
  - O uso do Kaspersky Endpoint Security não é compatível para unidades removíveis. A infraestrutura do Microsoft Azure define unidades removíveis como unidades de rede.
- Não há suporte para a instalação e o uso do Criptografia em Nível de Arquivo (FLE) em plataformas virtuais Citrix.
- Para oferecer suporte à compatibilidade do Kaspersky Endpoint Security for Windows com Citrix PVS, execute a instalação com a opção **Garantir a compatibilidade com Citrix PVS** ativada. Esta opção pode ser ativada no Assistente de instalação ou usando o parâmetro de linha de comando `/pCITRIXCOMPATIBILITY=1`. No caso de instalação remota, o arquivo KUD deve ser editado adicionando-se o seguinte parâmetro: `/pCITRIXCOMPATIBILITY=1`.
- Citrix XenDesktop. Antes de iniciar a clonagem, você deve desativar a Autodefesa para clonar máquinas virtuais que usam o vDisk.
- Ao preparar um modelo de máquina para a imagem principal Citrix XenDesktop com o Kaspersky Endpoint Security for Windows e o Agente de Rede do Kaspersky Security Center pré-instalados, adicione os seguintes tipos de exclusões ao arquivo de configuração:

```
[Rule-Begin]
Type=File-Catalog-Construction
Action=Catalog-Location-Guest-Modifiable
name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
[Rule-End]
```

Para obter detalhes sobre o Citrix XenDesktop, visite o site de suporte da Citrix.

- Em alguns casos, uma tentativa de desconectar com segurança uma unidade removível pode ser malsucedida em uma máquina virtual implementada em um hipervisor VMware ESXi. Tente desconectar o dispositivo com segurança mais uma vez.

- O Kaspersky Endpoint Security é compatível com o hipervisor VMware ESXi com as seguintes limitações:

  - O Kaspersky Endpoint Security pode ser incompatível com os drivers do Guest Introspection (vnetWFP.sys, vnetFLT.sys e outros). Para resolver a incompatibilidade, atualize os drivers para a versão mais recente ou os desinstale.

  - Em alguns casos, uma tentativa de remover com segurança um disco removível em uma máquina virtual pode não funcionar. Tente desconectar o dispositivo com segurança mais uma vez.

- Instalar o Kaspersky Endpoint Security em máquinas virtuais com o agente Citrix VDA pode terminar com um erro de compatibilidade. Isso acontece porque Citrix Provisioning Services tem compatibilidade limitada com soluções antivírus. Para obter as melhores práticas de uso de soluções antivírus com Citrix Provisioning Services, consulte o site de suporte da Citrix.

- O Kaspersky Endpoint Security ignora a verificação de uma unidade removível se a unidade estiver conectada a uma máquina virtual no hipervisor Citrix (a tarefa *Verificação de unidades removíveis*). Nesses dispositivos, o sistema operacional detecta a unidade removível conectada como uma unidade de rede. Nesses casos, basta usar a tarefa *Verificação personalizada*. O comportamento do aplicativo no Modo Standard e no Modo Light Agent é o mesmo.

- Se o Kaspersky Endpoint Security estiver instalado em uma máquina virtual em uma infraestrutura que usa a tecnologia Citrix App Layering, os arquivos detectados pelo aplicativo como infectados com o status *O objeto será excluído ao reiniciar* não serão removidos automaticamente quando a máquina virtual for reinicializada.

  Para excluir esses arquivos, você deve montar o arquivo VHDX que contém User Layer no computador do administrador do Citrix App Layering e executar uma verificação de malware no disco montado.

- Antes de criar um instantâneo da Golden Image de uma máquina virtual com o Kaspersky Endpoint Security instalado, é recomendável desligar a máquina virtual e criar um instantâneo "frio". Se você criar um instantâneo enquanto a máquina virtual estiver em execução (um instantâneo "quente"), não será possível garantir o funcionamento correto do aplicativo.

Compatibilidade com o Kaspersky Security Center

- No Kaspersky Security Center Web Console versão 14.1 e anteriores, os nomes de áreas funcionais de componentes da Inspeção do Log e do Monitor de integridade de arquivos não são exibidos corretamente na seção de configurações de permissões de acesso ao usuário das propriedades do Servidor de Administração.

- Após reparar o aplicativo, a proteção da conexão do computador ao Servidor de Administração será desativada. Após reparar o aplicativo, execute novamente a tarefa *Proteção da conexão do Servidor de Administração*.

- No Console de Administração do Kaspersky Security Center, a janela **Selecionar um usuário ou grupo de usuários** exibe apenas os primeiros 50 mil usuários da lista de usuários do Kaspersky Security Center. Consulte a Ajuda do Kaspersky Security Center para obter mais detalhes.

- Ao procurar os dispositivos gerenciados no console de administração do Kaspersky Security Center, a guia **Componentes do aplicativo** talvez exiba simultaneamente diversas variantes do nome do mesmo componente do aplicativo, inclusive nomes correspondentes a versões mais antigas do Kaspersky Endpoint Security. Os nomes de alguns componentes também podem ser duplicados.

  Para pesquisar pelo componente, basta selecionar uma das variantes exibidas. Para obter mais detalhes a descoberta de um dispositivo, consulte a Ajuda do Kaspersky Security Center.

- No Kaspersky Security Center Web Console 15.1 Update 2 com o plug-in da web do Kaspersky Endpoint Security for Windows versão 12.11 ou posterior e o Unified Protection and Management Plug-in instalado, as condições de ativação do perfil da política não funcionam. O Kaspersky Security Center não adiciona ao console novos dispositivos que atendem às condições de ativação do perfil.

Licença

- Se a mensagem do sistema *Erro ao receber dados* for exibida, verifique se o computador no qual você está executando a ativação tem acesso à rede ou defina as configurações de ativação por meio do Proxy de Ativação do Kaspersky Security Center.

- Na interface do aplicativo, a data de expiração da licença é exibida na hora local do computador.

- A instalação do aplicativo com um arquivo de chave integrado em um computador com acesso instável à Internet pode resultar na exibição temporária de eventos informando que o aplicativo não está ativado ou que a licença não permite a operação do componente. Durante o processo de instalação, isso é causado devido ao aplicativo ativar primeiro a licença de avaliação integrada. Requer acesso à Internet.

- Durante o período de avaliação, a instalação de qualquer atualização ou patch de aplicativo em um computador com acesso instável à Internet pode resultar na exibição temporária de eventos informando que o aplicativo não está ativado. Durante o processo de instalação da atualização, isso é causado devido ao aplicativo ativar primeiro a licença de avaliação integrada. Requer acesso à Internet.

- Se a licença de avaliação foi ativada automaticamente durante a instalação do aplicativo e, em seguida, o aplicativo foi removido sem salvar as informações da licença, o aplicativo não será ativado automaticamente com a licença de avaliação quando reinstalado. Nesse caso, ative o aplicativo manualmente.

- Caso esteja usando o Kaspersky Security Center versão 11 e o Kaspersky Endpoint Security versão 14.2, os relatórios de desempenho dos componentes podem funcionar incorretamente. Caso tenha instalado componentes do Kaspersky Endpoint Security não incluídos em sua licença, o Agente de Rede pode enviar erros de status de componentes para o log de eventos do Windows. Para evitar erros, remova os componentes não incluídos em sua licença.

Proteção Contra Ameaças ao Correio

- Ao verificar e-mails com a extensão Proteção Contra Ameaças ao Correio para Microsoft Outlook, recomendamos usar o Modo em Cache do Exchange Server (Use Cached Exchange Mode).

- O Kaspersky Endpoint Security não oferece suporte à versão de 64 bits do cliente de mail Microsoft Outlook. Isso significa que o Kaspersky Endpoint Security não verifica os arquivos do Microsoft Outlook (arquivos PST e OST) se uma versão de 64 bits do Microsoft Outlook estiver instalada no computador, mesmo se o correio estiver incluído no escopo da verificação.

- O Kaspersky Endpoint Security não é compatível com o Novo programa de e-mail do Microsoft Outlook.

- Se você desativou a desinfecção de ameaças detectadas pela Proteção Contra Ameaças ao Correio e recebeu um e-mail infectado em sua caixa de correio do Outlook, a Proteção Contra Ameaças da Web poderá bloquear a comunicação com o servidor Exchange por MAPI. A Proteção Contra Ameaças da Web gera então um evento de detecção de ameaça e o envia ao Kaspersky Security Center. Para restaurar a conexão entre o computador e o servidor Exchange, você deve excluir manualmente o e-mail infectado da caixa de correio do Outlook.

  Ao atualizar a versão do aplicativo sem reiniciar o computador, o nível da Proteção Contra Ameaças ao Correio é temporariamente reduzido (por até um minuto). Se você receber um e-mail infectado em sua caixa de correio do Outlook durante a atualização do aplicativo, a Proteção Contra Ameaças da Web também bloqueará a conexão com o servidor Exchange por MAPI. Para restaurar a conexão, exclua o e-mail infectado da caixa de correio do Outlook.

Mecanismo de Remediação

- O aplicativo somente restaura arquivos em dispositivos que tenham o sistema de arquivos NTFS ou FAT32.
- O aplicativo restaura arquivos com um tamanho de até 100 MB.
- 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.

Firewall

- Se uma regra de pacote de rede ou uma regra de rede de aplicativos especificar nomes DNS, o Kaspersky Endpoint Security pode enviar solicitações ao servidor DNS para determinar os endereços IP desses recursos. O Firewall usa endereços IP para monitorar a atividade de rede. Portanto, o aplicativo resolve nomes DNS para endereços IP. É recomendado usar nomes DNS nas regras apenas para computadores da LAN ou serviços internos.
- Para especificar uma regra para todos os endereços IPv6, adicione o intervalo de endereços ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. O Firewall não é compatível com a máscara ::/0.
- A filtração de pacotes ou conexões por endereço local, interface física e vida útil (TTL) do pacote é suportada nos seguintes casos:
  - Por endereço local para pacotes ou conexões de saída em regras de aplicativo para TCP e UDP e regras de pacotes.
  - Por endereço local para pacotes ou conexões de entrada (exceto UDP) em regras de blocos de aplicativos ou pacotes.
  - Pela vida útil (TTL) do pacote nas regras de pacotes para pacotes de entrada ou saída.
  - Por interface de rede para pacotes de entrada e saída ou conexões em regras de pacotes.

- Caso tenha configurado um adaptador de rede ou Vida útil do pacote (TTL) para uma regra de permissão de pacote, a prioridade dessa regra é menor do que uma regra de aplicativo de bloqueio. Em outras palavras, se a atividade de rede for bloqueada para um aplicativo (por exemplo, caso o aplicativo esteja no grupo de confiança de *Alta restrição*), não será possível permitir a atividade de rede do aplicativo usando uma regra de pacote com essas configurações. Em todos os outros casos, a prioridade de uma regra de pacote é maior do que regras de rede de aplicativos.

- Ao importar as regras de pacote de firewall, o Kaspersky Endpoint Security pode modificar os nomes das regras. O aplicativo determina regras com conjuntos idênticos de parâmetros gerais: protocolo, direção, portas remotas e locais, tempo de vida do pacote (TTL). Caso o conjunto de parâmetros principais seja idêntico para várias regras, o aplicativo atribuirá o mesmo nome a essas regras ou adicionará uma tag ao nome. Isso significa que o Kaspersky Endpoint Security importa todas as regras do pacote, mas o nome das regras com as configurações gerais idênticas pode ser alterado.

- Se tiver ativado o relatório de eventos do aplicativo em uma regra de rede, ao mover o aplicativo para um grupo confiável diferente, as restrições desse grupo de confiança não serão aplicadas. Portanto, se o aplicativo estiver no grupo de confiança Confiável, ele não terá restrições de rede. Assim, o relatório de eventos para esse aplicativo foi ativado e movido para o grupo de confiança *Não confiável*. O firewall não aplicará as restrições de rede para este aplicativo. Recomendamos mover primeiramente o aplicativo para o grupo confiável apropriado e então ativar o relatório de eventos. Se esse método não for adequado, é possível configurar restrições manualmente para o aplicativo nas configurações de regras de rede. A restrição será aplicada somente à interface local do aplicativo. Mover o aplicativo entre grupos de confiança na política funciona corretamente.

- Os componentes Firewall e Prevenção de intrusão têm configurações em comum: direitos do aplicativo e recursos protegidos. Se estas configurações forem alteradas para Firewall, o Kaspersky Endpoint Security aplica automaticamente as novas configurações ao componente de Prevenção de intrusão. Se, por exemplo, for permitida a alteração das configurações gerais da política de Firewall (o cadeado está aberto), as configurações de Prevenção de intrusão também se tornarão editáveis.

- Quando uma regra de pacote de rede é acionada no Kaspersky Endpoint Security 11.6.0 ou anterior, a coluna **Nome do aplicativo** no relatório do Firewall sempre exibirá o valor *Kaspersky Endpoint Security*. Além disso, o firewall bloqueará a conexão no nível do pacote para todos os aplicativos. Este comportamento foi modificado para o Kaspersky Endpoint Security 11.7.0 ou posterior. A coluna **Tipo de regra** foi adicionada ao relatório do Firewall. Quando uma regra de pacote de rede é acionada, o valor da coluna **Nome do aplicativo** permanece vazio.

- Se todas as atividades de rede forem bloqueadas pelo Firewall, o componente Proteção Contra Ameaças à Rede pode identificar um ataque do tipo Verificação de portas. Isso poderá acontecer porque o aplicativo inicia a Proteção Contra Ameaças à Rede antes do Firewall para detectar atividades suspeitas na rede.

Prevenção contra ataque BadUSB

- O Kaspersky Endpoint Security restabelece o tempo limite do bloqueio do dispositivo USB quando o computador está bloqueado (por exemplo, o tempo limite do bloqueio da tela decorreu). Ou seja, no caso de inserção de um código de autorização do dispositivo USB errado várias vezes e o aplicativo trava o dispositivo USB, o Kaspersky Endpoint Security permite repetir a tentativa de autorização após destravar o computador. Neste caso, o Kaspersky Endpoint Security não bloqueia o dispositivo USB por um período tal como foi especificado nas configurações do componente de prevenção contra ataque BadUSB.

- O Kaspersky Endpoint Security redefine o tempo limite de bloqueio do dispositivo USB quando a proteção do computador é pausada. Ou seja, no caso de inserção de um código de autorização de dispositivo USB errado várias vezes e o aplicativo travar o dispositivo USB, o Kaspersky Endpoint Security permite a repetição da tentativa de autorização depois de reiniciar a proteção do computador. Neste caso, o Kaspersky Endpoint Security não bloqueia o dispositivo USB por um período tal como foi especificado nas configurações do componente de prevenção contra ataque BadUSB.

Kaspersky Security Network

- O Kaspersky Endpoint Security não é compatível com o HTTPS quando se conecta com o KSN Proxy (caixa de seleção **Usar HTTPS** marcada nas configurações de conexão do KSN Proxy) caso o endereço do servidor inclua letras não latinas (símbolos diferentes de ASCII).

- No Kaspersky Security Center, ao mudar a utilização da Kaspersky Security Network global para a Kaspersky Security Network privada (KPSN), ou vice-versa, a opção de participar na Kaspersky Security Network será desativada na política do produto específico. Após a mudança, leia atentamente o texto da Declaração da Kaspersky Security Network e confirme seu consentimento para participar da KSN. Você pode ler o texto da Declaração na interface do aplicativo ou ao editar a política do produto.

- A partir do Kaspersky Endpoint Security 12.9 for Windows, ao mudar da KPSN para a KSN global, é necessário confirmar novamente sua concordância com a Declaração da Kaspersky Security Network. Para isso, você precisa ativar a Kaspersky Security Network nas configurações de política ou na interface do aplicativo e confirmar que concorda com a Declaração da Kaspersky Security Network. Se você já usou a KSN global, primeiro desative o uso da KSN, ative-a novamente e confirme sua concordância com a Declaração da Kaspersky Security Network. Se você não concordar com a Declaração da Kaspersky Security Network, o aplicativo não poderá acessar os dados da Kaspersky Security Network.

- O Kaspersky Endpoint Security não envia arquivos de texto (como arquivos TXT, CSV, LOG e DOCX sem macros) à Kaspersky Security Network para verificação. O aplicativo envia arquivos que possam representar uma ameaça à KSN para verificação. Esses arquivos incluem arquivos executáveis ou arquivos que possam conter código executável (como macros em arquivos DOCX). Outros componentes do aplicativo são responsáveis pela verificação de arquivos de texto. Você também pode verificar manualmente a reputação de um arquivo de texto no menu de contexto do arquivo. Se um arquivo de texto tiver uma reputação *Não confiável (Kaspersky Security Network)*, o aplicativo ignora a ação definida para ameaças detectadas.

Controle de aplicativos

- Ao configurar regras de Controle de Aplicativos, recomenda-se não adicionar mais de 100.000 condições de inclusão e exclusão combinadas para aplicativos em categorias diferentes, considerando que o Kaspersky Endpoint Security esteja sendo executado em um computador que atenda aos requisitos mínimos de hardware e utilize o Microsoft Windows 10.

- Somente os arquivos no formato ZIP são compatíveis com o funcionamento das regras de Controle de Aplicativos no Kaspersky Security Center Web Console. Arquivos em outros formatos, como RAR ou 7z, não são compatíveis. Essa restrição não existe caso o usuário trabalhe com regras de Controle de Aplicativos no Console de Administração (MMC).

- Ao trabalhar com as regras do Controle de Aplicativos no Kaspersky Security Center Web Console, o tamanho máximo compatível para um arquivo carregado é 104 MB. Essa restrição não existe caso o usuário trabalhe com regras de Controle de Aplicativos no Console de Administração (MMC).

- Ao trabalhar no Microsoft Windows 10 no modo lista de bloqueio de aplicativos, as regras de bloqueio podem ser aplicadas incorretamente, o que pode causar o bloqueio de aplicativos não especificados nas regras.

- Caso tenha adicionado novas *Regras de controle de aplicativos predefinidas* ao atualizar o Kaspersky Endpoint Security, não será possível aplicar essas regras a versões anteriores do aplicativo.

- Quando os aplicativos da web progressivos (PWA) são bloqueados pelo componente Controle de aplicativos, appManifest.xml é indicado como o aplicativo bloqueado no relatório.

- Ao adicionar o aplicativo padrão Bloco de Notas a uma regra de controle de aplicativos para Windows 11, não é recomendado especificar o caminho para o aplicativo. Em computadores que executam o Windows 11, o sistema operacional usa o Metro Notepad localizado na pasta `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe`. Nas versões anteriores do sistema operacional, o Bloco de Notas está localizado nas seguintes pastas:

  - `C:\Windows\notepad.exe`
  - `C:\Windows\System32\notepad.exe`
  - `C:\Windows\SysWOW64\notepad.exe`

  Ao adicionar o Bloco de Notas a uma regra de controle de aplicativos, é possível especificar o nome do aplicativo e o hash do arquivo a partir das propriedades do aplicativo em execução, por exemplo.

- Ao migrar a política KSWS para o perfil da política KES, o assistente de conversão de políticas e tarefas em lote (assistente de migração) renomeia as categorias de aplicativos se os nomes das categorias contiverem caracteres proibidos: `'` `*` `<` `>` `?` `\` `:` `|`. O assistente de migração substitui esses caracteres por caracteres `_`. Por exemplo, a categoria do aplicativo `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` é renomeada para `KSWS_Everyone_[C61F-3B7C-4D89-96A1]`.

Controle de Dispositivos

- O Kaspersky Endpoint Security pode registrar eventos de conexão e desconexão de dispositivos externos. Os serviços do Windows usam a conta de usuário do sistema para conectar ou desconectar dispositivos. Isso torna impossível saber qual é o usuário que está conectando ou desconectando o dispositivo. O Kaspersky Endpoint Security especifica a conta de usuário do SISTEMA no evento.

- O acesso aos dispositivos de impressora adicionados à lista confiável é bloqueado por regras de bloqueio de dispositivo e barramento.

- Para dispositivos MTP, o controle das operações de Leitura, Gravação e Conexão é suportado se você estiver usando os drivers integrados da Microsoft no sistema operacional. Se um usuário instalar um driver personalizado para trabalhar com um dispositivo (por exemplo, como parte do iTunes ou Android Debug Bridge), o controle das operações de Leitura e Gravação pode não funcionar.

- Ao trabalhar com dispositivos MTP, as regras de acesso são alteradas após reconectar o dispositivo.

- O componente Controle de Dispositivos registra eventos relacionados aos dispositivos monitorados, como conexão e desconexão de um dispositivo, leitura de um arquivo de um dispositivo, gravação de um arquivo em um dispositivo e outros eventos. O Kaspersky Endpoint Security somente registra os eventos de desconexão para os seguintes tipos de dispositivo: Dispositivos portáteis (MTP), Unidades removíveis, Disquetes, Unidades de CD/DVD. Para outros tipos de dispositivo, o aplicativo não registra os eventos de desconexão. O aplicativo registra a operação de conexão de um dispositivo com um computador para todos os tipos de dispositivos.

- Se você estiver adicionando um dispositivo à lista confiável com base em uma máscara de modelo e usar caracteres que estão incluídos no ID, mas não no nome do modelo, esses dispositivos não serão adicionados. Em uma estação de trabalho, esses dispositivos serão adicionados à lista confiável com base em uma máscara de ID.

- Quando o aplicativo é atualizado sem a reinicialização do computador, o Controle de Dispositivos não aplica as regras de acesso aos dispositivos reconectados. No entanto, caso o dispositivo esteja conectado antes da atualização, o Controle de Dispositivos aplicará as regras corretamente. Reinicie o computador para que o aplicativo funcione corretamente com os dispositivos reconectados.

- Em computadores com o Kaspersky Endpoint Security versão 12.0 instalado, o modo de acesso da impressora **Permitir e não registrar** para o tipo de dispositivo **Impressoras de rede** se chamará **Depende do barramento de conexão** se a política do Kaspersky Endpoint Security versão 12.1 estiver aplicada ao computador. Nesses modos, o aplicativo realiza as mesmas ações. No Kaspersky Endpoint Security versão 12.1, o modo de acesso para impressoras de rede é chamado corretamente de **Permitir e não registrar**.

- Desde o Kaspersky Endpoint Security 12.0 for Windows, o aplicativo permite configurar regras de impressão para impressoras (controle de impressão). Após instalar o aplicativo com controle de impressão ou atualizar o aplicativo para uma versão com controle de impressão, reinicie o computador. Até que o computador seja reiniciado, o Kaspersky Endpoint Security não aplicará regras de impressão e só poderá controlar o acesso às impressoras. Se a reinicialização do computador afetar negativamente os fluxos de trabalho em sua organização, você poderá reiniciar apenas o serviço spoolsv (spooler de impressão). O controle de impressões não é compatível com computadores baseados em Arm.

- Desde o Kaspersky Endpoint Security for Windows, o protocolo WPA3 é suportado pelo aplicativo para dispositivos do tipo **Wi-Fi**. Se uma política do Kaspersky Endpoint Security versão 12.2 for aplicada em um computador, o protocolo WPA2 será selecionado nos computadores com o Kaspersky Endpoint Security versão 11.11.0 e anteriores; o WPA2/WPA3 será selecionado para as versões 12.0 a 12.1; e o WPA3 será selecionado para as versões 12.2 e posteriores.

- Os dispositivos da Apple são classificados como dispositivos portáteis (MTP) e dispositivos do iTunes. O sistema operacional pode identificar incorretamente a conexão do dispositivo da Apple e não determiná-lo como um dispositivo portátil (MTP). Nesse caso, o dispositivo da Apple ficará indisponível no gerenciador de arquivos e acessível no aplicativo iTunes. Como resultado, o Kaspersky Endpoint Security controlará o acesso ao dispositivo da Apple apenas no aplicativo iTunes. Para acessar o dispositivo da Apple como um dispositivo portátil (MTP), acesse o Gerenciador de dispositivos e remova o driver USB do dispositivo móvel da Apple da lista de controladores USB. Após reiniciar o computador, o sistema operacional identificará o dispositivo da Apple como um dispositivo portátil (MTP) e um dispositivo do iTunes. O Kaspersky Endpoint Security controlará o acesso ao dispositivo no aplicativo iTunes e no gerenciador de arquivos.

- No Kaspersky Endpoint Security 12.3 for Windows, as configurações de acesso são diferentes para o tipo de dispositivo **Bluetooth**. Caso tenha especificado o valor **Depende do barramento de conexão** na versão anterior do aplicativo, depois de atualizar o aplicativo para a versão 12.3, o valor configurado muda para **Permitir e não registrar**. Isso não altera o comportamento do dispositivo.

- O Controle de Dispositivos é compatível com dispositivos Bluetooth somente por meio da pilha Microsoft Windows Bluetooth. O Controle de Dispositivos pode funcionar incorretamente com pilhas Bluetooth de terceiros.

- Caso o dispositivo Bluetooth oculte ou falsifique sua Classe de Dispositivo (COD), o Controle de Dispositivos poderá funcionar incorretamente.

- Em computadores com Windows 7 ou Windows 8 com certos drivers do adaptador Realtek Bluetooth, talvez não seja possível permitir apenas a conexão com os dispositivos Bluetooth como dispositivos de entrada (classe HID). Ou seja, caso o acesso aos dispositivos Bluetooth seja impedido nas configurações do aplicativo e os dispositivos de entrada sejam adicionados nas exclusões, o Controle de Dispositivos poderá evitar o acesso a todos os dispositivos Bluetooth.

Controle da Web

- Não há suporte para os formatos OGV e WEBM.

- Não há suporte para o protocolo RTMP.

- O Controle da Web é compatível apenas com WSL1. O aplicativo não controla o tráfego WSL2.

Controle Adaptativo de Anomalias

- Recomenda-se criar exclusões automaticamente com base no evento. Ao adicionar manualmente uma exclusão, adicione o caractere `*` ao início do caminho ao especificar o objeto de destino.

- O **Relatório sobre regras de Controle Adaptativo de Anomalias acionadas** não pode ser gerado se a amostra incluir até mesmo um evento cujo nome contenha mais de 260 caracteres.

- Não há suporte para a adição de exclusões ao repositório de Disparo de Regras do Controle Adaptativo de Anomalias se as propriedades de um objeto ou processo tiverem um valor com mais de 256 caracteres (por exemplo, o caminho para o objeto-alvo). É possível adicionar manualmente uma exclusão às configurações da Política. Também é possível adicionar uma exclusão ao Relatório de Regras de Controle Adaptativo de Anomalias disparadas.

- O Kaspersky Security Center 15.1 não pode gerar um relatório **Relatório sobre o estado das regras de Controle Adaptativo de Anomalias** para uma regra específica.

- As regras de Controle Adaptativo de Anomalias estão disponíveis somente no idioma correspondente ao idioma de instalação do plug-in da web. Se você alterar o idioma da interface, a Web Console exibirá uma lista de regras vazia. Para acessar as regras, altere novamente o idioma da interface para o idioma de instalação do plug-in da web.

Criptografia de drive (FDE)

- O Kaspersky Disk Encryption não é compatível com computadores baseados em Arm.

- A criptografia de unidade de disco BitLocker não é compatível com computadores que executam o Windows Home.

- Com a Criptografia de Unidade de Disco BitLocker, o usuário pode alterar manualmente a senha de autenticação usando a API do Windows. Nesses casos, o BitLocker ignora os requisitos de senha definidos na política do Kaspersky Endpoint Security. Em outras palavras, o usuário pode definir qualquer senha que desejar.

- Depois de instalar o aplicativo, você deve reiniciar o sistema operacional para que a criptografia do disco rígido funcione corretamente.

- O Agente de Autenticação não é compatível com hieróglifos ou os caracteres especiais `|` e `\`.

- Para obter o desempenho ideal do computador após a criptografia, é necessário que o processador seja compatível com o conjunto de instruções AES-NI (Intel Advanced Encryption Standard New Instructions). Se o processador não for compatível com AES-NI, o desempenho do computador pode diminuir.

- Quando há processos que tentam acessar dispositivos criptografados antes que o aplicativo conceda acesso a tais dispositivos, o aplicativo mostra um aviso informando que tais processos devem ser encerrados. Se os processos não puderem ser encerrados, reconecte os dispositivos criptografados.

- Os IDs exclusivos dos discos rígidos são exibidos nas estatísticas de criptografia do dispositivo em formato invertido.

- Não é recomendado formatar dispositivos enquanto eles estão sendo criptografados.

- Quando várias unidades removíveis são conectadas simultaneamente a um computador, a política de criptografia pode ser aplicada a apenas uma unidade removível. Quando os dispositivos removíveis são reconectados, a política de criptografia é aplicada corretamente.

- A criptografia pode falhar ao iniciar em um disco rígido altamente fragmentado. Desfragmente o disco rígido.

- Quando os discos rígidos são criptografados, a hibernação é bloqueada desde o momento em que a tarefa de criptografia é iniciada até a primeira reinicialização de um computador executando o Microsoft Windows 7/8/8.1/10, e após a instalação da criptografia do disco rígido até a primeira reinicialização dos sistemas operacionais Microsoft Windows 8/8.1/10. Quando os discos rígidos são descriptografados, a hibernação é bloqueada desde o momento em que a unidade de inicialização é totalmente descriptografada até a primeira reinicialização do sistema operacional. Quando a opção Início Rápido está habilitada no Microsoft Windows 8/8.1/10, o bloqueio da hibernação impede que você desligue o sistema operacional.

- Os computadores com Windows 7 não permitem a alteração da senha durante a recuperação quando o disco é criptografado com a tecnologia BitLocker. Depois que a chave de recuperação for inserida e o sistema operacional for carregado, o Kaspersky Endpoint Security não solicitará a alteração da senha ou do código PIN pelo usuário. Assim, é impossível definir uma nova senha ou um código PIN. Esse problema é derivado das peculiaridades do sistema operacional. Para continuar, é necessário criptografar novamente o disco rígido.

- Não é recomendado usar a ferramenta xbootmgr.exe com provedores adicionais ativados. Por exemplo, Expedidores, Rede ou Drivers.

- Não há suporte para a formatação de uma unidade removível criptografada em um computador com o Kaspersky Endpoint Security for Windows instalado.

- Não há suporte para a formatação de uma unidade removível criptografada com o sistema de arquivos FAT32 (a unidade é exibida como criptografada). Para formatar uma unidade, reformate-a para o sistema de arquivos NTFS.

- Vários agentes de download não podem coexistir em um computador criptografado.

- Uma tentativa de restaurar uma imagem de um disco GPT executável em um estado não criptografado, o sistema operacional pode torná-lo inoperável. Para evitar isso, siga estas recomendações:

  - Descriptografe totalmente o disco antes de restaurar a imagem do backup.

  - Use a cópia setor a setor ao criar a imagem.

  - Exclua os dados dos primeiros setores do disco criptografado antes de restaurar a imagem e reinicialize o disco.

- É impossível acessar uma unidade removível que foi criptografada anteriormente em um computador diferente quando todas as seguintes condições são atendidas simultaneamente:

  - Não há conexão com o servidor do Kaspersky Security Center.

  - O usuário está tentando autorização com um novo token ou senha.

  Se ocorrer uma situação semelhante, reinicie o computador. Depois que o computador for reiniciado, o acesso à unidade removível criptografada será concedido.

- A descoberta de dispositivos USB pelo Agente de Autenticação pode não ser suportada quando o modo xHCI para USB está habilitado nas configurações do BIOS.

- O Kaspersky Disk Encryption (FDE) para a parte SSD de um dispositivo usado para armazenar em cache os dados usados com mais frequência não é compatível com dispositivos SSHD.

- Não há suporte para a criptografia de discos rígidos em sistemas operacionais Microsoft Windows 8/8.1/10 de 32 bits em execução no modo UEFI.

- Reinicie o computador antes de criptografar um disco rígido descriptografado.

- A criptografia do disco rígido não é compatível com o Kaspersky Anti-Virus para UEFI. Não é recomendado usar criptografia de disco rígido em computadores que tenham o Kaspersky Anti-Virus para UEFI instalado.

- A criação de contas do Agente de autenticação com base em contas da Microsoft possui suporte, considerando as seguintes limitações:

  - Não há suporte para a tecnologia de Login único.

  - Não há suporte para a criação automática de contas do Agente de autenticação se a opção de criar contas para usuários que efetuaram login no sistema nos últimos N dias for selecionada.

- Se o nome de uma conta do Agente de Autenticação tiver o formato `<domain>/<Windows account name>`, depois de alterar o nome do computador, você também precisará alterar os nomes das contas que foram criadas para usuários locais deste computador. Por exemplo, imagine que haja um usuário local `Ivanov` no computador `Ivanov` e uma conta do Agente de autenticação com o nome `Ivanov/Ivanov` tenha sido criada para esse usuário. Se o nome do computador `Ivanov` tiver sido alterado para `Ivanov-PC`, você precisará alterar o nome da conta do Agente de Autenticação para o usuário `Ivanov` de `Ivanov/Ivanov` para `Ivanov-PC/Ivanov`. É possível mudar o nome da conta usando a tarefa de gerenciamento de conta local do Agente de Autenticação. Antes que o nome da conta seja alterado, é possível fazer a autenticação no ambiente de pré-inicialização usando o nome antigo (por exemplo, `Ivanov/Ivanov`).

- Se um usuário tiver permissão para acessar um computador que foi criptografado com a tecnologia Kaspersky Disk Encryption usando apenas um token e ele precisar concluir o procedimento de recuperação de acesso, certifique-se de que esse usuário tenha acesso com base em senha a este computador após o acesso ao computador criptografado ter sido restaurado. A senha que o usuário definiu ao restaurar o acesso pode não ser salva. Nesse caso, o usuário terá que concluir o procedimento para restaurar o acesso ao computador criptografado novamente na próxima vez que o computador for reiniciado.

- Ao descriptografar uma unidade de disco rígido usando a Ferramenta de recuperação FDE, o processo de descriptografia pode terminar com um erro se os dados no dispositivo de origem forem substituídos pelos dados descriptografados. Parte dos dados do disco rígido permanecerão criptografados. Recomenda-se escolher a opção de salvar os dados descriptografados em um arquivo nas configurações de descriptografia do dispositivo ao usar a Ferramenta de recuperação FDE.

- Se a senha do Agente de autenticação foi alterada, uma mensagem com o texto *Sua senha foi alterada com êxito. Clique em OK* aparece, porém se o usuário reiniciar o computador, a nova senha não será salva. A senha antiga deve ser usada para autenticação subsequente no ambiente de pré-inicialização.

- A criptografia de disco é incompatível com a tecnologia Intel Rapid Start.

- A criptografia de disco é incompatível com a tecnologia ExpressCache.

- Em alguns casos, ao tentar descriptografar uma unidade criptografada usando a Ferramenta de recuperação FDE, a ferramenta detecta erroneamente o status do dispositivo como "não criptografado" após a conclusão do procedimento de "Solicitação-Resposta". O log da ferramenta mostra um evento informando que o dispositivo foi descriptografado com êxito. Nesse caso, é necessário reiniciar o procedimento de recuperação de dados para descriptografar o dispositivo.

- Depois que o plug-in do Kaspersky Endpoint Security for Windows é atualizado no Web Console, as propriedades do computador cliente não mostram a chave de recuperação do BitLocker até que o serviço do Web Console seja reiniciado.

- Para ver as outras limitações do suporte de criptografia completa de disco e uma lista de dispositivos para os quais a criptografia de discos rígidos possui suporte, mas com restrições, consulte a Base de Dados de Conhecimento do Suporte Técnico.

Criptografia em Nível de Arquivo (FLE)

- A criptografia de arquivos não é compatível com computadores baseados em Arm.
- A criptografia de arquivos e pastas não é compatível com os sistemas operacionais Microsoft Windows Embedded.
- Após instalar o aplicativo, reinicie o sistema operacional para que a criptografia de arquivos e pastas funcione corretamente.
- O aplicativo é compatível com criptografia de arquivos apenas em dispositivos que tenham sistemas de arquivos NTFS e FAT32. Se um arquivo criptografado for transferido para um dispositivo com um sistema de arquivos não compatível (por exemplo, exFAT), o arquivo nesse dispositivo não será criptografado e pode ser modificado.
- Se um arquivo criptografado for armazenado em um computador que tenha funcionalidade de criptografia disponível e você acessar o arquivo de um computador onde a criptografia não está disponível, será fornecido acesso direto a esse arquivo. Um arquivo criptografado armazenado em uma pasta de rede em um computador que possui funcionalidade de criptografia disponível é copiado de forma descriptografada para um computador que não possui funcionalidade de criptografia disponível.
- É aconselhável descriptografar os arquivos que foram criptografados com o Encrypting File System antes de criptografar os arquivos com o Kaspersky Endpoint Security for Windows.
- Depois que um arquivo é criptografado, seu tamanho aumenta em 4 KB.
- Depois que um arquivo é criptografado, o atributo *Arquivo compactado* é definido nas propriedades do arquivo.
- Ao copiar o arquivo descriptografado para uma mídia removível, por exemplo, o arquivo pode permanecer criptografado. Isso pode ocorrer porque, quando o gerenciador de arquivos (como o explorer.exe) tenta acessar o arquivo criptografado, ele armazena o hash do arquivo em uma lista especial do processo. Depois de descriptografar o arquivo, quando o gerenciador de arquivos tenta obter acesso ao arquivo, o processo procura o hash do arquivo na lista. Se o hash for encontrado, o Kaspersky Endpoint Security mantém o arquivo criptografado. Para evitar isso, é necessário limpar a lista do processo. O sistema operacional limpa automaticamente a lista do processo conforme ela é preenchida. É possível esvaziar manualmente a lista. Para isso, você pode reiniciar o computador, reiniciar o processo utilizado para acessar o arquivo (como o explorer.exe) ou usar um gerenciador de arquivos diferente que ainda não tenha sido utilizado para abrir o arquivo criptografado.
- Se um arquivo descompactado de um arquivo criptografado tiver o mesmo nome de um arquivo já existente em seu computador, o último será sobrescrito pelo novo arquivo que foi descompactado de um arquivo criptografado. O usuário não é notificado sobre a operação de substituição.
- Antes de descompactar um arquivo criptografado, certifique-se de que há espaço livre em disco suficiente para acomodar os arquivos descompactados. Caso não tenha espaço em disco suficiente, a descompactação do arquivo poderá ser concluída, mas os arquivos poderão estar corrompidos. Neste caso, é possível que o Kaspersky Endpoint Security não exiba nenhuma mensagem de erro.
- A interface do Gerenciador de Arquivos Portátil não exibe mensagens sobre erros que ocorrem durante sua operação.
- O Kaspersky Endpoint Security for Windows não inicia o Gerenciador de Arquivos Portátil em um computador que tenha o componente Criptografia em Nível de Arquivo instalado.

- Não é possível usar o gerenciador de arquivos portátil para acessar uma unidade removível caso as seguintes condições sejam simultaneamente verdadeiras:

  - Não há conexão com o Kaspersky Security Center.

  - O Kaspersky Endpoint Security for Windows está instalado no computador.

  - A criptografia de dados (FDE ou FLE) não foi executada no computador.

  O acesso não é possível mesmo se o usuário souber a senha do gerenciador de arquivos portátil.

- Quando a criptografia de arquivo é usada, o aplicativo é incompatível com o programa de e-mail Sylpheed.

- O Kaspersky Endpoint Security for Windows não é compatível com as regras de restrição de acesso a arquivos criptografados para alguns aplicativos. Isso porque algumas operações de arquivos são realizadas por um aplicativo terceiro. Por exemplo, a cópia de arquivos é realizada pelo gerenciador de arquivos, não pelo próprio aplicativo. Assim, se o acesso a arquivos criptografados for negado ao cliente de e-mail do Outlook, o Kaspersky Endpoint Security vai permitir que o cliente de e-mail acesse o arquivo criptografado se o usuário tiver copiado os arquivos para a mensagem por meio da área de transferência ou usando a função arrastar e soltar. A operação de cópia foi realizada por um gerenciador de arquivos, para o qual as regras de restrição de acesso a arquivos criptografados não foram especificadas, ou seja, o acesso é permitido.

- Quando as unidades removíveis são criptografadas com suporte ao modo portátil, o controle de idade da senha não pode ser desabilitado.

- Não é possível alterar as configurações do arquivo de paginação. O sistema operacional usa os valores padrão em vez dos valores de parâmetros especificados.

- Use a remoção segura ao trabalhar com unidades removíveis criptografadas. Não podemos garantir a integridade dos dados se a unidade removível não for removida com segurança.

- Depois que os arquivos são criptografados, seus originais não criptografados são excluídos com segurança.

- Não há suporte para a sincronização de arquivos offline usando o Client-Side Caching (CSC). Criptografia de arquivos off-line ou a tecnologia Branch Caching sobre SMB para servidores também não é compatível. Recomenda-se proibir o gerenciamento offline de recursos compartilhados no âmbito de política de grupo. Os arquivos que estão no modo offline podem ser editados. Após a sincronização, as alterações feitas em um arquivo offline podem ser perdidas.

- Não há suporte para a criação de um arquivo compactado criptografado na raiz do disco rígido do sistema.

- Você pode ter problemas ao acessar arquivos criptografados pela rede. É recomendável mover os arquivos para uma fonte diferente ou certificar-se de que o computador que está sendo usado como servidor de arquivos seja gerenciado pelo mesmo Servidor de Administração do Kaspersky Security Center.

- Alterar o layout do teclado pode fazer com que a janela de entrada de senha para um arquivo compactado de extração automática criptografado seja travada. Para resolver o problema, feche a janela de entrada de senha, mude para o layout de teclado padrão em seu sistema operacional e digite novamente a senha do arquivo compactado criptografado.

- Quando a criptografia de arquivo é usada em sistemas que têm várias partições em um disco, é recomendável usar a opção que determina automaticamente o tamanho do arquivo pagefile.sys. Depois que o computador for reiniciado, o arquivo pagefile.sys pode mover-se entre as partições do disco.

- Depois de aplicar as regras de criptografia de arquivo, incluindo os arquivos na pasta *Meus Documentos*, certifique-se de que os usuários para os quais a criptografia foi aplicada possam acessar os arquivos criptografados. Para fazer isso, cada usuário deve entrar no sistema quando uma conexão com o Kaspersky Security Center estiver disponível. Se um usuário tentar acessar arquivos criptografados sem uma conexão com o Kaspersky Security Center, o sistema pode travar.

- Se os arquivos do sistema forem de alguma forma incluídos no escopo da criptografia em nível de arquivo, eventos relacionados a erros ao criptografar esses arquivos podem aparecer nos relatórios. Os arquivos especificados nesses eventos não são realmente criptografados.

- Não há suporte para os processos do Pico.

- Não há suporte para caminhos com distinção entre maiúsculas e minúsculas. Quando regras de criptografia ou regras de descriptografia são aplicadas, os caminhos nos eventos do produto são exibidos em letras minúsculas.

- Não é recomendado criptografar arquivos usados pelo sistema na inicialização. Se esses arquivos estiverem criptografados, uma tentativa de acessar arquivos criptografados sem uma conexão com o Kaspersky Security Center pode fazer com que o sistema trave ou resultar em solicitações de acesso a arquivos não criptografados.

- Se os usuários trabalharem em conjunto com um arquivo na rede sob regras FLE por meio de aplicativos que usam o método de mapeamento de arquivo para memória (como WordPad ou FAR) e aplicativos projetados para trabalhar com arquivos grandes (como Notepad ++), o arquivo na forma não criptografada pode ser bloqueado indefinidamente sem a capacidade de acessá-lo no computador no qual reside.

- O Kaspersky Endpoint Security não criptografa arquivos localizados no armazenamento em nuvem do OneDrive ou em outras pastas que tenham OneDrive como nome. O Kaspersky Endpoint Security também bloqueia a cópia de arquivos criptografados para as pastas do OneDrive caso os arquivos não sejam adicionados à regra de descriptografia.

- Quando o componente Criptografia em Nível de Arquivo é instalado, o gerenciamento de usuários e grupos não funciona no modo WSL (Windows Subsystem for Linux).

- Quando o componente Criptografia em Nível de Arquivo é instalado, não há suporte para a POSIX (Portable Operating System Interface) para renomear e excluir arquivos.

- Não é recomendado criptografar arquivos temporários, pois isso pode causar perda de dados. Por exemplo, o Microsoft Word cria arquivos temporários ao processar um documento. Caso os arquivos temporários sejam criptografados e o arquivo original não for, o usuário poderá receber um erro de *Acesso Negado* ao tentar salvar o documento. Além disso, o Microsoft Word pode salvar o arquivo, mas não será possível abrir o documento na próxima vez, ou seja, os dados serão perdidos. Para evitar a perda de dados, é preciso excluir a pasta de arquivos temporários das regras de criptografia.

Detection and Response (EDR, NDR, MDR, XDR, Sandbox)

- Não é possível verificar um objeto colocado em quarentena como resultado da tarefa *Mover arquivo para a Quarentena*.

- Não é possível colocar em quarentena um Alternate Data Stream (ADS) com mais de 4 MB. O Kaspersky Endpoint Security ignorará as ADS extensas sem notificar o usuário.

- O Kaspersky Endpoint Security não executa as tarefas de *Verificação de IOC* em unidades de rede se o caminho da pasta nas propriedades da tarefa começar com uma letra da unidade. O Kaspersky Endpoint Security é compatível somente com formato de caminho UNC para tarefas de *Verificação de IOC* em unidades de rede. Por exemplo, `\\server\shared_folder`.

- Para garantir que a tarefa *Verificação de IOC* funcione corretamente com o uso dos termos do EmailItem, o plug-in da Web do Kaspersky Endpoint Security deverá ser atualizado para a versão mais recente.

- Em computadores baseados em Arm, a tarefa *Verificação de IOC* é compatível apenas com arquivos de e-mail dos seguintes programas de e-mail: Versões de 32 bits e 64 bits do Outlook 2016 e Outlook 2021, 2024 e 365 para Arm64.

- Uma importação de um arquivo de configuração de aplicativo termina com um erro caso a configuração de integração com o Kaspersky Sandbox esteja ativada no arquivo de configuração. Antes de exportar as configurações do aplicativo, desative o Kaspersky Sandbox. Em seguida, execute o procedimento de exportação/importação. Após importar o arquivo de configuração, ative o Kaspersky Sandbox.

- Ao importar uma política de um arquivo KLP, o valor do parâmetro que determina a aceitação dos termos e condições do Contrato do Kaspersky Detection and Response Expert não é aplicado. Como resultado, após a importação da política, o Kaspersky Endpoint Security não executa as funções do Agente EDR. Para que o Agente EDR funcione, abra a política, altere qualquer parâmetro e salve as configurações da política.

- Quando um indicador de comprometimento for detectado durante a execução da tarefa *Verificação de IOC*, o aplicativo colocará o arquivo em quarentena somente pelo prazo do FileItem. Colocar um arquivo na quarentena para outros prazos não é compatível.

- O plug-in da Web do Kaspersky Endpoint Security for Windows 11.7.0 ou posterior é necessário para gerenciar os detalhes do alerta. Os detalhes de alertas são necessários para funciona com as soluções de Endpoint Detection and Response (EDR Optimum e EDR Expert). Os detalhes de alertas estão disponíveis apenas no Kaspersky Security Center Web Console e no Kaspersky Security Center Cloud Console.

- A migração da configuração [KES+KEA] para a configuração [KES+agente integrado] pode ser concluída com a remoção de erro do aplicativo Kaspersky Endpoint Agent. A remoção de erro do aplicativo foi corrigida na versão mais recente do Kaspersky Endpoint Agent. Para remover o Kaspersky Endpoint Agent, reiniciar o computador e criar uma tarefa de remoção do aplicativo.

- Não há suporte para a configuração [KES+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. Depois de migrar para a configuração do [KES+agente integrado], certifique-se de que o Kaspersky Endpoint Agent tenha sido removido do computador. Se o Kaspersky Endpoint Agent continuar funcionando após a migração, desinstale o aplicativo manualmente (por exemplo, usando a tarefa *Desinstalar aplicativo remotamente*).

  O instalador permite implementar o Kaspersky Endpoint Agent em um computador com o Kaspersky Endpoint 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 Endpoint Security e do Kaspersky Endpoint Agent.

- Ao gerar detalhes do alerta, o aplicativo fornece informações sobre a ameaça detectada, incluindo hashes de arquivos modificados. O Kaspersky Endpoint Security calcula o hash do arquivo ao gerar detalhes do alerta. Considere que o hash original do arquivo quando o evento de modificação de arquivo foi gerado pode não ser o mesmo hash calculado quando os detalhes do alerta foram gerados.

- O agente integrado, EDR (KATA), reinicia o isolamento de rede de um computador após a reinicialização do computador, mesmo que o período de isolamento tenha expirado. Para evitar o isolamento repetido do computador, é necessário desativar o isolamento de rede no console da Kaspersky Anti Targeted Attack Platform.

- Recomendamos atualizar o aplicativo após a conclusão do isolamento de rede. Depois de atualizar o Kaspersky Endpoint Security, o isolamento de rede pode ser interrompido.

- Os agentes integrados para EDR (KATA), EDR Optimum e EDR Expert não são compatíveis entre si. Portanto, a ativação do agente integrado EDR com uma licença Kaspersky Endpoint Detection and Response Add-on independente pode ser ignorada caso o Kaspersky Endpoint Security tenha sido ativado com funcionalidade EDR diferente. Por exemplo, a ativação do agente integrado EDR (KATA) com uma licença independente é ignorada caso o Kaspersky Endpoint Security tenha sido instalado com a licença [KES+EDR Optimum].

- No Kaspersky Endpoint Security versão 12.1, o EDR (KATA) Agent integrado do não é compatível com os seguintes metarquivos da tarefa *Obter metarquivos NTFS*: $Secure:$SDH:$INDEX_ROOT; $Secure:$SDH:$INDEX_ALLOCATION; $Secure:$SDH:$BITMAP; $Secure:$SII:$INDEX_ROOT; $Secure:$SII:$INDEX_ALLOCATION; $Secure:$SII:$BITMAP; $Extend\$UsnJrnl:$J:$DATA; $Extend\$UsnJrnl:$Max:$DATA. O suporte para esses metarquivos foi adicionado ao Kaspersky Endpoint Security versão 12.2.

- Ao migrar do Kaspersky Endpoint Agent para Kaspersky Endpoint Security para a solução Kaspersky Anti Targeted Attack Platform (EDR), pode haver alguns erros ao conectar o computador com os servidores do Central Node. Isso acontece porque o assistente de migração no Web Console ignora as seguintes configurações da política e não as migra:

  - Proibição de modificação de configurações **Configurações de conexão** ("bloqueado").

    Por padrão, as configurações podem ser modificadas (o "cadeado" está aberto). Portanto, as configurações não são aplicadas no computador. É necessário proibir as modificação das configurações e fechar o "cadeado".

  - Crypto-contêiner.

    Caso a autenticação de duas vias seja usada para conexão com os servidores do Central Node, é necessário adicionar novamente o crypto-contêiner. O assistente de migração migra corretamente o certificado TLS do servidor.

  O assistente de migração de tarefas e políticas no Console de Administração (MMC) migra todas as configurações para a solução Kaspersky Anti Targeted Attack Platform (EDR).

- O status de ativação do aplicativo é exibido incorretamente quando o aplicativo é instalado no modo do Endpoint Detection and Response Agent para oferecer suporte à solução Kaspersky Managed Detection and Response sem conexão com o Kaspersky Security Center. Após o download do arquivo BLOB, a área de notificação da barra de tarefas do Windows exibe um status incorreto: *O aplicativo não está ativado*. No entanto, a interface do aplicativo exibe o status de ativação corretamente. Reinicie o computador para que o aplicativo funcione corretamente.

- O Kaspersky Endpoint Security permite a integração com a solução Kaspersky Anti Targeted Attack Platform ao usar o componente EDR (KATA) ou o Endpoint Sensor (sem suporte). Observe que só é possível usar um dos componentes para interagir com a Kaspersky Anti Targeted Attack Platform. Para exibir o status do componente, abra as propriedades do computador no Console de Administração (MMC), na seção **Aplicativos**, abra as propriedades do Kaspersky Endpoint Security for Windows e vá para a seção **Componentes**. As seguintes considerações especiais valem para a exibição do status do componente para a interação com a Kaspersky Anti Targeted Attack Platform:

  - Para o plug-in de gerenciamento 12.0 e versões anteriores, o aplicativo exibe o status atual de **Endpoint Sensor**. No Kaspersky Endpoint Security 12.0 e versões anteriores, o componente EDR (KATA) não está disponível. O componente EDR (KATA) foi introduzido na versão 12.1.

  - Para o plug-in de gerenciamento 12.1 e versões posteriores, o aplicativo exibe o status geral do **Endpoint Detection and Response (KATA)** que pode significar o status do Endpoint Sensor ou o status do componente EDR (KATA). Isso depende da versão do aplicativo instalado no computador do usuário e dos componentes disponíveis que podem ser usados para interagir com a Kaspersky Anti Targeted Attack Platform.

- Iniciando com o Kaspersky Endpoint Security versão 12.6 e posterior, o Kaspersky Security Center Web Console versão 14.2 e anterior não exibem corretamente o nome do componente **Endpoint Detection and Response (KATA)** nas propriedades do computador. Em vez do componente **Endpoint Detection and Response (KATA)**, o aplicativo exibe o nome do componente **Endpoint Detection and Response Expert (KATA EDR)**. Para exibir a lista de componentes, abra as propriedades do computador no Web Console, na seção **Aplicativos**, abra as propriedades do Kaspersky Endpoint Security for Windows e vá para a seção **Componentes**. Iniciando com o Kaspersky Security Center Web Console versão 15.1 e posterior, o aplicativo exibe corretamente o nome do componente.

- Ao atualizar o plug-in de gerenciamento do Kaspersky Endpoint Detection and Response para a versão 15.3 instalada no Web Console versões 14.0–14.2, os detalhes do alerta não são exibidos corretamente. Para que os detalhes do alerta funcionem de forma correta, reinicie o Servidor de Administração do Kaspersky Security Center.

- O plug-in de gerenciamento do Kaspersky Endpoint Detection and Response versão 15.4 e posteriores não é compatível com a versão 14.0 do Kaspersky Security Center. Depois de atualizar o plug-in de gerenciamento, os detalhes do alerta não são exibidos corretamente.

- As soluções da classe Kaspersky Extended Detection and Response (XDR) versão 1.4 não são compatíveis com o plug-in da Web do Kaspersky Endpoint Security for Windows versão 12.12 ou superior. Você pode manter a versão atual do plug-in da Web ou atualizar a solução XDR para a versão 2.0 ou superior.

- O Kaspersky Endpoint Security não envia objetos destinados à arquitetura Arm para o Kaspersky Sandbox.

- O Kaspersky Endpoint Security é compatível com até 10.000 regras de filtragem de eventos de inclusão e exclusão do EDR Expert (on-premises) no total.

- As regras de filtragem de eventos do EDR Expert (on-premises) não serão transmitidas da política para dispositivos gerenciados que executam o Kaspersky Endpoint Security versão 14.0 ou anterior se o limite compatível de regras de filtragem armazenadas for excedido. O aplicativo exibirá um aviso correspondente.

- As versões 12.11–14.1 do Kaspersky Endpoint Security for Windows não oferecem suporte aos seguintes eventos de telemetria do EDR Expert (local):

  - LDAP Attribute Change
  - GPO Change
  - SCCM Local Config Mismatch
  - SCCM Config Change
  - SCCM Deployment Task
  - Smb Connection Open

  A partir da versão 14.2, o Kaspersky Endpoint Security oferece suporte a todos esses eventos de telemetria do EDR Expert (local), exceto LDAP Attribute Change.

Outras limitações

- Os sistemas operacionais Windows, a partir da versão 11 24H2, são compatíveis com a tecnologia UDP Receive Segment Coalescing Offload (URO). A tecnologia é ativada por padrão se uma placa de rede e drivers compatíveis estiverem instalados no computador. Desativar o URO no computador de um usuário pode reduzir significativamente o desempenho do aplicativo.

- O Kaspersky Endpoint Security é compatível com o subsistema WSL (Windows Subsystem for Linux) com restrições:

  - WSL 1. O aplicativo monitora o tráfego de rede e detecta ameaças via HTTP/HTTPS. Devido ao fato de que o Kaspersky Endpoint Security usa seu próprio certificado para verificar conexões HTTPS seguras, a operação de alguns aplicativos de terceiros pode ser interrompida.

  - WSL 2. O aplicativo não é compatível com WSL 2.

- Se o aplicativo retornar um erro ou travar durante a operação, ele poderá ser reiniciado automaticamente. Se o aplicativo encontrar erros recorrentes que fazem com que o aplicativo trave, o aplicativo executa as seguintes operações:

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

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

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

- Os endereços da Web adicionados à lista confiável podem ser processados incorretamente.

- No console do Kaspersky Security Center, não é possível salvar um arquivo no disco pela pasta **Avançado** → **Repositórios** → **Ameaças ativas**. Para salvar o arquivo, é preciso desinfectar o arquivo infectado. Ao desinfectá-lo, o aplicativo salvará uma cópia do arquivo no Backup. Agora, é possível salvar o arquivo no disco pela pasta **Avançado** → **Repositórios** → **Backup**.

- A herança das configurações de transferência de dados para o Servidor de Administração (**Configurações gerais** → **Relatórios e Armazenamento** → **Transferência de dados para o Servidor de Administração**) difere da herança de outras configurações. Caso tenha permitido a alteração das configurações de transmissão de dados na política (o "cadeado" está aberto), essas configurações serão redefinidas para os valores padrão nas propriedades do computador local no console, caso não tenham sido definidas anteriormente. Caso essas configurações tenham sido definidas anteriormente, seus valores serão restaurados. Ao excluir uma política, as configurações serão herdadas da mesma forma. Nesses casos, outras configurações nas propriedades do computador local serão herdadas da política.

- O Kaspersky Endpoint Security monitora o tráfego HTTP que está em conformidade com as normas RFC 2616, RFC 7540, RFC 7541, RFC 7301. Se o Kaspersky Endpoint Security detectar outro formato de troca de dados no tráfego HTTP, o aplicativo bloqueará essa conexão para prevenir o download de arquivos maliciosos da Internet.

- O Kaspersky Endpoint Security previne a comunicação sobre o protocolo QUIC. Os navegadores usam o protocolo de transporte padrão (TLS ou SSL) independentemente se o suporte QUIC estiver ativado no navegador ou não.

- Podem ocorrer erros de conexão TLS quando o software de terceiros funciona com a biblioteca Libcurl. Isso pode estar relacionado ao certificado Kaspersky que o Kaspersky Endpoint Security usa para verificar conexões criptografadas. Para continuar a operação, é possível desabilitar a validação de certificado para software de terceiros (não recomendado) ou adicionar um corpo de certificados Kaspersky ao armazenamento de certificados cURL. Para obter informações detalhadas, consulte a Base de conhecimento da Kaspersky.

- Quando o Kaspersky Endpoint Security for Windows é iniciado pela primeira vez, um aplicativo assinado digitalmente pode ser colocado temporariamente no grupo errado. O aplicativo assinado digitalmente será posteriormente colocado no grupo correto.

- Durante uma nova verificação de um objeto malicioso que foi bloqueado por um software de terceiros, o usuário não é notificado quando a ameaça é detectada novamente. O evento de nova detecção de ameaça é exibido no relatório do aplicativo e no relatório do Kaspersky Security Center.

- O relatório do Kaspersky Security Center sobre a criptografia de dispositivo não incluirá informações sobre os dispositivos criptografados por meio do Microsoft BitLocker em plataformas de servidor ou em estações de trabalho nas quais o componente Controle de Dispositivos não está instalado.

- Não é possível ativar a exibição de todas as entradas de relatório no Kaspersky Security Center Web Console. No Web Console, é possível alterar somente o número de entradas exibido nos relatórios. Por padrão, o Kaspersky Security Center Web Console exibe 1000 entradas de relatório. É possível ativar a exibição de todas as entradas de relatório no Console de Administração (MMC).

- Não é possível definir a exibição de mais de 1000 entradas de relatório no Kaspersky Security Center Console. Se for definido um valor maior do que 1000, o Kaspersky Security Center Console exibirá somente 1000 entradas de relatório.

- Ao usar uma hierarquia de política, as configurações da seção Criptografia de unidades removíveis em uma política filho estão acessíveis para edição se a política pai proibir a modificação dessas configurações.

- Você deve ativar o Logon de Auditoria nas configurações do sistema operacional para garantir o funcionamento adequado das exclusões para a proteção de pastas compartilhadas contra criptografia externa.

- Se a proteção de pasta compartilhada estiver ativada, o Kaspersky Endpoint Security for Windows monitora as tentativas de criptografar as pastas compartilhadas para cada sessão de acesso remoto iniciada antes da inicialização do Kaspersky Endpoint Security for Windows, mesmo se o computador a partir do qual a sessão de acesso remoto foi iniciada foi adicionado às exclusões. Se você não quiser que o Kaspersky Endpoint Security for Windows monitore as tentativas de criptografar pastas compartilhadas para sessões de acesso remoto iniciadas em um computador adicionado às exclusões e iniciado antes da inicialização do Kaspersky Endpoint Security for Windows, encerre e restabeleça a sessão de acesso remoto ou reinicie o computador no qual o Kaspersky Endpoint Security for Windows está instalado.

- Se a tarefa de atualização for executada com as permissões de uma conta de usuário específica, os patches do produto não serão baixados durante a atualização de uma fonte que requer autorização.

- O aplicativo pode falhar ao iniciar devido ao desempenho insuficiente do sistema. Para resolver esse problema, use a opção Ready Boot ou aumente o tempo limite do sistema operacional para iniciar os serviços.

- O aplicativo não pode funcionar no Safe Mode do Windows.

- Não podemos garantir que o Controle de áudio funcionará até depois da primeira reinicialização após a instalação do aplicativo.

- No Console de Administração (MMC), nas configurações de Prevenção de intrusão na janela de configuração de permissões do aplicativo, o botão **Remover** está indisponível. É possível remover um aplicativo de um grupo de confiança por meio do menu de contexto do aplicativo.

- Na interface local do aplicativo, nas configurações de Prevenção de intrusão, as permissões do aplicativo e os recursos protegidos não estarão disponíveis para visualização se o computador estiver sendo gerenciado por uma política. Rolar, pesquisar, filtrar e outros controles de janela estarão indisponíveis. É possível visualizar as permissões do aplicativo nas propriedades da política no Kaspersky Security Center Console.

- Quando os arquivos de rastreamento rotacionados são ativados, nenhum rastro é criado para o componente AMSI e o plug-in do Outlook.

- Os rastros de desempenho não podem ser coletados manualmente no Windows Server 2008.

- Não há suporte para os rastros de desempenho para o tipo de rastro "Reiniciar".

- O registro de dump não é compatível com processos do Pico.

- Desativar a opção **Desativar o gerenciamento externo de serviços do sistema** permitirá que você interrompa o serviço do aplicativo que foi instalado com o parâmetro `AMPPL=1` (por padrão, o valor do parâmetro é definido como `1` iniciando com a versão do sistema operacional Windows 10RS2). O parâmetro `AMPPL` com valor `1` permite o uso da tecnologia de Processos de Proteção para o serviço do produto.

- Para executar uma verificação personalizada de uma pasta, o usuário que inicia a verificação personalizada deve ter permissões para ler os atributos dessa pasta. Caso contrário, a verificação da pasta personalizada será impossível e terminará com um erro.

- Quando uma regra de verificação definida em uma política inclui um caminho sem o caractere `\` no final, por exemplo, `C:\folder1\folder2`, a verificação é executada para o caminho `C:\folder1\`.

- Se você estiver usando as políticas de restrição de software (Software Restriction Policies, SRP), o computador pode falhar durante o carregamento (tela escura). Para evitar problemas, é necessário permitir o uso de bibliotecas de aplicativos nas propriedades das SRP. Nas propriedades das SRP, adicione a regra com nível de segurança **Irrestrito** para o arquivo khkum.dll (item do menu **Nova Regra de Hash**). O arquivo está localizado na pasta `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.2\klhk\klhk_x64\`. Se tiver optado por usar esse método, será preciso, ainda, limpar a caixa de seleção **Baixar atualizações dos módulos do aplicativo** nas configurações da tarefa *Atualização* do Kaspersky Endpoint Security. Para obter detalhes sobre o uso das SRP, consulte a documentação da Microsoft.

  Também é possível desabilitar as SRP e usar o componente Controle de Aplicativos do Kaspersky Endpoint Security para controlar o uso de aplicativos.

- Caso o computador pertença a um domínio no Windows Group Policy Object (Group Policy Object, GPO) com o parâmetro DriverLoadPolicy definido como 8 (Good only), reiniciar o computador com o Kaspersky Endpoint Security instalado causa um BSOD. Para evitar a falha, o parâmetroEarly Launch Antimalware (ELAM) na Política do Grupo deve estar definido como 1 (Good and unknown). As configurações ELAM estão localizadas na política em: **Computer Configuration** → **Administrative Templates** → **System** → **Early Launch Antimalware**.

- Não há suporte para o gerenciamento das configurações do plug-in do Outlook por meio da API Rest.

- As configurações de execução de tarefas para um usuário específico não podem ser transferidas entre dispositivos por meio de um arquivo de configuração. Depois que as configurações forem aplicadas a partir de um arquivo de configuração, especifique manualmente o nome de usuário e a senha.

- Depois de instalar uma atualização, a tarefa de verificação de integridade não funciona até que o sistema seja reiniciado para aplicar a atualização.

- Quando o nível de rastreamento rotacionado é alterado por meio do utilitário de diagnóstico remoto, o Kaspersky Endpoint Security for Windows exibe incorretamente um valor em branco para o nível de rastreamento. No entanto, os arquivos de rastreamento são gravados de acordo com o nível de rastreamento correto. Quando o nível de rastreamento rotacionado é alterado por meio da interface local do aplicativo, o nível de rastreamento é modificado corretamente, mas o utilitário de diagnóstico remoto exibe incorretamente o nível de rastreamento definido pela última vez pelo utilitário. Isso pode fazer com que o administrador não tenha informações atualizadas sobre o nível de rastreamento atual e as informações relevantes podem estar ausentes caso um usuário altere manualmente o nível de rastreamento na interface local do aplicativo.

- Na interface local, as configurações de Proteção por senha não permitem alterar o nome da conta do administrador (KLAdmin por padrão). Para alterar o nome da conta do administrador, é necessário desativar a proteção por senha e, em seguida, ativar a Proteção por senha e especificar um novo nome para a conta do administrador.

- O aplicativo Kaspersky Endpoint Security é compatível com o Docker quando instalado em um servidor Windows Server 2019. A implementação dos contêineres em um computador com o Kaspersky Endpoint Security provoca uma falha fatal (BSOD).

- Caso o Kaspersky Endpoint Security esteja instalado em um servidor do SQL Server DBMS, o aplicativo enviará solicitações para a instância do servidor. Isso é necessário para verificar os trabalhos do Agente SQL Server e impedir a execução de trabalhos maliciosos. O Kaspersky Endpoint Security usa a conta de usuário do SQL Server para verificar trabalhos. O aplicativo envia solicitações ao servidor ao verificar a memória do sistema e após atualizar os bancos de dados de antivírus.

- A compatibilidade do Kaspersky Endpoint Security e do software Secret Net Studio é limitada:

  - O aplicativo Kaspersky Endpoint Security não é compatível com o componente Antivírus do software Secret Net Studio.

    O aplicativo não pode ser instalado em um computador onde o Secret Net Studio estiver implementado com o componente Antivírus. Para possibilitar a interoperabilidade, é necessário remover o componente Antivírus do Secret Net Studio.

  - O aplicativo Kaspersky Endpoint Security não é compatível com o componente de Proteção de disco e criptografia de dados do software Secret Net Studio.

    O aplicativo não pode ser instalado em um computador em que o Secret Net Studio estiver implementado com o componente de Proteção de disco e criptografia de dados. Para possibilitar a interoperabilidade, é preciso remover componente de Proteção de disco e criptografia de dados do Secret Net Studio.

  - O Secret Net Studio não é compatível com o componente de Criptografia em Nível de Arquivo (FLE) do Kaspersky Endpoint Security.

    Ao instalar o Kaspersky Endpoint Security com o componente Criptografia em Nível de Arquivo (FLE), o Secret Net Studio pode operar com erros. Para garantir a interoperabilidade, é necessário remover o componente Criptografia em Nível de Arquivo (FLE) do Kaspersky Endpoint Security.

- Ao importar as regras do Monitor de integridade do sistema, o aplicativo verifica o ID e o nome da regra. Caso os IDs das regras sejam iguais, o Kaspersky Endpoint Security substituirá as regras existentes pela nova regra. Ao exportar as regras, o aplicativo atribui IDs automaticamente. Regras com IDs idênticos podem existir, por exemplo, caso tenha editado manualmente os arquivos XML da regra exportada. Caso os IDs da regra sejam exclusivos, mas os nomes das regras forem iguais, o Kaspersky Endpoint Security adiciona `(1)` ao nome da regra, e assim sucessivamente.

- A partir da versão 12.11 do Kaspersky Endpoint Security for Windows, não é mais possível visualizar as configurações de uma política pai a partir de um grupo filho no Console Web. O Web Console também exibe um aviso: *Esta política foi herdada. Você pode editar as configurações da política somente no grupo de administração em que foi criada*.

- Notificações em pop-up com mais de 256 caracteres não são exibidas no Console de Administração (MMC).

- Os nomes dos componentes na política e no pacote de instalação talvez sejam diferentes. Por exemplo, o Endpoint Detection and Response Expert (on-premises) pode ser nomeado Endpoint Detection and Response (KATA), Endpoint Detection and Response Expert (on-premises) ou Kaspersky Anti Targeted Attack Platform Integration. Os nomes dos componentes também podem diferir dependendo da versão do aplicativo.

Glossário

Agente de Autenticação

Interface que permite concluir a autenticação para acessar discos rígidos criptografados e carregar o sistema operacional após a criptografia do disco rígido.

Agente de Rede

Um componente do Kaspersky Security Center que permite a interação entre o Servidor de Administração e os aplicativos da Kaspersky que estão instalados em um nó de rede específico (estação de trabalho ou servidor). Este componente é característico para todos os aplicativos da Kaspersky que executam no Windows. As versões dedicadas do Agente de Rede são destinadas a aplicativos que executam em outros sistemas operacionais.

Alarme falso

O alarme falso ocorre quando o aplicativo da Kaspersky informa que um arquivo não infectado está infectado porque a assinatura do arquivo é similar a do vírus.

Arquivo compactado

Um ou vários arquivos foram compactados em um único arquivo compactado. Um aplicativo especializado chamou um arquivador que é necessário para compactar e descompactar dados.

Arquivo infectado

Arquivo que contém código malicioso (o código de malware conhecido foi detectado durante a verificação do arquivo). A Kaspersky não recomenda a utilização de tais objetos, pois eles podem infectar o computador.

Arquivo infectável

Um arquivo que, devido a sua estrutura ou ao seu formato, pode ser usado por invasores como um "contêiner" para armazenar e difundir um código malicioso. Normalmente, são arquivos executáveis com extensões como .com, .exe e .dll. Existe um risco bastante alto de intrusão de código malicioso nesses arquivos.

Arquivo IOC

Um arquivo que contém um conjunto de indicadores de comprometimento (IOCs) que o aplicativo tenta corresponder para contar uma detecção. A probabilidade de detecção pode ser maior caso as correspondências exatas com vários arquivos IOC sejam encontradas para o objeto como resultado da verificação.

Autenticação Kerberos

Mecanismo de autenticação mútua pelo cliente e pelo servidor antes de estabelecer uma conexão entre eles, o que permite a comunicação por meio de redes inseguras. O mecanismo é baseado em um tíquete que o usuário obtém de um centro de autenticação confiável.

Banco de dados de endereços de phishing

Lista de endereços da web os quais os especialistas da Kaspersky determinaram que estão relacionados com ataques de phishing. O banco de dados é atualizado periodicamente e faz parte do Kit de distribuição do aplicativo da Kaspersky.

Banco de dados de endereços maliciosos

Uma lista de endereços da Web cujo conteúdo pode ser considerado perigoso. Essa lista é criada pelos especialistas da Kaspersky. Ela é atualizada periodicamente, sendo incluída no Kit de distribuição do aplicativo da Kaspersky.

Bancos de dados do Antivírus

Os bancos de dados contêm informações sobre ameaças à segurança do computador conhecidas da Kaspersky na data de publicação do banco de dados de antivírus. As assinaturas de banco de dados de antivírus ajudam a detectar código malicioso em objetos verificados. Os bancos de dados do antivírus são criados pelos peritos da Kaspersky e atualizados a cada hora.

Certificado de licença

Um documento que a Kaspersky transfere para o usuário com o arquivo de chave ou código de ativação. Ele contém informações sobre a licença concedida ao usuário.

Chave ativa

Chave que está atualmente em uso pelo aplicativo.

Cloud Discovery

O Cloud Discovery gerencia o acesso do usuário aos serviços na nuvem. Os serviços na nuvem incluem, por exemplo, o Microsoft Teams, o Salesforce e o Microsoft Office 365. Os serviços na nuvem são agrupados em categorias, por exemplo, *Compartilhamento de arquivos*, *Serviços de mensagens* e *E-mail*.

Desinfecção

Um método de processar objetos infectados que resulta em recuperação total ou parcial de dados. Nem todos os objetos infectados podem ser desinfectados.

Emissor de certificado

O centro de certificado que emitiu o certificado.

Escopo da verificação

Objetos que o Kaspersky Endpoint Security verifica ao executar uma tarefa de verificação.

Escopo de proteção

Objetos que são constantemente verificados pelo componente Proteção Essencial Contra Ameaças ao serem executados. O escopo de proteção de componentes diferentes tem propriedades diversas.

Forma normal de endereço de um recurso da Web

O formato normalizado do endereço de um recurso da web é uma representação textual de um endereço do recurso da web que é obtido por meio da normalização. *Normalização* é o processo no qual a representação textual do endereço de um recurso da Web é alterada segundo regras específicas (por exemplo, exclusão de login, senha do usuário e porta de conexão da representação textual do endereço do recurso da Web; além disso, o endereço do recurso da Web altera os caracteres que estão em maiúsculas para minúsculas).

Para fins da operação dos componentes de proteção, o objetivo da normalização de endereços de recurso da web é evitar a verificação de endereços de sites, que podem diferir em sintaxe, embora sejam fisicamente equivalentes, mais de uma vez.

Exemplo:

Endereço não normalizado: www.Example.com\.

Endereço normalizado: www.example.com\.

Gerenciador de Arquivos Portátil

Este é um aplicativo que fornece uma interface para trabalhar com arquivos criptografados em unidades removíveis quando a funcionalidade de criptografia não está disponível no computador.

Grupo de administração

Um conjunto de computadores que compartilham funções comuns e um conjunto de aplicativos da Kaspersky instalados neles. Os dispositivos são colocados em grupos a fim de que possam ser gerenciados convenientemente como uma única unidade. Um grupo poderá incluir outros grupos. É possível criar políticas de grupo e tarefas de grupo, para cada aplicativo instalado no grupo.

IOC

Indicador de comprometimento. Um conjunto de dados sobre um objeto ou atividade maliciosa.

Light Agent

Componente do Kaspersky Endpoint Security for Virtualization Light Agent. É instalado em cada máquina virtual que precisa ser protegida.

Máscara

Representação de um nome de arquivo e extensão usando curingas.

As máscaras de arquivos podem conter caracteres que são permitidos em nomes de arquivos, incluindo curingas:

- 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. A máscara ** está disponível apenas para a criação de exclusões de verificação.

- `?` (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.

Módulo de plataforma confiável

Um microchip desenvolvido para fornecer funções básicas relacionadas à segurança (por exemplo, para guardar chaves de criptografia). Um Módulo de Plataforma Confiável normalmente é instalado na placa mãe do computador e interage com todos os outros componentes do sistema via barramento de hardware.

Objeto OLE

Um arquivo anexado ou um arquivo que está incorporado em outro arquivo. Os aplicativos Kaspersky permitem a verificação da existência de vírus em objetos OLE. Por exemplo, se você inserir uma tabela do Microsoft Office Excel® em um documento do Microsoft Office Word, a tabela será verificada como um objeto OLE.

OpenIOC

Padrão aberto de descrições de indicador de compromisso (IOC) baseado em XML e incluindo mais de 500 diferentes Indicadores de compromisso.

Servidor de integração

Componente do Kaspersky Endpoint Security for Virtualization Light Agent. Interação entre os componentes do Kaspersky Endpoint Security e a infraestrutura virtual.

SVM

Máquina virtual segura – uma máquina virtual especial na qual o serviço de servidor de verificação (Servidor de proteção, um componente do Kaspersky Endpoint Security for Virtualization Light Agent) está instalado.

Tarefa

Funções executadas pelo aplicativo da Kaspersky como tarefas, por exemplo: Proteção de arquivo em tempo real, Verificação completa do dispositivo, Atualização do banco de dados.

Apêndices

Esta seção contém informações que complementam o corpo do documento.

Apêndice 1. Configurações do aplicativo

Você pode usar uma política, tarefas ou a interface do aplicativo para configurar o Kaspersky Endpoint Security. Informações detalhadas sobre os componentes do aplicativo são fornecidas nas seções correspondentes.

Proteção Contra Ameaças ao Arquivo

O componente Proteção Contra Ameaças ao Arquivo permite evitar infecção do sistema de arquivos do computador. Por padrão, o componente Proteção Contra Ameaças ao Arquivo está localizado de forma permanente na RAM do computador e verifica todos os arquivos abertos, salvos ou executados em tempo real. O componente verifica os arquivos em todas as unidades do computador, inclusive unidades conectadas. O componente fornece proteção ao computador com a ajuda de bancos de dados de antivírus, o serviço na nuvem Kaspersky Security Network e análise heurística.

O componente verifica os arquivos acessados pelo usuário ou aplicativo. Se um arquivo malicioso for detectado, o Kaspersky Endpoint Security bloqueará a operação do arquivo. O aplicativo desinfeta ou exclui o arquivo malicioso, dependendo das configurações do componente Proteção contra ameaças ao arquivo.

Durante a tentativa de acesso a um arquivo cujos conteúdos estão armazenados na nuvem do OneDrive, o Kaspersky Endpoint Security baixa e verifica os conteúdos do arquivo.

Configurações do componente Proteção Contra Ameaças ao Arquivo

Parâmetro	Descrição
Nível de segurança *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	Para Proteção contra Ameaças ao Arquivo, o Kaspersky Endpoint Security pode aplicar diferentes grupos de configurações. Estes grupos de configurações armazenados no aplicativo são denominados *níveis de segurança*: • **Alto**. Quando este nível de proteção de arquivo é selecionado, o Antivírus de Arquivos toma o controle mais estrito de todos os arquivos que são abertos, salvos e iniciados. O Componente de proteção de Ameaça de Arquivo verifica todos os tipos de arquivo em todos os discos rígidos, unidades removíveis e unidades de rede do computador. Ele também verifica arquivos compactados, pacotes de instalação e objetos OLE incorporados. • **Recomendado**. Esse nível de segurança de arquivo é recomendado pelos especialistas da Kaspersky Lab. O Componente de proteção de Ameaça de Arquivo só verifica os formatos de ficheiro especificados em todos os discos rígidos, unidades removíveis, e unidades de rede do computador e objetos de OLE incorporados. O Componente de proteção de Ameaça de Arquivo não verifica pacotes de instalação ou arquivos. • **Baixo**. As configurações desse nível de segurança de arquivo garantem a velocidade máxima de verificação. O componente File Threat Protection verifica somente arquivos com as extensões especificadas em todos os discos rígidos, unidades removíveis e unidades de rede do computador. O Componente de proteção de Ameaça de Arquivo não verifica arquivos compostos.
Tipos de arquivos *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	**Todos os arquivos**. Se esta configuração for ativada, o Kaspersky Endpoint Security verificará todos os arquivos sem exceção (todos os formatos e extensões). **Arquivos verificados por formato**. Se esta configuração for ativada, o aplicativo verificará apenas arquivos infetáveis. Antes de verificar um arquivo quanto a código malicioso, o cabeçalho interno do arquivo é analisado para determinar o formato do arquivo (por exemplo, .txt, .doc ou .exe). A verificação também procura arquivos com extensões específicas. **Arquivos verificados por extensão**. Se esta configuração for ativada, o aplicativo verificará apenas arquivos infetáveis. O formato do arquivo é determinado com base na extensão do arquivo.

Parâmetro	Descrição
Escopo da verificação	Contém objetos que são verificados pelo componente Proteção Contra Ameaças ao Arquivo. Um objeto de verificação pode ser um disco rígido, unidade removível, unidade de rede, pasta, arquivo ou arquivos múltiplos, definido por uma máscara. Por padrão, o componente Proteção Contra Ameaças ao Arquivo verifica somente arquivos iniciados em discos rígidos, unidades de rede ou unidades removíveis. O escopo de proteção para esses objetos não pode ser alterado ou excluído. Você também pode excluir um objeto (como unidades removíveis) das verificações.
Aprendizado de máquina e análise de assinatura *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	O machine learning e análise de assinatura usa o banco de dados do Kaspersky Endpoint Security que contém descrições de ameaças conhecidas e modos de neutralizá-las. A Proteção que usa este método fornece o nível de segurança aceitável mínimo. Com base nas recomendações dos especialistas da Kaspersky, o aprendizado de máquina e análise de assinatura sempre estarão ativados.
Análise Heurística *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	A tecnologia foi desenvolvida para detectar ameaças que não podem ser detectadas usando a versão atual dos bancos de dados do aplicativo Kaspersky. Detecta arquivos que podem estar infectados por um vírus desconhecido ou por uma nova variedade de um vírus conhecido. Ao verificar arquivos em busca de códigos maliciosos, o analisador heurístico executa instruções nos arquivos executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível de análise heurística assegura um equilíbrio entre a eficácia da verificação quanto a novas ameaças, a carga nos recursos do sistema operacional e a duração da análise heurística.
Ação ao detectar ameaça	**Desinfectar e excluir se a desinfecção falhar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Caso a desinfecção falhe, o aplicativo excluirá o arquivo. **Desinfectar e bloquear se a desinfecção falhar**. Caso esta opção seja selecionada, o aplicativo tentará desinfectar automaticamente todos os arquivos infectados e detectados. Se a desinfecção falhar, o aplicativo bloqueará o arquivo. **Bloquear**. Se esta opção for selecionada, o aplicativo bloqueará automaticamente o arquivo infectado sem tentar desinfectá-lo ou exclui-lo. Antes de tentar desinfectar ou excluir um arquivo infectado, o aplicativo cria uma cópia de backup do arquivo no caso de você precisar restaurá-lo ou se ele puder ser desinfetado no futuro.
Verificar somente arquivos novos e alterados	Verifica apenas os arquivos novos e aqueles que foram modificados desde a última vez em que foram verificados. Isso ajuda a reduzir a duração de uma verificação. Esse modo se aplica a arquivos simples e compostos.
Verificar arquivos compactados	Verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros arquivos compactados. O aplicativo verifica os arquivos por extensão e formato. Ao verificar os arquivos, o aplicativo executa uma descompactação recursiva. Isso permite detectar ameaças em arquivos multinível (arquivo dentro de arquivo).
Verificar pacotes de distribuição	Verificação de pacotes de distribuição de aplicativos 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 aplicativo 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	Verificar arquivos de formato de e-mail. O aplicativo verifica arquivos MSG e EML. Arquivos de formato de e-mail também incluem objetos OLE e arquivos MHT. O Kaspersky Endpoint Security verifica arquivos em formato de e-mail com menos de 1 MB, independentemente de a caixa de seleção estar marcada ou não.
Não descompactar arquivos compostos de grandes dimensões	Se esta caixa de seleção for marcada, o aplicativo não verificará arquivos compostos se o tamanho deles exceder o valor especificado. Se esta caixa de seleção estiver desmarcada, o aplicativo verificará os arquivos compostos de todos os tamanhos. O aplicativo verifica arquivos grandes extraídos de arquivos compactados independentemente de a caixa de seleção estar selecionada ou não.

Parâmetro	Descrição
Descompactar arquivos compostos em segundo plano	Se essa caixa de seleção estiver selecionada, o aplicativo fornece acesso a arquivos compostos maiores que o valor especificado antes da verificação desses arquivos. Nesse caso, o Kaspersky Endpoint Security descompacta e verifica os arquivos compostos em segundo plano. O aplicativo fornece acesso a arquivos compostos menores que esse valor somente após descompactar e verificar esses arquivos. Se a caixa de seleção não estiver selecionada, o aplicativo Kaspersky Endpoint Security fornecerá acesso a arquivos compostos somente após descompactar e verificar arquivos de qualquer tamanho.
Modo de verificação *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	O Kaspersky Endpoint Security verifica os arquivos acessados pelo usuário, sistema operacional ou um aplicativo em execução na conta do usuário. **Modo inteligente**. Nesse modo, a Proteção Contra Ameaças ao Arquivo verifica um objeto com base na análise das ações executadas com o objeto. Por exemplo, ao trabalhar com um documento do Microsoft Office, o Kaspersky Endpoint Security verifica o arquivo quando ele é aberto pela primeira vez e fechado pela última vez. O arquivo não é verificado durante as operações intermediárias de gravação. **Ao acessar e modificar**. Nesse modo, os objetos são verificados pela Proteção Contra Ameaças ao Arquivo sempre que houver uma tentativa de abri-los ou modificá-los. **Ao acessar**. Neste modo, os objetos são verificados pela Proteção Contra Ameaças ao Arquivo ao tentar abri-los. **Ao executar**. Neste modo, os objetos são verificados pela Proteção Contra Ameaças ao Arquivo apenas ao tentar executá-los.
Usar tecnologia iSwift *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iSwift é um avanço da tecnologia iChecker do sistema de arquivos NTFS.
Usar tecnologia iChecker *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	Esta tecnologia permite aumentar a velocidade de verificação, excluindo determinados arquivos da verificação. Os arquivos são excluídos da verificação usando um algoritmo especial que considera a data de lançamento dos bancos de dados do Kaspersky Endpoint Security, a data da última verificação do arquivo e qualquer modificação nas configurações da verificação. A tecnologia iChecker tem algumas limitações: ela não funciona com arquivos grandes e se aplica somente a objetos com uma estrutura reconhecida pelo aplicativo (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).
Pausar a Proteção Contra Ameaças ao Arquivo *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	Interrompe temporariamente e automaticamente a operação da Proteção Contra Ameaças ao Arquivo no horário especificado ou ao trabalhar com os aplicativos especificados.
Verificar as operações de arquivo executadas nos contêineres do Windows	Se uma ameaça for detectada dentro de um contêiner, o aplicativo aplica a ação selecionada para o componente Proteção Contra Ameaças ao Arquivo. **Interromper o contêiner caso a desinfecção falhe**. O aplicativo pode não ter direitos de leitura e gravação suficientes para o objeto detectado. Nesse caso, é impossível 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 de arquivo 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.

Proteção Contra Ameaças da Web

O componente Proteção Contra Ameaças da Web impede o download de arquivos maliciosos da Internet e também bloqueia a conexão com sites maliciosos e de phishing. O componente fornece proteção ao computador com a ajuda de bancos de dados de antivírus, o serviço na nuvem Kaspersky Security Network e análise heurística.

O Kaspersky Endpoint Security verifica o tráfego HTTP, HTTPS e FTP. O Kaspersky Endpoint Security verifica URLs e endereços IP.

Para usar a Proteção Contra Ameaças da Web, você deve concluir a configuração inicial do aplicativo:

- Para o monitoramento de tráfego HTTPS, ative a verificação de conexões criptografadas (ativada por padrão).
- Selecione as portas que o Kaspersky Endpoint Security deve monitorar (por padrão, o aplicativo monitora todas as portas).
- Selecione os aplicativos cujo tráfego você deseja que o Kaspersky Endpoint Security monitore. A maioria dos navegadores já está presente na lista de aplicativos recomendados pela Kaspersky. Se o seu navegador não estiver na lista, adicione-o manualmente.
- Recomendamos injetar um script de interação de página da web no tráfego da Web (por padrão, a injeção de script está desabilitada). Esse script ativa o registro de eventos da Proteção Contra Ameaças da Web para o log de eventos do aplicativo, log de eventos do SO e relatórios.

Quando um usuário tenta abrir um site malicioso ou de phishing, o Kaspersky Endpoint Security bloqueará o acesso e exibirá um aviso.

Configurações do componente Proteção Contra Ameaças da Web

Parâmetro	Descrição
Nível de segurança *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	Para Proteção Contra Ameaças da Web, o aplicativo pode aplicar diferentes grupos de configurações. Estes grupos de configurações armazenados no aplicativo são denominados *níveis de segurança*: • **Alto**. O nível de segurança sob o qual o componente Proteção Contra Ameaças da Web executa a verificação máxima do tráfego da web que o computador recebe através dos protocolos de FTP e HTTP. A Proteção Contra Ameaças da Web verifica detalhadamente todos os objetos de tráfego da web, usando o conjunto completo de bancos de dados do aplicativo, e executa a análise heurística mais profunda possível. • **Recomendado**. O nível de segurança que fornece o equilíbrio ideal entre o desempenho do aplicativo e a segurança do tráfego da Web. O componente Proteção Contra Ameaças da Web executa a análise heurística no nível de verificação média. Esse nível de segurança do tráfego da Web é recomendado pelos especialistas da Kaspersky. • **Baixo**. As configurações deste nível de segurança de tráfego da web asseguram a velocidade máxima de verificação de tráfego da web. O componente Proteção Contra Ameaças da Web executa a análise heurística no nível de verificação leve.
Ação ao detectar ameaça	**Bloquear**. Se esta opção for selecionada, quando o componente Proteção Contra Ameaças da Web detectar um objeto infectado no tráfego da Web, ele bloqueará o acesso ao objeto e exibirá uma notificação no navegador. **Informar**. Se essa opção estiver selecionada e um objeto infectado for detectado no tráfego da Web, o Kaspersky Endpoint Security permitirá que esse objeto seja baixado no computador, mas adicionará informações sobre o objeto infectado à lista de ameaças ativas.
Verificar se o endereço está no banco de dados de endereços da Web maliciosos *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	A verificação de links para determinar se estão incluídos no banco de dados de endereços da Web maliciosos permite rastrear sites que foram incluídos na lista de bloqueio. O banco de dados de endereços Web maliciosos é mantido pela Kaspersky, incluído no pacote de instalação do aplicativo e atualizado durante as atualizações do banco de dados do Kaspersky Endpoint Security.
Usar a análise heurística *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	A tecnologia foi desenvolvida para detectar ameaças que não podem ser detectadas usando a versão atual dos bancos de dados do aplicativo Kaspersky. Detecta arquivos que podem estar infectados por um vírus desconhecido ou por uma nova variedade de um vírus conhecido. Quando o tráfego da Web for verificado quanto a vírus e outros aplicativos que apresentam uma ameaça, o analisador heurístico executará instruções nos arquivos executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível de análise heurística assegura um equilíbrio entre a eficácia da verificação quanto a novas ameaças, a carga nos recursos do sistema operacional e a duração da análise heurística.

Parâmetro	Descrição
Verificar se o endereço está no banco de dados de endereços da Web de phishing *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	O banco de dados de endereços Web de phishing inclui os endereços Web de sites atualmente conhecidos que são usados para iniciar ataques de phishing. A Kaspersky complementa esse banco de dados de links de phishing com endereços obtidos da organização internacional Anti-Phishing Working Group. O banco de dados de endereços de phishing está incluído no pacote de instalação do aplicativo e é complementado com atualizações de banco de dados do Kaspersky Endpoint Security.
Não verificar tráfego da Web de endereços confiáveis	Caso esta opção seja selecionada, o componente Proteção Contra Ameaças da Web não verificará o conteúdo de páginas da Web ou sites cujos endereços estão incluídos na lista endereços da Web confiáveis. Você pode adicionar tanto o endereço especifico como a máscara de endereço de uma página da Web/site à lista de endereços da Web confiáveis. Também é possível criar uma lista geral de exclusões para conexões criptografadas. Nesse caso, o Kaspersky Endpoint Security não verifica o tráfego HTTPS de endereços da Web confiáveis quando os componentes Proteção Contra Ameaças da Web, Proteção Contra Ameaças ao Correio e Controle da Web estão fazendo seu trabalho.

Proteção Contra Ameaças ao Correio

O componente Proteção contra ameaças de correio verifica os anexos das mensagens de e-mail recebidas e enviadas para detectar vírus e outras ameaças. O componente fornece proteção ao computador com a ajuda de bancos de dados de antivírus, o serviço na nuvem Kaspersky Security Network e análise heurística.

A Proteção Contra Ameaças ao Correio pode verificar as mensagens recebidas e enviadas. O aplicativo é compatível com POP3, SMTP, IMAP e NNTP nos seguintes clientes de e-mail:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- Correio do MyOffice
- R7-Office Organizer

Para verificar o tráfego nos programas de e-mail Mozilla Thunderbird, MyOffice Mail e R7-Office Organizer, é necessário adicionar o certificado da Kaspersky ao armazenamento de certificados e selecionar o armazenamento de certificados próprio.

A Proteção Contra Ameaças ao Correio não oferece suporte a outros protocolos e clientes de e-mail.

A Proteção Contra Ameaças ao Correio pode nem sempre ser capaz de obter acesso a mensagens no *nível de protocolo* (por exemplo, ao usar a solução Microsoft Exchange). Por essa razão, a Proteção Contra Ameaças ao Correio inclui uma extensão para Microsoft Office Outlook. A extensão permite verificar mensagens no *nível do cliente de e-mail*. A extensão Proteção Contra Ameaças ao Correio é compatível com as versões de 32 e 64 bits do Outlook 2010, 2013, 2016, 2019, 2021, 2024 e 365. Em computadores baseados em Arm, a extensão Proteção Contra Ameaças ao Correio é compatível com as versões de 32 e 64 bits do Outlook 2016, Outlook 2021, Outlook 2024 e Outlook 365 para Arm64.

O componente Proteção Contra Ameaças ao Correio não verifica as mensagens se o programa de e-mail estiver aberto em um navegador.

Quando um arquivo malicioso for detectado em um anexo, o Kaspersky Endpoint Security adiciona informações sobre a ação executada ao assunto da mensagem, por exemplo, *[Message has been processed]<assunto da mensagem>*.

Configurações do componente Proteção Contra Ameaças ao Correio

Parâmetro	Descrição
Nível de segurança *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	Para a Proteção Contra Ameaças ao Correio, o aplicativo poderá aplicar diferentes grupos de configurações. Estes grupos de configurações armazenados no aplicativo são denominados *níveis de segurança*: • **Alto**. Quando este nível de segurança de e-mail é selecionado, o componente Proteção Contra Ameaças ao Correio verifica as mensagens de e-mail mais detalhadamente. O componente Proteção Contra Ameaças ao Correio verifica mensagens de e-mail enviadas e recebidas e realiza uma análise heurística profunda. O nível de segurança de e-mails alto é recomendado para ambientes de alto risco. Um exemplo desse tipo de ambiente é uma conexão com um serviço de e-mail gratuito, de uma rede doméstica que não tem uma proteção de e-mail centralizada. • **Recomendado**. O nível de segurança do e-mail que fornece o equilíbrio ideal entre o desempenho do aplicativo e a segurança do e-mail. O componente Proteção Contra Ameaças ao Correio verifica mensagens de e-mail enviadas e recebidas e realiza uma análise heurística de nível médio. Esse nível de segurança de tráfego de e-mail é recomendado por especialistas da Kaspersky. • **Baixo**. Quando este nível de segurança de e-mail é selecionado, o componente Proteção Contra Ameaças ao Correio verifica apenas mensagens de e-mail recebidas, executa a análise heurística superficial e não verifica arquivos compactados anexados a mensagens de e-mail. Nesse nível de segurança de e-mail, o componente Proteção Contra Ameaças ao Correio verifica mensagens de e-mail na velocidade máxima e usa um mínimo de recursos do sistema operacional. O nível de segurança de e-mail baixo é recomendado para utilização em um ambiente bem protegido. Um exemplo desse ambiente poderia ser uma LAN corporativa com segurança de e-mail centralizada.
Ação ao detectar ameaça	**Desinfectar e excluir se a desinfecção falhar**. Quando um objeto infectado é detectado em uma mensagem de entrada ou saída, o aplicativo tenta desinfectar o objeto detectado. O usuário poderá acessar a mensagem com um anexo seguro. Caso o objeto não possa ser desinfectado, o aplicativo excluirá o objeto infectado. O aplicativo adiciona informações sobre a ação executada ao assunto da mensagem: *[A mensagem foi processada] <assunto da mensagem>*. **Desinfectar e bloquear se a desinfecção falhar**. Quando um objeto infectado é detectado em uma mensagem de entrada, o aplicativo tenta desinfectar o objeto detectado. O usuário poderá acessar a mensagem com um anexo seguro. Caso o objeto não possa ser desinfectado, o aplicativo adicionará um aviso ao assunto da mensagem. O usuário poderá acessar a mensagem com o anexo original. Quando um objeto infectado é detectado em uma mensagem de saída, o aplicativo tenta desinfectar o objeto detectado. Caso o objeto não possa ser desinfectado, o aplicativo bloqueará a transmissão da mensagem e o programa de e-mail exibirá um erro. **Bloquear**. Caso um objeto infectado seja detectado em uma mensagem recebida, o aplicativo adiciona um aviso ao assunto da mensagem. O usuário poderá acessar a mensagem com o anexo original. Caso um objeto infectado seja detectado em uma mensagem de saída, o aplicativo bloqueará a transmissão da mensagem e o programa de e-mail exibirá um erro.
Escopo de proteção *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	O *Escopo da proteção* inclui objetos que o componente verifica ao ser executado: mensagens recebidas e enviadas ou apenas mensagens recebidas. Para proteger seus computadores, você precisa apenas verificar as mensagens recebidas. É possível ativar a verificação de mensagens enviadas para impedir que arquivos infectados sejam enviados em arquivos compactados. Também é possível ativar a verificação de mensagens enviadas se quiser impedir que arquivos em formatos específicos sejam enviados, tais como arquivos de áudio e vídeo, por exemplo.
Verificar tráfego POP3, SMTP, NNTP e IMAP	Verificação feita pelo componente Proteção Contra Ameaças ao Correio do tráfego que é transferido por meio dos protocolos POP3, SMTP, NNTP e IMAP.
Conectar a extensão do Microsoft Outlook	Se a caixa de seleção estiver marcada, a verificação de mensagens de e-mail transmitidas através dos protocolos POP3, SMTP, NNTP e IMAP será ativada no lado da extensão integrada ao Microsoft Outlook. Se o e-mail for verificado por meio da extensão para o Microsoft Outlook, recomenda-se utilizar o Cached Exchange Mode. Para obter informações mais detalhadas sobre o Modo de cache do Exchange e recomendações sobre seu uso, consulte a Base de Dados de Conhecimento Microsoft.
Análise heurística *(disponível apenas no Console de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	A tecnologia foi desenvolvida para detectar ameaças que não podem ser detectadas usando a versão atual dos bancos de dados do aplicativo Kaspersky. Detecta arquivos que podem estar infectados por um vírus desconhecido ou por uma nova variedade de um vírus conhecido. Ao verificar arquivos em busca de códigos maliciosos, o analisador heurístico executa instruções nos arquivos executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível de análise heurística assegura um equilíbrio entre a eficácia da verificação quanto a novas ameaças, a carga nos recursos do sistema operacional e a duração da análise heurística.

Parâmetro	Descrição
Verificar arquivos compactados anexados	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). Se, durante a verificação, o aplicativo detectar uma senha para um arquivo compactado no texto da mensagem, essa senha será usada para verificar o conteúdo do arquivo compactado em busca de aplicativos maliciosos. Nesse caso, a senha não é salva. O arquivo compactado é descompactado durante a verificação. Caso ocorra um erro de aplicativo durante o processo de descompactação, será possível excluir manualmente os arquivos descompactados salvos no seguinte caminho: %systemroot%\temp. Os arquivos têm o prefixo PR.
Verificar arquivos anexos com formato 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 aplicativo verifica arquivos em formato do Office com menos de 1 MB, independentemente de a caixa de seleção estar marcada ou não.
Não verificar arquivos compactados com mais de N MB	Se esta caixa de seleção for marcada, o componente Proteção contra ameaças de correio excluirá arquivos compactados anexados a mensagens de e-mail da verificação se o seu tamanho exceder o valor especificado. Se a caixa de seleção for desmarcada, o componente Proteção contra ameaças de correio verificará arquivos compactados de anexo de e-mail de qualquer tamanho.
Limitar o tempo para a verificação de arquivos compactados a N seg	Se a caixa de seleção for marcada, o tempo alocado para verificar arquivos compactados anexados a mensagens de e-mail será limitado ao período especificado.
Filtro de anexos	O filtro de anexos não é aplicado a mensagens de e-mail enviadas. **Desativar a filtragem**. Se esta opção for selecionada, o componente de Proteção Contra Ameaças ao Correio não filtrará arquivos anexados a mensagens de e-mail. **Renomear anexos dos tipos selecionados**. Se você selecionar essa opção, o componente de Proteção Contra Ameaças ao Correio substituirá o último caractere da extensão encontrado nos arquivos anexados dos tipos especificados pelo caractere de sublinhado (por exemplo, anexo.doc_). Portanto, para abrir o arquivo, o usuário deve renomeá-lo. **Excluir anexos dos tipos selecionados**. Se esta opção for selecionada, o componente Proteção Contra Ameaças ao Correio excluirá arquivos anexados dos tipos especificados de mensagens de e-mail. Na lista de máscaras do arquivo, você pode especificar os tipos de arquivos anexados para renomear ou excluir das mensagens de e-mail.

Proteção Contra Ameaças à Rede

O componente *Proteção Contra Ameaças à Rede* (também chamado de Intrusion Detection System, IDS) monitora o tráfego de rede de entrada em busca de atividades com características de ataques de rede. Quando o aplicativo detecta uma tentativa de ataque de rede no computador do usuário, ele bloqueia a conexão de rede com o computador atacante. 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.

Parâmetro	Descrição
Considerar verificação de portas e a saturação da rede como ataques	*Saturação de rede* é um ataque aos recursos de rede de uma organização (como servidores da web). Esse ataque consiste no envio de um grande número de solicitações para sobrecarregar a largura de banda dos recursos de rede. Quando isso acontece, os usuários não conseguem acessar os recursos de rede da organização. Um ataque de *verificação de portas* consiste em varrer portas UDP, portas TCP e serviços de rede no computador. Esse ataque permite ao atacante identificar o grau de vulnerabilidade do computador antes de efetuar outros tipos mais perigosos de ataques de rede. A verificação de portas também permite ao invasor identificar o sistema operacional no computador e selecionar os ataques de rede apropriados para esse sistema operacional. Se esta caixa de seleção estiver marcada, o Kaspersky Endpoint Security monitorará o tráfego de rede para detectar esses ataques. Caso um ataque seja detectado, o aplicativo notifica o usuário e envia o evento correspondente ao Kaspersky Security Center. O aplicativo fornece informações sobre o computador atacante, que são necessárias para as ações oportunas de resposta a ameaças. É possível desativar a detecção desses tipos de ataques caso alguns dos aplicativos permitidos realizem operações típicas desses tipos de ataques. Isso ajudará a evitar alarmes falsos.
Bloquear dispositivos de ataque por N min	Caso esta opção seja ativada, o componente Proteção Contra Ameaças à Rede adicionará o computador atacante à lista bloqueada. Isso significa que o componente Proteção Contra Ameaças à Rede bloqueia a conexão de rede com o computador de ataque depois da primeira tentativa de ataque de rede pelo período de tempo especificado. Esse bloqueio protege automaticamente o computador do usuário contra a ocorrência de ataques de rede futuros que se originem do mesmo endereço. O tempo mínimo que um computador atacante deve gastar na lista de bloqueio é um minuto. O tempo máximo é de 999 minutos. É possível ver a lista de bloqueio na janela da ferramenta Monitor de Rede. O Kaspersky Endpoint Security limpa a lista de bloqueio quando o aplicativo é reiniciado e quando as configurações de proteção contra ameaças à rede são alteradas.
Exclusões	A lista contém endereços IP dos quais a Proteção Contra Ameaças à Rede não bloqueia ataques de rede. É possível adicionar um endereço IP com porta e protocolo especificados. O aplicativo não registra informações sobre ataques de rede dos endereços IP que estão na lista de exclusões.
Proteção contra MAC spoofing	Um *ataque de falsificação de MAC* consiste em alterar o endereço MAC de um dispositivo de rede (placa de rede). Como resultado, um invasor pode redirecionar dados enviados para um dispositivo para outro dispositivo e obter acesso a esses dados. O Kaspersky Endpoint Security permite bloquear ataques de MAC spoofing e receber notificações sobre os ataques.

Firewall

O componente Firewall bloqueia conexões não autorizadas ao computador enquanto conectado na Internet ou na rede local. O Firewall também controla a atividade de rede dos aplicativos no computador. Isso permite proteger sua LAN contra roubo de identidade e outros ataques. O componente fornece proteção ao computador com a ajuda de bancos de dados antivírus, o serviço na nuvem da Kaspersky Security Network e *regras de rede* predefinidas.

O agente de rede é usado para interação com o Kaspersky Security Center. O Firewall cria automaticamente as regras de rede necessárias para que o aplicativo e o agente de rede funcionem. Como resultado, o Firewall abre várias portas no computador. Quais portas serão abertas depende da função do computador (por exemplo, ponto de distribuição). Para saber mais sobre as portas que serão abertas no computador, consulte a Ajuda do Kaspersky Security Center.

Regras de rede

Você pode configurar regras de rede nos seguintes níveis:

- *Regras de pacotes de rede*. As regras de pacotes de rede impõem restrições a pacotes de rede, seja qual for o aplicativo. Estas regras restringem o tráfego de rede de entrada e de saída através de portas específicas do protocolo de dados selecionado. O Kaspersky Endpoint Security predefiniu regras de pacotes de rede com permissões recomendadas por especialistas da Kaspersky.

- *Regras de rede de aplicativos*. As regras de rede de aplicativos impõem restrições à atividade de rede de um aplicativo específico. Elas têm em conta não só as características do pacote de rede, mas também o aplicativo específico para o qual este pacote de rede é direcionado ou que emitiu este pacote de rede.

O acesso controlado de aplicativos aos recursos, processos e dados pessoais do sistema operacional é fornecido pelo componente Prevenção de Intrusão do Host usando *direitos de aplicativo*.

Durante a primeira inicialização do aplicativo, o Firewall executa as seguintes ações:

1. Verifica a segurança do aplicativo usando bancos de dados de antivírus baixados.

2. Verifica a segurança do aplicativo na Kaspersky Security Network.

   A participação na Kaspersky Security Network é recomendada para ajudar o Firewall a funcionar de maneira mais eficiente.

3. Coloca o aplicativo em um dos grupos de confiança: *Confiável*, *Baixa restrição*, *Alta restrição*, *Não confiável*.

   Um grupo confiável define os direitos aos quais o Kaspersky Endpoint Security se refere ao controlar a atividade do aplicativo. O Kaspersky Endpoint Security coloca um aplicativo em um grupo de confiança, dependendo do nível de perigo que esse aplicativo pode representar para o computador.

   O Kaspersky Endpoint Security coloca um aplicativo em um grupo de confiança para os componentes Firewall e Prevenção de Intrusão do Host. Você não pode alterar o grupo de confiança apenas para o Firewall ou Prevenção de Intrusão do Host.

   Se você se recusou a participar do KSN ou não há rede, o Kaspersky Endpoint Security coloca o aplicativo em um grupo de confiança, dependendo das configurações do componente Prevenção de Intrusão do Host. Após receber a reputação do aplicativo da KSN, o grupo de confiança pode ser alterado automaticamente.

4. Bloqueia a atividade de rede do aplicativo, dependendo do grupo de confiança. Por exemplo, os aplicativos no grupo de confiança de *Alta restrição* não têm permissão para usar nenhuma conexão de rede.

Na próxima vez em que o aplicativo for iniciado, a Prevenção de Intrusão do Host verificará sua integridade. Se o aplicativo não estiver modificado, o componente usará as regras de rede atuais para ele. Se o aplicativo foi modificado, o Kaspersky Endpoint Security o analisará como se estivesse sendo iniciado pela primeira vez.

Prioridades de regra de rede

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

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

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

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

Tipos da conexão de rede

O Firewall permite controlar a atividade da rede, dependendo do tipo da conexão de rede. O Kaspersky Endpoint Security recebe o tipo da conexão de rede do sistema operacional do computador. O tipo da conexão de rede no sistema operacional é definido pelo usuário ao configurar a conexão. Você pode alterar o tipo da conexão de rede nas configurações do Kaspersky Endpoint Security. O firewall monitorará a atividade da rede, dependendo do tipo de rede, especificado nas configurações do Kaspersky Endpoint Security, e não do sistema operacional.

Os seguintes tipos de conexão de rede estão disponíveis:

- **Rede pública**. A rede não está protegida por aplicativos antivírus, firewalls ou filtros (como Wi-Fi em um café). Quando o usuário utiliza um computador que está conectado a uma rede desse tipo, o Firewall bloqueia o acesso a arquivos e impressoras desse computador. Os usuários externos também não podem acessar dados por meio de pastas compartilhadas e acesso remoto à área de trabalho deste computador. O Firewall filtra a atividade de rede de cada aplicativo, de acordo com as regras de rede definidas para cada uma.

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

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

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

Configurações do componente Firewall

Parâmetro	Descrição
Regras de pacotes	Tabela com uma lista de regras de pacotes de rede. As regras de pacotes de rede tem a função de impor restrições a pacotes de rede, seja qual for o aplicativo. Estas regras restringem o tráfego de rede de entrada e de saída através de portas específicas do protocolo de dados selecionado. A tabela enumera regras de pacotes de rede pré-configuradas que são recomendadas pela Kaspersky para proteção ideal do tráfego de rede de computadores executados em sistemas operacionais Microsoft Windows. O Firewall estabelece a prioridade de execução de cada regra de pacotes de rede. O Firewall processa as regras de pacotes de rede na ordem em que aparecem na lista de regras de pacote de rede, ou seja, de cima para baixo. O Firewall localiza e aplica a regra de pacotes de rede no topo da lista que mais está adequada a conexão de rede, permitindo ou bloqueando a atividade de rede. O Firewall ignora todas as regras do pacote de rede subsequentes para a conexão de rede específica. As regras de pacotes de rede têm prioridade sobre as regras de rede dos aplicativos.
Redes disponíveis	Esta tabela contém informações sobre conexões da rede que o Firewall detecta no computador. O status de *Rede pública* é atribuído à Internet por padrão. Não é possível alterar o status da Internet.
Regras para aplicativos	**Aplicativo**. Tabela de aplicativos que são controlados pelo componente Firewall. Os Aplicativos são atribuídos a grupos de confiança. Um grupo de confiança define os direitos usados pelo Kaspersky Endpoint Security ao controlar a atividade de rede dos aplicativos. Você pode selecionar um aplicativo em uma única lista de todos os aplicativos instalados nos computadores sob a influência de uma política e adicionar o aplicativo a um grupo de confiança. **Regras de rede**. Tabela de regras de rede para aplicativos que fazem parte de um grupo de confiança. De acordo com essas regras, o firewall regula a atividade de rede de aplicativos. A tabela exibe as regras de rede predefinidas recomendadas pelos especialistas da Kaspersky. Essas regras de rede foram adicionadas para proteger de maneira ideal o tráfego de rede dos computadores que executam os sistemas operacionais Windows. Não é possível excluir as regras de rede predefinidas.

Prevenção contra ataque BadUSB

Alguns vírus modificam o firmware dos dispositivos USB para enganar o sistema operacional em detectar o dispositivo USB como um teclado. 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 como um teclado pelo sistema operacional, o aplicativo solicitará que o usuário insira um código numérico gerado pelo próprio aplicativo usando esse teclado ou, se disponível, o teclado virtual (veja a figura abaixo). Esse procedimento é conhecido como autorização do teclado.

Caso o código tenha sido digitado corretamente, o aplicativo salva 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 (ver figura abaixo), a aplicativo bloqueia a entrada a partir do 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.

Autorização do teclado

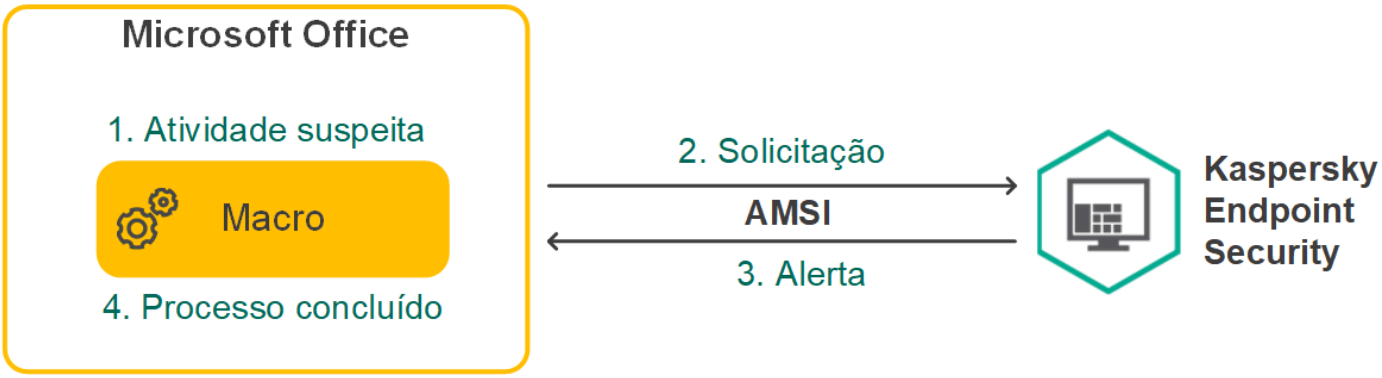
Configurações do componente Prevenção contra ataque BadUSB

Parâmetro	Descrição
Proibir o uso do Teclado na tela para a autorização de dispositivos USB	Caso o botão de alternância esteja ativado, o aplicativo proibirá o uso do Teclado na tela para a autorização de um dispositivo USB do qual um código de autorização não poderá ser inserido.
Proibir o uso do código de barras para autorização de dispositivos USB	Caso esse botão de alternância esteja ativado, o aplicativo não exibirá o código de barras na notificação de autenticação do leitor de código de barras.
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, se você permitir cinco tentativas para inserir o código de autorização, o aplicativo bloqueará o dispositivo USB após a quinta tentativa malsucedida. O Kaspersky Endpoint Security exibe a duração do bloqueio do dispositivo USB. Após esse tempo, haverá novamente cinco tentativas para inserir o código de autorização.
Tempo limite ao atingir o número máximo de tentativas	Duração do bloqueio do dispositivo USB após o número especificado de tentativas malsucedidas de inserir o código de autorização. Os valores válidos são de 1 a 180 (minutos).

Proteção AMSI

O componente de Proteção AMSI 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 Endpoint Security para uma verificação adicional e receber os resultados da verificação desses objetos. Aplicativos de terceiros podem incluir, por exemplo, aplicativos do Microsoft Office (veja a figura abaixo). Para obter detalhes sobre a AMSI, consulte a documentação da Microsoft.

A Proteção AMSI pode apenas detectar e notificar aplicativos de terceiros sobre a ameaça. Após receber uma notificação de uma ameaça, o aplicativo de terceiros não permite executar ações maliciosas (por exemplo, encerramentos a ação).



Exemplo de operação AMSI

O componente de Proteção AMSI pode recusar uma solicitação de um aplicativo de terceiros, por exemplo, se esse aplicativo exceder o número máximo de solicitações em um intervalo especificado. O Kaspersky Endpoint Security envia ao Servidor de Administração informações sobre uma solicitação rejeitada de um aplicativo de terceiros. O componente de proteção AMSI não nega as solicitações de aplicativos de terceiros para os quais a integração contínua com o componente de proteção AMSI está ativada.

A Proteção AMSI está disponível para os seguintes sistemas operacionais para estações de trabalho e servidores:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multisessão
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multisessão
- Windows Server 2016 Essentials / Standard / Datacenter (incluindo o modo Server Core)
- Windows Server 2019 Essentials / Standard / Datacenter (incluindo o modo Server Core)
- Windows Server 2022 Standard / Datacenter / Datacenter Azure Edition (incluindo o modo Server Core)
- Windows Server 2025 Standard / Datacenter

Configurações de Proteção AMSI

Parâmetro	Descrição
Verificar arquivos compactados	Verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros arquivos compactados. O aplicativo verifica os arquivos por extensão e formato. Ao verificar os arquivos, o aplicativo executa uma descompactação recursiva. Isso permite detectar ameaças em arquivos multinível (arquivo dentro de arquivo).
Verificar pacotes de distribuição	Verificação de pacotes de distribuição de aplicativos 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 aplicativo verifica arquivos em formato do Office com menos de 1 MB, independentemente de a caixa de seleção estar marcada ou não.
Não descompactar arquivos compostos de grandes dimensões	Se esta caixa de seleção for marcada, o aplicativo não verificará arquivos compostos se o tamanho deles exceder o valor especificado. Se esta caixa de seleção estiver desmarcada, o aplicativo verificará os arquivos compostos de todos os tamanhos. O aplicativo verifica arquivos grandes extraídos de arquivos compactados independentemente de a caixa de seleção estar selecionada ou não.

Prevenção de 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, os exploits podem utilizar um ataque de estouro de buffer. Para isso, o exploit envia uma grande quantidade de dados para um aplicativo vulnerável. Ao processar esses dados, o aplicativo vulnerável executa um código malicioso. Como resultado desse ataque, o exploit pode iniciar uma instalação não autorizada de malware. Quando há uma tentativa de executar um arquivo executável de um aplicativo vulnerável que não foi realizada pelo usuário, o Kaspersky Endpoint Security bloqueia a execução do arquivo ou notifica o usuário.

O componente Prevenção de Exploits também monitora as portas de rede quanto a processos de aplicativos que possam ameaçar a segurança do computador. O aplicativo obtém informações sobre esses processos em bancos de dados de antivírus.

Configurações do componente de Prevenção de Exploit

Parâmetro	Descrição
Na detecção de exploit	**Bloquear**. Se esse item for selecionado ao detectar uma exploit, o Kaspersky Endpoint Security bloqueará as operações dessa exploit e registrará as informações sobre ela. **Informar**. Se esse item for selecionado, quando o Kaspersky Endpoint Security detectar um exploit, ele registrará uma entrada contendo as informações sobre o exploit e adicionará informações sobre ele na lista de ameaças ativas.
Ativar a proteção da memória de processos do sistema	Se este botão de alternância estiver ativado, o Kaspersky Endpoint Security bloqueará os processos externos que tentam acessar a memória do processo do sistema.

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 Endpoint Security executará a ação de resposta selecionada. A funcionalidade do Kaspersky Endpoint Security com base em padrões de atividades perigosas fornece defesa proativa ao computador.

O componente Detecção de Comportamento também monitora as portas de rede quanto aos processos de aplicativos que possam ameaçar a segurança do computador. O aplicativo obtém informações sobre esses processos em bancos de dados de antivírus.

Configurações do componente de Detecção de Comportamento

Parâmetro	Descrição
Ação ao detectar atividade de malware	**Excluir**. Se esta opção for selecionada, ao detectar uma atividade maliciosa, o Kaspersky Endpoint Security excluirá o arquivo executável do aplicativo malicioso e criará uma cópia do arquivo no Backup. **Bloquear**. Se esta opção for selecionada, ao detectar atividade maliciosa, o Kaspersky Endpoint Security encerrará este aplicativo. **Informar**. Se essa opção for selecionada e a atividade maliciosa de um aplicativo for detectada, o Kaspersky Endpoint Security não encerrará esse aplicativo, mas adicionará informações sobre a atividade maliciosa à lista de ameaças ativas.

Prevenção de Intrusão do Host

O componente Prevenção de Intrusão do Host impede que os aplicativos executem ações perigosas para o sistema, e garante o controle de acesso aos recursos do sistema operacional e aos dados pessoais. O componente fornece proteção ao computador com a ajuda de bancos de dados antivírus e o serviço na nuvem Kaspersky Security Network.

O componente controla a operação de aplicativos usando *direitos de aplicativo*. Os direitos do aplicativo incluem os seguintes parâmetros de acesso:

- Acesso aos recursos do sistema operacional (por exemplo, opções de inicialização automática, chaves do Registro)
- Acesso a dados pessoais (como arquivos e aplicativos)

A atividade de rede dos aplicativos é controlada pelo componente Firewall por meio das *regras de rede*.

Durante a primeira inicialização do aplicativo, o componente de Prevenção de Intrusão do Host executa as seguintes ações:

1. Verifica a segurança do aplicativo usando bancos de dados de antivírus baixados.
2. Verifica a segurança do aplicativo na Kaspersky Security Network.

   Recomendamos a participação na Kaspersky Security Network para ajudar o componente Prevenção de Intrusão do Host a funcionar de maneira mais eficiente.

3. Coloca o aplicativo em um dos grupos de confiança: *Confiável*, *Baixa restrição*, *Alta restrição*, *Não confiável*.

   Um grupo confiável define os direitos aos quais o Kaspersky Endpoint Security se refere ao controlar a atividade do aplicativo. O Kaspersky Endpoint Security coloca um aplicativo em um grupo de confiança, dependendo do nível de perigo que esse aplicativo pode representar para o computador.

   O Kaspersky Endpoint Security coloca um aplicativo em um grupo de confiança para os componentes Firewall e Prevenção de Intrusão do Host. Você não pode alterar o grupo de confiança apenas para o Firewall ou Prevenção de Intrusão do Host.

   Se você se recusou a participar do KSN ou não há rede, o Kaspersky Endpoint Security coloca o aplicativo em um grupo de confiança, dependendo das configurações do componente Prevenção de Intrusão do Host. Após receber a reputação do aplicativo da KSN, o grupo de confiança pode ser alterado automaticamente.

4. Bloqueia as ações do aplicativo, dependendo do grupo de confiança. Por exemplo, aplicativos do grupo de confiança *Alta restrição* têm acesso negado aos módulos do sistema operacional.

Na próxima vez em que o aplicativo for iniciado, a Prevenção de Intrusão do Host verificará sua integridade. Se o aplicativo não for alterado, o componente usará os direitos atuais do aplicativo para ele. Se o aplicativo foi modificado, o Kaspersky Endpoint Security o analisará como se estivesse sendo iniciado pela primeira vez.

Parâmetro	Descrição
Direitos de aplicativos	Tabela de aplicativos que são monitorados pelo componente de Prevenção de Intrusão do Host. Os Aplicativos são atribuídos a grupos de confiança. Um grupo confiável define os direitos aos quais o Kaspersky Endpoint Security se refere ao controlar a atividade do aplicativo. Você pode selecionar um aplicativo em uma única lista de todos os aplicativos instalados nos computadores sob a influência de uma política e adicionar o aplicativo a um grupo de confiança. Os direitos de acesso ao aplicativo são apresentados nas seguintes tabelas: • **Registro do sistema e arquivos**. Tabela de direitos de acesso para recursos do sistema operacional e dados pessoais para aplicativos pertencentes ao grupo confiável. • **Direitos**. Tabela de direitos de acesso para processos e recursos do sistema operacional para aplicativos pertencentes ao grupo de confiança. • **Regras de rede**. Tabela de regras de rede para aplicativos que fazem parte de um grupo de confiança. De acordo com essas regras, o Firewall regula a atividade de rede de aplicativos. A tabela exibe as regras de rede predefinidas recomendadas pelos especialistas da Kaspersky. Essas regras de rede foram adicionadas para proteger de maneira ideal o tráfego de rede dos computadores que executam os sistemas operacionais Windows. Não é possível excluir as regras de rede predefinidas.
Recursos protegidos	A tabela contém recursos do computador categorizados. O componente Prevenção de Intrusão do Host monitora tentativas de outros aplicativos de acessar recursos na tabela. Um recurso pode ser uma categoria de registro, um Arquivo ou pasta; ou uma chave do registro.
Grupo de confiança para aplicativos iniciados antes da inicialização do Kaspersky Endpoint Security	Um grupo de confiança no qual o Kaspersky Endpoint Security colocará aplicativos iniciados antes do Kaspersky Endpoint Security.
Atualizar regras para aplicativos anteriormente desconhecidos da KSN	Se a caixa de seleção for marcada, o componente Prevenção de Intrusão do Host atualizará os direitos de aplicativos anteriormente desconhecidos usando o banco de dados do Kaspersky Security Network.
Confiar em aplicativos assinados digitalmente	Caso esta caixa de seleção esteja marcada, o componente de Prevenção de Intrusão do Host colocará os aplicativos com a assinatura digital de fornecedores confiáveis no grupo *Confiável.* *Fornecedores confiáveis* são aqueles fornecedores de software de confiança da Kaspersky. Também é possível adicionar certificados de fornecedores manualmente ao armazenamento de certificados confiáveis. Caso esta caixa de seleção esteja desmarcada, o componente de Prevenção de Intrusão do Host não considerará os aplicativos com assinatura digital como confiáveis e usará outros parâmetros para determinar o grupo de confiança deles.
Excluir regras para aplicativos não iniciados por mais de N dias (de 1 a 90)	Se a caixa de seleção estiver selecionada, o Kaspersky Endpoint Security excluirá automaticamente as informações sobre o aplicativo (grupo de confiança e direitos de acesso) se as seguintes condições forem atendidas: • Você colocou o aplicativo manualmente em um grupo de confiança ou configurou seus direitos de acesso. • O aplicativo não foi iniciado dentro do período definido. Se o grupo confiável e os direitos de um aplicativo forem determinados automaticamente, o Kaspersky Endpoint Security exclui as informações sobre esse aplicativo após 30 dias. Não é possível alterar o período de armazenamento para as informações do aplicativo ou desativar a exclusão automática. Na próxima vez que você iniciar esse aplicativo, o Kaspersky Endpoint Security analisará o aplicativo como se estivesse iniciando-o pela primeira vez.
Grupo de confiança para aplicativos não incluídos em outros grupos	Os itens nesta lista suspensa determinam a qual grupo de confiança o Kaspersky Endpoint Security atribuirá um aplicativo desconhecido. Você pode selecionar um dos seguintes itens: • **Baixa restrição**. • **Alta restrição**. • **Não confiável**.

Mecanismo de Remediação

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

Ao reverter a atividade de Malware no sistema operacional, o Kaspersky Endpoint Security processa os seguintes tipos da atividade de Malware:

- **Atividade de arquivo**

  O Kaspersky Endpoint Security executa as seguintes ações:

  - Exclui arquivos executáveis que foram criados por malware (em todas as mídias, exceto unidades de rede).
  - Exclui arquivos executáveis que foram criados por programas infiltrados por malware.
  - Restaura arquivos que foram modificados ou excluídos por malware.

  O recurso de recuperação de arquivo tem algumas limitações.

- **Atividade de registro**

  O Kaspersky Endpoint Security executa as seguintes ações:

  - Exclui chaves do registro que foram criadas pelo malware.
  - Não restaura chaves do registro que foram modificadas ou excluídas pelo malware.

- **Atividade de sistema**

  O Kaspersky Endpoint Security executa as seguintes ações:

  - Encerra os processos que foram iniciados por malware.
  - Encerra os processos nos quais um aplicativo malicioso foi injetado.
  - Não retoma processos que foram interrompidos por malware.

- **Atividade de rede**

  O Kaspersky Endpoint Security executa as seguintes ações:

  - Bloqueia a atividade de rede do malware.
  - Bloqueia a atividade de rede de processos que foram invadidos pelo malware.

Uma reversão das ações do malware pode ser iniciada pelo componente Proteção Contra Ameaças ao Arquivo ou Detecção de Comportamento ou durante uma verificação de malware.

O procedimento de reverter operações de malware afeta um conjunto de dados definido rigidamente. A reversão não tem efeitos adversos no sistema operacional ou na integridade dos dados do computador.

Kaspersky Security Network

	Para melhorar a proteção do computador, o Kaspersky Endpoint 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 Endpoint Security a novas ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos positivos. Caso participe da Kaspersky Security Network, os serviços da KSN fornecem à Kaspersky Endpoint Security informações sobre a reputação dos endereços da Web verificados, além de informações sobre a categoria e a reputação dos arquivos verificados. Para obter mais detalhes sobre a configuração de acesso à KSN, consulte a Ajuda do Kaspersky Security Center.

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 Endpoint 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 Endpoint 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 LAN corporativa é proibida por lei ou restrita pelas políticas de segurança corporativa.

Parâmetro	Descrição
Ativar modo KSN estendido	O *modo KSN estendido* é um modo no qual o Kaspersky Endpoint Security envia dados adicionais para a Kaspersky. O Kaspersky Endpoint Security usa o KSN para detectar ameaças independentemente da posição do botão de alternância.
Ativar modo na nuvem	O *Modo nuvem* refere-se ao modo operacional do aplicativo no qual o Kaspersky Endpoint Security usa uma versão simplificada dos bancos de dados de antivírus. A Kaspersky Security Network oferece suporte ao funcionamento do aplicativo quando bancos de dados de antivírus leves estão em uso. A versão leve dos bancos de dados de antivírus permite usar aproximadamente metade da RAM do computador que, de outra forma, seria usada nos bancos de dados comuns. Se você não participa da Kaspersky Security Network ou se o modo de nuvem está desativado, o Kaspersky Endpoint Security faz o download da versão completa dos bancos de dados antivírus dos servidores da Kaspersky. Se o botão de alternância estiver ativado, o Kaspersky Endpoint Security usará a versão simplificada dos bancos de dados antivírus, o que reduz a carga nos recursos do sistema operacional. O Kaspersky Endpoint Security baixará a versão leve dos bancos de dados antivírus durante a próxima atualização depois que a caixa de seleção for marcada. Se o botão de alternância estiver desativado, o Kaspersky Endpoint Security usará a versão completa dos bancos de dados antivírus. O Kaspersky Endpoint Security baixará a versão completa dos bancos de dados antivírus durante a próxima atualização depois que a caixa de seleção for desmarcada.
Status do computador quando os servidores da KSN estão indisponíveis *(disponível apenas no console do Kaspersky Security Center)*	Os itens nessa lista suspensa determinam o status de um computador no Kaspersky Security Center quando os servidores da KSN estão indisponíveis.
Usar o Servidor de Administração como um servidor proxy da KSN *(disponível apenas no console do Kaspersky Security Center)*	Se a caixa de seleção for marcada, o Kaspersky Endpoint Security usará o serviço Proxy da KSN. Você pode definir as configurações do serviço KSN Proxy nas propriedades do Servidor de Administração.
Usar servidores da Kaspersky Security Network se o servidor proxy da KSN não estiver disponível *(disponível apenas no console do Kaspersky Security Center)*	Se a caixa de seleção for marcada, o Kaspersky Endpoint Security usará os servidores da KSN quando o serviço KSN Proxy estiver indisponível. Os servidores da KSN podem ser localizados no lado da Kaspersky e no lado de terceiros (quando a Kaspersky Private Security Network for usada).

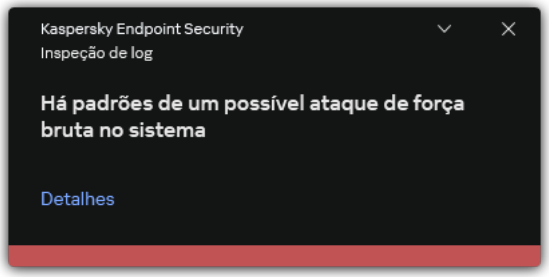
Inspeção do Log

O componente estará disponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para servidores. O componente estará indisponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para estações de trabalho.

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 Endpoint 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* (veja a figura abaixo).

Caso queira usar a Inspeção de Log, certifique-se de que as configurações de segurança da política de auditoria estejam definidas e que o sistema esteja registrando os eventos relevantes (para mais informações, consulte o site de suporte técnico da Microsoft.).



Notificação de Inspeção de Log

Configurações de Inspeção de Log

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.

Anticryptor

O componente Anticryptor analisa a atividade em pastas compartilhadas. Se esta atividade combinar com uma assinatura de fluxo de comportamento que é típica para a criptografia externa, o Kaspersky Endpoint Security executa a ação selecionada.

O Kaspersky Endpoint Security evita a criptografia externa somente de arquivos localizados na mídia com o sistema de arquivo NTFS e que não são criptografados pelo sistema EFS.

Parâmetro	Descrição
Exclusões por nome ou endereço IP	**Exclusões por nome ou endereço IP**. Lista de computadores dos quais tentativas de criptografar pastas compartilhadas não serão monitoradas. Para aplicar a lista de exclusões de computadores da proteção de pastas compartilhadas contra criptografia externa, você deve ativar a auditoria de logon na política de auditoria de segurança do Windows. A auditoria de logon está desativada por padrão. Para obter mais informações sobre a política de auditoria de segurança do Windows, visite o Site da Microsoft. **Exclusões por máscara**. Exclusões do escopo de proteção. 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, a 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. 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. • `?` (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.
Ação ao detectar ameaça	• **Informar**. Caso essa opção esteja selecionada, ao detectar uma tentativa de modificação de arquivos em pastas compartilhadas, o Kaspersky Endpoint Security adicionará as informações sobre a tentativa na lista de ameaças ativas, adicionará uma entrada nos relatórios da interface do aplicativo local e enviará as informações sobre a atividade maliciosa detectada ao Kaspersky Security Center. • **Bloquear conexão por (min) N min**. Caso esta opção seja selecionada, ao detectar uma tentativa de modificação dos arquivos em pastas compartilhadas, o Kaspersky Endpoint Security bloqueia o acesso à modificação de arquivo 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 (min) N min** seja selecionada, os arquivos modificados são restaurados a partir das cópias de backup.
Escopo de proteção	O *escopo de proteção* é uma lista de caminhos para pastas compartilhadas nas quais o Kaspersky Endpoint Security monitora a atividade do arquivo. O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara. Por padrão, o aplicativo identifica automaticamente as pastas compartilhadas e monitora a atividade de arquivos em todas as pastas.

Controle da Web

O Controle da Web gerencia o acesso dos usuários aos recursos da Web. Isso ajuda a reduzir o tráfego e o uso inadequado do tempo de trabalho. Quando um usuário tenta abrir um site proibido pelo Controle da Web, o Kaspersky Endpoint Security bloqueará o acesso e exibirá um aviso (veja a figura abaixo).

Para usar o Controle da Web, você deve concluir a configuração inicial do aplicativo:

- Para o monitoramento de tráfego HTTPS, ative a verificação de conexões criptografadas (ativada por padrão).
- Selecione as portas que o Kaspersky Endpoint Security deve monitorar (por padrão, o aplicativo monitora todas as portas).

- Selecione os aplicativos cujo tráfego você deseja que o Kaspersky Endpoint Security monitore. A maioria dos navegadores já está presente na lista de aplicativos recomendados pela Kaspersky. Se o seu navegador não estiver na lista, adicione-o manualmente.

- Recomendamos injetar um script de interação de página da web no tráfego da Web (por padrão, a injeção de script está desabilitada). Esse script permite o registro de eventos do Controle da Web para o log de eventos do aplicativo, log de eventos do sistema operacional e relatórios.

Métodos de gerenciamento de acesso à sites

O Controle da Web permite que você configure o acesso à sites usando os seguintes métodos:

- **Categoria do site**. Os sites são categorizados de acordo com o serviço de nuvem Kaspersky Security Network, análise heurística e o banco de dados de sites conhecidos (incluídos nos bancos de dados de aplicativos). Por exemplo, é possível restringir o acesso do usuário à categoria *Redes sociais* ou a outras categorias.

- **Tipo de dados**. É possível restringir o acesso dos usuários aos dados de um site e ocultar imagens, por exemplo. O Kaspersky Endpoint Security determina o tipo de dados com base no formato do arquivo e não na sua extensão.

  O Kaspersky Endpoint Security não verifica arquivos dentro de arquivos. Por exemplo, se os arquivos de imagem foram colocados em um arquivo, o Kaspersky Endpoint Security identifica o tipo de dados *Arquivos compactados* e não como *Gráficos*.

- **Endereço individual**. Você pode inserir um endereço web ou usar máscaras.

Você pode usar simultaneamente vários métodos para regular o acesso à sites. Por exemplo, é possível restringir o acesso ao tipo de dado dos *Arquivos dos aplicativos do Office* apenas para a categoria de site *E-mail baseado na Web*.

Regras de acesso de site

O Controle da Web gerencia o acesso do usuário a sites usando *regras de acesso*. Você pode definir as seguintes configurações avançadas para uma regra de acesso à site:

- Usuários aos quais se aplica a regra.

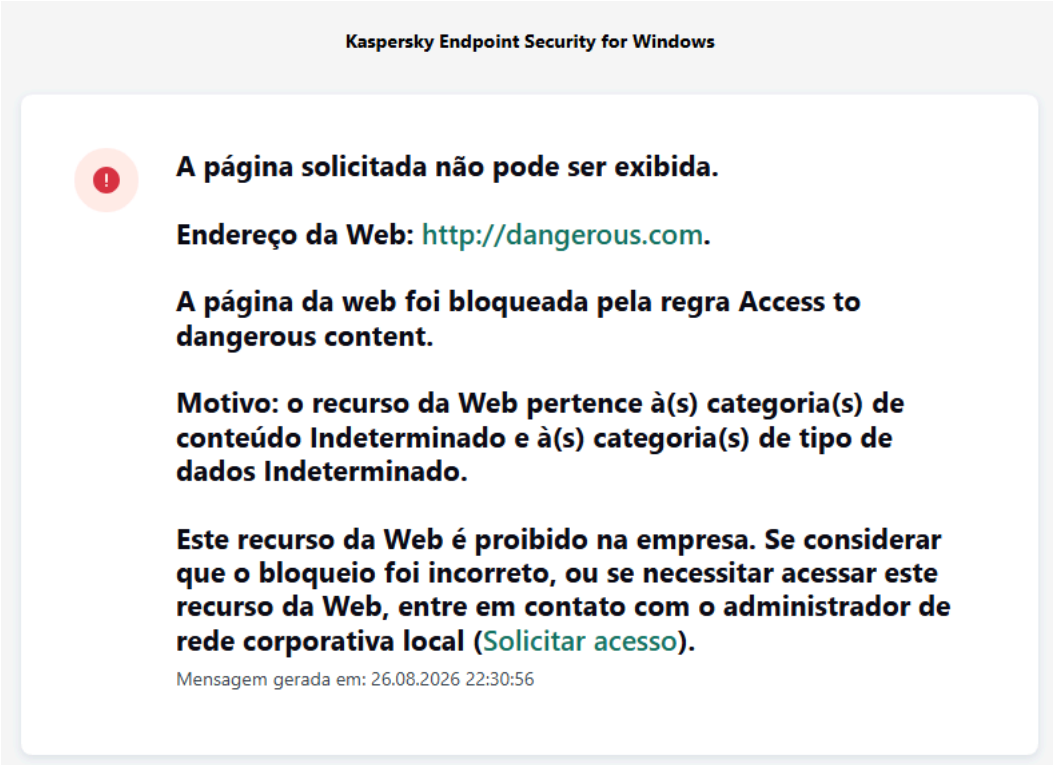
  Por exemplo, é possível restringir o acesso à Internet através de um navegador para todos os usuários da empresa, exceto os do departamento de TI.

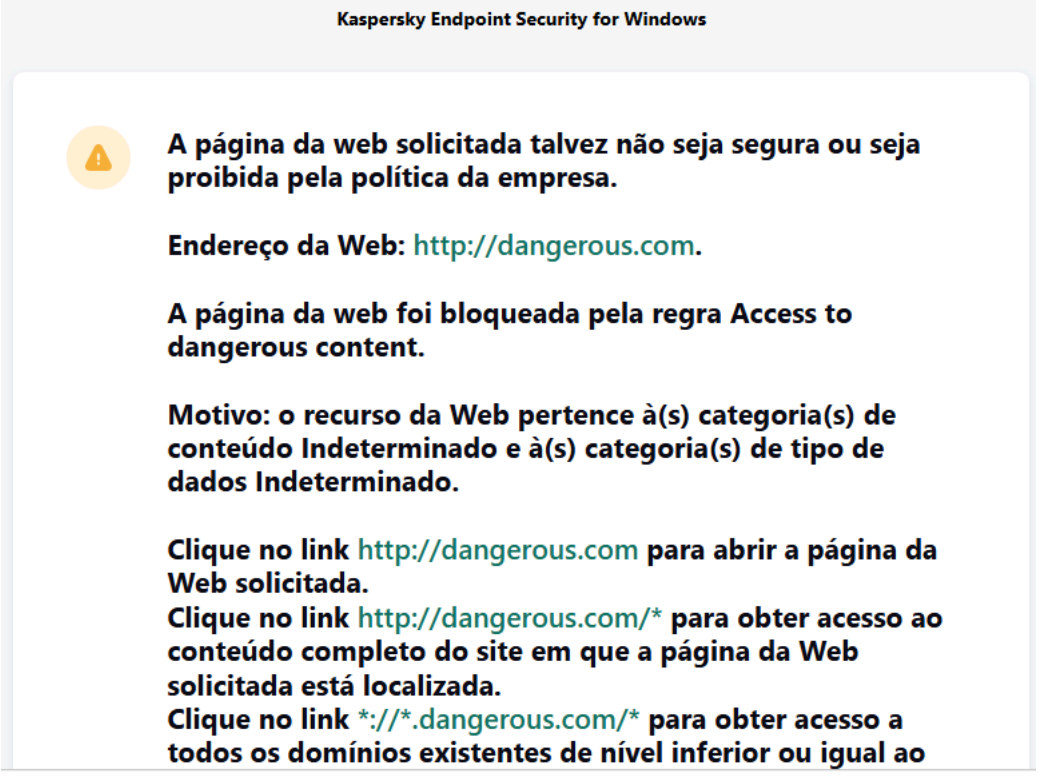
- Agendamento da regra.

  Por exemplo, é possível restringir o acesso à Internet por meio de um navegador apenas durante o horário de trabalho.

Prioridades da regra de acesso

Cada regra tem uma prioridade. Quanto mais alta uma regra estiver na lista, mais alta será sua prioridade. Se um site foi adicionado a várias regras, o Controle da Web regula o acesso ao site com base na regra com a maior prioridade. Por exemplo, o Kaspersky Endpoint Security pode identificar um portal corporativo como uma rede social. Para restringir o acesso às redes sociais e dar acesso ao portal corporativo, crie duas regras: uma regra de bloqueio para a categoria *Redes sociais* e uma regra de permissão para o portal corporativo. A regra de acesso ao portal web corporativo deve ter uma prioridade maior do que a regra de acesso para redes sociais.





Mensagens de Controle da Web

Parâmetro	Descrição
Regras de acesso aos recursos da Web	Lista contendo regras de acesso de recurso da Web. Cada regra tem uma prioridade. Quanto mais alta uma regra estiver na lista, mais alta será sua prioridade. Se um site foi adicionado a várias regras, o Controle da Web regula o acesso ao site com base na regra com a maior prioridade.
Regra padrão	A *Regra padrão* é uma regra de acesso a recursos da Web que não são abrangidos por nenhuma outra regra. As seguintes opções estão disponíveis: • **Permitir tudo, exceto a lista de regras**, também conhecida como modo de lista de bloqueio para sites proibidos. • **Negar tudo, exceto a lista de regras**, também conhecida como modo de lista de permissão para sites permitidos.
Encerrar as sessões de navegador ativas após a aplicação da regra	Caso a caixa de seleção seja marcada, o Controle da Web encerrará a conexão com os recursos da Web bloqueados imediatamente após a aplicação da política. O navegador interrompe imediatamente o download de dados da página da Web. Quando o usuário atualiza a página da Web ou vai para outra página da Web proibida, o aplicativo exibe um aviso. O Controle da Web permite a desconexão imediata de recursos da Web somente em navegadores da Web. Para outros aplicativos, o Controle da Web apenas restringe novas conexões. Caso a caixa de seleção esteja desmarcada, o Controle da Web restringirá somente as novas conexões aos recursos da Web proibidos. O Controle da Web não encerra conexões ativas.
Modelos	**Aviso**. O campo de entrada consiste em um modelo da mensagem que é exibida se uma regra para avisar sobre tentativas de acessar um recurso da Web não desejado for acionada. **Mensagem sobre bloqueio**. O campo de entrada contém o modelo da mensagem que aparece se uma regra que bloqueia o acesso a um recurso da Web for acionada. **Mensagem para o administrador**. O modelo da mensagem a ser enviada ao administrador de LAN caso o usuário considere que o bloqueio seja um erro. Depois que o usuário solicitar o acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio de acesso à página da Web para o administrador**. A descrição do evento contém uma mensagem ao administrador com variáveis substituídas. É possível visualizar esses eventos no console do Kaspersky Security Center com o uso da seleção de eventos predefinida **Pedidos de usuário**. Caso sua organização não tenha o Kaspersky Security Center implantado ou não haja conexão com o Servidor de Administração, o aplicativo enviará uma mensagem ao administrador para o endereço de e-mail especificado. Variáveis especiais são fornecidas para gerenciar o modelo de mensagem (por exemplo, `%USER_NAME%`). As variáveis permitem que um mesmo modelo de mensagem seja utilizado em diferentes computadores.
Criar log de abertura de páginas autorizadas	O Kaspersky Endpoint Security registra dados em visitas a todos os sites, incluindo sites permitidos. O Kaspersky Endpoint Security envia eventos para o Kaspersky Security Center, para o log local do Kaspersky Endpoint Security e para o log de eventos do Windows. Para monitorar a atividade da Internet do usuário, você tem que definir as configurações para salvar eventos. Navegadores compatíveis com a função de monitoramento: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. O monitoramento da atividade do usuário não funciona em outros navegadores. O monitoramento da atividade da Internet do usuário pode exigir mais recursos do computador quando descriptografar tráfego HTTPS.

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.

Se o Controle de dispositivos estiver ativado, o aplicativo retransmitirá as informações sobre os dispositivos conectados ao Kaspersky Security Center. É possível visualizar a lista de dispositivos conectados no Kaspersky Security Center na pasta **Avançado** → **Repositórios** → **Hardware**.

Níveis de acesso do dispositivo

O Controle de Dispositivos controla o acesso nos seguintes níveis:

- **Tipo de dispositivo**. Por exemplo, impressoras, unidades removíveis e unidades de CD/DVD.

  Você pode configurar o acesso do dispositivo da seguinte forma:

  - Permitir – ✓.
  - Bloquear – ⊘.
  - Por regras (apenas impressoras e dispositivos portáteis) – .
  - Depende do barramento de conexão (exceto Wi-Fi) – .
  - Bloquear com exceções (somente Wi-Fi) – .

- **Barramento de conexão**. Um *barramento de conexão* é uma interface usada para conectar dispositivos ao computador (por exemplo, USB ou FireWire). Se o modo **Depende do barramento de conexão** estiver selecionado para o tipo de dispositivo, o aplicativo permitirá ou negará o acesso ao dispositivo, dependendo da interface de conexão (por exemplo, USB).

  Você pode configurar o acesso do dispositivo da seguinte forma:

  - Permitir – ✓.
  - Bloquear – ⊘.

- **Dispositivos confiáveis**. *Dispositivos confiáveis* aqueles aos quais os usuários especificados têm acesso total a qualquer momento.

  Você pode adicionar dispositivos confiáveis com base nos seguintes dados:

  - **Dispositivos por ID**. Cada dispositivo possui um identificador exclusivo (Hardware ID ou HWID). É possível visualizar o ID nas propriedades do dispositivo usando ferramentas do sistema operacional. Exemplo de ID de dispositivo: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Adicionar dispositivos por ID é conveniente se você deseja adicionar vários dispositivos específicos.

  - **Dispositivos por modelo**. Cada dispositivo tem um Vendor ID (VID) e um Product ID (PID). É possível visualizar os IDs nas propriedades do dispositivo usando ferramentas do sistema operacional. Modelo para inserir o VID e o PID: `VID_1234&PID_5678`. Adicionar dispositivos por modelo é conveniente se você usar dispositivos de um determinado modelo em sua empresa. Dessa forma, você pode adicionar todos os dispositivos deste modelo.

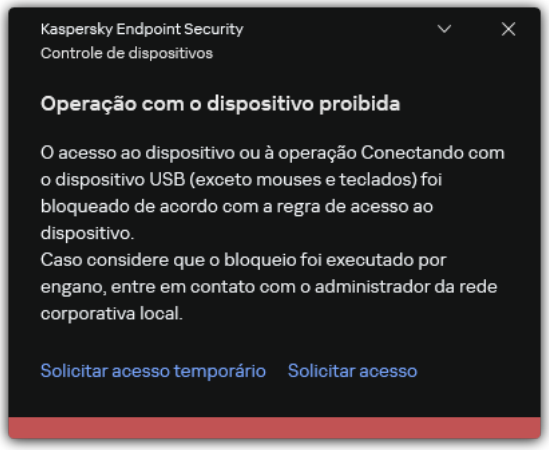
  - **Dispositivos por máscara de ID**. Se você estiver usando vários dispositivos com IDs semelhantes, poderá adicionar dispositivos à lista confiável usando máscaras. O caractere `*` substitui qualquer conjunto de caracteres. O Kaspersky Endpoint Security não suporta o caractere `?` ao inserir uma máscara. Por exemplo, `WDC_C*`.

  - **Dispositivos por modelo de máscara**. Se você estiver usando vários dispositivos com VIDs ou PIDs semelhantes (por exemplo, dispositivos do mesmo fabricante), poderá adicionar dispositivos à lista confiável usando máscaras. O caractere `*` substitui qualquer conjunto de caracteres. O Kaspersky Endpoint Security não suporta o caractere `?` ao inserir uma máscara. Por exemplo, `VID_05AC&PID_*`.

O Controle de Dispositivos regula o acesso do usuário a dispositivos usando *regras de acesso*. O Controle de Dispositivos também permite salvar eventos de conexão/desconexão do dispositivo. Para salvar eventos, é necessário configurar o registro de eventos em uma política.

Se o acesso a um dispositivo depender do barramento de conexão (o status), o Kaspersky Endpoint Security não salva eventos de conexão/desconexão de dispositivos. Para permitir que o Kaspersky Endpoint Security salve eventos de conexão/desconexão de dispositivos, conceda o acesso ao tipo correspondente de dispositivo (o status) ou adicione o dispositivo à lista confiável.

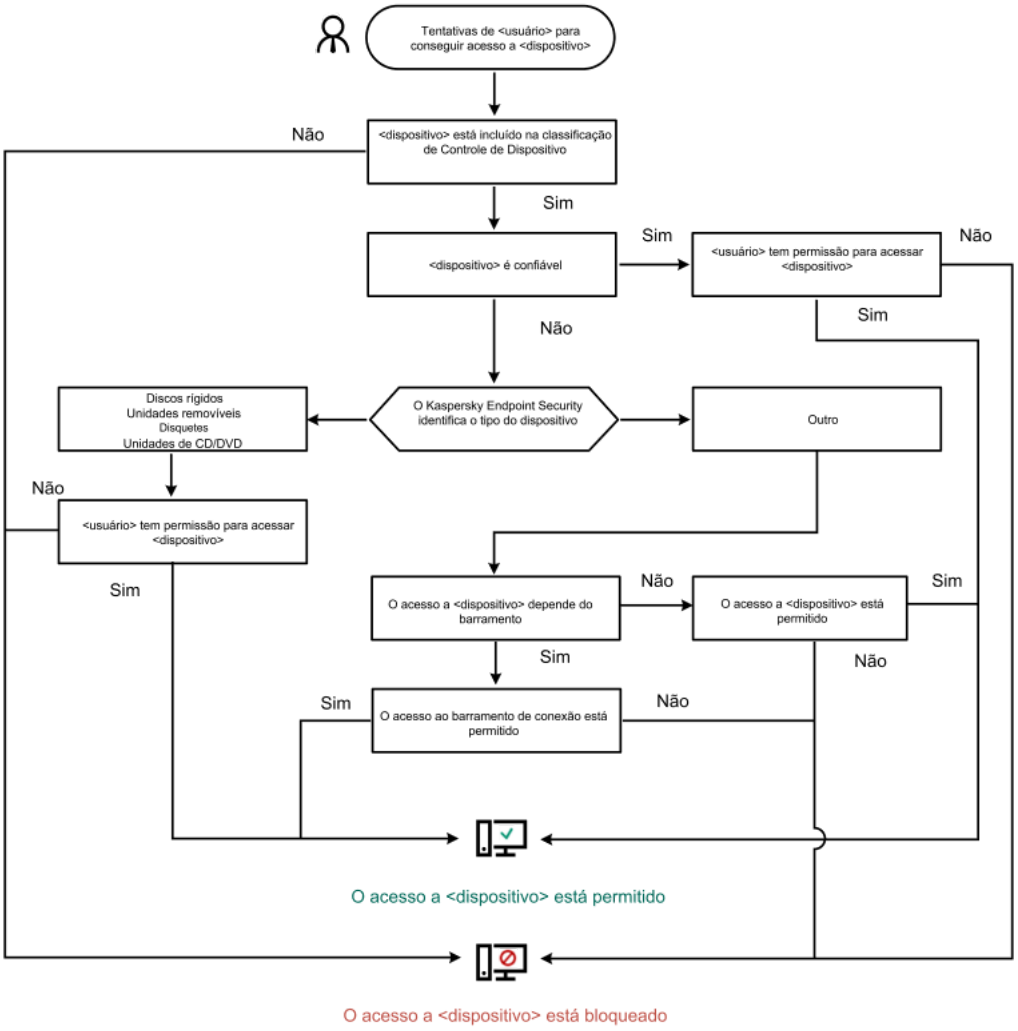
Quando um dispositivo que estiver bloqueado pelo Controle de Dispositivos for conectado ao computador, o Kaspersky Endpoint Security vai bloquear o acesso e exibir uma notificação (veja a figura abaixo).



Notificação do Controle de Dispositivos

Algoritmo de operação do Controle de Dispositivos

O Kaspersky Endpoint Security decide se permite ou não o acesso a um dispositivo quando o usuário o conecta ao computador (veja a figura a seguir).



Algoritmo de operação do Controle de Dispositivos

Se um dispositivo estiver conectado e o acesso for permitido, você poderá editar a regra de acesso e bloquear o acesso. Nesse caso, na próxima vez que alguém tentar acessar o dispositivo (como exibir a árvore de pastas ou executar operações de leitura ou gravação), o Kaspersky Endpoint Security bloqueará o acesso. O dispositivo que não está no sistema de arquivos é bloqueado somente na próxima vez que for conectado.

Se um usuário do computador com Kaspersky Endpoint Security instalado precisar solicitar acesso a um dispositivo que o usuário acredita estar bloqueado por engano, envie ao usuário as instruções de acesso a solicitação.

Parâmetro	Descrição
Permitir solicitações de acesso temporário *(disponível apenas no console do Kaspersky Security Center)*	Se a caixa de seleção for marcada, o botão **Solicitar acesso** estará disponível pela interface local do Kaspersky Endpoint Security. Com o uso desse botão, o usuário pode solicitar o acesso temporário a um dispositivo bloqueado.
Dispositivos e redes Wi-Fi	Esta tabela contém todos os tipos possíveis de dispositivos segundo a classificação do componente Controle de Dispositivos, inclusive os seus respetivos status de acesso.
Barramentos de conexão	Uma lista de todos os barramentos de conexão disponíveis segundo a classificação do componente Controle de Dispositivos, inclusive os seus respetivos status de acesso. O Kaspersky Endpoint Security permite ou nega o acesso aos dispositivos, dependendo do tipo de barramento de conexão, caso o modo **Depende do barramento de conexão** seja selecionado.
Dispositivos confiáveis	Lista de dispositivos e usuários confiáveis aos quais é concedido acesso a esses dispositivos.
Mesclar valores ao herdar *(disponível apenas no console do Kaspersky Security Center)*	Isso mescla a lista de dispositivos confiáveis nas políticas pai e filho do Kaspersky Security Center. Para mesclar listas, a política filho deve ser configurada para herdar as configurações da política pai do Kaspersky Security Center. Se a caixa de seleção estiver marcada, os itens da lista da política pai do Kaspersky Security Center serão exibidos nas políticas filho. Desta forma, é possível, por exemplo, criar uma lista consolidada de dispositivos confiáveis para toda a empresa. Os itens de lista herdados em uma política filho não podem ser excluídos ou editados. Os itens na lista de dispositivos confiáveis que são mesclados durante a herança podem ser excluídos e editados apenas na política pai. Você pode adicionar, editar ou excluir itens da lista nas políticas de nível inferior. Se os itens nas listas da política pai e filho corresponderem, esses itens serão exibidos como o mesmo item da política pai. Se a caixa de seleção não estiver marcada, os itens das listas não serão mesclados ao herdar as configurações das políticas do Kaspersky Security Center. Essa funcionalidade também permite mesclar listas em perfis de política. Para mesclar listas, no perfil de prioridade mais alta, ative a herança de configurações de um perfil de prioridade mais baixa. Para obter mais detalhes sobre as prioridades de perfil da política, consulte a ajuda do Kaspersky Security Center.
Antibridging	O antibridging inibe a criação de pontes de rede, impedindo o estabelecimento simultâneo de várias conexões de rede para um computador. Isso permite que você proteja uma rede corporativa de ataques a redes não protegidas e não autorizadas. O Antibridging bloqueia o estabelecimento de várias conexões de acordo com as prioridades dos dispositivos. Quanto mais alto um dispositivo estiver na lista, maior será sua prioridade. Se uma conexão ativa e uma nova conexão forem do mesmo tipo (por exemplo, Wi-Fi), o Kaspersky Endpoint Security bloqueia a conexão ativa e permite a nova conexão. Se uma conexão ativa e uma nova conexão forem de tipos diferentes (por exemplo, um adaptador de rede e Wi-Fi), o Kaspersky Endpoint Security bloqueia a conexão com a prioridade mais baixa e permite a conexão com a prioridade mais alta. O Antibridging oferece suporte à operação com os seguintes tipos de dispositivos: adaptador de rede, Wi-Fi e modem.
Modelos de mensagem	**Mensagem sobre bloqueio**. Modelo da mensagem que é exibida quando um usuário tenta acessar um dispositivo bloqueado. Essa mensagem também é exibida quando um usuário tenta executar uma operação no conteúdo do dispositivo que foi bloqueado para esse usuário. **Mensagem para o administrador**. Um modelo da mensagem que é enviada ao administrador da rede local quando o usuário acredita que o acesso ao dispositivo está bloqueado ou uma operação com o conteúdo do dispositivo é proibida por engano. Depois que o usuário solicitar o acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio de acesso ao dispositivo para o administrador**. A descrição do evento contém uma mensagem ao administrador com variáveis substituídas. É possível visualizar esses eventos no console do Kaspersky Security Center com o uso da seleção de eventos predefinida **Pedidos de usuário**. Caso sua organização não tenha o Kaspersky Security Center implantado ou não haja conexão com o Servidor de Administração, o aplicativo enviará uma mensagem ao administrador para o endereço de e-mail especificado.

Controle de aplicativos

O Controle de aplicativos gerencia a inicialização de aplicativos nos computadores dos usuários. Isso permite que você implemente uma política de segurança corporativa ao usar aplicativos. O Controle de aplicativos também reduz o risco de infecção do computador, restringindo o acesso aos aplicativos.

A configuração do Controle de aplicativos consiste nas seguintes etapas:

1. Criar categorias de aplicativos.

   O administrador cria categorias de aplicativos que o administrador deseja gerenciar. As categorias de aplicativos destinam-se a todos os computadores da rede corporativa, independentemente dos grupos de administração. Para criar uma categoria, você pode usar os seguintes critérios: Categoria KL (por exemplo, *Navegadores* ou outra categoria), hash de arquivo, fornecedor do aplicativo e outros critérios.

2. Criar regras de Controle de aplicativos.

   O administrador cria regras de Controle de aplicativos na política para o grupo de administração. A regra inclui as categorias de aplicativos e o status de inicialização dos aplicativos dessas categorias: bloqueados ou permitidos. O administrador pode criar muitas regras. Um aplicativo pode corresponder aos critérios de várias regras. A prioridade da regra de bloqueio é mais alta do que a de permissão. O Kaspersky Endpoint Security verifica se um aplicativo corresponde a uma regra sempre que for iniciado. O Kaspersky Endpoint Security compara sequencialmente o aplicativo com todas as regras de Controle de Aplicativos.

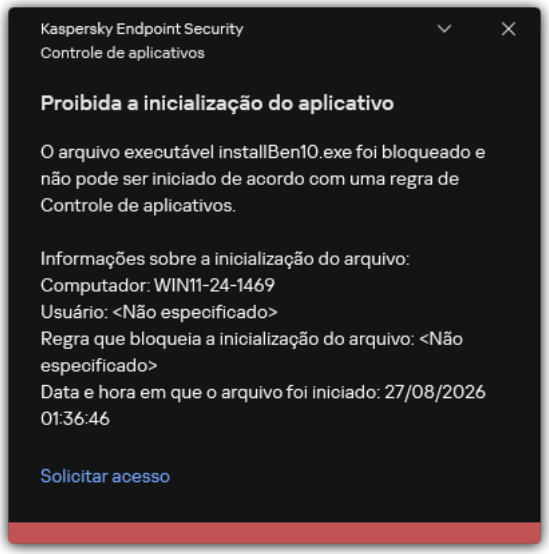
3. Selecionar o modo de Controle de aplicativos.

   O administrador escolhe o modo para trabalhar com aplicativos que não estão incluídos em nenhuma das regras: (Lista de bloqueio e de permissão de aplicativos).

Quando um usuário tenta iniciar um aplicativo proibido, o Kaspersky Endpoint Security impede o início do aplicativo e exibe uma notificação (veja a figura abaixo).

Um *modo de teste* é fornecido para verificar a configuração do Controle de aplicativos. Nesse modo, o Kaspersky Endpoint Security faz o seguinte:

- Permite a inicialização de aplicativos, inclusive os proibidos.
- Mostra uma notificação sobre a inicialização de um aplicativo proibido e adiciona informações ao relatório no computador do usuário.
- Envia dados sobre a inicialização de aplicativos proibidos ao Kaspersky Security Center.



Notificações do Controle de aplicativos

Modos de operação do Controle de aplicativos

O componente Controle de aplicativos opera em dois modos:

- **Lista de bloqueio**. Nesse modo, o Controle de aplicativos permite que os usuários iniciem todos os aplicativos, exceto os que são proibidos nas regras de Controle de aplicativos.

  Esse modo de Controle de aplicativos é ativado por padrão.

- **Lista de permissão**. Nesse modo, o Controle de aplicativos impede que os usuários iniciem aplicativos, exceto os que são permitidos e não proibidos nas regras de Controle de aplicativos.

  Se as regras de permissão do Controle de aplicativos estiverem totalmente configuradas, o componente bloqueará a inicialização de todos os novos aplicativos que não foram verificados pelo administrador da LAN, enquanto permite a operação do sistema operacional e dos aplicativos confiáveis nos quais os usuários confiam no trabalho.

  Você pode ler as recomendações sobre a configuração de regras de Controle de aplicativos no modo de lista de permissão.

O Controle de aplicativos pode ser configurado para operar nesses modos, usando a interface local do Kaspersky Endpoint Security e usando o Kaspersky Security Center.

No entanto, o Kaspersky Security Center oferece ferramentas que não estão disponíveis na interface local do Kaspersky Endpoint Security, como as ferramentas necessárias para as seguintes tarefas:

- Criar categorias de aplicativos.

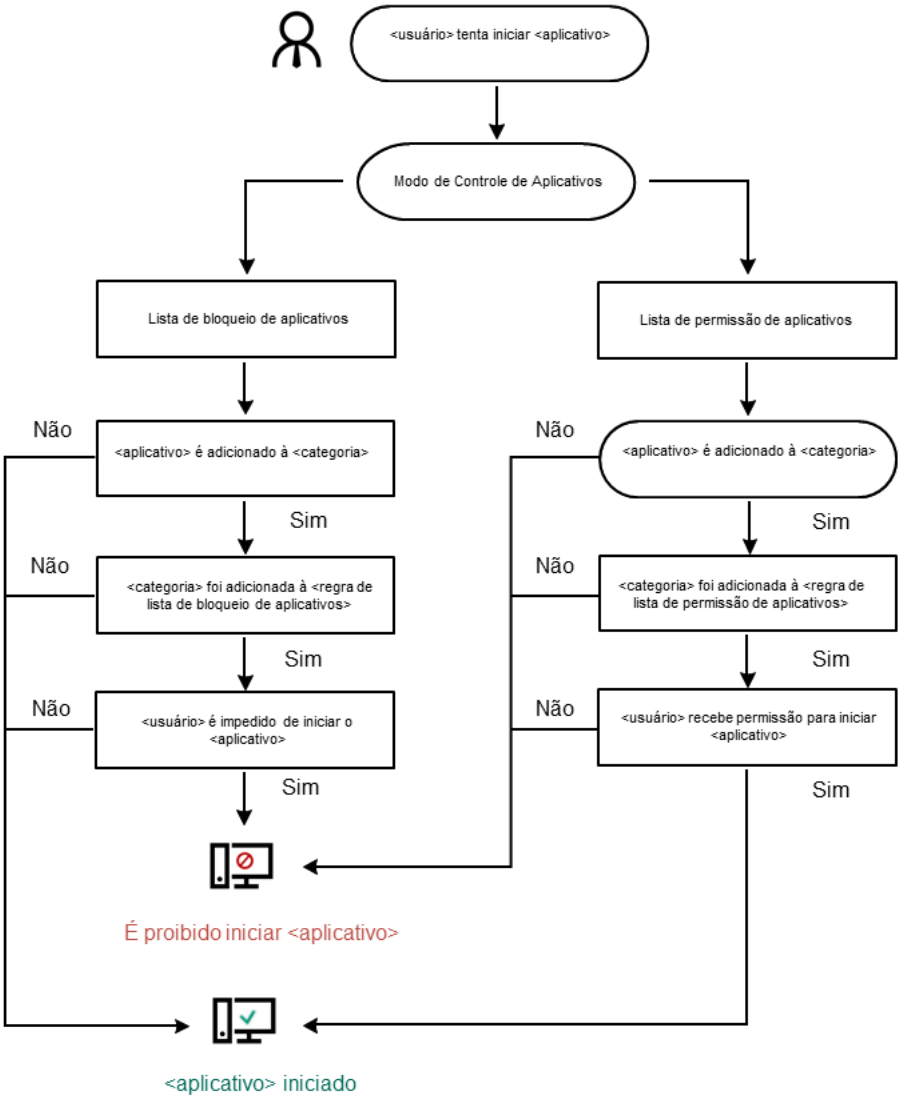
  As regras de Controle de aplicativos criadas no console de administração do Kaspersky Security Center são baseadas nas categorias de aplicativos personalizadas e não nas condições de inclusão e exclusão, como é o caso da interface local do Kaspersky Endpoint Security.

- Receber informações sobre os aplicativos que estão instalados nos computadores da rede local corporativa.

É por isso que é recomendável usar o Kaspersky Security Center para configurar a operação do componente Controle de aplicativos.

Algoritmo de operação do controle de aplicativos

O Kaspersky Endpoint Security usa um algoritmo para tomar uma decisão sobre iniciar um aplicativo (veja a figura abaixo).



Algoritmo de operação do controle de aplicativos

Parâmetro	Descrição
Ação bloqueada por regras durante inicialização de aplicativos	**Aplicar regras**. O Kaspersky Endpoint Security gerencia a inicialização de aplicativos de acordo com o modo selecionado. **Testar regras**. O Kaspersky Endpoint Security permitirá a inicialização de um aplicativo que esteja bloqueado no modo atual do Controle de Aplicativos, mas registrará informações sobre a sua inicialização no relatório.
Modo Controle de Inicialização de Aplicativos	Você pode escolher uma das seguintes opções: • **Lista de bloqueio**. Caso esta opção seja selecionada, o Controle de aplicativos permitirá a todos os usuários iniciar qualquer aplicativo, exceto nos casos quando os aplicativos satisfazem as condições de regras de bloqueio do Controle de aplicativos. • **Lista de permissão**. Caso esta opção seja selecionada, o Controle de aplicativos impedirá todos os usuários de iniciar qualquer aplicativo, exceto nos casos quando os aplicativos satisfazem as condições de regras de permissão do Controle de aplicativos. Quando o modo **Lista de permissão** é selecionado, duas regras de Controle de Aplicativos são automaticamente criadas: • **Golden Image**. • **Atualizadores confiáveis**. Você não pode editar as configurações de ou apagar regras automaticamente criadas. Você pode ativar ou desativar estas regras.
Monitorar o carregamento de módulos DLL	Se a caixa de seleção for marcada, o Kaspersky Endpoint Security controlará o carregamento de módulos DLL quando os usuários tentarem iniciar aplicativos. As informações sobre o módulo DLL e o aplicativo que carregou este módulo DLL são registradas no relatório. Ao ativar o controle sobre o carregamento de módulos DLL e drivers, certifique-se de que uma das regras a seguir seja ativada nas configurações do Controle de Aplicativos: a regra **Golden Image** padrão ou outra regra que contenha a categoria KL de "**Golden Image\Certificados confiáveis**" e garanta que os módulos DLL e drivers confiáveis sejam carregados antes da inicialização do Kaspersky Endpoint Security. A ativação do controle de carregamento de módulos DLL e drivers quando a regra **Golden Image** é desativada pode causar instabilidade no sistema operacional. O Kaspersky Endpoint Security monitora somente os módulos DLL e drivers carregados desde que a caixa de seleção foi marcada. Depois de marcar a caixa de seleção, é recomendável reiniciar o computador para garantir que o aplicativo monitore todos os módulos DLL e drivers, incluindo aqueles carregados antes do Kaspersky Endpoint Security iniciar.
Usar verificação rigorosa de assinatura digital	É possível selecionar um certificado como uma condição de acionamento para uma regra de Controle de Aplicativos. Se essa caixa de seleção estiver marcada, o Kaspersky Endpoint Security aplicará regras somente a aplicativos assinados com certificados do armazenamento de certificados do sistema confiável. Os aplicativos assinados com esses certificados também são considerados confiáveis pelos componentes de proteção, por exemplo, a tarefa *Verificação de malware*. No entanto, caso um certificado de outro armazenamento seja especificado em uma regra de controle de aplicativos, o Kaspersky Endpoint Security não aplicará tal regra. Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security aplicará regras a aplicativos assinados por um certificado do armazenamento de certificados raiz confiáveis do Windows. Esses aplicativos não fazem parte da zona confiável. Os componentes de proteção monitoram a atividade desses aplicativos.
Modelos de mensagens sobre o bloqueio de aplicativo	**Mensagem sobre bloqueio**. Modelo da mensagem que é exibida quando uma regra de Controle de Aplicativos que impede a inicialização de um aplicativo é acionada. **Mensagem para o administrador**. Modelo da mensagem que um usuário pode enviar ao administrador da rede local corporativa, se o usuário acreditar que um aplicativo foi bloqueado por engano. Depois que o usuário solicitar o acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio de inicialização do aplicativo para o administrador**. A descrição do evento contém uma mensagem ao administrador com variáveis substituídas. É possível visualizar esses eventos no console do Kaspersky Security Center com o uso da seleção de eventos predefinida **Pedidos de usuário**. Caso sua organização não tenha o Kaspersky Security Center implantado ou não haja conexão com o Servidor de Administração, o aplicativo enviará uma mensagem ao administrador para o endereço de e-mail especificado.

Controle Adaptativo de Anomalias

O componente estará disponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para computadores pessoais. O componente estará indisponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para servidores.

O componente de Controle Adaptativo de Anomalias monitora e bloqueia ações suspeitas que não são típicas dos computadores em uma rede empresarial. O Controle Adaptativo de Anomalias usa um conjunto de regras para rastrear comportamentos incomuns (por exemplo, a regra *Inicialização do Microsoft PowerShell pelo aplicativo Office*). As regras são criadas pelos especialistas da Kaspersky com base em cenários típicos de atividade maliciosa. Você pode configurar como o Controle Adaptativo de Anomalias manipula cada regra e, por exemplo, permitir a execução de scripts do PowerShell que automatizam determinadas tarefas de fluxo de trabalho. Kaspersky Endpoint Security atualiza o conjunto de regras junto com os bancos de dados do aplicativo. As atualizações para os conjuntos de regras devem ser confirmadas manualmente.

Configurações de Controle Adaptativo de Anomalias

A configuração do controle Adaptativo de Anomalias adaptável consiste nas seguintes etapas:

1. Treinamento do Controle Adaptativo de Anomalias.

   Depois de ativar o Controle Adaptativo de Anomalias, suas regras funcionam *modo de treinamento*. Durante o treinamento, o Controle Adaptativo de Anomalias monitora o acionamento de regras e envia os eventos do Kaspersky Security Center. Cada regra tem sua própria duração do modo de treinamento. A duração do modo de treinamento é definida pelos especialistas da Kaspersky. Normalmente, o modo de treinamento é ativado por duas semanas.

   Se uma regra não foi acionada durante o treinamento, o Controle Adaptativo de Anomalias considerará as ações associadas a essa regra como incomuns. O Kaspersky Endpoint Security irá bloquear todas as ações associadas a essa regra.

   Caso uma regra tenha sido acionada durante o treinamento, o Kaspersky Endpoint Security registra os eventos no relatório de acionamento da regra e no repositório do **Acionadores de regra no estado de Treinamento inteligente**.

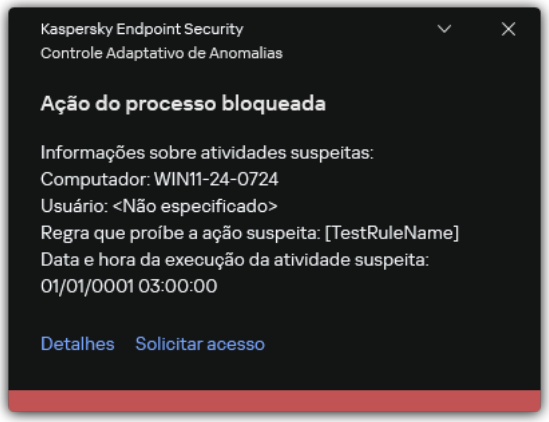
2. Analisando o relatório de acionamento de regras.

   O administrador analisa o relatório de acionamento de regra ou o conteúdo do repositório **Acionadores de regra no estado de Treinamento inteligente**. Em seguida, o administrador pode selecionar o comportamento do Controle Adaptativo de Anomalias quando a regra for acionada: bloquear ou permitir. O administrador também pode continuar a monitorar como a regra funciona e estender a duração do modo de treinamento. Se o administrador não realizar nenhuma ação, o aplicativo também continuará a funcionar no modo de treinamento. O período do modo de treinamento é reiniciado.

O Controle Adaptativo de Anomalias é configurado em tempo real por meio dos seguintes canais:

- O Controle Adaptativo de Anomalias inicia automaticamente o bloqueio das ações associadas às regras que nunca foram acionadas no modo de treinamento.
- O Kaspersky Endpoint Security adiciona novas regras ou remove as obsoletas.
- O administrador configura a operação do Controle Adaptativo de Anomalias após revisar o relatório de acionamento de regras e o conteúdo do repositório **Acionadores de regra no estado de Treinamento inteligente**. Recomendamos verificar o relatório sobre o acionamento de regras e o conteúdo do armazenamento **Acionadores de regra no estado de Treinamento inteligente**.

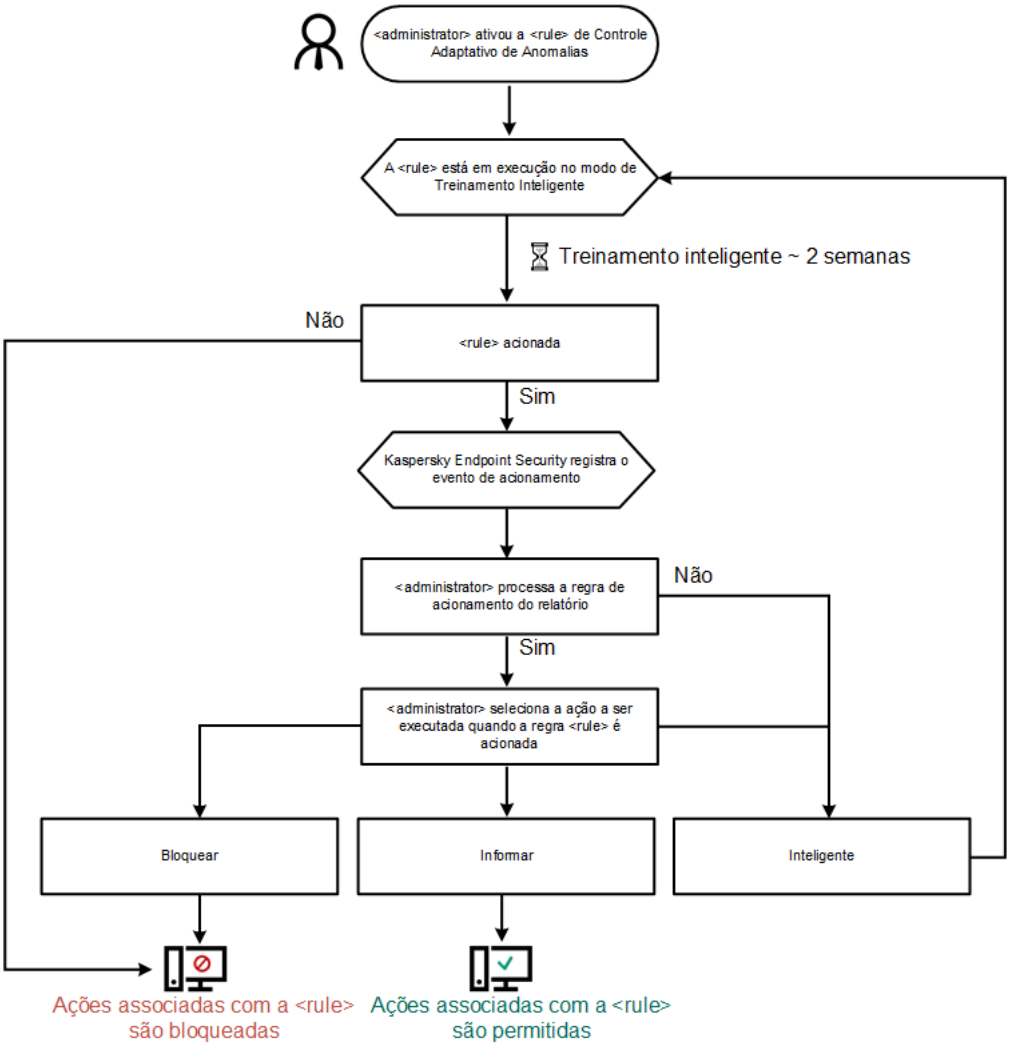
Quando um aplicativo malicioso tenta executar uma ação, o Kaspersky Endpoint Security bloqueia a ação e exibe uma notificação (veja a figura abaixo).



Notificações do Controle Adaptativo de Anomalias

Algoritmo operacional do Controle Adaptativo de Anomalias

O Kaspersky Endpoint Security decide se permite ou bloqueia uma ação associada a uma regra com base no algoritmo a seguir (veja a figura abaixo).



Algoritmo operacional do Controle Adaptativo de Anomalias

Configurações do componente Controle Adaptativo de Anomalias

Parâmetro	Descrição
Relatório sobre o estado das regras de Controle Adaptativo de Anomalias *(disponível apenas no console do Kaspersky Security Center)*	Este relatório contém informações sobre o status das regras de detecção do Controle Adaptativo de Anomalias (por exemplo, *Desativado* ou *Bloquear*). O relatório é gerado para todos os grupos de administradores.
Relatório sobre regras de Controle Adaptativo de Anomalias acionadas *(disponível apenas no console do Kaspersky Security Center)*	Este relatório contém informações sobre ações atípicas detectadas pelo Controle Adaptativo de Anomalias. O relatório é gerado para todos os grupos de administradores.

Parâmetro	Descrição
Regras	Quadro de regras do Controle Adaptativo de Anomalias. As regras são criadas pelos especialistas da Kaspersky com base em cenários típicos de atividade maliciosa.
Modelos	**Mensagem sobre bloqueio**. Modelo da mensagem exibida a um usuário quando uma regra do Controle Adaptativo de Anomalias que bloqueia uma ação atípica é acionada. **Mensagem para o administrador**. Modelo da mensagem que pode ser enviada por um usuário ao administrador da rede corporativa local se o usuário considerar o bloqueio como um erro. Depois que o usuário solicitar o acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio de atividade do aplicativo para o administrador**. A descrição do evento contém uma mensagem ao administrador com variáveis substituídas. É possível visualizar esses eventos no console do Kaspersky Security Center com o uso da seleção de eventos predefinida **Pedidos de usuário**. Caso sua organização não tenha o Kaspersky Security Center implantado ou não haja conexão com o Servidor de Administração, o aplicativo enviará uma mensagem ao administrador para o endereço de e-mail especificado.

Monitor de integridade do sistema

O componente estará disponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para servidores. O componente estará indisponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para estações de trabalho.

A partir da versão 12.6 o Kaspersky Endpoint Security for Windows inclui o componente do monitor de integridade do sistema em vez do componente do 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 Endpoint 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 *Verificação de integridade do sistema*, 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.

Configurações do Monitor de integridade do sistema

Parâmetro	Descrição
Modo de operação para regras de bloqueio	• **Bloquear**. Neste modo, o monitor de integridade do sistema bloqueia as ações com arquivos e chaves do registro do escopo de monitoramento e gera um evento correspondente. • **Informar**. Neste modo, o monitor de integridade do sistema permite executar ações com arquivos e chaves do registro do escopo de monitoramento e gera um evento correspondente.

Parâmetro	Descrição
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.
Monitorar dispositivos	O Monitor de integridade do sistema monitora a conexão e desconexão de dispositivos externos.
Monitorar os arquivos e o registro	O Monitor de integridade do sistema monitora as alterações em arquivos, pastas e registro.
Verificação de integridade do sistema	A verificação de integridade do sistema sob demanda é uma tarefa que pode ser manualmente executada ou por agendamento. Para executar a tarefa *Verificação de integridade do sistema*, 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.

Endpoint Sensor

O Endpoint Sensor não está incluído no Kaspersky Endpoint Security 11.4.0.

Você pode gerenciar o Endpoint Sensor no Kaspersky Security Center Web Console e no Console de Administração do Kaspersky Security Center. Não é possível gerenciar o Endpoint Sensor no Kaspersky Security Center Cloud Console.

O *Endpoint Sensor* foi desenvolvido para interagir com qualquer Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* é uma solução projetada para a detecção oportuna de ameaças sofisticadas, como ataques direcionados, ameaças persistentes avançadas (APT) e ataques de dia zero, entre outros. A Kaspersky Anti Targeted Attack Platform inclui três unidades funcionais:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

É possível adquirir todas as unidades funcionais ou unidades individuais separadamente. Para obter informações detalhadas sobre a solução, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform.

O gerenciamento do Endpoint Sensor possui as seguintes limitações:

- Você pode definir as configurações do Endpoint Sensor em uma política, desde que o Kaspersky Endpoint Security, versões 11.0.0 a 11.3.0, esteja instalado no computador. Para obter mais informações sobre como definir as configurações do Endpoint Sensor utilizando a política, consulte os artigos de ajuda das versões anteriores do Kaspersky Endpoint Security.
- Se o Kaspersky Endpoint Security 11.4.0, ou posterior, estiver instalado no computador, você não poderá definir o Endpoint Sensor na política.

O Endpoint Sensor é instalado nos computadores cliente. Nesses computadores, o componente monitora constantemente os processos, as conexões ativas de rede e os arquivos modificados. O Endpoint Sensor transmite as informações ao servidor da KATA.

A funcionalidade de componente está disponível nos seguintes sistemas operacionais:

- Windows 7 Service Pack 1 Home / Professional / Enterprise;
- Windows 8.1.1 Professional / Enterprise;
- Windows 10 RS3 Home / Professional / Education / Enterprise;
- Windows 10 RS4 Home / Professional / Education / Enterprise;
- Windows 10 RS5 Home / Professional / Education / Enterprise;
- Windows 10 RS6 Home / Professional / Education / Enterprise;
- Windows Server 2008 R2 Foundation / Standard / Enterprise (64 bits);
- Windows Server 2012 Foundation / Standard / Enterprise (64 bits);
- Windows Server 2012 R2 Foundation / Standard / Enterprise (64 bits);
- Windows Server 2016 Essentials / Standard (64 bits).

Para obter informações detalhadas sobre a operação KATA, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform.

Sandbox

O Kaspersky Endpoint Security for Windows inclui um agente interno para integração com a solução Kaspersky Sandbox. O componente *Sandbox* detecta e bloqueia automaticamente ameaças avançadas em computadores. O Sandbox analisa o comportamento do objeto para detectar atividades maliciosas e características de atividades de ataques direcionados à infraestrutura de TI da organização. O Sandbox analisa e verifica objetos em servidores especiais com imagens virtuais implantadas de sistemas operacionais Microsoft Windows (servidores Sandbox). Para obter informações detalhadas sobre a solução, consulte a ajuda do Kaspersky Sandbox e a ajuda da Kaspersky Anti Targeted Attack Platform.

A partir da versão 12.7, o Kaspersky Endpoint Security for Windows oferece suporte ao componente Sandbox que faz parte da solução Kaspersky Anti Targeted Attack Platform. Ao contrário da solução Kaspersky Sandbox, o componente KATA Sandbox permite apenas verificar os arquivos automaticamente e também manualmente pelo menu de contexto do arquivo.

O KATA Sandbox requer a Kaspersky Anti Targeted Attack Platform 7.0 ou posterior para ser implementado.

O componente só pode ser gerenciado usando o Kaspersky Security Center Web Console. Não é possível gerenciar esse componente usando o Console de Administração (MMC).

Configurações do componente Sandbox

Parâmetro	Descrição
Modo de integração	**Kaspersky Sandbox**. Integração com a solução Kaspersky Sandbox. O aplicativo envia os arquivos para serem verificados pelo Kaspersky Sandbox apenas no modo automático. **KATA Sandbox**. Integração com o componente Sandbox da solução Kaspersky Anti Targeted Attack Platform. É possível selecionar o modo de envio de arquivos para verificação: • **Manualmente**. O usuário envia manualmente o arquivo para verificação pelo menu de contexto (**Enviar para o Sandbox**). • **Automaticamente**. O aplicativo detecta os objetos automaticamente para enviá-los ao Sandbox para verificação. • **Combinado**.
Configurações de conexão do servidor	**Tempo limite (mseg)**. Tempo de conexão esgotado para o Sandbox (para Kaspersky Sandbox) ou servidor do Central Node (para KATA). Depois de decorrido o tempo limite configurado, o Kaspersky Endpoint Security envia uma solicitação ao próximo servidor. É possível aumentar o tempo de conexão esgotado para o servidor caso a velocidade da sua conexão seja baixa ou instável. O tempo limite de solicitação recomendado é de 0.5 segundo ou menos. **Fila de solicitações**. Tamanho da pasta da fila de solicitações. Ao enviar vários objetos para verificação no Sandbox, o Kaspersky Endpoint Security cria uma fila de solicitações. Por padrão, o tamanho da pasta da fila de solicitações é limitado a 100 MB. Depois que o tamanho máximo é atingido, o Sandbox para de adicionar novas solicitações à fila e envia o evento correspondente ao Kaspersky Security Center. É possível configurar o tamanho da pasta da fila de solicitações dependendo da configuração do seu servidor. **Certificado TLS do servidor**. Para configurar uma conexão confiável com o servidor do Sandbox (para o Kaspersky Sandbox) ou o servidor do Central Node (para o KATA), é necessário preparar um certificado TLS. Em seguida, é necessário adicionar o certificado ao computador com o uso de uma política. Também é preciso adicionar o certificado ao servidor do Sandbox (para o Kaspersky Sandbox) ou ao servidor do Central Node (para o KATA). **Usar autenticação bidirecional** (somente para KATA Sandbox). Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor do Central Node, obter um contêiner de criptografia e definir uma senha para proteger o contêiner criptográfico. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner criptográfico no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform). Depois de definir as configurações do Central Node, é necessário também habilitar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner criptográfico protegido por senha.
Conexão com servidores do Sandbox	**Kaspersky Sandbox**. Configurações de conexão do servidor do Sandbox. Os servidores usam imagens virtuais implantadas de sistemas operacionais Microsoft Windows para executar os objetos que precisam ser verificados. É possível inserir um endereço IP (IPv4 ou IPv6) ou um nome de domínio totalmente qualificado. **KATA Sandbox**. Configurações de conexão do servidor do Central Node. O Central Node escolhe as configurações ideais para a verificação e equilibra a carga entre os servidores do Sandbox.
Ação ao detectar ameaça	**Mover cópia para a Quarentena, excluir objeto**. Caso a opção seja selecionada, o Kaspersky Endpoint Security exclui o objeto malicioso encontrado no computador. Antes de excluir o objeto, o Kaspersky Endpoint Security cria uma cópia de backup, caso o objeto precise ser restaurado posteriormente. O Kaspersky Endpoint Security move a cópia de backup para a quarentena. **Executar a Verificação de áreas críticas**. Caso essa opção seja selecionada, o Kaspersky Endpoint Security executa a tarefa *Verificação de áreas críticas*. Por padrão, o Kaspersky Endpoint Security verifica a memória kernel, os processos de execução e os setores de inicialização de disco. **Criar tarefa de Verificação de IOC**. Caso a opção esteja selecionada, o Kaspersky Endpoint Security cria automaticamente uma tarefa de *Verificação de IOC (tarefa Verificação de IOC autônoma)*. Para esta tarefa, é possível configurar o modo de execução, o escopo da verificação e a ação na detecção de IOC (*Mover cópia para a Quarentena, excluir objeto* ou *Executar a Verificação de áreas críticas*). Para modificar outras configurações da tarefa de *Verificação de IOC*, acesse as configurações de tarefa.
Adicionar escopo da verificação de IOC	**Áreas críticas de arquivos**. Caso a opção seja selecionada, o Kaspersky Endpoint Security fará uma verificação de IOC apenas em áreas críticas de arquivos do computador: memória kernel e setores de inicialização. **Áreas de arquivo na unidade do sistema do computador**. Se essa opção estiver selecionada, o Kaspersky Endpoint Security verificará a unidade do sistema do computador em busca de IOCs.
Executar a tarefa de Verificação de IOC	**Manualmente**. Modo de execução no qual é possível iniciar a tarefa *Verificação de IOC* manualmente, quando conveniente. **Automaticamente**. Modo de execução no qual o Kaspersky Endpoint Security executa a tarefa *Verificação de IOC* automaticamente após a detecção de uma ameaça. **Executar apenas quando o computador estiver ocioso**. Modo de execução no qual o Kaspersky Endpoint Security executa a tarefa de *Verificação de IOC* caso o protetor de tela esteja ativo ou se a tela estiver bloqueada. Caso o usuário desbloqueie o computador, o Kaspersky Endpoint Security pausa a tarefa. Isso significa que a tarefa pode levar vários dias para ser concluída.

Managed Detection and Response

O Kaspersky Endpoint Security for Windows é compatível com a integração da solução Managed Detection and Response. A solução *Kaspersky Managed Detection and Response (MDR)* detecta e analisa automaticamente os incidentes de segurança em sua infraestrutura. Para isso, o MDR usa dados de telemetria recebidos de terminais 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 do Managed Detection and Response

Parâmetro	Descrição
Arquivo de configuração do MDR	O arquivo BLOB contém o ID do cliente e informações sobre a licença do Kaspersky Managed Detection and Response. O arquivo BLOB está localizado dentro do arquivo comprimido ZIP do arquivo de configuração do MDR. É possível obter o arquivo ZIP no Console do Kaspersky Managed Detection and Response. Para saber informações detalhadas sobre o arquivo BLOB, consulte a Ajuda do Kaspersky Managed Detection and Response.

Endpoint Detection and Response

O Kaspersky Endpoint Security for Windows inclui um agente integrado para a solução Kaspersky Endpoint Detection and Response Optimum (doravante também "EDR Optimum"). A partir da versão 11.8.0, o Kaspersky Endpoint Security for Windows inclui um agente integrado para a solução Kaspersky Endpoint Detection and Response Expert (doravante também "EDR Expert"). O *Kaspersky Endpoint Detection and Response* é uma gama de soluções para proteger a infraestrutura corporativa de TI contra ameaças cibernéticas avançadas. A funcionalidade das soluções combina a detecção automática de ameaças com a capacidade de reagir a essas ameaças para neutralizar ataques avançados, incluindo novos exploits, ransomwares, ataques sem arquivo, bem como métodos que usam ferramentas de sistema legítimas. O EDR Expert oferece mais monitoramento de ameaças e funcionalidade de resposta do que o EDR Optimum. Para obter informações detalhadas sobre a solução, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

O Kaspersky Endpoint Detection and Response revisa e analisa o desenvolvimento de ameaças e fornece à *equipe de segurança* ou ao *Administrador* as informações sobre o possível ataque necessárias para uma resposta oportuna. O Kaspersky Endpoint Detection and Response exibe os detalhes de alertas e uma janela separada. Um *alerta* é um evento na infraestrutura de TI corporativa que o aplicativo identificou como incomum ou suspeito e que pode representar uma ameaça de segurança para a infraestrutura de TI corporativa. *Detalhes de alertas* é uma ferramenta para visualizar todas as informações coletadas sobre uma ameaça detectada. Os detalhes da alertas incluem, por exemplo, o histórico de arquivos aparentes no computador. Para obter detalhes sobre o gerenciamento dos detalhes de alertas, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

É possível configurar o componente Endpoint Detection and Response Optimum no Web Console e Cloud Console. As configurações do componente Endpoint Detection and Response Expert (cloud) estão disponíveis somente no Cloud Console.

Parâmetro	Descrição
Ativar a criação de log do sistema avançado	A telemetria estendida melhora a precisão da detecção de IOC, mas usa mais recursos do computador. Recomendamos ativar a telemetria estendida no computador para a verificação retrospectiva IOC. A *Verificação retrospectiva IOC* é um modo de tarefa de *Verificação de IOC* no qual o Kaspersky Endpoint Security verifica os indicadores de comprometimento com o uso de dados de um determinado período de tempo. Este modo é destinado à pesquisa de indicadores de comprometimento pela telemetria do computador protegido, como atividade de rede, processos, arquivos e outras telemetrias. Caso a telemetria estendida esteja desativada, o Kaspersky Endpoint Security poderá alternar as informações sobre os indicadores de comprometimento detectados.
Isolamento de rede	Isolamento automático do computador da rede em resposta a ameaças detectadas. Quando o isolamento de rede é ativado, o aplicativo corta todas as conexões ativas e bloqueia todas as novas conexões TCP/IP no computador. O aplicativo deixa apenas as seguintes conexões ativas: • Conexões listadas em exclusões de isolamento de rede. • Conexões iniciadas pelos serviços do Kaspersky Endpoint Security. • Conexões iniciadas pelo Agente de Rede do Kaspersky Security Center.
Desbloquear automaticamente o dispositivo isolado em (horas)	O isolamento de rede pode ser desativado automaticamente após um tempo especificado ou manualmente. Por padrão, o Kaspersky Endpoint Security desativa o isolamento de rede 5 horas após o início do isolamento.
Exclusões de isolamento de rede	Lista de regras para exclusões do isolamento de rede. As conexões de rede que correspondem às regras não são bloqueadas em computadores quando o isolamento de rede é ativado. Para configurar as exclusões de isolamento de rede, é possível utilizar a lista de *perfis de rede padrão*. Por padrão, as exclusões incluem os perfis de rede contendo as regras que garantem a operação ininterrupta de dispositivos com funções de servidor DNS/DHCP e cliente DNS/DHCP. Também é possível modificar as configurações dos perfis de rede padrão ou definir as exclusões manualmente. As exclusões especificadas nas propriedades da política são aplicadas apenas se o isolamento de rede for ativado automaticamente em resposta a uma ameaça detectada. As exclusões especificadas nas propriedades do computador são aplicadas apenas se o isolamento de rede for ativado manualmente nas propriedades do computador no console do Kaspersky Security Center ou nos detalhes de alertas.
Prevenção de execução	Controle a execução de arquivos executáveis e scripts e abertura de arquivos de formato Office. Por exemplo, é possível impedir a execução de aplicativos considerados inseguros no computador selecionado. A prevenção de execução é compatível com um conjunto de extensões de arquivos do office e um conjunto de intérpretes de script. Para usar o componente Prevenção de execução, você precisa adicionar regras de prevenção de execução. A *Regra de prevenção de execução* é um conjunto de critérios que o aplicativo leva em consideração ao reagir à execução de um objeto, por exemplo, ao bloquear a execução de um objeto. O aplicativo identifica os arquivos por seus caminhos ou somas de verificação calculados usando algoritmos de hash MD5 e SHA256.
Ação na execução ou abertura de objeto proibido	**Bloquear e adicionar ao log de eventos**. Neste modo, o aplicativo bloqueia a execução de objetos ou a abertura de documentos que atendam aos critérios da regra de prevenção. O aplicativo também publica um evento sobre as tentativas de execução de objetos ou documentos abertos no log de eventos do Windows e no log de eventos do Kaspersky Security Center. **Adicionar ao log de eventos**. Neste modo, o Kaspersky Endpoint Security publica um evento sobre tentativas de execução de objetos executáveis ou documentos abertos que correspondem aos critérios da regra de prevenção no log de eventos do Windows e no Kaspersky Security Center, mas não bloqueia a tentativa de executar ou abrir o objeto ou documento. O item está selecionado por padrão.
Regras de prevenção de execução	A *Regra de prevenção de execução* é um conjunto de critérios que o aplicativo leva em consideração ao reagir à execução de um objeto, por exemplo, ao bloquear a execução de um objeto. O aplicativo identifica os arquivos por seus caminhos ou somas de verificação calculados usando algoritmos de hash MD5 e SHA256.

Parâmetro	Descrição
Cloud Sandbox	*Cloud Sandbox* é uma tecnologia que permite detectar ameaças avançadas em um computador. O Kaspersky Endpoint Security encaminha automaticamente arquivos detectados para a Cloud Sandbox analisar. O Cloud Sandbox executa esses arquivos em um ambiente isolado para identificar atividades maliciosas e avaliar a sua reputação. Os dados desses arquivos são enviados para a Kaspersky Security Network. Portanto, caso o Cloud Sandbox detecte um arquivo malicioso, o Kaspersky Endpoint Security executará a ação apropriada para eliminar essa ameaça em todos os computadores em que esse arquivo for detectado. A tecnologia Cloud Sandbox está habilitada permanentemente e disponível para todos os usuários da Kaspersky Security Network, independentemente do tipo de licença em uso. Caso a caixa de seleção esteja marcada, o Kaspersky Endpoint Security habilitará o contador de ameaças detectadas usando o Cloud Sandbox na janela principal do aplicativo debaixo **Tecnologias de detecção de ameaças**. O Kaspersky Endpoint Security também indicará a tecnologia de detecção de ameaças Cloud Sandbox em eventos do aplicativo e no *Relatório de ameaças* no console do Kaspersky Security Center.

Endpoint Detection and Response Expert (on-premises)

Endpoint Detection and Response Expert (on-premises)

O Kaspersky Endpoint Security for Windows é compatível com a integração com a solução Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* é uma solução de cibersegurança empresarial que inclui aplicativos da Kaspersky que permitem a uma organização se defender contra a maioria dos tipos de riscos cibernéticos e abranger os cenários mais importantes de propagação de ameaças. Os componentes do EDR Expert (on-premises) são implementados na Open Single Management Platform (OSMP). Esta plataforma executa cenários multiplataforma em uma única interface e permite a integração de aplicativos da Kaspersky com aplicativos de terceiros em um sistema de segurança abrangente.

Um dos elementos centrais da solução é o componente *SIEM*. O componente SIEM rastreia eventos provenientes de todos os componentes e correlaciona esses eventos entre si com o uso de regras definidas pelo fornecedor e pelo usuário. O EDR Expert (on-premises) analisa os logs e a telemetria recebidos da infraestrutura corporativa para detectar automaticamente ataques e permite investigar incidentes usando um gráfico de investigação unificado que combina todos os eventos coletados no EDR Expert (on-premises), inclusive eventos de aplicativos da Kaspersky e de produtos de segurança da informação de terceiros.

Para responder a incidentes avançados, o EDR Expert (on-premises) usa cenários predefinidos e definidos pelo usuário. Também é possível usar ações de resposta de aplicativos de terceiros e cenários de resposta que envolvem vários aplicativos.

Endpoint Detection and Response (KATA)

O Kaspersky Endpoint Security for Windows é compatível com o trabalho do componente Kaspersky Endpoint Detection and Response como parte da solução Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* é uma solução projetada para a detecção oportuna de ameaças sofisticadas, como ataques direcionados, ameaças persistentes avançadas (APT) e ataques de dia zero, entre outros. A Kaspersky Anti Targeted Attack Platform inclui três unidades funcionais:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

É possível adquirir todas as unidades funcionais ou unidades individuais separadamente. Para obter informações detalhadas sobre a solução, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform.

O Kaspersky Endpoint Security é instalado em computadores individuais na infraestrutura corporativa de TI e monitora continuamente os processos, as conexões de rede abertas e os arquivos em modificação. As informações sobre eventos no computador são enviadas para o servidor do Kaspersky Anti Targeted Attack Platform. Nesse caso, o Kaspersky Endpoint Security também envia informações ao servidor do Kaspersky Anti Targeted Attack Platform sobre ameaças descobertas pelo aplicativo, além das informações sobre o processamento dos resultados dessas ameaças.

A integração do EDR (KATA) e NDR (KATA) é configurada no console do Kaspersky Security Center. Então, o agente integrado é gerenciado com o uso do console Kaspersky Anti Targeted Attack Platform, inclusive a execução de tarefas, gerenciamento de objetos em quarentena, exibição de relatórios e outras ações.

Configurações do Endpoint Detection and Response Expert (on-premises)

Parâmetro	Descrição
Conexão com servidores de coleta de telemetria	Um *servidor de coleta de telemetria* é um servidor que faz parte de uma solução SIEM que coleta, normaliza, correlaciona, analisa e armazena informações sobre eventos que ocorrem no computador. Configure os seguintes itens para estabelecer conexão com os servidores de coleta de telemetria (KUMA): • **Tempo limite (s)**. Tempo limite máximo de resposta do servidor. Quando o tempo limite se esgotar, o Kaspersky Endpoint Security tentará estabelecer conexão com um servidor diferente. • **Certificado do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor. É possível obter um certificado TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor, obter um contêiner de criptografia e definir uma senha para protegê-lo. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner de criptografia na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). Depois de definir as configurações do servidor, é necessário também ativar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner de criptografia protegido por senha. O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.
Endereço e **Porta** (servidores de coleta de telemetria)	Configurações para conexão com servidores de coleta de telemetria. É possível inserir um endereço IP (IPv4 ou IPv6). É possível adicionar vários endereços de servidores de coleta de telemetria. O Kaspersky Endpoint Security tenta se conectar ao servidor usando o primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar usando o segundo endereço IP na lista e assim sucessivamente.
Enviar telemetria aos servidores de coleta de telemetria	Essa funcionalidade permite desativar completamente o envio de telemetria para o servidor KATA. Por exemplo, se você estiver usando a Kaspersky Anti Targeted Attack Platform junto com outra solução que também utiliza telemetria, é possível desativar o envio de telemetria para a KATA (EDR). Isso permite otimizar a carga do servidor para essas soluções. Caso tenha a solução Managed Detection and Response e KATA (EDR) implantados, será possível usar a telemetria MDR e criar tarefas de Resposta a Ameaças no KATA (EDR). • **Enviar apenas telemetria com IOA**. Isso permite otimizar a telemetria e enviar apenas a telemetria com IOA. *Indicadores de ataque (IOA)* é uma regra que contém uma descrição de comportamentos suspeitos no sistema que podem indicar um ataque direcionado. O aplicativo compara o comportamento contínuo no sistema com essas regras e registra os eventos que indicam um ataque direcionado. O aplicativo usa a tecnologia *de verificação de streaming*, que permite fazer o rastreamento de eventos em tempo real. • **Atraso máximo na transmissão de eventos (segundos)**. O aplicativo sincroniza com o servidor para enviar eventos após expirar o intervalo de sincronização. A configuração padrão é 30 segundos. • **Limitar o número de pacotes de eventos por transmissão**. O aplicativo sincroniza com o servidor quando o buffer está cheio de eventos. A configuração padrão é 1024 eventos. Esta função permite desativar o armazenamento em buffer de eventos antes da sincronização com o servidor.
Ativar a limitação de solicitações	Esse recurso ajuda a otimizar a carga no computador. Se essa funcionalidade estiver ativada, o aplicativo restringirá a transmissão de eventos. Caso o número de eventos exceda os limites configurados, o Kaspersky Endpoint Security interromperá o envio de eventos. Defina as configurações de telemetria: • **Número máximo de eventos por hora**. O aplicativo analisa o fluxo de dados de telemetria e restringe o envio de eventos caso ele exceda o limite de eventos configurado por hora. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. A configuração padrão é de 3 mil eventos por hora. Caso o aplicativo esteja instalado em um servidor, o fluxo de dados de telemetria será maior. Para servidores, é recomendável aumentar o valor para 60 mil eventos por hora. • **Porcentagem de excesso de limite de evento**. O aplicativo ordena os eventos por tipo (por exemplo, eventos "alterações no registro") e restringe a transmissão de eventos caso a proporção de eventos do mesmo tipo para o número total de eventos exceda o limite configurado em porcentagem. O Kaspersky Endpoint Security retoma o envio de eventos quando a proporção de outros eventos para o número total de eventos torna-se volumosa o suficiente novamente. A configuração padrão é 15%.
Enviar solicitação de sincronização para o servidor a cada (min.)	Frequência de solicitações de sincronização enviadas ao servidor. Durante a sincronização, o Kaspersky Endpoint Security envia informações sobre as configurações e tarefas modificadas do aplicativo.

Parâmetro	Descrição
Conexão com servidores de resposta	Um *servidor de resposta* é um dispositivo que recebe e verifica dados, estuda o comportamento de objetos e publica os resultados desses estudos. Configure os seguintes itens para conexão dos servidores de resposta: • **Tempo limite (s)**. Tempo limite máximo de resposta do servidor. Quando o tempo limite se esgotar, o Kaspersky Endpoint Security tentará estabelecer conexão com um servidor diferente. • **Certificado do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor. É possível obter um certificado TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor, obter um contêiner de criptografia e definir uma senha para protegê-lo. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner de criptografia na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). Depois de definir as configurações do servidor, é necessário também ativar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner de criptografia protegido por senha.
Endereço e **Porta** (servidores de resposta)	Configurações para conexão com servidores de resposta. É possível inserir um endereço IP (IPv4 ou IPv6). É possível adicionar vários endereços de servidores de coleta de telemetria. O Kaspersky Endpoint Security tenta se conectar ao servidor usando o primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar usando o segundo endereço IP na lista e assim sucessivamente.

Configurações do Endpoint Detection and Response (KATA)

Parâmetro	Descrição
Enviar solicitação de sincronização para o servidor a cada (min.)	Frequência de solicitações de sincronização enviadas ao servidor. Durante a sincronização, o Kaspersky Endpoint Security envia informações sobre as configurações e tarefas modificadas do aplicativo.
Conexão com servidores KATA	Configure os seguintes itens para conexão do servidor do Central Node: • **Tempo limite (s)**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite se esgota, o Kaspersky Endpoint Security tenta estabelecer conexão com um servidor de Central Node diferente. • **Certificado do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor do Central Node. É possível obter um certificado TLS no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform). • **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor do Central Node, obter um contêiner de criptografia e definir uma senha para proteger o contêiner criptográfico. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner criptográfico no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform). Depois de definir as configurações do Central Node, é necessário também habilitar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner criptográfico protegido por senha. O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.
Endereço e **Porta** (servidores KATA)	Configurações para conexão com servidores da Kaspersky Anti Targeted Attack Platform. Insira o endereço IP (IPv4 ou IPv6) e a porta do servidor Central Node a ser conectado. É possível adicionar vários endereços de servidor do nó central. O Kaspersky Endpoint Security tenta se conectar ao servidor usando o primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar usando o segundo endereço IP na lista e assim sucessivamente.
Enviar telemetria à KATA	Essa funcionalidade permite desativar completamente o envio de telemetria para o servidor KATA. Por exemplo, se você estiver usando a Kaspersky Anti Targeted Attack Platform junto com outra solução que também utiliza telemetria, é possível desativar o envio de telemetria para a KATA (EDR). Isso permite otimizar a carga do servidor para essas soluções. Caso tenha a solução Managed Detection and Response e KATA (EDR) implantados, será possível usar a telemetria MDR e criar tarefas de Resposta a Ameaças no KATA (EDR). Defina as configurações de telemetria: • **Atraso máximo na transmissão de eventos (segundos)**. O aplicativo sincroniza com o servidor para enviar eventos após expirar o intervalo de sincronização. A configuração padrão é 30 segundos. • **Número máximo de pacotes de eventos**. O aplicativo sincroniza com o servidor quando o buffer está cheio de eventos. A configuração padrão é 1024 eventos.

Parâmetro	Descrição
Ativar a limitação de solicitações	Esse recurso ajuda a otimizar a carga no computador. Se essa funcionalidade estiver ativada, o aplicativo restringirá a transmissão de eventos. Caso o número de eventos exceda os limites configurados, o Kaspersky Endpoint Security interromperá o envio de eventos. Defina as configurações de telemetria: • **Número máximo de eventos por hora**. O aplicativo analisa o fluxo de dados de telemetria e restringe o envio de eventos caso ele exceda o limite de eventos configurado por hora. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. A configuração padrão é de 3 mil eventos por hora. Caso o aplicativo esteja instalado em um servidor, o fluxo de dados de telemetria será maior. Para servidores, é recomendável aumentar o valor para 60 mil eventos por hora. • **Porcentagem de excesso de limite de evento**. O aplicativo ordena os eventos por tipo (por exemplo, eventos "alterações no registro") e restringe a transmissão de eventos caso a proporção de eventos do mesmo tipo para o número total de eventos exceda o limite configurado em porcentagem. O Kaspersky Endpoint Security retoma o envio de eventos quando a proporção de outros eventos para o número total de eventos torna-se volumosa o suficiente novamente. A configuração padrão é 15%.

Network Detection and Response (KATA)

O Kaspersky Endpoint Security for Windows é compatível com o trabalho do componente Kaspersky Network Detection and Response como parte da solução Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* é uma solução projetada para a detecção oportuna de ameaças sofisticadas, como ataques direcionados, ameaças persistentes avançadas (APT) e ataques de dia zero, entre outros. A Kaspersky Anti Targeted Attack Platform inclui três unidades funcionais:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

É possível adquirir todas as unidades funcionais ou unidades individuais separadamente. Para obter informações detalhadas sobre a solução, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform.

O Kaspersky Endpoint Security é instalado em computadores individuais na infraestrutura corporativa de TI e monitora continuamente os processos, as conexões de rede abertas e os arquivos em modificação. As informações sobre eventos no computador são enviadas para o servidor do Kaspersky Anti Targeted Attack Platform. Nesse caso, o Kaspersky Endpoint Security também envia informações ao servidor do Kaspersky Anti Targeted Attack Platform sobre ameaças descobertas pelo aplicativo, além das informações sobre o processamento dos resultados dessas ameaças.

A integração do EDR (KATA) e NDR (KATA) é configurada no console do Kaspersky Security Center. Então, o agente integrado é gerenciado com o uso do console Kaspersky Anti Targeted Attack Platform, inclusive a execução de tarefas, gerenciamento de objetos em quarentena, exibição de relatórios e outras ações.

Parâmetro	Descrição
Configurações de conexão do servidor	**Tempo limite (seg)**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite se esgota, o Kaspersky Endpoint Security tenta estabelecer conexão com um servidor de Central Node diferente. **Certificado TLS do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor do Central Node. É possível obter um certificado TLS no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform). **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para usar a autenticação bidirecional, é necessário ativá-la nas configurações do servidor do Central Node, obter um contêiner de criptografia e definir uma senha para proteger o contêiner criptográfico. Um *contêiner criptográfico* é um arquivo PFX com um certificado e uma chave privada. É possível obter um contêiner criptográfico no console da Kaspersky Anti Targeted Attack Platform (consulte as instruções na ajuda da Kaspersky Anti Targeted Attack Platform). Depois de definir as configurações do Central Node, é necessário também habilitar a autenticação bidirecional nas configurações do Kaspersky Endpoint Security e carregar um contêiner criptográfico protegido por senha. O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.
Endereço e **Porta**	Configurações para conexão com servidores da Kaspersky Anti Targeted Attack Platform. Insira o endereço IP (IPv4 ou IPv6) e a porta do servidor Central Node a ser conectado. É possível adicionar vários endereços de servidor do nó central. O Kaspersky Endpoint Security tenta se conectar ao servidor usando o primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar usando o segundo endereço IP na lista e assim sucessivamente.
Enviar solicitação de sincronização para o servidor NDR a cada (min.)	Frequência de solicitações de sincronização enviadas ao servidor. Durante a sincronização, o Kaspersky Endpoint Security envia informações sobre as configurações e tarefas modificadas do aplicativo.
Atraso máximo na transmissão de eventos (segundos)	O aplicativo sincroniza com o servidor para enviar eventos após expirar o intervalo de sincronização. A configuração padrão é 30 segundos.
Ativar a limitação de solicitações	Esse recurso ajuda a otimizar a carga no computador. Se essa funcionalidade estiver ativada, o aplicativo restringirá a transmissão de eventos. Caso o número de eventos exceda os limites configurados, o Kaspersky Endpoint Security interromperá o envio de eventos.
Número máximo de eventos por hora	O aplicativo analisa o fluxo de dados de telemetria e restringe o envio de eventos caso ele exceda o limite de eventos configurado por hora. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. A configuração padrão é de 3 mil eventos por hora. Caso o aplicativo esteja instalado em um servidor, o fluxo de dados de telemetria será maior. Para servidores, é recomendável aumentar o valor para 60 mil eventos por hora.
Porcentagem de excesso de limite de evento	O aplicativo ordena os eventos por tipo (por exemplo, eventos "alterações no registro") e restringe a transmissão de eventos caso a proporção de eventos do mesmo tipo para o número total de eventos exceda o limite configurado em porcentagem. O Kaspersky Endpoint Security retoma o envio de eventos quando a proporção de outros eventos para o número total de eventos torna-se volumosa o suficiente novamente. A configuração padrão é 15%.

Integração KUMA

O Kaspersky Endpoint Security for Windows é compatível com a solução Kaspersky Unified Monitoring and Analysis Platform. A *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* é uma solução de gerenciamento de eventos e informações de segurança (SIEM) para a infraestrutura de TI das organizações. O KUMA permite detectar, analisar e mitigar as ameaças de segurança antes que elas possam causar danos.

Parâmetro	Descrição
Atraso máximo ao enviar eventos (s)	O aplicativo sincroniza com o servidor para enviar eventos após expirar o intervalo de sincronização. A configuração padrão é 30 segundos.
Conexão com servidores KUMA	**Tempo limite (s)**. Tempo máximo de espera por uma resposta do servidor do KUMA (por padrão, o valor é de 5 segundos). Quando o tempo limite se esgotar, o Kaspersky Endpoint Security tenta estabelecer conexão com um servidor da KUMA diferente. **Certificado do servidor**. Certificado TLS para estabelecer uma conexão confiável com o servidor da KUMA. Você pode obter um certificado TLS no console da Kaspersky Unified Monitoring and Analysis Platform (consulte as instruções na ajuda da Kaspersky Unified Monitoring and Analysis Platform). Para estabelecer uma conexão confiável, no console KUMA, nas configurações do conector tcp, é necessário selecionar o modo TLS **With verification** (consulte as configurações do conector do tipo tcp na ajuda da Kaspersky Unified Monitoring and Analysis Platform). **Usar autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma conexão segura entre o KES e a KUMA. Para usar a autenticação bidirecional, no console do KUMA, nas configurações do conector, é necessário selecionar o modo TLS **Custom PFX with client authentication** (consulte as configurações do conector na ajuda da Kaspersky Unified Monitoring and Analysis Platform). Em seguida, é necessário baixar um certificado de servidor e definir uma senha para proteger o contêiner criptográfico. O contêiner criptográfico deve ser protegido por senha. Não é possível adicionar um contêiner criptográfico sem senha.
Servidores KUMA	Configurações da conexão com os servidores da Kaspersky Unified Monitoring and Analysis Platform. É possível inserir um endereço IP (IPv4 ou IPv6). É possível adicionar vários endereços de servidor da KUMA. O Kaspersky Endpoint Security tenta se conectar ao servidor usando o primeiro endereço IP. Caso a conexão não possa ser estabelecida, o Kaspersky Endpoint Security tenta se conectar usando o segundo endereço IP na lista e assim sucessivamente.

Criptografia Completa do Disco

Você pode selecionar uma tecnologia de criptografia: O Kaspersky Disk Encryption ou criptografia de unidade de disco da BitLocker (aqui também mencionada simplesmente como "BitLocker").

Kaspersky Disk Encryption

O Kaspersky Disk Encryption não é compatível com computadores baseados em Arm.

Após a criptografia dos discos rígidos do sistema, na próxima inicialização do sistema o usuário deve concluir a autenticação usando o Agente de autenticação antes que os discos rígidos possam ser acessados e o sistema operacional seja carregado. Isso requer inserir a senha do token ou cartão inteligente conectado ao computador ou o nome de usuário e a senha da conta do Agente de autenticação criada pelo administrador da rede local usando a tarefa de *Gerenciar contas do Agente de Autenticação*. Estas contas são baseadas nas contas do Microsoft Windows com a qual os usuários fazem login no sistema operacional. Também é possível usar a tecnologia Single Sign-On (SSO) que permite efetuar login automaticamente no sistema operacional com o uso do nome de usuário e da senha da conta do Agente de Autenticação.

A autenticação do usuário no Agente de autenticação pode ser realizada de duas formas:

- Insira o nome e a senha da conta do Agente de Autenticação criada pelo administrador de rede local usando as ferramentas do Kaspersky Security Center.
- Insira a senha de um token ou cartão inteligente conectado ao computador.

> O uso de um token ou cartão inteligente estará disponível somente se os discos rígidos do computador tiverem sido criptografados usando o algoritmo de criptografia AES256. Se os discos rígidos do computador foram criptografados usando o algoritmo de criptografia AES56, a adição do arquivo de certificado eletrônico ao comando será negada.

Criptografia de Unidade de Disco BitLocker

O BitLocker é uma tecnologia de criptografia incorporada nos sistemas operacionais Windows. O Kaspersky Endpoint Security permite controlar e gerenciar o Bitlocker usando a infraestrutura do Kaspersky Next. O BitLocker criptografa volumes lógicos. O BitLocker não pode ser usado para criptografia de unidades removíveis. Para obter detalhes sobre o BitLocker, consulte a documentação da Microsoft.

> Ao criptografar o disco, o BitLocker coloca o carregador de inicialização e outros arquivos auxiliares no system partition. Esta partição não é criptografada. O sistema operacional cria a partição do sistema automaticamente durante a instalação do Windows. Se o disco estiver totalmente particionado antes da instalação do Windows, o sistema operacional não poderá criar uma partição do sistema. Nesse caso, quando a criptografia de disco do BitLocker for iniciada, o sistema operacional solicitará ao usuário para reparticionar o disco e criar uma partição do sistema. Depois de criar uma partição do sistema, o sistema operacional inicia a criptografia do BitLocker.

O BitLocker fornece armazenamento seguro de chaves de acesso usando um módulo de plataforma confiável. Um *Trusted Platform Module (TPM)* é um microchip desenvolvido para fornecer funções básicas relacionadas à segurança (por exemplo, armazenar chaves de criptografia). Um Módulo de plataforma confiável geralmente é instalado na placa-mãe do computador e interage com todos os outros componentes do sistema através do barramento de hardware. O uso do TPM é a maneira mais segura de armazenar chaves de acesso do BitLocker, pois o TPM fornece verificação de integridade do sistema antes da inicialização. Você ainda pode criptografar unidades em um computador sem um TPM. Nesse caso, a chave de acesso será criptografada com uma senha. O BitLocker usa os seguintes métodos de autenticação:

- TPM.
- TPM e PIN.
- Senha.

Após criptografar o disco rígido do sistema, o usuário precisa passar pela autenticação do BitLocker para inicializar o sistema operacional. Após a autenticação, o BitLocker permite que o usuário faça login. O BitLocker não oferece suporte à tecnologia de login único (SSO).

Após criptografar uma unidade, o BitLocker cria uma chave de recuperação. O Kaspersky Endpoint Security envia a chave de recuperação ao Kaspersky Security Center para que seja possível restaurar o acesso ao disco, por exemplo, caso um usuário esqueça a senha.

Se um usuário criptografar um disco usando o BitLocker, o Kaspersky Endpoint Security enviará a chave de recuperação e informações sobre a criptografia de disco ao Kaspersky Security Center.

Se você estiver usando políticas de grupo do Windows, desative o gerenciamento do BitLocker nas configurações de política. As configurações de política do Windows podem entrar em conflito com as configurações de política do Kaspersky Endpoint Security. Ao criptografar uma unidade, podem ocorrer erros.

Configurações do componente Kaspersky Disk Encryption

Parâmetro	Descrição
Modo de criptografia	**Criptografar todos os discos rígidos**. Caso esta opção seja selecionada, o aplicativo criptografará todos os discos rígidos quando a política for aplicada. Se o computador tiver vários sistemas operacionais instalados, depois da criptografia você será capaz só de carregar o sistema operacional que manda instalar o aplicativo. **Descriptografar todos os discos rígidos**. Caso esta opção seja selecionada o aplicativo descriptografará todos os discos rígidos anteriormente criptografados quando a política for aplicada. **Manter inalterado**. Se este item for selecionado, o aplicativo deixará as unidades no seu estado prévio quando a política for aplicada. Se a unidade foi criptografada, permanece criptografada. Se a unidade foi descriptografada, permanece descriptografada. Esse item está selecionado por padrão.
Durante a criptografia, criar automaticamente contas do Agente de Autenticação para usuários do Windows	Se a caixa de seleção estiver marcada, o aplicativo cria contas do Agente de Autenticação com base na lista de contas de usuários do Windows no computador. Por padrão, o Kaspersky Endpoint Security usa todas as contas locais e de domínio com as quais o usuário efetuou login no sistema operacional nos últimos 30 dias.
Conf. de criação de conta do Agente de Autenticação	**Todas as contas no computador**. Todas as contas no computador que estiveram ativas em algum momento. **Todas as contas de domínio no computador**. Todas as contas no computador que pertencem a algum domínio e que estiveram ativas em algum momento. **Todas as contas locais no computador**. Todas as contas locais no computador que estiveram ativas a qualquer momento. **Conta de serviço com uma senha única**. A conta de serviço é necessária para obter acesso ao computador, por exemplo, quando o usuário esquece a senha. Também é possível usar a conta de serviço como conta reserva. É necessário inserir o nome da conta (por padrão, `ServiceAccount`). O Kaspersky Endpoint Security cria uma senha automaticamente. É possível encontrar a senha no console do Kaspersky Security Center. **Administrador local**. O Kaspersky Endpoint Security cria uma conta de usuário do Agente de Autenticação para o administrador local do computador. **Gerente do computador**. O Kaspersky Endpoint Security cria uma conta de usuário do Agente de Autenticação para a conta do gerente do computador. É possível ver qual conta tem a função de gerente de computador nas propriedades do computador no Active Directory. Por padrão, a função de gerente do computador não está definida, ou seja, não corresponde a nenhuma conta. **Conta ativa**. O Kaspersky Endpoint Security cria automaticamente uma conta do Agente de Autenticação para a conta que está ativa no momento da criptografia do disco.
Criar automaticamente contas do Agente de Autenticação para todos os usuários do computador ao fazer login	Se a caixa de seleção estiver marcada, o aplicativo verificará as informações sobre as contas de usuários do Windows no computador antes de iniciar o agente de autenticação. Se o Kaspersky Endpoint Security detectar uma conta de usuário do Windows que não tenha uma conta do Agente de Autenticação, o aplicativo criará uma nova conta para acessar unidades criptografadas. A nova conta do Agente de Autenticação terá as seguintes configurações padrão: proteção por senha somente no início da sessão e mudança de senha na primeira autenticação. Portanto, não é necessário adicionar manualmente as contas do Agente de Autenticação usando a tarefa *Gerenciar contas do Agente de Autenticação* para computadores com unidades já criptografadas.
Salvar nome de usuário inserido no Agente de Autenticação	Se a caixa de seleção for marcada, o aplicativo salvará o nome da conta do Agente de autenticação. Não será necessário inserir o nome da conta na próxima vez que você tentar concluir a autorização no Agente de Autenticação na mesma conta.

Parâmetro	Descrição
Criptografar somente espaço usado em disco (reduz o tempo de criptografia)	Esta caixa ativa / desativa a opção que limita a área de criptografia a setores de disco rígido só ocupados. Este limite permite reduzir o tempo de criptografia. Ativar ou desativar o recurso **Criptografar somente espaço usado em disco (reduz o tempo de criptografia)** após o início da criptografia não modifica essa configuração até que os discos rígidos sejam descriptografados. Você deve marcar ou desmarcar a caixa de seleção antes da criptografia inicial. Se a caixa de seleção estiver selecionada, somente as porções da unidade de disco rígido que são ocupadas por arquivos serão criptografadas. O Kaspersky Endpoint Security criptografa automaticamente novos dados à medida que são adicionados. Se a caixa de seleção estiver desmarcada, a unidade de disco rígido inteira será criptografada, inclusive fragmentos residuais de arquivos anteriormente excluídos e modificados. Esta opção é recomendada para novas unidades de disco rígido cujos dados não foram modificados ou excluídos. Se você estiver aplicando a criptografia em um disco rígido que já está no uso, recomenda-se criptografar o disco rígido inteiro. Isso garante a proteção de todos os dados; até mesmo de dados excluídos que podem ser recuperados. Por padrão, a caixa de seleção está desmarcada.
Ativar Legacy USB Support (não recomendado)	Essa caixa de seleção ativa ou desativa a funcionalidade Legacy USB Support. *Legacy USB Support* **é** uma função do BIOS/UEFI que permite usar dispositivos USB (como um token de segurança) durante a fase de inicialização do computador antes de iniciar o sistema operacional (modo BIOS). O Legacy USB Support não afetará o suporte a dispositivos USB depois que o sistema operacional for iniciado. Se a caixa de seleção for marcada, o suporte a dispositivos USB será ativado durante a inicialização do computador. Quando a função Legacy USB Support está ativada, o Agente de Autenticação no modo BIOS não será compatível com o funcionamento de tokens via USB. Recomenda-se usar esta opção somente quando houver um problema de compatibilidade de hardware e somente para os computadores nos quais o problema ocorreu.
Configurações da senha	Configurações de força da senha da conta do Agente de autenticação. Ao usar a tecnologia de Login único, o Agente de Autenticação ignora os requisitos de segurança de senha especificados no Kaspersky Security Center. Você pode definir os requisitos de força da senha nas configurações do sistema operacional.
Usar a tecnologia de autenticação única (SSO)	A tecnologia de SSO permite usar as mesmas credenciais de conta para acessar discos rígidos criptografados e entrar no sistema operacional. Se a caixa de seleção estiver marcada, você tem que inserir as credenciais da conta para acessar os discos rígidos criptografados e efetuar login automaticamente no sistema operacional. Se a caixa de seleção for desmarcada, você terá de inserir separadamente as credenciais para acessar os discos rígidos criptografados e as credenciais da conta de usuário para login automático no sistema operacional.
Encapsular provedores de credenciais de terceiros	O Kaspersky Endpoint Security é compatível com o provedor de credenciais de terceiros ADSelfService Plus. Ao trabalhar com provedores de credenciais de terceiros, o Agente de Autenticação intercepta a senha antes que o sistema operacional seja carregado. Isso significa que um usuário precisa inserir uma senha apenas uma vez ao entrar no Windows. Depois de entrar no Windows, o usuário pode utilizar os recursos de um provedor de credenciais de terceiros para autenticação em serviços corporativos, por exemplo. Os provedores de credenciais de terceiros também permitem que os usuários redefinam a própria senha de forma independente. Nesse caso, o Kaspersky Endpoint Security atualizará automaticamente a senha do Agente de Autenticação. Caso esteja usando um provedor de credenciais de terceiros que não seja compatível com o aplicativo, será possível encontrar algumas limitações na operação da tecnologia Single Sign-On.
Ajuda	**Autenticação**. Texto de ajuda que aparece na janela do Agente de autenticação ao inserir as credenciais da conta. **Alterar senha**. Texto de ajuda que aparece na janela do Agente de autenticação ao alterar a senha da conta do Agente de autenticação. **Recuperar senha**. Texto de ajuda que aparece na janela do Agente de autenticação ao recuperar a senha da conta do Agente de autenticação.

Configurações do componente de Criptografia de unidade de disco da BitLocker

Parâmetro	Descrição
Modo de criptografia	**Criptografar todos os discos rígidos**. Caso esta opção seja selecionada, o aplicativo criptografará todos os discos rígidos quando a política for aplicada. Se o computador tiver vários sistemas operacionais instalados, depois da criptografia você será capaz só de carregar o sistema operacional que manda instalar o aplicativo. **Descriptografar todos os discos rígidos**. Caso esta opção seja selecionada o aplicativo descriptografará todos os discos rígidos anteriormente criptografados quando a política for aplicada. **Manter inalterado**. Se este item for selecionado, o aplicativo deixará as unidades no seu estado prévio quando a política for aplicada. Se a unidade foi criptografada, permanece criptografada. Se a unidade foi descriptografada, permanece descriptografada. Esse item está selecionado por padrão.
Permitir o uso de autenticação BitLocker que requer entrada de teclado pré-inicialização em tablets	Utilizar uma autenticação que requer a entrada de dados em um ambiente de pré-inicialização, mesmo se a plataforma não oferecer suporte para a entrada de pré-inicialização (por exemplo, com teclados sensíveis ao toque em tablets). A tela sensível ao toque de computadores tablet não está disponível no ambiente de pré-inicialização. Para concluir a autenticação do BitLocker em computadores tablet, o usuário precisa conectar um teclado USB, por exemplo. Se a caixa de seleção for marcada, o uso da autenticação que precisa de entrada de pré-inicialização será permitido. Recomenda-se usar esta definição apenas para dispositivos que têm ferramentas de introdução de dados alternativas em um ambiente de pré-inicialização, como um teclado USB além de teclados sensíveis ao toque. Se a caixa de seleção estiver desmarcada, a criptografia de unidade de disco da BitLocker não é possível em tablets.
Usar criptografia de hardware (Windows 8 e versões posteriores)	Se a caixa de seleção for marcada, o aplicativo aplicará a criptografia de hardware. Isso permite aumentar a velocidade da criptografia e usar menos recursos de computador.
Criptografar somente espaço usado em disco (Windows 8 e versões posteriores)	Esta caixa ativa / desativa a opção que limita a área de criptografia a setores de disco rígido só ocupados. Este limite permite reduzir o tempo de criptografia. Ativar ou desativar o recurso **Criptografar somente espaço usado em disco (reduz o tempo de criptografia)** após o início da criptografia não modifica essa configuração até que os discos rígidos sejam descriptografados. Você deve marcar ou desmarcar a caixa de seleção antes da criptografia inicial. Se a caixa de seleção estiver selecionada, somente as porções da unidade de disco rígido que são ocupadas por arquivos serão criptografadas. O Kaspersky Endpoint Security criptografa automaticamente novos dados à medida que são adicionados. Se a caixa de seleção estiver desmarcada, a unidade de disco rígido inteira será criptografada, inclusive fragmentos residuais de arquivos anteriormente excluídos e modificados. Esta opção é recomendada para novas unidades de disco rígido cujos dados não foram modificados ou excluídos. Se você estiver aplicando a criptografia em um disco rígido que já está no uso, recomenda-se criptografar o disco rígido inteiro. Isso garante a proteção de todos os dados; até mesmo de dados excluídos que podem ser recuperados. Por padrão, a caixa de seleção está desmarcada.

Parâmetro	Descrição
Método de autenticação	**Somente senha (Windows 8 e versões posteriores)** Caso esta opção seja selecionada, o Kaspersky Endpoint Security solicita ao usuário uma senha quando o usuário tenta acessar uma unidade criptografada. Esta opção pode ser selecionada quando o Trusted Platform Module (TPM) não está sendo usado. **Módulo de plataforma confiável (TPM)** Caso esta opção seja selecionada, o BitLocker usará um Trusted Platform Module (TPM). Um *Trusted Platform Module (TPM)* é um microchip desenvolvido para fornecer funções básicas relacionadas à segurança (por exemplo, armazenar chaves de criptografia). Um Módulo de Plataforma Confiável normalmente é instalado na placa mãe do computador e interage com todos os outros componentes do sistema via barramento de hardware. Para computadores que executam o Windows 7 ou Windows Server 2008 R2, somente a criptografia usando um módulo TPM está disponível. Se um módulo TPM não estiver instalado, a criptografia do BitLocker não será possível. O uso de senha nesses computadores não é suportado. Um dispositivo equipado com um Módulo de plataforma confiável pode criar chaves de criptografia que podem ser descriptografados apenas com o dispositivo. Um Trusted Platform Module criptografa chaves de criptografia com a sua própria chave de armazenamento de raiz. A chave de armazenamento de raiz é armazenada dentro do Trusted Platform Module. Isso fornece um nível adicional da proteção contra tentativas de cortar chaves de criptografia. Esta ação é selecionada por padrão. É possível definir uma camada adicional de proteção para o acesso à chave de criptografia e criptografar a chave com uma senha ou um PIN: • **Usar o PIN para TPM**. Se esta caixa de seleção estiver selecionada, um usuário pode usar um código PIN para obter acesso a uma chave de criptografia que é armazenada em Módulo de plataforma confiável (TPM). Se esta caixa de seleção estiver desmarcada, os usuários estão proibidos de usar códigos PIN. Para acessar a chave de criptografia, o usuário deve digitar a senha. • **Módulo de plataforma confiável (TPM), ou senha, caso o TPM não esteja disponível**. Se essa opção for selecionada, o usuário poderá utilizar uma senha para obter acesso a chaves de criptografia quando um Módulo de plataforma confiável (TPM) não estiver disponível. Se a caixa de seleção estiver desmarcada e o TPM não estiver disponível, a criptografia completa do disco não será iniciada. O método de autenticação selecionado deve ser configurado especificando os requisitos de senha ou PIN: • **Comprimento mínimo do PIN (caracteres)** (o valor padrão é 6). • **Comprimento mínimo da senha (caracteres)** (o valor padrão é 8). • **Número máximo de senhas/PINs armazenados** (o valor padrão é 5). • **Limitar período de validade da senha / PIN para TPM (dias)** (desativado por padrão). • **Usar o PIN aprimorado (letras e números)**. O *PIN Aprimorado* permite o uso de outros caracteres além dos caracteres numéricos: letras latinas maiúsculas e minúsculas, caracteres especiais e espaços. Desativado por padrão.
Recriar automaticamente a chave de recuperação (dias)	Atualizar automaticamente a senha para restaurar o acesso a uma unidade protegida pelo BitLocker. Caso a caixa de seleção esteja marcada, especifique o período de validade da senha da chave de recuperação. Isso ajuda a evitar o reuso da senha da chave de recuperação.

Criptografia em Nível de Arquivo

A criptografia de arquivos não é compatível com computadores baseados em Arm.

O componente estará disponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para computadores pessoais. O componente estará indisponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para servidores.

Você pode compilar listas de arquivos por extensão ou por grupos de extensões e listas de pastas armazenadas em unidades do computador local, bem como criar regras para criptografar arquivos criados por aplicativos específicos. Depois que uma política é aplicada, o Kaspersky Endpoint Security criptografa e descriptografa os seguintes arquivos:

- adicionados individualmente a listas para criptografia e descriptografia;
- arquivos armazenados em pastas adicionadas a listas para criptografia e descriptografia;
- arquivos criados por aplicativos separados.

A criptografia de arquivos possui os seguintes recursos especiais:

- O Kaspersky Endpoint Security criptografa/descriptografa arquivos em pastas predefinidas apenas para perfis de usuários locais do sistema operacional. O Kaspersky Endpoint Security não criptografa ou descriptografa arquivos em pastas predefinidas de perfis de usuários móveis, perfis de usuários obrigatórios, perfis de usuários temporários ou em pastas redirecionadas.
- O Kaspersky Endpoint Security não criptografa arquivos cuja modificação possa prejudicar o sistema operacional e os aplicativos instalados. Por exemplo, os arquivos e pastas a seguir com todas as pastas aninhadas estão na lista de exclusões da criptografia:
  - %WINDIR%;
  - %PROGRAMFILES% e %PROGRAMFILES(X86)%;
  - Arquivos de registro do Windows.

  A lista de exclusões da criptografia não pode ser visualizada nem editada. Embora arquivos e pastas na lista de exclusões da criptografia possam ser adicionados à lista de criptografia, eles não serão criptografados durante a criptografia de arquivos.

Configurações do componente Criptografia a nível de arquivo

Parâmetro	Descrição
Modo de criptografia	**Manter inalterado**. Se este item for selecionado, o Kaspersky Endpoint Security deixará os arquivos e as pastas inalterados sem criptografá-los ou descriptografá-los. **De acordo com as regras**. Se esse item for selecionado, o Kaspersky Endpoint Security criptografa os arquivos e pastas de acordo com as regras de criptografia, descriptografa os arquivos e pastas de acordo com as regras de descriptografia e regula o acesso dos aplicativos aos arquivos criptografados de acordo com as regras do aplicativo. **Descriptografar todos**. Se este item for selecionado, o Kaspersky Endpoint Security descriptografará todos os arquivos e pastas criptografados.

Parâmetro	Descrição
Criptografia	Esta guia mostra regras de criptografia de arquivos e pastas armazenados em unidades locais. Você pode adicionar arquivos da seguinte maneira: • **Pastas predefinidas**. O Kaspersky Endpoint Security permite que você adicione as seguintes áreas: **Documentos**. Arquivos na pasta *Documentos* padrão do sistema operacional e suas subpastas. **Favoritos**. Arquivos na pasta *Favoritos* padrão do sistema operacional e suas subpastas. **Área de trabalho**. Arquivos na pasta da *Área de trabalho* padrão do sistema operacional e suas subpastas. **Arquivos temporários**. Arquivos temporários relacionados ao funcionamento de aplicativos instalados no computador. Por exemplo, os aplicativos do Microsoft Office criam arquivos temporários que contêm cópias de backup dos documentos. **Arquivos do Outlook**. Arquivos relacionados ao funcionamento do cliente de e-mail do Outlook: arquivos de dados (PST), arquivos de dados off-line (OST), arquivos de catálogo de endereços off-line (OAB) e arquivos de catálogo de endereços pessoal (PAB). • **Pasta personalizada**. Você pode inserir o caminho até a pasta. Ao adicionar um caminho de pasta, siga as seguintes regras: Use uma variável de ambiente (por exemplo, `%FOLDER%\UserFolder\`). Você pode usar uma variável de ambiente apenas uma vez e apenas no início do caminho. Não use caminhos relativos. Não use os caracteres `*` e `?`. Não use caminhos UNC. Use `;` ou `,` como caracteres de separação. • **Arquivos por extensão**. Você pode selecionar grupos de extensões da lista, como os *Arquivos* do grupo de extensões. Você também pode adicionar manualmente a extensão do arquivo.
Descriptografia	Esta guia mostra regras de descriptografia de arquivos e pastas armazenados em unidades locais.
Regras para aplicativos	A guia exibe uma tabela que contém regras de acesso ao arquivo criptografado e regras de criptografia de arquivos criados ou modificados por aplicativos individuais.
Pacotes criptografados	Requisitos de força de senha a serem atendidos ao criar pacotes criptografados.

Criptografia de unidades removíveis

A criptografia de unidades removíveis não é compatível em computadores baseados em Arm.

O componente estará disponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para computadores pessoais. O componente estará indisponível se o Kaspersky Endpoint Security estiver instalado em um computador que rode o Windows para servidores.

O Kaspersky Endpoint Security tem suporte para criptografia de arquivos nos sistemas de arquivos FAT32 e NTFS. Se uma unidade removível com um sistema de arquivos sem suporte for conectada ao computador, a tarefa de criptografia dessa unidade removível terminará com um erro, e o Kaspersky Endpoint Security atribuirá o status somente leitura à unidade removível.

Para proteger dados em unidades removíveis, você pode usar os seguintes tipos de criptografia:

- Full Disk Encryption (FDE).

  Criptografia de toda a unidade removível, incluindo o sistema de arquivos.

  Não é possível acessar dados criptografados fora da rede corporativa. Também é impossível acessar dados criptografados dentro da rede corporativa se o computador não estiver conectado ao Kaspersky Security Center (por exe., em um computador convidado).

- File Level Encryption (FLE).

Criptografia de apenas arquivos em uma unidade removível. O sistema de arquivos permanece inalterado.

> A criptografia de arquivos em unidades removíveis fornece a capacidade de acessar dados fora da rede corporativa usando um modo especial chamado *modo portátil*.

Durante a criptografia, o Kaspersky Endpoint Security cria uma chave mestra. O Kaspersky Endpoint Security salva a chave mestra nos seguintes repositórios:

- Kaspersky Security Center.
- Computador do usuário.

  A chave mestra é criptografada com a chave secreta do usuário.
- Unidade removível.

  A chave mestra é criptografada com a chave pública do Kaspersky Security Center.

Depois que a criptografia estiver concluída, os dados na unidade removível podem ser acessados dentro da rede corporativa, como se estivesse em uma unidade removível comum, sem criptografia.

Acesso a dados criptografados

Quando uma unidade removível com dados criptografados é conectada, o Kaspersky Endpoint Security executa as seguintes ações:

1. Verifica se há uma chave mestra no armazenamento local no computador do usuário.

   Se a chave mestra for encontrada, o usuário obterá acesso aos dados na unidade removível.

   Se a chave mestra não for encontrada, o Kaspersky Endpoint Security executa as seguintes ações:

   a. Envia uma solicitação ao Kaspersky Security Center.

      Após receber a solicitação, o Kaspersky Security Center envia uma resposta que contém a chave mestra.

   b. O Kaspersky Endpoint Security salva a chave mestra no armazenamento local no computador do usuário para operações subsequentes com a unidade removível criptografada.
2. Descriptografa os dados.

Recursos especiais de criptografia de unidade removível

A criptografia de unidades removíveis possui os seguintes recursos especiais:

- A política com configurações predefinidas para criptografia de unidades removíveis é formada por um grupo específico de computadores gerenciados. Portanto, o resultado de aplicar a política do Kaspersky Security Center configurada para criptografia/descriptografia de unidades removíveis depende do computador ao qual a unidade removível está conectada.
- O Kaspersky Endpoint Security não criptografa/descriptografa arquivos de somente leitura armazenados em unidades removíveis.

- Os tipos de dispositivo a seguir têm suporte como unidades removíveis:
  - mídia de dados conectadas por barramento USB
  - discos rígidos conectados por barramento USB e FireWire
  - unidades SSD conectadas por barramento USB e FireWire

Configurações do componente de criptografia de unidades removíveis

Parâmetro	Descrição
Modo de criptografia	**Criptografar toda a unidade removível**. Se este item for selecionado, ao aplicar a política com as configurações de criptografia especificadas para unidades removíveis, o Kaspersky Endpoint Security criptografará unidades removíveis setor por setor, inclusive os seus sistemas de arquivos. **Criptografar todos os arquivos**. Se esse item for selecionado ao aplicar a política com as configurações de criptografia especificadas para unidades removíveis, o Kaspersky Endpoint Security criptografa todos os arquivos armazenados em unidades removíveis. O Kaspersky Endpoint Security não criptografa novamente arquivos que já estão criptografados. Os conteúdos do sistema de arquivos de uma unidade removível, inclusive a estrutura de pastas e os nomes de arquivos criptografados, não são criptografados e permanecem acessíveis. **Criptografar apenas novos arquivos**. Se este item for selecionado, ao aplicar a política com as configurações de criptografia especificadas de unidades removíveis, o Kaspersky Endpoint Security criptografará apenas os arquivos que foram adicionados ou modificados nas unidades removíveis depois que a política do Kaspersky Security Center foi aplicada pela última vez. Este modo de criptografia é conveniente quando uma unidade removível é usada tanto para fins pessoais como de trabalho. Este modo de criptografia permite deixar todos os arquivos antigos inalterados e criptografar apenas aqueles arquivos que o usuário cria em um computador de trabalho com o Kaspersky Endpoint Security instalado e a funcionalidade de criptografia ativada. Por conseguinte, o acesso a arquivos pessoais sempre está disponível, mesmo que o Kaspersky Endpoint Security esteja instalado ou não no computador com a funcionalidade de criptografia ativada. **Descriptografar toda a unidade removível**. Se este item for selecionado, ao aplicar a política com as configurações de criptografia especificadas para unidades removíveis, o Kaspersky Endpoint Security decodifica todos os arquivos criptografados armazenados em unidades removíveis, bem como os sistemas de arquivos das unidades removíveis se eles foram criptografados anteriormente. **Manter inalterado**. Se este item for selecionado, o aplicativo deixará as unidades no seu estado prévio quando a política for aplicada. Se a unidade foi criptografada, permanece criptografada. Se a unidade foi descriptografada, permanece descriptografada. Esse item está selecionado por padrão.
Modo portátil	Esta caixa de seleção ativa/desativa a preparação de uma unidade removível que permite acessar arquivos armazenados nesta unidade removível em computadores fora da rede corporativa. Se esta caixa de seleção for marcada, o Kaspersky Endpoint Security incitará o usuário a especificar uma senha antes de criptografar arquivos em uma unidade removível de acordo com o aplicativo da política. A senha é necessária para acessar arquivos criptografados em uma unidade removível em computadores fora da rede corporativa. Você pode configurar a força da senha. O modo portátil está disponível para os modos **Criptografar todos os arquivos** ou **Criptografar apenas novos arquivos**.
Criptografar somente espaço usado em disco	Esta caixa de seleção ativa/desativa o modo de criptografia no qual apenas os setores de disco ocupados são criptografados. Este modo é recomendado para novas unidades cujos dados não foram modificados ou excluídos. Se a caixa de seleção estiver selecionada, somente as porções da unidade que são ocupadas por arquivos serão criptografadas. O Kaspersky Endpoint Security criptografa automaticamente novos dados à medida que são adicionados. Se a caixa de seleção estiver desmarcada, a unidade inteira será criptografada, inclusive fragmentos residuais de arquivos anteriormente excluídos e modificados. A habilidade de criptografar apenas o espaço ocupado está disponível apenas para o modo **Criptografar toda a unidade removível**. Depois que a criptografia for iniciada, ativar/desativar a função **Criptografar somente espaço usado em disco** não modificará esta definição. Você deve marcar ou desmarcar a caixa de seleção antes da criptografia inicial.

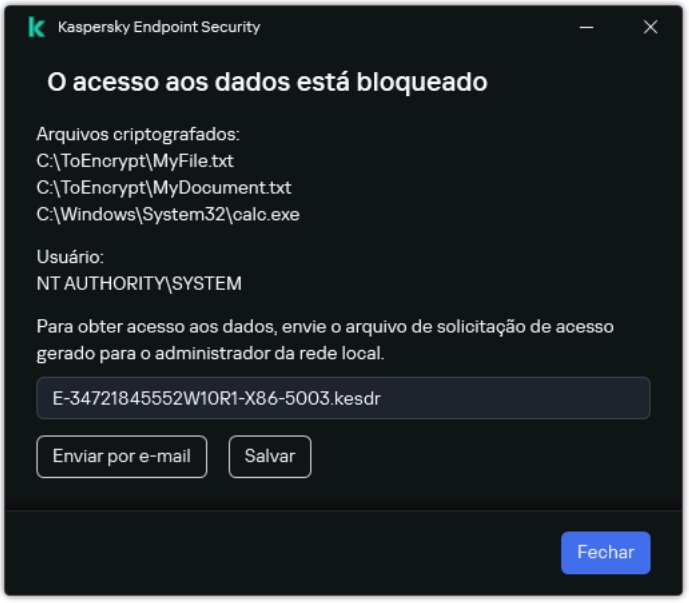
Parâmetro	Descrição

Regras personalizadas	Esta tabela contém dispositivos para os quais as regras de criptografia personalizadas são definidas. Você pode criar regras de criptografia para unidades removíveis individuais das seguintes maneiras:
	• Adicione uma unidade removível a partir da lista de dispositivos confiáveis para Controle de Dispositivos.
	• Adicione manualmente uma unidade removível:
	  • Por ID do dispositivo (Hardware ID ou HWID)
	  • Por modelo do dispositivo: Vendor ID (VID) e Product ID (PID)

Permitir criptografia de unidades removíveis no modo off-line	Se esta caixa de seleção for marcada, o Kaspersky Endpoint Security criptografa unidades removíveis quando não há conexão com o Kaspersky Security Center. Nesta caixa, os dados necessitados para decifrar unidades removíveis são guardados no disco rígido do computador ao qual a unidade removível é unida e não é transmitida ao Kaspersky Security Center. Se a caixa de seleção for desmarcada, o Kaspersky Endpoint Security não criptografará unidades removíveis sem uma conexão com o Kaspersky Security Center.
Configurações da senha de criptografia / Gerenciador de Arquivos Portátil	Configurações de força da senha para o Gerenciador de arquivos portátil.

Modelos (criptografia de dados)

Após a criptografia de dados, o Kaspersky Endpoint Security pode restringir o acesso aos dados, por exemplo, devido a uma alteração na infraestrutura da organização e no Servidor de Administração do Kaspersky Security Center. Se um usuário não tiver acesso aos dados criptografados, ele poderá solicitar ao administrador acesso aos dados. Em outras palavras, o usuário precisa enviar um arquivo de solicitação de acesso ao administrador. O usuário precisa fazer o upload do arquivo de resposta recebido do administrador para o Kaspersky Endpoint Security. O Kaspersky Endpoint Security permite solicitar o acesso aos dados do administrador por e-mail (veja a figura abaixo).



Solicitação de acesso a dados criptografados

Um modelo é fornecido para relatar a falta de acesso aos dados criptografados. Para conveniência do usuário, você pode preencher os seguintes campos:

- **Para**. Insira o endereço de e-mail do grupo de administradores com direitos sobre os recursos de criptografia de dados.
- **Assunto**. Insira o assunto do e-mail com sua solicitação de acesso aos arquivos criptografados. Você pode, por exemplo, adicionar tags para filtrar mensagens.
- **Mensagem do usuário**. Se necessário, altere o conteúdo da mensagem. Você pode usar variáveis para obter os dados necessários (por exemplo, a variável `%USER_NAME%`).

Exclusões

Uma *zona confiável* é uma lista de objetos e aplicativos configuradas pelo administrador de sistema que o Kaspersky Endpoint 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 Endpoint 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.

Iniciando com o Kaspersky Endpoint Security 12.5 for Windows, você pode adicionar telemetria EDR à zona confiável. Isso permite otimizar os dados que o aplicativo envia para o servidor de coleta de telemetria da solução Kaspersky Anti Targeted Attack Platform (EDR).

A partir do Kaspersky Endpoint Security 12.6 for Windows, as exclusões de verificação e aplicativos confiáveis são adicionadas na zona confiável. As exclusões predefinidas de verificação e aplicativos confiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, Microsoft Exchange e System Center Configuration Manager. Isso significa que não será necessário configurar manualmente uma zona confiável para o aplicativo nos servidores.

A partir do Kaspersky Endpoint Security 12.8 for Windows, é possível instalar o aplicativo no modo Light Agent para proteger ambientes virtuais. Exclusões de verificação e aplicativos confiáveis predefinidos podem ajudar a configurar rapidamente o Kaspersky Endpoint Security em ambientes virtuais Citrix e VMware.

Exclusões de verificação

Uma *exclusão de verificação* é um conjunto de condições que devem ser atendidas para que o Kaspersky Endpoint Security não verifique um determinado objeto em busca de vírus e outras ameaças. As exclusões de verificação tornam possível usar em segurança software legítimo que pode ser explorado por criminosos para danificar o computador ou os dados do usuário. Esses aplicativos não têm necessariamente uma finalidade maliciosa, mas podem ser explorados por hackers. Para obter informações detalhadas sobre aplicativos legítimos que invasores podem usar para comprometer o computador ou os dados do usuário, acesse o site da Enciclopédia da Kaspersky.

Estes aplicativos poderão ser bloqueados pelo Kaspersky Endpoint Security. Para impedir que eles sejam bloqueados, você pode configurar exclusões de verificação para os aplicativos em uso. Para fazer isso, adicione o nome ou o nome da máscara que está listada na Enciclopédia de TI da Kaspersky à zona confiável. Por exemplo, você costuma usar o aplicativo Radmin para a administração remota de computadores. O Kaspersky Endpoint Security considera esta atividade como suspeita e poderá bloqueá-la. Para evitar que o aplicativo seja bloqueado, crie uma exclusão de verificação com o nome ou máscara de nome listado na Enciclopédia de TI da Kaspersky.

Se um aplicativo que reúne informações e as envia para serem processadas for instalado no seu computador, o Kaspersky Endpoint Security pode classificar este aplicativo como malware. Para evitar isto, você pode excluir o aplicativo da verificação configurando o Kaspersky Endpoint Security como descrito neste documento.

Exclusões de verificação são usadas pelos seguintes componentes e tarefas do aplicativo que são configurados pelo administrador do sistema:

- Detecção de Comportamento.
- Prevenção de Exploits.
- Prevenção de Intrusão do Host.
- Proteção Contra Ameaças ao Arquivo.
- Proteção Contra Ameaças da Web.
- Proteção Contra Ameaças ao Correio.
- Tarefa de *Verificação de malware*

Lista de aplicativos confiáveis

A *lista de aplicativos confiáveis* é uma lista de aplicativos cuja atividade de arquivo e rede (inclusive atividade maliciosa) e acesso ao registro do sistema e que não são monitorados pelo Kaspersky Endpoint Security. Por padrão, o Kaspersky Endpoint Security monitora todos os objetos que são abertos, executados ou salvos por qualquer processo do aplicativo e controla a atividade de todos os aplicativos e tráfego de rede criada por eles. Depois que um aplicativo é adicionado à lista de aplicativos confiáveis, o Kaspersky Endpoint Security para de monitorar a atividade do aplicativo.

A diferença entre exclusões de verificação e aplicativos confiáveis é que, para as exclusões, o Kaspersky Endpoint 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 Endpoint Security detectará o arquivo e eliminará a ameaça. Se a pasta for adicionada às exclusões, o Kaspersky Endpoint 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 Endpoint Security podem ser consideradas seguras por vários aplicativos. Por exemplo, a interceptação de dados digitados no teclado é um processo de rotina dos programas que alternam automaticamente o layout do teclado (como o Punto Switcher). Para considerar as especificidades desses aplicativos e desativar o monitoramento de suas atividades, é recomendável adicioná-los à lista de aplicativos confiáveis.

Os aplicativos confiáveis ajudam a evitar problemas de compatibilidade entre o Kaspersky Endpoint Security e outros aplicativos (por exemplo, o problema de verificação dupla do tráfego de rede de um computador de terceiros pelo Kaspersky Endpoint 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 Endpoint Security por meio das exclusões de verificação.

Parâmetro	Descrição

Tipos de objetos detectados	Independentemente das configurações do aplicativo definidas, o Kaspersky Endpoint Security sempre detecta e bloqueia vírus, worms e cavalos de Troia. Eles podem causar grandes danos ao computador.

- **Vírus e worms**

  Subcategoria: Vírus e worms (Viruses_and_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 *Overwriting* gravam seu código sobre o código do arquivo que é infectado e apagam, assim, o conteúdo do arquivo. O arquivo infectado deixa de funcionar e não pode ser restaurado. Os vírus *Parasitic* modificam os arquivos para deixá-los total ou parcialmente funcionais. *Companion* não modifica arquivos, mas, em vez disso, cria arquivos duplicados. 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 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 por meio de Internet Relay Chats, ou seja, 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.
Net-Worm	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 (exploração) 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.
P2P-Worm	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 (incluindo ransomware)**

  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.
Trojan	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 Trojan-Dropper 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 a ele 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.
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
Constructor	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	Explorações	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, uma exploração pode gravar ou ler arquivos ou solicitar páginas da Web "infectadas". Explorações 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. Uma exploração 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. Uma exploração incorporada 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 explorações. Nuker exploits são pacotes de rede que desativam os computadores.
FileCryptor	Criptografadores	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: Software legítimo que pode ser usado por intrusos para danificar 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
Cliente-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.
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.
Cliente-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.

- **Software legítimo que pode ser usado por intrusos para danificar seu computador ou dados pessoais**

  Subcategoria: Software legítimo que pode ser usado por intrusos para danificar 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
Cliente-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.
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.
Cliente-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 Endpoint 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 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 Endpoint 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.

Exclusões

Esta tabela contém informações sobre exclusões de verificação.

> Recomendamos especificar os caminhos relativos em vez de caminhos absolutos. Isso permite excluir não apenas os objetos do sistema de arquivos, mas também os objetos sem arquivos. Por exemplo, `*\Program Files (x86)\Folder\Subfolder`.

Você pode excluir objetos das verificações usando os seguintes métodos:

- Insira o caminho para o Arquivo ou pasta.
- Insira o hash do objeto.

- 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.
  - `?` (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 em qualquer lugar em um caminho de arquivo ou pasta. Por exemplo, se quiser que o escopo da verificação inclua a pasta Downloads para todas as contas de usuário no computador, insira a máscara `C:\Users\*\Downloads\`.

    O Kaspersky Endpoint Security é compatível com variáveis de ambiente

    > O Kaspersky Endpoint Security não é compatível com a variável de ambiente `%userprofile%` ao gerar uma lista de exclusões por meio do 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.

- Digite o nome do objeto de acordo com a classificação da Enciclopédia da Kaspersky (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 aplicativo exclui os objetos `Client-IRC`, `Client-P2P` e `Client-SMTP` das verificações.

> O Kaspersky Endpoint Security oculta a lista de exclusões de verificação na interface do usuário do aplicativo caso a configuração de exclusões de verificação seja bloqueada pelo administrador no console (símbolo de "cadeado fechado") e as exclusões de verificação local sejam proibidas (a caixa de seleção **Permitir o uso de exclusões locais** estará desmarcada).

Aplicativos confiáveis

Esta tabela enumera aplicativos confiáveis cuja atividade não é monitorada pelo Kaspersky Endpoint Security durante a sua operação.

O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.

> O Kaspersky Endpoint 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.

O componente Controle de Aplicativos controla a inicialização de cada aplicativo, mesmo que ele não tenha sido incluído na tabela de aplicativos confiáveis.

> O Kaspersky Endpoint Security oculta a lista consolidada de aplicativos confiáveis na interface do usuário do aplicativo caso a configuração de aplicativos confiáveis seja bloqueada pelo administrador no console (símbolo de "cadeado fechado") e os aplicativos confiáveis locais sejam proibidos (a caixa de seleção **Permitir o uso de aplicativos locais confiáveis** estará desmarcada).

Mesclar valores ao herdar *(disponível apenas no console do Kaspersky Security Center)*	Isso mescla a lista de exclusões de verificação e aplicativos confiáveis nas políticas pai e filho do Kaspersky Security Center. Para mesclar listas, a política filho deve ser configurada para herdar as configurações da política pai do Kaspersky Security Center. Se a caixa de seleção estiver marcada, os itens da lista da política pai do Kaspersky Security Center serão exibidos nas políticas filho. Desta forma, é possível, por exemplo, criar uma lista consolidada de aplicações confiáveis para toda a empresa. Os itens de lista herdados em uma política filho não podem ser excluídos ou editados. Os itens na lista de exclusões de verificação e na lista de aplicativos confiáveis que são mesclados durante a herança podem ser excluídos e editados apenas na política pai. Você pode adicionar, editar ou excluir itens da lista nas políticas de nível inferior. Se os itens nas listas da política pai e filho corresponderem, esses itens serão exibidos como o mesmo item da política pai. Se a caixa de seleção não estiver marcada, os itens das listas não serão mesclados ao herdar as configurações das políticas do Kaspersky Security Center. Essa funcionalidade também permite mesclar listas em perfis de política. Para mesclar listas, no perfil de prioridade mais alta, ative a herança de configurações de um perfil de prioridade mais baixa. Para obter mais detalhes sobre as prioridades de perfil da política, consulte a ajuda do Kaspersky Security Center .
Permitir o uso de exclusões locais / Permitir o uso de aplicativos locais confiáveis *(disponível apenas no console do Kaspersky Security Center)*	*Exclusões locais e aplicativos locais confiáveis (zona confiável local)* - lista definida pelo usuário de objetos e aplicativos no Kaspersky Endpoint Security para um computador específico. O Kaspersky Endpoint Security não monitora objetos e aplicativos da zona confiável local. Dessa forma, os usuários podem criar suas próprias listas locais de exclusões e aplicativos confiáveis, além da zona confiável geral em uma política. Se a caixa de seleção estiver marcada, um usuário pode criar uma lista local de exclusões de verificação e uma lista local de aplicativos confiáveis. 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, um usuário pode acessar apenas as listas gerais de exclusões de verificação e aplicativos confiáveis geradas na política.
Telemetria do EDR (KATA) / NDR (KATA) *(disponível apenas no console do Kaspersky Security Center)*	Esta tabela contém informações sobre exclusões de telemetria EDR.
Telemetria KUMA *(disponível apenas no console do Kaspersky Security Center)*	Lista de eventos a ser enviada para a Kaspersky Unified Monitoring and Analysis Platform (KUMA). O Kaspersky Endpoint Security funciona nos seguintes modos: • **Enviar todos os eventos**. Neste modo, o aplicativo envia todos os eventos do log do Windows, exceto os eventos adicionados nas regras de exclusão. • **Enviar apenas os eventos selecionados**. Neste modo, o aplicativo envia apenas os eventos adicionados nas regras de inclusão.
Armazenamento de certificados de sistema confiáveis	Se um dos armazenamentos/repositórios de certificados de sistema confiáveis for selecionado, o Kaspersky Endpoint Security exclui os aplicativos assinados com uma assinatura digital confiável das verificações. O Kaspersky Endpoint Security atribui automaticamente esses aplicativos ao grupo **Confiável**. Se **Não usar** for selecionado, o Kaspersky Endpoint Security verifica os aplicativos independentemente de eles terem ou não uma assinatura digital. O Kaspersky Endpoint Security coloca um aplicativo em um grupo de confiança, dependendo do nível de perigo que esse aplicativo pode representar para o computador.

Configurações do aplicativo

Você pode definir as seguintes configurações gerais do aplicativo:

- Modo de operação
- Autodefesa
- Desempenho
- Informações de depuração
- Status do computador quando as configurações são aplicadas

Parâmetro	Descrição
Iniciar o aplicativo na inicialização do computador (recomendado)	Caso a opção seja selecionada, o Kaspersky Endpoint Security é iniciado após o carregamento do sistema operacional, protegendo o computador durante a sessão inteira. Caso a opção seja selecionada, o Kaspersky Endpoint 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.
Usar Tecnologia de Desinfecção Avançada (requer recursos consideráveis do computador)	Normalmente, o Kaspersky Endpoint Security encerra o malware detectado antes que o computador seja infectado. A Tecnologia de Desinfecção Avançada protege o computador contra malware já ativo (infecção ativa), minimizando assim o risco de perda de dados e a disseminação da ameaça. Caso esta tecnologia esteja ativada, quando uma atividade maliciosa for detectada, o Kaspersky Endpoint Security exibirá uma notificação pop-up. Na sua notificação, o Kaspersky Endpoint Security oferece ao usuário a opção para executar a Desinfecção avançada do computador. Depois que o usuário aprovar o procedimento, o Kaspersky Endpoint Security neutraliza a ameaça e, em seguida, reinicia o computador. A tecnologia de desinfecção avançada usa uma grande quantidade de recursos de computação, o que talvez torne os outros aplicativos mais lentos. Quando a aplicativo estiver no processo de detecção de uma infecção ativa, algumas funcionalidades do sistema operacional podem não estar disponíveis. A disponibilidade do sistema operacional é restabelecida quando a desinfecção avançada é concluída e o computador é reiniciado. Se o Kaspersky Endpoint Security estiver instalado em um computador que executa o Windows for Servers, o Kaspersky Endpoint Security não mostrará a notificação. Portanto, o usuário não pode selecionar uma ação para desinfectar uma ameaça ativa. Para desinfetar uma ameaça, é necessário ativar a tecnologia de desinfecção avançada nas configurações do aplicativo e ativar a desinfecção avançada imediatamente nas configurações de tarefa de *Verificação de malware*. Em seguida, será necessário iniciar a tarefa de *Verificação de malware*.
Usar o Kaspersky Security Center como servidor proxy para ativação *(disponível apenas no console do Kaspersky Security Center)*	Caso a caixa de seleção esteja marcada, o aplicativo usará o Servidor de Administração do Kaspersky Security Center como um servidor proxy para se conectar com os servidores de ativação. Isso é necessário quando se usa um código de ativação para ativar o aplicativo em um segmento de rede isolado sem acesso à Internet. Caso esteja ativando o aplicativo com um arquivo de chave, o acesso à Internet não será necessário.
Ativar a Autodefesa	Caso a funcionalidade esteja ativada, o Kaspersky Endpoint Security impedirá que haja alteração ou exclusão de arquivos no disco rígido, processos da memória e entradas no registro do sistema.
Bloquear o gerenciamento externo de serviços do aplicativo	Caso esta funcionalidade esteja ativada, o Kaspersky Endpoint Security não permitirá o gerenciamento de serviços de aplicativos com o uso de aplicativos de terceiros (como o CMD). Quando ocorre uma tentativa de gerenciamento de serviços do aplicativo por meio de aplicativos de terceiros, uma notificação aparece na barra de tarefas do Microsoft Windows, acima do ícone do aplicativo (a menos que o serviço de notificação tenha sido desativado pelo usuário). É possível permitir o gerenciamento externo de serviços de aplicativo somente em computadores incompatíveis com a tecnologia AM-PPL ou em computadores com a tecnologia desativada.

Parâmetro	Descrição
Adiar tarefas agendadas quando estiver em modo de bateria	Se esta caixa de seleção estiver marcada, o modo de economia de energia será ativado quando o computador estiver funcionando com bateria. O Kaspersky Endpoint Security adia tarefas agendadas. Você pode iniciar tarefas de verificação e de atualização manualmente, se necessário. Quando o modo de economia de energia está ativado e um computador está funcionando com a bateria, as seguintes tarefas não são executadas, mesmo que estejam programadas: • *Verificação completa*. • *Verificação de áreas críticas*. • *Verificação personalizada*. • *Verificação de integridade do aplicativo*. • *Verificação de IOC*. • *Atualização de bancos de dados e módulos do aplicativo* (somente patches) O aplicativo ignora as atualizações agendadas dos bancos de dados somente quando o laptop está sendo alimentado pela bateria e o nível de carga está abaixo de 30% (valor padrão). Você pode alterar o nível mínimo de carga da bateria a partir do qual o aplicativo começa a ignorar as atualizações agendadas dos bancos de dados de antivírus editando o Registro. Em todos os outros casos, o Kaspersky Endpoint Security atualiza os bancos de dados de acordo com o agendamento, independentemente do laptop estar conectado ou funcionando com energia da bateria ou se o aplicativo estiver no modo de economia de energia.
Conceder recursos a outros aplicativos	O consumo de recursos do computador pelo Kaspersky Endpoint 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 Endpoint 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 Endpoint 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 Endpoint Security leva mais tempo. Por padrão, o aplicativo está configurado para ceder recursos a outros aplicativos.
Limitar a utilização da CPU para tarefas de verificação	Para otimizar o desempenho do Kaspersky Endpoint Security, é possível limitar o uso da CPU pela tarefa *Verificação de malware*. Caso a caixa de seleção esteja marcada, a carga média em todos os núcleos da CPU da tarefa *Verificação de malware* aproxima-se do valor especificado. Por padrão, a caixa de seleção está desmarcada.
Ativar gravação do dump	Se a caixa de seleção for marcada, o Kaspersky Endpoint Security escreverá dumps quando ele travar. Se a caixa de seleção for desmarcada, o Kaspersky Endpoint Security não gravará dumps. O aplicativo também exclui arquivos de dump existentes do disco rígido do computador.
Ativar proteção de arquivos de dump e de rastreamento	Se a caixa de seleção for marcada, o acesso aos arquivos de despejo será concedido aos administradores de sistema e local, bem como ao usuário que ativou a gravação do dump. Somente administradores locais e do sistema podem acessar arquivos de rastreamento. Se a caixa de seleção for desmarcada, qualquer usuário poderá acessar arquivos de dump e de rastreamento.
Status do computador quando as configurações são aplicadas *(disponível apenas no console do Kaspersky Security Center)*	Configurações para exibir os status de computadores clientes com o Kaspersky Endpoint Security instalado no Web Console quando ocorrem erros ao aplicar uma política ou executar uma tarefa. Estão disponíveis os seguintes status: *OK*, *Aviso* e *Crítico*.
Instalar atualizações sem reiniciar o computador	Atualizar o aplicativo sem reinício do computador permite que você garanta a operação ininterrupta dos servidores. É possível atualizar o aplicativo sem reiniciar a partir da versão 11.10.0. Para atualizar uma versão anterior do aplicativo, é necessário reiniciar o computador. A partir da versão 11.11.0, é possível realizar as ações a seguir sem reiniciar o computador: • instalar patches • alterar o conjunto de componentes de aplicativos • instalar o Kaspersky Endpoint Security sobre o Kaspersky Security for Windows Server O valor padrão do parâmetro varia a depender do tipo do sistema operacional. Se o aplicativo estiver instalado em uma estação de trabalho, a opção de atualização do aplicativo sem reiniciar ficará desabilitada. Se o aplicativo estiver instalado em um servidor, a opção de atualização do aplicativo sem reiniciar ficará habilitada.

Parâmetro	Descrição
Compatibilidade com ferramentas de administração remota *(disponível apenas no console do Kaspersky Security Center)*	Caso o uso do Kaspersky Endpoint 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 esta opção seja selecionada, 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 Endpoint Security não esteja causando problemas com a sua RAT. Caso esta opção não seja selecionada, o modo de compatibilidade RAT será desativado. Por padrão, a caixa de seleção está desmarcada. Exemplo: Ao usar o navegador no modo RemoteApp, é possível que o Kaspersky Endpoint 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 do 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.

Relatórios e armazenamento

Relatórios

As informações sobre a operação de cada componente do Kaspersky Endpoint Security, os eventos de criptografia de dados, o desempenho de cada tarefa de verificação, a tarefa de atualização e de verificação de integridade e a operação geral do aplicativo são registrados nos relatórios.

Os relatórios são armazenados na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\Report`.

Backup

O *Backup* armazena cópias de backup de arquivos que foram excluídos ou modificados durante a desinfecção. Uma *cópia backup* é uma cópia de arquivo criada antes que o arquivo seja desinfectado ou excluído. As cópias de backup de arquivos são armazenadas em um formato especial e não representam uma ameaça.

As cópias de backup dos arquivos são armazenadas na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

Os usuários no grupo de Administradores têm permissão para acessar essa pasta. Direitos de acesso limitados a essa pasta são concedidos ao usuário cuja conta foi usada para instalar o Kaspersky Endpoint Security.

O Kaspersky Endpoint Security não fornece a capacidade de configurar permissões de acesso de usuário a cópias backup de arquivos.

Quarentena

A *Quarentena* é um armazenamento local especial no computador. O usuário pode colocar em quarentena arquivos que considere perigosos para o computador. Os arquivos em quarentena são armazenados em um estado criptografado e não ameaçam a segurança do dispositivo. O Kaspersky Endpoint Security usa a Quarentena somente quando estiver integrado com as soluções Detection and Response da Kaspersky. Em outros casos, o Kaspersky Endpoint Security coloca o arquivo relevante no Backup. Para obter informações sobre o gerenciamento da Quarentena como parte das soluções, consulte a Ajuda do Kaspersky Sandbox, a Ajuda do Kaspersky Endpoint Detection and Response Optimum, a Ajuda do Kaspersky Endpoint Detection and Response Expert, a Ajuda da Kaspersky Anti Targeted Attack Platform e a Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises).

A quarentena só pode ser configurada usando o Web Console. Também é possível usar o Web Console para gerenciar objetos em quarentena (restaurar, excluir, adicionar, etc). É possível restaurar os objetos localmente no computador usando a linha de comando.

O Kaspersky Endpoint Security usa a conta do sistema (SISTEMA) para os arquivos da quarentena.

Configurações de relatórios e armazenamento

Parâmetro	Descrição
Excluir relatórios após (dias)	Se a caixa de seleção estiver marcada, o prazo máximo de armazenamento do relatório será limitado ao intervalo de tempo definido. O período máximo padrão de armazenamento dos relatórios é de 30 dias. Após este período, o Kaspersky Endpoint Security exclui as entradas mais antigas do arquivo de relatório automaticamente.
Limitar a tamanho de arquivos de relatórios a (MB)	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 Endpoint Security exclui as entradas mais antigas do arquivo de relatório automaticamente quando for ultrapassado o tamanho máximo.
Excluir objetos após (dias)	Se a caixa de seleção estiver marcada, o prazo máximo de armazenamento do arquivo será limitado ao intervalo de tempo definido. O período máximo padrão de armazenamento de arquivos é de 30 dias. Depois da expiração do período máximo de armazenamento, o Kaspersky Endpoint Security excluirá os arquivos mais antigos do Backup.
Limitar o tamanho do backup a (MB)	Se a caixa de seleção estiver marcada, o tamanho máximo de armazenamento será limitado ao valor definido. Por padrão, a dimensão máxima é 1024 MB. Para evitar ultrapassar o tamanho máximo de armazenamento, o Kaspersky Endpoint Security exclui os arquivos mais antigos do arquivo automaticamente quando o tamanho máximo é atingido.
Limitar o tamanho da Quarentena	Caso a caixa de seleção esteja marcada, o tamanho máximo da quarentena será limitado ao valor definido. Por padrão, a dimensão máxima é 1024 MB. Quando a quarentena atingir o tamanho máximo, o Kaspersky Endpoint Security envia o evento *Não há espaço suficiente no armazenamento da Quarentena* ao Kaspersky Security Center e publica o evento no log de eventos do Windows. Enquanto isso, o aplicativo interrompe a quarentena de novos objetos. É preciso esvaziar a quarentena manualmente.
Notificar quando o armazenamento da Quarentena atingir (%)	Valor limite da quarentena. Por exemplo, é possível definir o limite da quarentena para 50%. Quando a quarentena atingir o limite, o Kaspersky Endpoint Security envia o evento correspondente ao Kaspersky Security Center e publica o evento no log de eventos do Windows. Enquanto isso, o aplicativo continua colocando novos objetos em quarentena.

Parâmetro	Descrição
Transferência de dados para o Servidor de Administração *(disponível apenas no Kaspersky Security Center)*	Categoria de eventos em computadores clientes cujas informações devem ser retransmitidas ao Servidor de Administração. Você pode desativar a transferência de alguns dados para otimizar o espaço em disco no Servidor de Administração. O aplicativo envia eventos das seguintes categorias: • **Sobre os arquivos na Quarentena**. É possível visualizar a lista de arquivos em quarentena no console do Kaspersky Security Center na pasta **Avançado** → **Repositórios** → **Quarentena**. O Kaspersky Endpoint Security usa a Quarentena somente quando estiver integrado com as soluções Detection and Response da Kaspersky. • **Sobre os arquivos no Backup**. É possível visualizar a lista de arquivos no Backup no console do Kaspersky Security Center na pasta **Avançado** → **Repositórios** → **Backup**. • **Sobre os arquivos não processados**. É possível visualizar a lista de arquivos não processados no console do Kaspersky Security Center na pasta **Avançado** → **Repositórios** → **Ameaças ativas**. • **Sobre os dispositivos instalados**. É possível visualizar a lista de dispositivos conectados no console do Kaspersky Security Center na pasta **Avançado** → **Repositórios** → **Hardware**. A lista de dispositivos também está disponível nas propriedades do computador e na política do Kaspersky Endpoint Security for Windows (seção **Controle de dispositivos**). • **Sobre os aplicativos iniciados**. É possível visualizar a lista de arquivos executáveis no console do Kaspersky Security Center na pasta **Avançado** → **Gerenciamento de aplicativos** → **Arquivos executáveis**. A lista de arquivos executáveis também está disponível nas propriedades do computador. • **Sobre os erros de criptografia de arquivos**. É possível visualizar a lista erros na criptografia de arquivos no console do Kaspersky Security Center na pasta **Avançado** → **Criptografia e proteção de dados** → **Eventos de criptografia**. A lista de erros também está disponível nas propriedades do computador. • **Relatório sobre o estado das regras de Controle Adaptativo de Anomalias**. Você pode visualizar o relatório no console do Kaspersky Security Center no nodo **Servidor de Administração** da guia **Relatórios**. Esse relatório também está disponível nas propriedades da política do Kaspersky Endpoint Security for Windows (seção **Controle Adaptativo de Anomalias**). • **Relatório sobre regras de Controle Adaptativo de Anomalias acionadas**. Você pode visualizar o relatório no console do Kaspersky Security Center no nodo **Servidor de Administração** da guia **Relatórios**. Esse relatório também está disponível nas propriedades da política do Kaspersky Endpoint Security for Windows (seção **Controle Adaptativo de Anomalias**). • **Sobre uma cadeia de desenvolvimento de ameaças**. Você pode visualizar os detalhes da detecção no Kaspersky Security Center Web Console na seção **Monitoramento** → **Alertas**. As informações sobre a cadeia de desenvolvimento de ameaças são usadas pelas soluções do Kaspersky Endpoint Detection and Response.

Configurações de rede

É possível configurar o servidor proxy usado para a conexão com a Internet e para atualização dos bancos de dados do antivírus; basta selecionar o modo de monitoramento de porta de rede e configurar a verificação de conexões criptografadas.

Opções de rede

Parâmetro	Descrição
Limitar o tráfego em conexões medidas	Se essa caixa de seleção estiver marcada, o aplicativo limitará o tráfego de rede quando a conexão com a Internet for limitada. O Kaspersky Endpoint 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.
Injetar script no tráfego da Web para interagir com páginas da Web	Se a caixa de seleção for selecionada, o Kaspersky Endpoint Security injetará um script de interação de página da Web no tráfego da Web. Este script garante que o componente Controle da Web funcione corretamente. O script permite o registro de eventos do Controle da Web. Sem esse script, você não pode habilitar o monitoramento da atividade do usuário na Internet. Os especialistas da Kaspersky recomendam injetar esse script de interação da página da Web no tráfego para garantir a operação correta do Controle da Web.
Configurações do servidor proxy	Configurações do servidor proxy usadas por usuários de computadores clientes para acessarem a Internet. O Kaspersky Endpoint Security usa essas configurações para certos componentes de proteção, inclusive para atualizar bancos de dados e módulos do aplicativo. Para a configuração automática de um servidor proxy, o Kaspersky Endpoint Security usa o protocolo WPAD (Web Proxy Auto-Discovery Protocol). Se o endereço IP do servidor proxy não puder ser determinado usando esse protocolo, o aplicativo o endereço do servidor proxy especificado nas configurações do Microsoft Internet Explorer.
Ignorar servidor proxy para endereços locais	Se a caixa de seleção for marcada, o Kaspersky Endpoint Security não usará um servidor proxy executando uma atualização de uma pasta compartilhada.

Parâmetro	Descrição
Configurações de autenticação do servidor proxy	Para autenticar o aplicativo no servidor proxy para acesso à Internet, é necessário inserir as credenciais do usuário. O Kaspersky Endpoint Security oferece suporte à autenticação automática no servidor proxy. Se a autenticação automática falhar, o aplicativo solicita que o usuário insira as credenciais. **Não usar autenticação**. **Autenticação NTLM**. Autenticação NTLM com a conta do usuário atual (padrão). **Autenticação NTLM com nome de usuário e senha**. Autenticação NTLM com credenciais especificadas manualmente. **Nome de usuário e senha**. Autenticação com credenciais especificadas manualmente. **Autenticação automática**. **Autenticação Kerberos**. Autenticação Kerberos com a conta do usuário atual. Para garantir que a autenticação Kerberos funcione corretamente ao usar registros CNAME para o endereço do servidor proxy, é necessário registrar um Nome Principal de Serviço (SPN) para cada registro CNAME. **Autenticação Kerberos com nome de usuário e senha**. Autenticação Kerberos com credenciais especificadas manualmente. Se a autenticação Kerberos for selecionada, o Kaspersky Endpoint Security poderá, dependendo das configurações do servidor proxy, realizar a autenticação usando o protocolo Kerberos ou NTLM.
Portas monitoradas	**Monitorar todas as portas de rede**. Neste modo de monitoramento de porta de rede, os componentes de proteção (Proteção Contra Ameaças ao Arquivo, Proteção contra ameaças da Web e Proteção contra ameaças de correio) monitoram os fluxos de dados transmitidos por meio de quaisquer portas de rede abertas do computador. **Monitorar somente 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. **Monitorar todas as portas de aplicativos na lista recomendada pela Kaspersky**. Uma lista predefinida de aplicativos cujas portas de rede são monitoradas pelo Kaspersky Endpoint Security é usada. Por exemplo, a lista inclui o Google Chrome, Adobe Reader, Java e outros aplicativos. **Monitorar todas as portas dos aplicativos especificados**. Uma lista de aplicativos cujas portas de rede são monitoradas pelo Kaspersky Endpoint Security é usada.
Verificação de conexões criptografadas	O Kaspersky Endpoint Security verifica o tráfego de rede criptografado transmitido através dos seguintes protocolos: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. O Kaspersky Endpoint Security tem suporte para os seguintes modos de verificação de conexões criptografadas: • **Não verificar conexões criptografadas**. O Kaspersky Endpoint Security não terá acesso ao conteúdo de sites cujos endereços comecem com `https://`. • **Verificar conexões criptografadas após solicitação de componentes de proteção**. O Kaspersky Endpoint Security verificará o tráfego criptografado apenas quando solicitado pelos componentes Proteção Contra Ameaças da Web, Proteção Contra Ameaças ao Correio e Controle da Web. • **Sempre verificar conexões criptografadas**. O Kaspersky Endpoint Security verificará o tráfego de rede criptografado mesmo se os componentes de proteção estiverem desativados. O Kaspersky Endpoint Security não verifica conexões criptografadas estabelecidas por aplicativos confiáveis para os quais a verificação de tráfego está desativada. O Kaspersky Endpoint Security não verifica conexões criptografadas da lista predefinida de sites confiáveis. A lista predefinida de sites confiáveis é criada por especialistas da Kaspersky. Esta lista é atualizada com os bancos de dados de antivírus do aplicativo. É possível visualizar a lista predefinida de sites confiáveis apenas na interface do Kaspersky Endpoint Security. Não é possível visualizar a lista no Console do Kaspersky Security Center.

Parâmetro	Descrição
Certificados raiz confiáveis	Lista de certificados raiz confiáveis. O Kaspersky Endpoint Security permite a instalação de certificados raiz confiáveis nos computadores dos usuários caso, por exemplo, seja necessário implementar um novo centro de certificação. O aplicativo permite adicionar um certificado para uma loja especial de certificado Kaspersky Endpoint Security. Neste caso, o certificado é considerado confiável somente para o aplicativo Kaspersky Endpoint Security. Em outras palavras, o usuário pode ter acesso a um site com um novo certificado no navegador. Caso outro aplicativo tente acessar o site, é possível ocorrer um erro de conexão devido a um problema de certificado. Para adicionar ao sistema de armazenamento de certificados, é possível usar as políticas do grupo do Active Directory.
Acesso a um domínio com um certificado não confiável	• **Permitir**. Ao visitar um domínio com um certificado não confiável, o Kaspersky Endpoint Security permitirá a conexão da rede. Ao abrir um domínio com um certificado não confiável em um navegador, o Kaspersky Endpoint Security exibe uma página HTML com um aviso e o motivo de o acesso ao domínio não ser recomendado. Um usuário pode clicar no link da página de aviso HTML para obter o acesso ao recurso da Web solicitado. Se um aplicativo ou serviço de terceiros estabelecer conexão com um domínio com um certificado não confiável, o Kaspersky Endpoint Security cria seu próprio certificado para verificar o tráfego. O novo certificado possui o status *Não confiável*. Isso é necessário para avisar o aplicativo de terceiros sobre a conexão não confiável, pois a página HTML não pode ser exibida nesse caso e a conexão pode ser estabelecida em modo de segundo plano. • **Bloquear**. Ao visitar um domínio com um certificado não confiável, o Kaspersky Endpoint Security bloqueará a conexão da rede. Ao abrir um domínio com um certificado não confiável em um navegador, o Kaspersky Endpoint Security exibe uma página HTML com o motivo pelo qual o domínio está bloqueado.
Acesso a um domínio com um erro de verificação de conexões criptografadas	• **Bloquear**. Caso um erro de verificação de conexão criptografada ocorra, o Kaspersky Endpoint Security bloqueará a conexão de rede. • **Permitir e adicionar domínio às exclusões**. Caso um erro de verificação de conexão criptografada ocorra, o Kaspersky Endpoint Security adicionará o domínio que resultou no erro à lista de domínios com erros de verificação e não monitorará o tráfego de rede criptografado quando este domínio for acessado. É possível visualizar uma lista de domínios com erros de verificação de conexões criptografadas apenas na interface local do aplicativo. Para limpar o conteúdo da lista, você precisa selecionar **Bloquear**. O Kaspersky Endpoint Security também gera um evento para o erro de verificação de conexões criptografadas.
Bloquear conexões SSL 2.0	Se a caixa de seleção estiver marcada, o aplicativo monitora e bloqueia as conexões de rede estabelecidas por meio do protocolo SSL 2.0. Se a caixa de seleção for desmarcada, o aplicativo não bloqueará as conexões de rede estabelecidas por meio do protocolo SSL 2.0. No entanto, o aplicativo não monitora o tráfego de rede por meio desse protocolo.
Bloquear conexões SSL 3.0	Se a caixa de seleção for marcada, o aplicativo bloqueará as conexões de rede estabelecidas por meio do protocolo SSL 3.0. Se a caixa de seleção for desmarcada, o aplicativo não bloqueará as conexões de rede estabelecidas por meio do protocolo SSL 3.0. O aplicativo monitora o tráfego de rede por meio desse protocolo. Todos os componentes do aplicativo funcionam sem restrições.
Bloquear conexões TLS 1.0	Se a caixa de seleção for marcada, o aplicativo bloqueará as conexões de rede estabelecidas por meio do protocolo TLS 1.0. Se a caixa de seleção for desmarcada, o aplicativo não bloqueará as conexões de rede estabelecidas por meio do protocolo TLS 1.0. O aplicativo monitora o tráfego de rede por meio desse protocolo. Todos os componentes do aplicativo funcionam sem restrições.
Descriptografar conexões criptografadas com sites que usam certificados EV	Os certificados EV (Extended Validation Certificate) confirmam a autenticidade dos sites e aumentam a segurança da conexão. Os navegadores usam um ícone de fechadura na sua barra de endereço para indicar que um site possui um certificado EV. Os navegadores também podem colorir total ou parcialmente a barra de endereço em verde. Se a caixa de seleção estiver selecionada, o aplicativo descriptografa e monitora as conexões criptografadas que usam um certificado EV. Se a caixa de seleção estiver desmarcada, o aplicativo não tem acesso ao conteúdo do tráfego HTTPS. Por esse motivo, o aplicativo monitora o tráfego HTTPS apenas com base no endereço do site, por exemplo, `https://bing.com`. Se você estiver abrindo um site com um certificado EV pela primeira vez, a conexão criptografada será descriptografada independentemente se a caixa foi ou não marcada.

Parâmetro	Descrição
Configurar endereços confiáveis	Uma lista de endereços da Web para os quais o Kaspersky Endpoint Security não verifica conexões de rede criptografadas é usada. Nesse caso, o Kaspersky Endpoint Security não verifica o tráfego HTTPS de endereços da Web confiáveis quando os componentes Proteção Contra Ameaças da Web, Proteção Contra Ameaças ao Correio e Controle da Web estão fazendo seu trabalho. É possível inserir um nome de domínio ou um endereço IP. O Kaspersky Endpoint Security é compatível com o caractere `*` para inserção de uma máscara no nome de domínio. O Kaspersky Endpoint Security não é compatível com o símbolo `*` para endereços IP. É possível selecionar um intervalo de endereços IP usando uma máscara de sub-rede (por exemplo, 198.51.100.0/24). Exemplos: • `domain.com`: o registro inclui os seguintes endereços: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. O registro é exclusivo de subdomínios (por exemplo, `subdomain.domain.com`). • `subdomain.domain.com`: o registro inclui os seguintes endereços: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. O registro é exclusivo do domínio `domain.com`. • `*.domain.com`: o registro inclui os seguintes endereços: `https://movies.domain.com`, `https://images.domain.com/page123`. O registro é exclusivo do domínio `domain.com`.
Configurar aplicativos confiáveis	Lista de aplicativos cuja atividade não é monitorada pelo Kaspersky Endpoint Security durante a sua operação. Você pode selecionar os tipos de atividade de aplicativo que o Kaspersky Endpoint Security não monitorará (por exemplo, não varre o tráfego de rede). O Kaspersky Endpoint Security oferece suporte a variáveis de ambiente e aos caracteres `*` e `?` ao inserir uma máscara.
Para verificar conexões criptografadas em aplicativos com armazenamento de certificados próprio, use *(disponível apenas na interface do Kaspersky Endpoint Security)*	Se esta caixa de seleção estiver marcada, o aplicativo verifica o tráfego criptografado no navegador Mozilla Firefox e no programa de e-mail Thunderbird. O acesso a alguns sites pelo protocolo HTTPS pode ser bloqueado. Para verificar o tráfego no navegador Mozilla Firefox e o cliente de correio Thunderbird, é necessário ativar a verificação de conexões criptografadas. Caso a verificação de conexões criptografadas esteja desativada, o aplicativo não verifica o tráfego no navegador Mozilla Firefox e no cliente de correio Thunderbird. O aplicativo usa o certificado raiz da Kaspersky para descriptografar e analisar o tráfego criptografado. Você pode selecionar o armazenamento/repositório de certificados que conterá o certificado raiz da Kaspersky. • **Repositório de certificados do Windows (recomendado)**. O certificado raiz da Kaspersky é adicionado a este repositório durante a instalação do Kaspersky Endpoint Security. • **Armazenamento de certificados próprio**. Mozilla Firefox e Thunderbird usam seus próprios repositórios de certificados. Se o armazenamento de certificados do Mozilla for selecionado, você precisará adicionar manualmente o certificado raiz da Kaspersky a este armazenamento por meio das propriedades do navegador.

Interface

Você pode definir as configurações da interface do aplicativo.

Configurações da interface

Parâmetro	Descrição
Interação com o usuário *(disponível apenas no console do Kaspersky Security Center)*	**Exibir interface simplificada**. Em um computador cliente, a janela principal do aplicativo está inacessível e apenas o ícone na área de notificação do Windows está disponível. No menu de contexto do ícone, o usuário pode executar um número limitado de operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security também exibe apenas as notificações que exigem ação do usuário acima do ícone do aplicativo. **Exibir interface do usuário**. Em um computador cliente, a janela principal do Kaspersky Endpoint Security e o ícone na área de notificação do Windows estão disponíveis. No menu de contexto do ícone, o usuário pode executar operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security também exibe notificações acima do ícone do aplicativo. **Ocultar a seção Monitoramento de atividades do aplicativo**. No computador cliente, na janela principal do Kaspersky Endpoint Security, o botão **Monitoramento de atividades do aplicativo** não está disponível. O *Monitoramento de atividades do aplicativo* é uma ferramenta desenvolvida para exibir informações sobre a atividade de aplicativos no computador de um usuário em tempo real. **Não exibir interface do usuário**. Em um computador cliente, nenhum sinal da operação do Kaspersky Endpoint Security é exibido. O ícone na área de notificação do Windows e as notificações não estão disponíveis.

Parâmetro	Descrição
Acessar tarefas locais	Se a caixa de seleção for marcada, as tarefas locais serão exibidas na interface local do Kaspersky Endpoint 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 essa caixa de seleção estiver desmarcada, as tarefas locais ficarão ocultas na interface do aplicativo. 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 Endpoint Security, ou ao trabalhar com a linha de comando. Um usuário ainda pode iniciar uma verificação de um Arquivo ou pasta selecionando a opção **Verificar Vírus** no menu de contexto do arquivo ou da pasta. A tarefa de verificação é iniciada com os valores padrões de configurações da tarefa de verificação personalizada.
Visualizar tarefas de grupo	Se a caixa de seleção for marcada, as tarefas de grupo serão exibidas na interface local do Kaspersky Endpoint Security. O usuário pode visualizar a lista de todas as tarefas na interface do aplicativo. Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security exibe uma lista de tarefas vazia.
Gerenciar tarefas de grupo	Se a caixa de seleção estiver marcada, os usuários podem iniciar e interromper as tarefas de grupo especificadas no console do Kaspersky Security Center. Os usuários podem iniciar e parar tarefas na interface do aplicativo ou na interface simplificada do aplicativo. Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security inicia tarefas agendadas automaticamente ou o administrador inicia tarefas manualmente no console do Kaspersky Security Center.
Configurar notificações	Uma tabela com as configurações de notificações sobre eventos de níveis de importância diferentes que podem ocorrer durante a operação de um componente, uma tarefa ou do aplicativo inteiro. O Kaspersky Endpoint Security mostra notificações sobre esses eventos na tela, envia-os por e-mail ou registra-os.
Configurar notificações por e-mail	Configurações do servidor SMTP para entrega de notificações sobre eventos registrados durante o funcionamento do aplicativo. Por padrão, o Kaspersky Endpoint Security usa as configurações de notificação por e-mail do Kaspersky Security Center. Para obter mais detalhes sobre as configurações de notificações por e-mail, consulte a Ajuda do Kaspersky Security Center. Se precisar configurar notificações por e-mail individuais, você pode editar as seguintes configurações: • **Endereço do remetente**. Endereço de e-mail do remetente. Não é recomendado usar um endereço inexistente. • **Servidor SMTP**. Um ou mais endereços de servidores de e-mail de sua organização (por exemplo, `mail.company.com`). É possível inserir um endereço IP (IPv4 ou IPv6). Para autenticar o usuário no servidor SMTP, insira as credenciais do remetente nos campos correspondentes. Para testar as notificações por e-mail, você pode enviar uma mensagem de teste. • **End. do destinatário**. Endereços de e-mail dos destinatários para os quais o aplicativo enviará notificações. • **Modo de envio**. Modo de envio de notificações por e-mail. O Kaspersky Endpoint Security pode enviar mensagens imediatamente quando ocorre um evento; de forma alternativa, a solução pode seguir uma programação pré-configurada.
Mostrar o status do aplicativo na área de notificações	Categorias de eventos do aplicativo que fazem com que o ícone do Kaspersky Endpoint Security seja alterado na área de notificação da barra de tarefas do Microsoft Windows (ou) e resultam em uma notificação pop-up.
Notificações de status do banco de dados antimalware local	Configurações de notificações sobre bancos de dados de antivírus desatualizados utilizados pelo aplicativo.
Proteção por senha	Se o botão de alternância estiver ativado, o Kaspersky Endpoint Security solicitará uma senha ao usuário quando ele tentar executar uma operação que esteja dentro do escopo da Proteção por senha. O escopo de proteção por senha inclui operações proibidas (como desativar componentes de proteção) e as contas de usuário às quais o escopo de proteção por senha é aplicado. Depois que a Proteção por senha estiver ativada, o Kaspersky Endpoint Security solicitará a definição de uma senha para a conta KLAdmin.
Suporte ao usuário / Links para recursos da Web *(disponível apenas no console do Kaspersky Security Center)*	Lista de links a recursos da Web que contêm informações sobre suporte técnico do Kaspersky Endpoint Security. Os links adicionados são exibidos na janela **Suporte** da interface local do Kaspersky Endpoint Security em vez dos links padrão.
Suporte ao usuário / Descrição *(disponível apenas no console do Kaspersky Security Center)*	Mensagem exibida na janela **Suporte** da interface local do Kaspersky Endpoint Security.

Gerenciar configurações

Você pode salvar as configurações atuais do Kaspersky Endpoint Security em um arquivo e usá-las para configurar rapidamente o aplicativo em um computador diferente. Também é possível usar um arquivo de configuração ao implementar o aplicativo por meio do Kaspersky Security Center com um pacote de instalação. Você pode restaurar as configurações padrão a qualquer momento.

As definições de gerenciamento da configuração do aplicativo estão disponíveis apenas na interface do Kaspersky Endpoint Security.

Definições de gerenciamento de configuração de aplicativo

Configurações	Descrição
Importar	Extraia configurações do aplicativo em um formato de arquivo CFG e aplique-as.
Exportar	Salve as configurações atuais do aplicativo em um arquivo no formato CFG.
Restaurar	É possível restaurar as configurações do aplicativo recomendadas pela Kaspersky a qualquer momento. Quando as configurações são restauradas, o nível de segurança **Recomendado** é definido para todos os componentes de proteção.

Atualizar bancos de dados e módulos do software aplicativo

A atualização dos bancos de dados e dos módulos do aplicativo do Kaspersky Endpoint Security assegura ao computador a versão de proteção mais recente. No mundo todo, novos tipos de vírus e malware surgem diariamente. Os bancos de dados do Kaspersky Endpoint Security contêm informações sobre ameaças e formas de neutralizá-las. Para detectar ameaças rapidamente, é necessário atualizar regularmente os bancos de dados e os módulos do aplicativo.

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.

Atualizações frequentes exigem uma licença em vigor. Se não houver uma licença atual, será possível executar a atualização apenas uma vez.

O computador precisa estar conectado à Internet para que o pacote de atualização possa ser baixado dos servidores de atualização da Kaspersky. Por padrão, as configurações de conexão com a Internet são definidas automaticamente. Se você usar um servidor proxy, é necessário ajustar as configurações do servidor proxy.

As atualizações são baixadas por meio do protocolo HTTPS. Elas também podem ser baixadas por meio do protocolo HTTP quando é impossível baixar atualizações pelo protocolo HTTPS.

Ao executar a atualização, os seguintes objetos são baixados e instalados no computador:

- Bancos de dados do Kaspersky Endpoint Security. A proteção do computador é fornecida utilizando bancos de dados com assinatura de vírus e outras ameaças e informações sobre a forma de neutralizá-las. Os componentes de proteção usam estas informações quando procuram e neutralizam arquivos infectados no computador. Os bancos de dados são constantemente atualizados com registros de novas ameaças e métodos para neutralizá-las. Portanto, é recomendável fazer a atualização dos bancos de dados regularmente.

  Além dos bancos de dados do Kaspersky Endpoint Security, também são atualizadas as unidades de rede que ativam os componentes do aplicativo de interceptação de tráfego de rede.

- Módulos do aplicativo. Além dos bancos de dados do Kaspersky Endpoint Security, faça também a atualização dos módulos do programa. A atualização dos módulos do aplicativo soluciona os problemas relativos a vulnerabilidades neste; adiciona novas funções ou aprimora as existentes.

Durante a atualização, os bancos de dados e os módulos do aplicativo no computador são comparados com a versão mais recente na fonte de atualização. Se forem encontradas diferenças nos bancos de dados e nos módulos do aplicativo, em relação às respectivas versões mais recentes, são instaladas as atualizações que faltam no computador.

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 Endpoint 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 resultados da atualização e sobre todos os eventos que ocorrem durante o desempenho da tarefa de atualização são registradas no relatório do Kaspersky Endpoint Security.

Se o aplicativo estiver funcionando em modo Light Agent, considerações especiais estarão envolvidas na atualização de módulos e bancos de dados do aplicativo.

Configurações da atualização do banco de dados e módulo de aplicativo

Parâmetro	Descrição
Cronograma de atualização dos bancos de dados	**Automaticamente**. Neste modo, o aplicativo verifica a fonte de atualização quanto à disponibilidade de novos pacotes de atualização com certa frequência. A frequência da verificação para o pacote de atualização aumenta durante os surtos e as reduções de vírus quando não há nenhum. Depois de detectar um pacote de atualização novo, o Kaspersky Endpoint Security baixa o pacote e instala atualizações no seu computador. **Manualmente**. Este modo de execução da tarefa de atualização permite iniciar a tarefa de atualização manualmente. **Por agendamento**. Neste modo de execução da tarefa de atualização, o Kaspersky Endpoint Security executa a tarefa de atualização conforme a agendamento que você especificou. Se esse modo de execução da tarefa de atualização for selecionado, você também poderá iniciar a tarefa de atualização do Kaspersky Endpoint Security manualmente.
Executar tarefas ignoradas	Caso a caixa de seleção esteja marcada, o Kaspersky Endpoint Security iniciará a tarefa de verificação ignorada assim que possível. A tarefa pode ser ignorada, por exemplo, se o computador estiver desligado na hora de início agendada para a tarefa de verificação. Quando o aplicativo tem a oportunidade de executar tarefas perdidas, ele executa as tarefas aleatoriamente dentro de um determinado intervalo de tempo para distribuir a carga no computador. Caso a caixa de seleção seja desmarcada, o Kaspersky Endpoint Security não executará as tarefas ignoradas. Em vez disso, ele executará a próxima tarefa de acordo com o agendamento atual.

Parâmetro	Descrição
Fontes de atualização	A *fonte de atualização* é um recurso que contém as atualizações dos bancos de dados e dos módulos do aplicativo do Kaspersky Internet Security. As fontes de atualização incluem o servidor do Kaspersky Security Center, servidores de atualização da Kaspersky e pastas de rede ou locais. Caso os servidores de atualização da Kaspersky não estejam disponíveis, o Kaspersky Endpoint Security poderá usar domínios alternativos para atualizar os bancos de dados e módulos do software do aplicativo. Para obter informações detalhadas, consulte a Base de Conhecimento do Suporte Técnico. A lista padrão de fontes de atualização inclui os servidores de atualização do Kaspersky Security Center e da Kaspersky. É possível adicionar outras fontes de atualização à lista. Você pode especificar servidores FTP ou HTTP e pastas compartilhadas como fontes de atualização. O Kaspersky Endpoint Security não oferece suporte as atualizações de servidores HTTPS, a menos que sejam servidores de atualização da Kaspersky. Se vários recursos forem selecionados como fontes de atualização, o Kaspersky Endpoint Security tentará se conectar a cada um deles, começando pelo primeiro na lista, e executará a tarefa de atualização fazendo a recuperação do pacote de atualização da primeira fonte disponível. Por padrão, o Kaspersky Endpoint Security usa o servidor do Kaspersky Security Center como a primeira fonte de atualização. Isso ajuda a conservar o tráfego durante a atualização. Se uma política não for aplicada ao computador, os servidores da Kaspersky serão selecionados como a primeira fonte de atualização nas configurações da tarefa de *Atualização de bancos de dados e módulos do aplicativo* local, pois o aplicativo pode não ter acesso ao servidor do Kaspersky Security Center. Se o aplicativo estiver em execução no modo Light Agent, uma pasta no SVM será selecionada como a fonte de atualização.
Executar atualizações do banco de dados como	Por padrão, a tarefa de atualização do Kaspersky Endpoint Security é executada em nome da conta de usuário usada para fazer login no sistema operacional. No entanto, o Kaspersky Endpoint Security pode ser atualizado a partir de uma fonte de atualização que o usuário não pode acessar devido à falta de direitos necessários (por exemplo, de uma pasta compartilhada que contém um pacote de atualização) ou uma fonte de atualização para a qual a autenticação do servidor proxy não está configurada. Nas configurações do aplicativo, especifique o usuário com os direitos necessários e execute a tarefa de atualização do aplicativo usando esta conta de usuário.
Baixar atualizações dos módulos do aplicativo	Baixar atualizações do módulo do aplicativo com atualizações do banco de dados do aplicativo. Se a caixa de seleção for marcada, o Kaspersky Endpoint Security notifica o usuário sobre atualizações disponíveis do módulo do aplicativo a e inclui atualizações do módulo do aplicativo no pacote de atualização enquanto executa a tarefa de atualização. O modo como as atualizações do módulo do aplicativo são aplicadas é determinado pelas seguintes configurações: • **Instalar atualizações críticas e confirmadas**. Se esta opção for selecionada, quando as atualizações do módulo do aplicativo estiverem disponíveis, o Kaspersky Endpoint 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 Endpoint 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 está selecionada por padrão. Se a caixa de seleção for desmarcada, o Kaspersky Endpoint Security não notificará o usuário sobre atualizações disponíveis do módulo do aplicativo e não incluirá atualizações do módulo do aplicativo no pacote de atualização enquanto executa a tarefa de atualização. 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. A caixa de seleção está marcada por padrão.
Copiar atualizações para a pasta	Se esta caixa de seleção for marcada, o Kaspersky Endpoint Security copia o pacote de atualização para a pasta compartilhada especificada abaixo da caixa de seleção. A partir de então, outros computadores na rede local poderão receber o pacote de atualização desta pasta compartilhada. Isso reduz o tráfego de Internet porque o pacote de atualização é baixado só uma vez. A seguinte pasta é especificada por padrão: `C:\ProgramData\Kaspersky Lab\KES.14.2\Update distribution\`.

Parâmetro	Descrição
Servidor proxy para atualizações *(disponível apenas na interface do Kaspersky Endpoint Security)*	Configurações do servidor proxy para acesso à Internet de usuários de computadores clientes para atualizar módulos de aplicativos e bancos de dados. Para a configuração automática de um servidor proxy, o Kaspersky Endpoint Security usa o protocolo WPAD (Web Proxy Auto-Discovery Protocol). Caso o endereço IP do servidor proxy não possa ser determinado com o uso desse protocolo, o Kaspersky Endpoint Security usará o endereço do servidor proxy especificado nas configurações do navegador Microsoft Internet Explorer.
Ignorar servidor proxy para endereços locais *(disponível apenas na interface do Kaspersky Endpoint Security)*	Se a caixa de seleção for marcada, o Kaspersky Endpoint Security não usará um servidor proxy executando uma atualização de uma pasta compartilhada.

Apêndice 2. Grupos de confiança de aplicativos

O Kaspersky Endpoint Security categoriza todos os aplicativos iniciados no computador em grupos de confiança. Os aplicativos são categorizados em grupos de confiança de acordo com o nível de risco que representam para o sistema operacional.

Os grupos de confiança são os seguintes:

- **Confiável**. Este grupo inclui aplicativos em que uma ou mais das seguintes condições são preenchidas:
  - Aplicativos são assinados digitalmente por fornecedores confiáveis.
  - Aplicativos são armazenados no banco de dados de aplicativos confiáveis do Kaspersky Security Network.
  - O usuário colocou o aplicativo no grupo *Confiável*.

  Estes aplicativos podem executar qualquer operação sem restrições.
- **Baixa restrição**. Este grupo inclui aplicativos em que as seguintes condições são preenchidas:
  - Aplicativos não são assinados digitalmente por fornecedores confiáveis.
  - Aplicativos não são armazenados no banco de dados de aplicativos confiáveis do Kaspersky Security Network.
  - O usuário colocou o aplicativo no grupo *Baixa restrição*.

  Estes aplicativos estão sujeitos a restrições mínimas de acesso aos recursos do sistema.
- **Alta restrição**. Este grupo inclui aplicativos em que as seguintes condições são preenchidas:
  - Aplicativos não são assinados digitalmente por fornecedores confiáveis.
  - Aplicativos não são armazenados no banco de dados de aplicativos confiáveis do Kaspersky Security Network.
  - O usuário colocou o aplicativo no grupo *Alta restrição*.

  Estes aplicativos estão sujeitos a altas restrições de acesso aos recursos do sistema.

- **Não confiável**. Este grupo inclui aplicativos em que as seguintes condições são preenchidas:
  - Aplicativos não são assinados digitalmente por fornecedores confiáveis.
  - Aplicativos não são armazenados no banco de dados de aplicativos confiáveis do Kaspersky Security Network.
  - O usuário colocou o aplicativo no grupo *Não confiável*.

  Para esses aplicativos, todas as operações estão bloqueadas.

Apêndice 3. Extensões de arquivo para verificação rápida de unidades removíveis

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

Apêndice 4. Tipos de arquivos para o filtro de anexos da Proteção Contra Ameaças ao Correio

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

Se você ativar a filtragem de anexos de e-mail, o componente Proteção Contra Ameaças ao Correio pode renomear ou excluir arquivos com as seguintes extensões:

com – arquivo executável de um aplicativo de até 64 KB

exe – arquivo executável ou arquivo autoextraível

sys – arquivo do sistema Microsoft Windows

prg – texto de programa 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

Apêndice 5. Configurações de rede para interação com serviços externos

O Kaspersky Endpoint Security e o Kaspersky Security Center usam um canal de comunicação criptografado com TLS (Transport Layer Security) para trabalhar com serviços externos da Kaspersky.

O Kaspersky Endpoint Security usa as seguintes configurações de rede para interagir com serviços externos.

Configurações de rede

Endereço	Descrição
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protocolo: `HTTPS` Porta: `443`	Ativar o aplicativo.

Endereço	Descrição

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
Protocolo: `HTTPS`
Porta: `443`
	Atualizar bancos de dados e módulos do software do aplicativo.

`downloads.upd.kaspersky.com` Protocolo: `HTTPS` Porta: `443`	• Atualizar bancos de dados e módulos do software do aplicativo. • Verificando o acesso aos servidores da Kaspersky. Se o acesso aos servidores que usam o sistema DNS não for possível, o aplicativo usará um DNS público. Isso é necessário para garantir que os bancos de dados de antivírus estejam atualizados e o nível de segurança para o computador seja mantido. O Kaspersky Endpoint Security usa a lista a seguir de servidores de DNS público na seguinte ordem: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168). As solicitações emitidas pelo aplicativo podem conter endereços de domínios e o endereço IP público do usuário porque o aplicativo estabelece uma conexão TCP/UDP com o servidor DNS. Essas informações são necessárias, por exemplo, para validar o certificado de um recurso da Web ao usar HTTPS. Se o Kaspersky Endpoint Security estiver usando um servidor DNS público, o processamento dos dados será regido pela política de privacidade do serviço relevante. Se você quiser evitar que o Kaspersky Endpoint Security use um servidor DNS público, entre em contato com o Suporte Técnico para obter um patch privado.
`touch.kaspersky.com` Protocolo: `HTTP`	• Recebimento do tempo confiável para verificar o período de validade do certificado (conexão TLS). • Aviso sobre o acesso negado a um recurso da Web no navegador quando a Proteção Contra Ameaças da Web estiver em execução.

Endereço	Descrição

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
`cm.k.kaspersky-labs.com`
Protocolo: `HTTP`
Porta: `80`
	Atualizar bancos de dados e módulos do software do aplicativo.

`ds.kaspersky.com`
`dc1.ksn.kaspersky-labs.com`
`dc1-file.ksn.kaspersky-labs.com`
`dc1-pp.ksn.kaspersky-labs.com`
`dc1-st.ksn.kaspersky-labs.com`
Protocolo: `HTTPS`
Porta: `443`
	Usar a Kaspersky Security Network.

`ksn-a-stat-geo.kaspersky-labs.com`
`ksn-file-geo.kaspersky-labs.com`
`ksn-verdict-geo.kaspersky-labs.com`
`ksn-url-geo.kaspersky-labs.com`
`ksn-a-p2p-geo.kaspersky-labs.com`
`ksn-info-geo.kaspersky-labs.com`
`ksn-cinfo-geo.kaspersky-labs.com`
Protocolo: `KSN`
Porta: `443`, `1443`
	Usar a Kaspersky Security Network.

`click.kaspersky.com`
`redirect.kaspersky.com`
Protocolo: `HTTPS`
Porta: `443`
	Siga os links da interface.

Configurações, usadas para criptografia

Endereço	Descrição

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protocolo: `HTTP`
Porta: `80`
	Infraestrutura de chave pública (PKI).

Apêndice 6. Eventos do aplicativo

Informações sobre a operação de cada componente do Kaspersky Endpoint Security, eventos de criptografia de dados, a conclusão de cada tarefa de verificação de malware, a tarefa de atualização e de verificação de integridade e a operação geral do aplicativo são registrados no log de eventos do Kaspersky Security Center e no log de eventos do Windows.

O Kaspersky Endpoint Security gera eventos dos seguintes tipos: eventos gerais e eventos específicos. Os eventos específicos são criados somente pelo Kaspersky Endpoint Security for Windows. Eventos específicos possuem um ID simples, como `000000cb`. Os eventos específicos contém as seguintes configurações requeridas:

- `GNRL_EA_DESCRIPTION` é o conteúdo do evento.
- `GNRL_EA_ID` é o ID do serviço do evento.
- `GNRL_EA_SEVERITY` é o status do evento. `1` – *Informações*, `2` – *Advertência*, `3` – *Falha funcional*, `4` – *Crítico*.
- `EVENT_TYPE_DISPLAY_NAME` é o título do evento.
- `TASK_DISPLAY_NAME` é o nome do componente do aplicativo que iniciou o evento.

Os eventos gerais podem ser criados pelo Kaspersky Endpoint Security for Windows, assim como outros aplicativos da Kaspersky (por exemplo, Kaspersky Security for Windows Server). Eventos gerais possuem um ID mais complexo, como `GNRL_EV_VIRUS_FOUND`. Além das configurações necessárias, os eventos gerais contêm configurações avançadas.

Por quanto tempo os eventos são armazenados no servidor

Crítico

A licença expirou

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	`201`
ID do evento do Kaspersky Security Center	`GNRL_EV_LICENSE_EXPIRATION`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

A licença está quase expirada

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	`203`
ID do evento do Kaspersky Security Center	`000000cb`

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Bancos de dados ausentes ou corrompidos

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	206
ID do evento do Kaspersky Security Center	000000ce
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Os bancos de dados estão obsoletos

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	207
ID do evento do Kaspersky Security Center	000000cf
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

A execução automática do aplicativo está desativada

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	209
ID do evento do Kaspersky Security Center	000000d1
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro de ativação

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	229
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Ameaça ativa detectada. A Desinfecção avançada deve ser iniciada

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	231
ID do evento do Kaspersky Security Center	000000e7

Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Servidores da KSN indisponíveis

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	2023
ID do evento do Kaspersky Security Center	000007e7
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Não há espaço suficiente no armazenamento da Quarentena

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	343
ID do evento do Kaspersky Security Center	00000157
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto não restaurado da Quarentena

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	346
ID do evento do Kaspersky Security Center	0000015a
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto não excluído da Quarentena

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	348
ID do evento do Kaspersky Security Center	0000015c
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Um aplicativo que não é um navegador tem permissão para visitar um site com um certificado não confiável

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	57
ID do evento do Kaspersky Security Center	00000039

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Falha ao verificar uma conexão criptografada. O domínio foi adicionado à lista de exclusões

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	`60`
ID do evento do Kaspersky Security Center	`0000003c`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto malicioso detectado (bases locais)

Status	!
Componente	Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças da Web Proteção Contra Ameaças ao Correio Proteção AMSI Prevenção de Intrusão do Host Detecção de Comportamento Anticryptor Prevenção de Exploits Verificação de malware
ID de evento do Windows	`302`
ID do evento do Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Parâmetros do evento	• `GNRL_EA_PARAM_1` é o hash do objeto (SHA256). • `GNRL_EA_PARAM_2` é o nome do objeto. Quando a criptografia externa de pastas compartilhadas é detectada, o aplicativo mostra o caminho para o arquivo de destino. • `GNRL_EA_PARAM_5` é o nome da ameaça de acordo com a classificação da Kaspersky, por exemplo, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` é o nome do usuário da sessão. • `GNRL_EA_PARAM_8` é o tipo de ameaça (`tipo`). • `GNRL_EA_PARAM_9` são as informações adicionais sobre o objeto detectado: Componente de aplicativo (`engine`). Tecnologia de detecção de ameaça (`method`). Ameaças detectadas pela Kaspersky Private Security Network (`blacklist`): `true` ou `false`. EDR version. Identificador de ameaça no EDR. Hash MD5 do objeto.
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto malicioso detectado (KSN)

Status	!
Componente	Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças da Web Proteção Contra Ameaças ao Correio Proteção AMSI Prevenção de Intrusão do Host Detecção de Comportamento Anticryptor Prevenção de Exploits Verificação de malware
ID de evento do Windows	`302`
ID do evento do Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Parâmetros do evento	• `GNRL_EA_PARAM_1` é o hash do objeto (SHA256). • `GNRL_EA_PARAM_2` é o nome do objeto. • `GNRL_EA_PARAM_5` é o nome da ameaça de acordo com a classificação da Kaspersky, por exemplo, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` é o nome do usuário da sessão. • `GNRL_EA_PARAM_8` é o tipo de ameaça (`tipo`). • `GNRL_EA_PARAM_9` são as informações adicionais sobre o objeto detectado: Componente de aplicativo (`engine`). Tecnologia de detecção de ameaça (`method`). Ameaças detectadas pela Kaspersky Private Security Network (`blacklist`): `true` ou `false`. EDR version. Identificador de ameaça no EDR. Hash MD5 do objeto.
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Não é possível desinfectar

Status	!
Componente	Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças ao Correio Prevenção de Intrusão do Host Detecção de Comportamento Anticryptor Verificação de malware
ID de evento do Windows	`312`
ID do evento do Kaspersky Security Center	`GNRL_EV_OBJECT_NOTCURED`
Parâmetros do evento	• `GNRL_EA_PARAM_1` é o hash do objeto (SHA256). • `GNRL_EA_PARAM_2` é o nome do objeto. • `GNRL_EA_PARAM_5` é o nome da ameaça de acordo com a classificação da Kaspersky, por exemplo, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` é o nome do usuário da sessão. • `GNRL_EA_PARAM_8` é o tipo de ameaça (`tipo`). • `GNRL_EA_PARAM_9` são as informações adicionais sobre o objeto detectado: Componente de aplicativo (`engine`). Tecnologia de detecção de ameaça (`method`). Ameaças detectadas pela Kaspersky Private Security Network (`blacklist`): `true` ou `false`. EDR version. Identificador de ameaça no EDR. Hash MD5 do objeto.
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Não pode ser excluído

Status	!
Componente	Proteção Contra Ameaças ao Arquivo Prevenção de Intrusão do Host Detecção de Comportamento Anticryptor Verificação de malware
ID de evento do Windows	313
ID do evento do Kaspersky Security Center	00000139
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro de processamento

Status	!
Componente	Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças da Web Proteção Contra Ameaças ao Correio Prevenção de Intrusão do Host Proteção AMSI Verificação de malware
ID de evento do Windows	317
ID do evento do Kaspersky Security Center	0000013d
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Processo encerrado

Status	!
Componente	Proteção Contra Ameaças ao Arquivo Prevenção de Intrusão do Host Detecção de Comportamento Verificação de malware
ID de evento do Windows	452
ID do evento do Kaspersky Security Center	000001c4
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Não foi possível encerrar o processo

Status	!
Componente	Proteção Contra Ameaças ao Arquivo Prevenção de Intrusão do Host Detecção de Comportamento Verificação de malware
ID de evento do Windows	453
ID do evento do Kaspersky Security Center	000001c5
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Link perigoso bloqueado

Status	!
Componente	Proteção Contra Ameaças da Web
ID de evento do Windows	362
ID do evento do Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_BLOCKED
Parâmetros do evento	• GNRL_EA_PARAM_2 é o caminho para o objeto. • GNRL_EA_PARAM_5 é o nome do objeto de acordo com a classificação Kaspersky. • GNRL_EA_PARAM_7 é o nome do usuário da sessão. • GNRL_EA_PARAM_8 é o tipo de ameaça (tipo). • GNRL_EA_PARAM_9 são as informações adicionais sobre o objeto detectado: Componente de aplicativo (engine). Tecnologia de detecção de ameaça (method). Ameaça detectada pela KSN Privada (blacklist): true ou false.
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Link perigoso aberto

Status	!
Componente	Proteção Contra Ameaças da Web
ID de evento do Windows	363
ID do evento do Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_REPORTED
Parâmetros do evento	• GNRL_EA_PARAM_2 é o caminho para o objeto. • GNRL_EA_PARAM_5 é o nome do objeto de acordo com a classificação Kaspersky. • GNRL_EA_PARAM_7 é o nome do usuário da sessão. • GNRL_EA_PARAM_8 é o tipo de ameaça (tipo). • GNRL_EA_PARAM_9 são as informações adicionais sobre o objeto detectado: Componente de aplicativo (engine). Tecnologia de detecção de ameaça (method). Ameaça detectada pela KSN Privada (blacklist): true ou false.
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Detectado link perigoso aberto anteriormente

Status	!
Componente	Proteção Contra Ameaças da Web
ID de evento do Windows	1201
ID do evento do Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_PASSED
Parâmetros do evento	• GNRL_EA_PARAM_2 é o caminho para o objeto. • GNRL_EA_PARAM_5 é o nome do objeto de acordo com a classificação Kaspersky. • GNRL_EA_PARAM_7 é o nome do usuário da sessão. • GNRL_EA_PARAM_8 é o tipo de ameaça (tipo). • GNRL_EA_PARAM_9 são as informações adicionais sobre o objeto detectado: Componente de aplicativo (engine). Tecnologia de detecção de ameaça (method). Ameaça detectada pela KSN Privada (blacklist): true ou false.
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Ação do processo bloqueada

Status	!
Componente	Controle Adaptativo de Anomalias
ID de evento do Windows	`2200`
ID do evento do Kaspersky Security Center	`GNRL_EV_ADSEC_DETECT`
Parâmetros do evento	• `GNRL_EA_PARAM_1` é o nome da regra do controle adaptativo de anomalia. • `GNRL_EA_PARAM_2` é o ID da regra heurística. • `GNRL_EA_PARAM_3` é o nome do usuário da sessão. • `GNRL_EA_PARAM_4` está no processo de origem. • `GNRL_EA_PARAM_5` está no objeto de origem. • `GNRL_EA_PARAM_6` está no processo de destino. • `GNRL_EA_PARAM_7` é o objeto de destino. • `GNRL_EA_PARAM_8` são as informações adicionais sobre o objeto detectado: Somas de verificação do processo de origem/objeto e processo de destino/objeto. Processo bloqueado (`verdict_type`): `true` ou `false`. ID de segurança do usuário (SID).
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Teclado não autorizado

Status	!
Componente	Prevenção contra ataque BadUSB
ID de evento do Windows	`2051`
ID do evento do Kaspersky Security Center	`00000803`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

A solicitação AMSI foi bloqueada

Status	!
Componente	Proteção AMSI
ID de evento do Windows	`2200`
ID do evento do Kaspersky Security Center	`00000898`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Atividade de rede bloqueada

Status	!
Componente	Firewall
ID de evento do Windows	`602`
ID do evento do Kaspersky Security Center	`00000329`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Ataque de rede detectado

Status	!
Componente	Proteção Contra Ameaças à Rede
ID de evento do Windows	`651`
ID do evento do Kaspersky Security Center	`GNRL_EV_ATTACK_DETECTED`
Parâmetros do evento	• `GNRL_EA_PARAM_1` é o nome do ataque. • `GNRL_EA_PARAM_2` é o protocolo. • `GNRL_EA_PARAM_3` é o endereço IP do computador agindo como a fonte do ataque à rede. O endereço IP está indicado na ordem de byte do host. Por exemplo, `2886729929` para `172.16.0.201`. • `GNRL_EA_PARAM_4` é o número da porta. • `GNRL_EA_PARAM_5` é um endereço IPv6, por exemplo, `12B012B012B012B012B012B012B012B0`. • `GNRL_EA_PARAM_6` é o endereço IP do computador alvo para o ataque à rede. O endereço IP está indicado na ordem de byte do host. Por exemplo, `2886729929` para `172.16.0.201`.
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Proibida a inicialização do aplicativo

Status	!
Componente	Controle de aplicativos
ID de evento do Windows	`702`
ID do evento do Kaspersky Security Center	`GNRL_EV_APPLICATION_LAUNCH_DENIED`
Parâmetros do evento	• `GNRL_EA_PARAM_2` é o nome do usuário da sessão. • `GNRL_EA_PARAM_3` é o identificador de categoria criado manualmente. • `GNRL_EA_PARAM_4` é o ID da categoria do aplicativo. • `GNRL_EA_PARAM_5` é a informação sobre a assinatura digital do aplicativo. • `GNRL_EA_PARAM_6` é o nome do arquivo executável do aplicativo (por exemplo, chrome.exe). • `GNRL_EA_PARAM_7` é o caminho do arquivo executável. • `GNRL_EA_PARAM_8` é o hash do objeto (SHA256). • `GNRL_EA_PARAM_9` é a versão do aplicativo que o usuário está tentando executar.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Processo proibido foi iniciado antes da inicialização do Kaspersky Endpoint Security

Status	!
Componente	Controle de aplicativos
ID de evento do Windows	`710`
ID do evento do Kaspersky Security Center	`000002c6`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Acesso negado (bases locais)

Status	!
Componente	Controle da Web

ID de evento do Windows	752
ID do evento do Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED
Parâmetros do evento	• GNRL_EA_PARAM_1 é o URL. • GNRL_EA_PARAM_2 é o nome do usuário da sessão. • GNRL_EA_PARAM_3 é o nome da regra do controle da web.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Acesso negado (KSN)

Status	!
Componente	Controle da Web
ID de evento do Windows	752
ID do evento do Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED_BY_KSN
Parâmetros do evento	• GNRL_EA_PARAM_1 é o URL. • GNRL_EA_PARAM_2 é o nome do usuário da sessão. • GNRL_EA_PARAM_3 é o nome da regra do controle da web.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Operação com o dispositivo proibida

Status	!
Componente	Controle de dispositivos
ID de evento do Windows	802
ID do evento do Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Parâmetros do evento	• GNRL_EA_PARAM_1 é o ID do hardware (HWID). • GNRL_EA_PARAM_2 é o nome do usuário da sessão.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Conexão de rede bloqueada

Status	!
Componente	Controle de dispositivos
ID de evento do Windows	809
ID do evento do Kaspersky Security Center	00000329
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

A operação com o dispositivo é proibida até que o Kaspersky Endpoint Security seja iniciado

Status	!
Componente	Controle de dispositivos
ID de evento do Windows	816
ID do evento do Kaspersky Security Center	00000330

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

A conexão do dispositivo é proibida até que o Kaspersky Endpoint Security seja iniciado

Status	!
Componente	Controle de dispositivos
ID de evento do Windows	817
ID do evento do Kaspersky Security Center	00000331
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro ao atualizar componente

Status	!
Componente	Atualização
ID de evento do Windows	1011
ID do evento do Kaspersky Security Center	000003f3
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro ao distribuir atualizações do componente

Status	!
Componente	Atualização
ID de evento do Windows	1012
ID do evento do Kaspersky Security Center	000003f4
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Erro de atualização local

Status	!
Componente	Atualização
ID de evento do Windows	1014
ID do evento do Kaspersky Security Center	000003f6
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Erro de atualização de rede

Status	!
Componente	Atualização
ID de evento do Windows	1015
ID do evento do Kaspersky Security Center	000003f7

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Não é possível iniciar duas tarefas simultaneamente

Status	ⓘ
Componente	Atualização
ID de evento do Windows	`1017`
ID do evento do Kaspersky Security Center	`000003f9`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro ao verificar os bancos de dados e módulos do aplicativo

Status	ⓘ
Componente	Atualização
ID de evento do Windows	`1018`
ID do evento do Kaspersky Security Center	`000003fa`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro de interação com o Kaspersky Security Center

Status	ⓘ
Componente	Atualização
ID de evento do Windows	`1019`
ID do evento do Kaspersky Security Center	`000003fb`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Nem todos os componentes foram atualizados

Status	ⓘ
Componente	Atualização
ID de evento do Windows	`1021`
ID do evento do Kaspersky Security Center	`000003fd`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Atualização concluída com êxito, falha na distribuição de atualizações

Status	ⓘ
Componente	Atualização
ID de evento do Windows	`1023`
ID do evento do Kaspersky Security Center	`000003ff`

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Erro interno de tarefa

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	101
ID do evento do Kaspersky Security Center	00000065
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Falha na instalação do patch

Status	!
Componente	Atualização
ID de evento do Windows	2153
ID do evento do Kaspersky Security Center	00000869
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Falha na reversão do patch

Status	!
Componente	Atualização
ID de evento do Windows	2156
ID do evento do Kaspersky Security Center	0000086c
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro na aplicação das regras de criptografia/descriptografia do arquivo

Status	!
Componente	Criptografia de dados
ID de evento do Windows	904
ID do evento do Kaspersky Security Center	00000388
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro na criptografia/descriptografia do arquivo

Status	!
Componente	Criptografia de dados
ID de evento do Windows	912

ID do evento do Kaspersky Security Center	`GNRL_EV_ENCRYPTION_ERROR`
Parâmetros do evento	• `GNRL_EA_PARAM_1` é o caminho para o arquivo. • `GNRL_EA_PARAM_2` é a causa do erro. • `GNRL_EA_PARAM_3` é o tipo do dispositivo.
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Acesso ao arquivo bloqueado

Status	!
Componente	Criptografia de dados
ID de evento do Windows	`940`
ID do evento do Kaspersky Security Center	`GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION`
Parâmetros do evento	• `GNRL_EA_PARAM_1` é o objeto de destino. • `GNRL_EA_PARAM_2` é o nome do usuário da sessão. • `GNRL_EA_PARAM_3` é o nome do arquivo executável do aplicativo (por exemplo, chrome.exe) que está tentando obter acesso ao arquivo.
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Erro ao ativar o modo portátil

Status	!
Componente	Criptografia de dados
ID de evento do Windows	`951`
ID do evento do Kaspersky Security Center	`000003b7`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro ao desativar o modo portátil

Status	!
Componente	Criptografia de dados
ID de evento do Windows	`953`
ID do evento do Kaspersky Security Center	`000003b9`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro ao criar pacote criptografado

Status	!
Componente	Criptografia de dados
ID de evento do Windows	`931`
ID do evento do Kaspersky Security Center	`000003a3`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro ao criptografar/descriptografar dispositivo

Status	!
Componente	Criptografia de dados
ID de evento do Windows	1305
ID do evento do Kaspersky Security Center	00000519
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Não foi possível carregar o módulo de criptografia

Status	!
Componente	Criptografia de dados
ID de evento do Windows	1311
ID do evento do Kaspersky Security Center	0000051f
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

A tarefa de gerenciamento de contas do Agente de Autenticação terminou com um erro

Status	!
Componente	Criptografia de dados
ID de evento do Windows	1340
ID do evento do Kaspersky Security Center	0000053c
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

A política não pode ser aplicada

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	1312
ID do evento do Kaspersky Security Center	00000520
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Falha ao atualizar FDE

Status	!
Componente	Criptografia de dados
ID de evento do Windows	1342
ID do evento do Kaspersky Security Center	0000053e
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Falha na reversão da atualização de FDE (para mais informações, consulte a Ajuda on-line do Kaspersky Endpoint Security for Windows)

Status	!
Componente	Criptografia de dados
ID de evento do Windows	1344
ID do evento do Kaspersky Security Center	00000540
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O servidor da Kaspersky Anti Targeted Attack Platform está indisponível

Status	!
Componente	Endpoint Sensor
ID de evento do Windows	2100
ID do evento do Kaspersky Security Center	00000834
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Falha ao excluir objeto

Status	!
Componente	Sandbox
ID de evento do Windows	2252
ID do evento do Kaspersky Security Center	000008cc
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto não está na quarentena (Sandbox)

Status	!
Componente	Sandbox
ID de evento do Windows	2603
ID do evento do Kaspersky Security Center	00000a2b
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Ocorreu um erro interno

Status	!
Componente	Sandbox
ID de evento do Windows	2607
ID do evento do Kaspersky Security Center	00000a2f
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Certificado de servidor do Sandbox inválido

Status	!
Componente	Sandbox
ID de evento do Windows	2613
ID do evento do Kaspersky Security Center	00000a35
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O nó do Sandbox está indisponível

Status	!
Componente	Sandbox
ID de evento do Windows	2614
ID do evento do Kaspersky Security Center	00000a36
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro ao processar o objeto no Sandbox

Status	!
Componente	Sandbox
ID de evento do Windows	2617
ID do evento do Kaspersky Security Center	00000a39
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

A carga máxima para o Sandbox foi excedida

Status	!
Componente	Sandbox
ID de evento do Windows	2618
ID do evento do Kaspersky Security Center	00000a3a
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

IOC encontrado

Status	!
Componente	Endpoint Detection and Response
ID de evento do Windows	2651
ID do evento do Kaspersky Security Center	00000a5b
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Falha de verificação de licença do Sandbox

Status	!
Componente	Sandbox
ID de evento do Windows	2620
ID do evento do Kaspersky Security Center	00000a3c
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro no envio da tarefa de verificação para o Sandbox por um usuário

Status	!
Componente	Sandbox
ID de evento do Windows	2623
ID do evento do Kaspersky Security Center	00000a3e
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro ao criar a tarefa do Sandbox

Status	!
Componente	Sandbox
ID de evento do Windows	2621
ID do evento do Kaspersky Security Center	00000a3d
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Inicialização de objeto bloqueada

Status	!
Componente	Endpoint Detection and Response
ID de evento do Windows	2553
ID do evento do Kaspersky Security Center	000009f9
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Inicialização de processo bloqueada

Status	!
Componente	Endpoint Detection and Response
ID de evento do Windows	2551
ID do evento do Kaspersky Security Center	000009f7
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Execução de script bloqueada

Status	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2559
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O objeto não está na quarentena (Endpoint Detection and Response)

Status	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2556
ID do evento do Kaspersky Security Center	000009fc
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

A inicialização de processo não está bloqueada

Status	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2561
ID do evento do Kaspersky Security Center	00000a01
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O objeto não está bloqueado

Status	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2562
ID do evento do Kaspersky Security Center	00000a02
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

A execução de scripts não está bloqueada

Status	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2563
ID do evento do Kaspersky Security Center	00000a03
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro ao alterar componentes do aplicativo

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	1401
ID do evento do Kaspersky Security Center	00000579
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Há padrões de um possível ataque de força bruta no sistema

Status	!
Componente	Inspeção de log
ID de evento do Windows	2800
ID do evento do Kaspersky Security Center	00000af0
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Há padrões de uma possível violação do Log de Eventos do Windows

Status	!
Componente	Inspeção do Log
ID de evento do Windows	2801
ID do evento do Kaspersky Security Center	00000af1
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Ações atípicas detectadas em nome de um novo serviço instalado

Status	!
Componente	Inspeção do Log
ID de evento do Windows	2802
ID do evento do Kaspersky Security Center	00000af2
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Detectado logon atípico que usa credenciais explícitas

Status	!
Componente	Inspeção de log
ID de evento do Windows	2803
ID do evento do Kaspersky Security Center	00000af3
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Existem padrões de um possível ataque PAC se passando por Kerberos (MS14-068) no sistema

Status	!
Componente	Inspeção de log
ID de evento do Windows	2804
ID do evento do Kaspersky Security Center	00000af4
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Alterações suspeitas detectadas no grupo de administradores integrado privilegiado

Status	!
Componente	Inspeção do Log
ID de evento do Windows	2805
ID do evento do Kaspersky Security Center	00000af5
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Há uma atividade atípica detectada durante a sessão de logon na rede

Status	!
Componente	Inspeção de log
ID de evento do Windows	2806
ID do evento do Kaspersky Security Center	00000af6
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Acionada regra de inspeção de log

Status	!
Componente	Inspeção de log
ID de evento do Windows	2807
ID do evento do Kaspersky Security Center	00000af7
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Evento atípico acontecendo com muita frequência. Iniciada agregação de evento

Status	!
Componente	Inspeção do Log
ID de evento do Windows	2808
ID do evento do Kaspersky Security Center	00000af8
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Relatório sobre evento atípico para o período de agregação

Status	!
Componente	Inspeção do Log
ID de evento do Windows	2809
ID do evento do Kaspersky Security Center	00000af9
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro ao conectar ao servidor da EDR Expert

Status	!
Componente	Endpoint Detection and Response Expert (on-premises)
ID de evento do Windows	2850
ID do evento do Kaspersky Security Center	00000b22
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Certificado inválido do servidor EDR Expert

Status	!
Componente	Endpoint Detection and Response Expert (on-premises)
ID de evento do Windows	2851
ID do evento do Kaspersky Security Center	00000b23
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Certificado inválido do agente no servidor EDR Expert

Status	!
Componente	Endpoint Detection and Response Expert (on-premises)
ID de evento do Windows	2852
ID do evento do Kaspersky Security Center	00000b24
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro ao conectar ao servidor de resposta da EDR Expert

Status	!
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID de evento do Windows	2858
ID do evento do Kaspersky Security Center	00000b22
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Certificado inválido do servidor de resposta da EDR Expert

Status	!
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID de evento do Windows	2859
ID do evento do Kaspersky Security Center	00000b23
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Certificado inválido do agente no servidor de reposta da EDR Expert

Status	!
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID de evento do Windows	2860
ID do evento do Kaspersky Security Center	00000b24
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro de conexão com o servidor de coleta de telemetria da EDR Expert

Status	!
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID de evento do Windows	2854
ID do evento do Kaspersky Security Center	00000b22
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Certificado inválido do servidor de coleta de telemetria da EDR Expert

Status	!
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID de evento do Windows	2855
ID do evento do Kaspersky Security Center	00000b23
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Certificado inválido do agente no servidor de coleta de telemetria da EDR Expert

Status	!
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID de evento do Windows	2856
ID do evento do Kaspersky Security Center	00000b24

Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro ao conectar ao servidor da NDR

Status	ⓘ
Componente	Network Detection and Response (KATA)
ID de evento do Windows	3080
ID do evento do Kaspersky Security Center	00000c08
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Certificado inválido do servidor NDR

Status	ⓘ
Componente	Network Detection and Response (KATA)
ID de evento do Windows	3081
ID do evento do Kaspersky Security Center	00000c09
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Certificado inválido do agente no servidor NDR

Status	ⓘ
Componente	Network Detection and Response (KATA)
ID de evento do Windows	3082
ID do evento do Kaspersky Security Center	00000c0a
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O dispositivo está conectado a um Servidor de Administração não confiável. Entre em contato com o administrador

Status	ⓘ
Componente	Proteção da conexão do Servidor de Administração
ID de evento do Windows	3301
ID do evento do Kaspersky Security Center	00000ce5
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

A alteração de um arquivo ou pasta foi detectada

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	2950
ID do evento do Kaspersky Security Center	00000b86

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

Mudanças de objeto com muita frequência. Iniciada agregação de eventos

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	`2955`
ID do evento do Kaspersky Security Center	`00000b8b`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Relatório sobre mudança de objeto para o período de agregação

Status	ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	`2953`
ID do evento do Kaspersky Security Center	`00000b89`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	`2956`
ID do evento do Kaspersky Security Center	`00000b8c`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

A alteração de registro foi detectada

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	`2951`
ID do evento do Kaspersky Security Center	`00000b87`
Log de eventos do Windows (padrão)	–

Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

Conexão/desconexão do dispositivo detectada

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	2952
ID do evento do Kaspersky Security Center	00000b88
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

O escopo de monitoramento inclui objetos incorretos

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	2903
ID do evento do Kaspersky Security Center	00000b89
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

Muitas tentativas de execução de operações restritas com o objeto. A agregação de eventos foi iniciada

Status	ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	2963
ID do evento do Kaspersky Security Center	00000b93
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Uma operação com os arquivos do escopo de monitoramento foi bloqueada

Status	ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	2959
ID do evento do Kaspersky Security Center	00000b8f

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

Modificação de registro bloqueada

Status	!
Componente	Monitor de integridade do sistema
ID de evento do Windows	`2960`
ID do evento do Kaspersky Security Center	`00000b90`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

Erro de processamento

Status	!
Componente	Monitor de integridade do sistema
ID de evento do Windows	`2954`
ID do evento do Kaspersky Security Center	`00000b8a`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Monitor de integridade do sistema: acionamento de regras desativado para contas de usuários sem identificador de segurança (SID) correspondente

Status	!
Componente	Monitor de integridade do sistema
ID de evento do Windows	`2964`
ID do evento do Kaspersky Security Center	`00000b94`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Controle de aplicativos: acionamento de regras desativado para contas de usuários sem identificador de segurança (SID) correspondente

Status	!
Componente	Controle de aplicativos
ID de evento do Windows	`711`
ID do evento do Kaspersky Security Center	`000002c7`

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Controle de dispositivos: acionamento de regras desativado para contas de usuários sem identificador de segurança (SID) correspondente

Status	!
Componente	Controle de dispositivos
ID de evento do Windows	`810`
ID do evento do Kaspersky Security Center	`0000032a`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Controle da Web: acionamento de regras desativado para contas de usuários sem identificador de segurança (SID) correspondente

Status	!
Componente	Controle da Web
ID de evento do Windows	`757`
ID do evento do Kaspersky Security Center	`000002f5`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Controle Adaptativo de Anomalias: acionamento de regras desativado para contas de usuários sem identificador de segurança (SID) correspondente

Status	!
Componente	Controle Adaptativo de Anomalias
ID de evento do Windows	`504`
ID do evento do Kaspersky Security Center	`000001f8`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Inspeção de log: acionamento de regras desativado para contas de usuários sem identificador de segurança (SID) correspondente

Status	!
Componente	Inspeção de log
ID de evento do Windows	`2810`
ID do evento do Kaspersky Security Center	`00000afa`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

O SVM está indisponível

Status	!
Componente	Light Agent

ID de evento do Windows	3151
ID do evento do Kaspersky Security Center	00000c4f
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto malicioso detectado. A desinfecção avançada deve ser iniciada em um modelo de máquina virtual

Status	!
Componente	Light Agent
ID de evento do Windows	3182
ID do evento do Kaspersky Security Center	00000c6e
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

A conexão de rede que foi estabelecida por meio do protocolo em desuso foi bloqueada

Status	!
Componente	Proteção
ID de evento do Windows	75
ID do evento do Kaspersky Security Center	0000004b
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro de conexão com o servidor KUMA

Status	!
Componente	Integração KUMA
ID de evento do Windows	2854
ID do evento do Kaspersky Security Center	00000b26
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Certificado inválido do servidor KUMA

Status	!
Componente	Integração KUMA
ID de evento do Windows	2855
ID do evento do Kaspersky Security Center	00000b27
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Certificado inválido do agente no servidor KUMA

Status	!
Componente	Integração KUMA

ID de evento do Windows	2856
ID do evento do Kaspersky Security Center	00000b28
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro de conexão com o servidor SIEM

Status	!
Componente	Integração KUMA
ID de evento do Windows	3250
ID do evento do Kaspersky Security Center	00000cb2
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Certificado inválido do servidor do SIEM

Status	!
Componente	Integração KUMA
ID de evento do Windows	3251
ID do evento do Kaspersky Security Center	00000cb3
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Certificado inválido do agente no servidor do SIEM

Status	!
Componente	Integração KUMA
ID de evento do Windows	3252
ID do evento do Kaspersky Security Center	00000cb4
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Falha funcional

A tarefa não pode ser executada

Status	!
Componente	Auditoria do Sistema
ID de evento do Windows	212
ID do evento do Kaspersky Security Center	000000d4
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Configurações de tarefa inválidas. Configurações não aplicadas

Status	⊘
Componente	Auditoria do Sistema
ID de evento do Windows	707
ID do evento do Kaspersky Security Center	000002c3
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Aviso

O aplicativo falhou durante a sessão anterior

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	237
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

A licença vai expirar em breve

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	204
ID do evento do Kaspersky Security Center	000000cc
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Os bancos de dados estão desatualizados

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	208
ID do evento do Kaspersky Security Center	000000d0
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

As atualizações automáticas estão desativadas

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	210
ID do evento do Kaspersky Security Center	000000d2

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

A Autodefesa está desativada

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	211
ID do evento do Kaspersky Security Center	000000d3
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Componentes de proteção desativados

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	214
ID do evento do Kaspersky Security Center	000000d6
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

O computador está sendo executado em modo de segurança

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	215
ID do evento do Kaspersky Security Center	000000d7
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Existem arquivos não processados

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	216
ID do evento do Kaspersky Security Center	000000d8
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Política do grupo aplicada

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	219
ID do evento do Kaspersky Security Center	000000db

Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Tarefa interrompida

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	222
ID do evento do Kaspersky Security Center	000000de
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Saia e reabra o aplicativo para concluir a atualização

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	224
ID do evento do Kaspersky Security Center	0000057b
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

É necessário reiniciar o computador

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	225
ID do evento do Kaspersky Security Center	000000e1
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

A licença permite o uso de componentes que não foram instalados

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	226
ID do evento do Kaspersky Security Center	000000e2
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Desinfecção Avançada iniciada

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	232
ID do evento do Kaspersky Security Center	000000e8

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Desinfecção Avançada concluída

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	233
ID do evento do Kaspersky Security Center	000000e9
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Chave de reserva inválido

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	230
ID do evento do Kaspersky Security Center	000000e6
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

A assinatura expira em breve

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	240
ID do evento do Kaspersky Security Center	000000f0
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Bloqueado

Status	⚠
Componente	Detecção de Comportamento Anticryptor Prevenção de Exploits Proteção Contra Ameaças da Web
ID de evento do Windows	331

ID do evento do Kaspersky Security Center	`GNRL_EV_OBJECT_BLOCKED`
Parâmetros do evento	• `GNRL_EA_PARAM_1` é o hash do objeto (SHA256). • `GNRL_EA_PARAM_2` é o nome do objeto. Quando a criptografia externa de pastas compartilhadas é detectada, o aplicativo mostra o caminho para o arquivo de destino. • `GNRL_EA_PARAM_5` é o nome da ameaça de acordo com a classificação da Kaspersky, por exemplo, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` é o nome do usuário da sessão. • `GNRL_EA_PARAM_8` é o tipo de ameaça (`tipo`). • `GNRL_EA_PARAM_9` são as informações adicionais sobre o objeto detectado: Componente de aplicativo (`engine`). Tecnologia de detecção de ameaça (`method`). Ameaças detectadas pela Kaspersky Private Security Network (`blacklist`): `true` ou `false`. EDR version. Identificador de ameaça no EDR. Hash MD5 do objeto.
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

As configurações do sistema operacional não permitem controlar o acesso a redes Wi-Fi

Status	⚠
Componente	Controle de dispositivos
ID de evento do Windows	`249`
ID do evento do Kaspersky Security Center	`000000f9`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Objeto não restaurado do Backup

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	`336`
ID do evento do Kaspersky Security Center	`00000150`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Atividade de rede suspeita detectada

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	`2001`
ID do evento do Kaspersky Security Center	`000007d1`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Conexão criptografada encerrada

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	250
ID do evento do Kaspersky Security Center	000007d3
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

A participação na KSN está desativada

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	2021
ID do evento do Kaspersky Security Center	000007e5
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

O processamento de algumas funções do SO está desativado

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	245
ID do evento do Kaspersky Security Center	000000f5
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O armazenamento da Quarentena está quase sem espaço

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	344
ID do evento do Kaspersky Security Center	00000158
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Conexão de rede bloqueada

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	809
ID do evento do Kaspersky Security Center	00000abe
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Não é possível criar uma cópia de backup

Status	⚠
Componente	Proteção Contra Ameaças ao Arquivo Detecção de Comportamento Anticryptor Prevenção de Intrusão do Host Verificação de malware
ID de evento do Windows	`310`
ID do evento do Kaspersky Security Center	`00000136`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto não processado

Status	⚠
Componente	Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças ao Correio Prevenção de Intrusão do Host Proteção AMSI Verificação de malware
ID de evento do Windows	`314`
ID do evento do Kaspersky Security Center	`0000013a`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto criptografado

Status	⚠
Componente	Prevenção de Intrusão do Host
ID de evento do Windows	`320`
ID do evento do Kaspersky Security Center	`00000140`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Objeto corrompido

Status	⚠
Componente	Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças da Web Proteção Contra Ameaças ao Correio Proteção AMSI Prevenção de Intrusão do Host Verificação de malware
ID de evento do Windows	`321`
ID do evento do Kaspersky Security Center	`00000141`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Foi detectado um software legítimo que pode ser usado por intrusos para danificar seu computador ou dados pessoais (bancos locais)

Status	⚠
Componente	Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças da Web Proteção Contra Ameaças ao Correio Prevenção de Intrusão do Host Proteção AMSI Detecção de Comportamento Anticryptor Anticryptor Verificação de malware
ID de evento do Windows	`303`
ID do evento do Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Parâmetros do evento	• `GNRL_EA_PARAM_1` é o hash do objeto (SHA256). • `GNRL_EA_PARAM_2` é o nome do objeto. • `GNRL_EA_PARAM_5` é o nome da ameaça de acordo com a classificação da Kaspersky, por exemplo, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` é o nome do usuário da sessão. • `GNRL_EA_PARAM_8` é o tipo de ameaça (`tipo`).
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Foi detectado um software legítimo que pode ser usado por intrusos para danificar seu computador ou dados pessoais (KSN)

Status	⚠
Componente	Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças da Web Proteção Contra Ameaças ao Correio Prevenção de Intrusão do Host Proteção AMSI Detecção de Comportamento Anticryptor Anticryptor Verificação de malware
ID de evento do Windows	`303`
ID do evento do Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Parâmetros do evento	• `GNRL_EA_PARAM_1` é o hash do objeto (SHA256). • `GNRL_EA_PARAM_2` é o nome do objeto. • `GNRL_EA_PARAM_5` é o nome da ameaça de acordo com a classificação da Kaspersky, por exemplo, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` é o nome do usuário da sessão. • `GNRL_EA_PARAM_8` é o tipo de ameaça (`tipo`).
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto excluído

Status	⚠
Componente	Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças ao Correio Prevenção de Intrusão do Host Prevenção de Exploits Detecção de Comportamento Anticryptor Verificação de malware

ID de evento do Windows	307
ID do evento do Kaspersky Security Center	GNRL_EV_OBJECT_DELETED
Parâmetros do evento	• GNRL_EA_PARAM_1 é o hash do objeto (SHA256). • GNRL_EA_PARAM_2 é o nome do objeto. • GNRL_EA_PARAM_5 é o nome da ameaça de acordo com a classificação da Kaspersky, por exemplo, EICAR-Test-File. • GNRL_EA_PARAM_7 é o nome do usuário da sessão. • GNRL_EA_PARAM_8 é o tipo de ameaça (tipo). • GNRL_EA_PARAM_9 são as informações adicionais sobre o objeto detectado: Componente de aplicativo (engine). Tecnologia de detecção de ameaça (method). Ameaças detectadas pela Kaspersky Private Security Network (blacklist): true ou false. EDR version. Identificador de ameaça no EDR. Hash MD5 do objeto.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto desinfectado

Status	⚠
Componente	Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças ao Correio Prevenção de Intrusão do Host Verificação de malware
ID de evento do Windows	306
ID do evento do Kaspersky Security Center	GNRL_EV_OBJECT_CURED
Parâmetros do evento	• GNRL_EA_PARAM_1 é o hash do objeto (SHA256). • GNRL_EA_PARAM_2 é o nome do objeto. • GNRL_EA_PARAM_5 é o nome da ameaça de acordo com a classificação da Kaspersky, por exemplo, EICAR-Test-File. • GNRL_EA_PARAM_7 é o nome do usuário da sessão. • GNRL_EA_PARAM_8 é o tipo de ameaça (tipo). • GNRL_EA_PARAM_9 são as informações adicionais sobre o objeto detectado: Componente de aplicativo (engine). Tecnologia de detecção de ameaça (method). Ameaças detectadas pela Kaspersky Private Security Network (blacklist): true ou false. EDR version. Identificador de ameaça no EDR. Hash MD5 do objeto.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

O objeto será desinfectado ao reiniciar

Status	⚠
Componente	Prevenção de Intrusão do Host Proteção Contra Ameaças ao Arquivo Verificação de malware
ID de evento do Windows	324
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

O objeto será excluído ao reiniciar

Status	⚠
Componente	Detecção de Comportamento Anticryptor Prevenção de Exploits Prevenção de Intrusão do Host Proteção Contra Ameaças ao Arquivo Verificação de malware
ID de evento do Windows	323
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Objeto excluído de acordo com as configurações

Status	⚠
Componente	Proteção Contra Ameaças ao Correio
ID de evento do Windows	342
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Reversão concluída

Status	⚠
Componente	Proteção Contra Ameaças ao Arquivo Detecção de Comportamento Anticryptor Prevenção de Exploits Verificação de malware
ID de evento do Windows	455
ID do evento do Kaspersky Security Center	000001c7
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro ao remover a versão anterior do aplicativo

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	246
ID do evento do Kaspersky Security Center	000000f6
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O download do objeto foi bloqueado

Status	⚠
Componente	Proteção Contra Ameaças da Web

ID de evento do Windows	341
ID do evento do Kaspersky Security Center	GNRL_EV_OBJECT_BLOCKED
Parâmetros do evento	• GNRL_EA_PARAM_1 é o hash do objeto (SHA256). • GNRL_EA_PARAM_2 é o nome do objeto. • GNRL_EA_PARAM_5 é o nome da ameaça de acordo com a classificação da Kaspersky, por exemplo, EICAR-Test-File. • GNRL_EA_PARAM_7 é o nome do usuário da sessão. • GNRL_EA_PARAM_8 é o tipo de ameaça (tipo). • GNRL_EA_PARAM_9 são as informações adicionais sobre o objeto detectado: Componente de aplicativo (engine). Tecnologia de detecção de ameaça (method). Ameaças detectadas pela Kaspersky Private Security Network (blacklist): true ou false. EDR version. Identificador de ameaça no EDR. Hash MD5 do objeto.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Erro na autorização do teclado

Status	⚠
Componente	Prevenção contra ataque BadUSB
ID de evento do Windows	2052
ID do evento do Kaspersky Security Center	00000804
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O resultado da verificação do objeto foi enviada para um aplicativo de terceiros

Status	⚠
Componente	Proteção AMSI
ID de evento do Windows	1512
ID do evento do Kaspersky Security Center	GNRL_EV_OBJECT_REPORTED
Parâmetros do evento	• GNRL_EA_PARAM_1 é o hash do objeto (SHA256). • GNRL_EA_PARAM_2 é o nome do objeto. • GNRL_EA_PARAM_5 é o nome da ameaça de acordo com a classificação da Kaspersky, por exemplo, EICAR-Test-File. • GNRL_EA_PARAM_7 é o nome do usuário da sessão. • GNRL_EA_PARAM_8 é o tipo de ameaça (tipo). • GNRL_EA_PARAM_9 são as informações adicionais sobre o objeto detectado: Componente de aplicativo (engine). Tecnologia de detecção de ameaça (method). Ameaças detectadas pela Kaspersky Private Security Network (blacklist): true ou false. EDR version. Identificador de ameaça no EDR. Hash MD5 do objeto.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Configurações da tarefa aplicadas com êxito

Status	⚠
Componente	Controle de aplicativos

ID de evento do Windows	708
ID do evento do Kaspersky Security Center	000002c4
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Aviso sobre conteúdo indesejado (bases locais)

Status	⚠
Componente	Controle da Web
ID de evento do Windows	708
ID do evento do Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Parâmetros do evento	• GNRL_EA_PARAM_1 é o URL. • GNRL_EA_PARAM_2 é o nome do usuário da sessão. • GNRL_EA_PARAM_3 é o nome da regra do controle da web.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Aviso sobre conteúdo indesejado (KSN)

Status	⚠
Componente	Controle da Web
ID de evento do Windows	708
ID do evento do Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Parâmetros do evento	• GNRL_EA_PARAM_1 é o URL. • GNRL_EA_PARAM_2 é o nome do usuário da sessão. • GNRL_EA_PARAM_3 é o nome da regra do controle da web.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Conteúdo não recomendado foi acessado após aviso

Status	⚠
Componente	Controle da Web
ID de evento do Windows	754
ID do evento do Kaspersky Security Center	000002f2
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Acesso temporário ao dispositivo ativado

Status	⚠
Componente	Controle de dispositivos
ID de evento do Windows	803
ID do evento do Kaspersky Security Center	000002f2
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Operação cancelada pelo usuário

Status	⚠
Componente	Atualização
ID de evento do Windows	1016
ID do evento do Kaspersky Security Center	000003f8
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

O usuário optou por cancelar a política de criptografia

Status	⚠
Componente	Criptografia de dados
ID de evento do Windows	1306
ID do evento do Kaspersky Security Center	0000051a
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Interrompida a aplicação das regras de criptografia/descriptografia do arquivo

Status	⚠
Componente	Criptografia de dados
ID de evento do Windows	903
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Criptografia/descriptografia do arquivo interrompida

Status	⚠
Componente	Criptografia de dados
ID de evento do Windows	914
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Criptografia/descriptografia do dispositivo interrompida

Status	⚠
Componente	Criptografia de dados
ID de evento do Windows	1303
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Falha ao instalar ou atualizar os drivers do Kaspersky Disk Encryption na imagem WinRE

Status	⚠
Componente	Criptografia de dados
ID de evento do Windows	1345
ID do evento do Kaspersky Security Center	00000541
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Falha ao verificar a assinatura do módulo

Status	⚠
Componente	Verificação de integridade do sistema
ID de evento do Windows	2002
ID do evento do Kaspersky Security Center	000007d2
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

A inicialização do aplicativo foi bloqueada

Status	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2105
ID do evento do Kaspersky Security Center	00000839
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

A abertura do documento foi bloqueada

Status	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2106
ID do evento do Kaspersky Security Center	0000083a
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O processo foi encerrado pelo administrador do servidor da Kaspersky Anti Targeted Attack Platform

Status	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2112
ID do evento do Kaspersky Security Center	00000840
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O aplicativo foi encerrado pelo administrador do servidor da Kaspersky Anti Targeted Attack Platform

Status	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2113
ID do evento do Kaspersky Security Center	00000841
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O arquivo ou o processo foram encerrados pelo administrador do servidor da Kaspersky Anti Targeted Attack Platform

Status	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2111
ID do evento do Kaspersky Security Center	0000083f
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O arquivo foi restaurado da quarentena no servidor da Kaspersky Anti Targeted Attack Platform pelo administrador

Status	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2110
ID do evento do Kaspersky Security Center	0000083e
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O arquivo foi enviado para a quarentena no servidor da Kaspersky Anti Targeted Attack Platform pelo administrador

Status	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2109
ID do evento do Kaspersky Security Center	0000083d
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

A atividade de rede de todos os aplicativos de terceiros foi bloqueada

Status	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2107
ID do evento do Kaspersky Security Center	0000083b
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

A atividade de rede de todos os aplicativos de terceiros foi desbloqueada

Status	⚠
Componente	Endpoint Sensor
ID de evento do Windows	`2108`
ID do evento do Kaspersky Security Center	`0000083c`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O objeto será excluído ao reiniciar (Sandbox)

Status	⚠
Componente	Sandbox
ID de evento do Windows	`2605`
ID do evento do Kaspersky Security Center	`00000a2d`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O tamanho total das tarefas de verificação excedeu o limite

Status	⚠
Componente	Sandbox
ID de evento do Windows	`2612`
ID do evento do Kaspersky Security Center	`00000a34`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Inicialização de objeto permitida, evento registrado

Status	⚠
Componente	Endpoint Detection and Response
ID de evento do Windows	`2553`
ID do evento do Kaspersky Security Center	`000009fa`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Inicialização de processo permitida, evento registrado

Status	⚠
Componente	Endpoint Detection and Response
ID de evento do Windows	`2554`
ID do evento do Kaspersky Security Center	`000009f8`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O objeto será excluído ao reiniciar (Endpoint Detection and Response)

Status	⚠
Componente	Endpoint Detection and Response
ID de evento do Windows	2558
ID do evento do Kaspersky Security Center	000009fe
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Isolamento de rede

Status	⚠
Componente	Endpoint Detection and Response
ID de evento do Windows	2700
ID do evento do Kaspersky Security Center	00000a8c
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Encerramento do isolamento de rede

Status	⚠
Componente	Endpoint Detection and Response
ID de evento do Windows	2701
ID do evento do Kaspersky Security Center	00000a8d
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

É necessário reiniciar o computador para concluir a tarefa

Status	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	225
ID do evento do Kaspersky Security Center	0000057b
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Conexão a um site com um certificado não confiável estabelecida por decisão do usuário

Status	⚠
Componente	Network Detection and Response (KATA)
ID de evento do Windows	70
ID do evento do Kaspersky Security Center	00000046
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Mensagem de bloqueio de inicialização do aplicativo para o administrador

Status	⚠
Componente	Controle de aplicativos
ID de evento do Windows	503
ID do evento do Kaspersky Security Center	GNRL_EV_AC_USER_REQUEST
Parâmetros do evento	• GNRL_EA_DESCRIPTION é a mensagem para o usuário. • GNRL_EA_PARAM_2 é o nome do usuário da sessão. • GNRL_EA_PARAM_6 é o nome do arquivo executável do aplicativo (por exemplo, chrome.exe). • GNRL_EA_PARAM_7 é o caminho do arquivo executável. • GNRL_EA_PARAM_8 é o hash do objeto (SHA256). • GNRL_EA_PARAM_9 é a versão do aplicativo que o usuário está tentando executar.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Mensagem de bloqueio de acesso ao dispositivo para o administrador

Status	⚠
Componente	Controle de dispositivos
ID de evento do Windows	804
ID do evento do Kaspersky Security Center	GNRL_EV_DC_USER_REQUEST
Parâmetros do evento	• c_er_descr é a mensagem para o usuário. • GNRL_EA_PARAM_1 é o ID do hardware (HWID). • GNRL_EA_PARAM_2 é o nome do usuário da sessão.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Mensagem de bloqueio de acesso à página da Web para o administrador

Status	⚠
Componente	Controle da Web
ID de evento do Windows	755
ID do evento do Kaspersky Security Center	GNRL_EV_WC_USER_REQUEST
Parâmetros do evento	• GNRL_EA_DESCRIPTION é a mensagem para o usuário. • GNRL_EA_PARAM_1 é o URL. • GNRL_EA_PARAM_2 é o nome do usuário da sessão.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Conexão com o dispositivo bloqueada

Status	⚠
Componente	Controle de dispositivos
ID de evento do Windows	807
ID do evento do Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Parâmetros do evento	• GNRL_EA_PARAM_1 é o ID do hardware (HWID). • GNRL_EA_PARAM_2 é o nome do usuário da sessão.

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Mensagem de bloqueio de atividade do aplicativo para o administrador

Status	⚠
Componente	Controle Adaptativo de Anomalias
ID de evento do Windows	`503`
ID do evento do Kaspersky Security Center	`GNRL_EV_ADSEC_USER_REQUEST`
Parâmetros do evento	• `GNRL_EA_DESCRIPTION` é a mensagem para o usuário. • `GNRL_EA_PARAM_1` é o nome da regra do controle adaptativo de anomalia. • `GNRL_EA_PARAM_2` é o ID da regra heurística. • `GNRL_EA_PARAM_3` é o nome do usuário da sessão. • `GNRL_EA_PARAM_4` está no processo de origem. • `GNRL_EA_PARAM_5` está no objeto de origem. • `GNRL_EA_PARAM_6` está no processo de destino. • `GNRL_EA_PARAM_7` é o objeto de destino. • `GNRL_EA_PARAM_8` são as informações adicionais sobre o objeto detectado: Hashes do processo de origem / objeto e processo de destino / objeto. Processo bloqueado (`verdict_type`): `true` ou `false`. ID de segurança do usuário (SID).
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

A inicialização do aplicativo cliente do serviço de nuvem está bloqueada

Status	⚠
Componente	Cloud Discovery
ID de evento do Windows	`2212`
ID do evento do Kaspersky Security Center	`000008a4`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Acesso ao serviço de nuvem bloqueado

Status	⚠
Componente	Cloud Discovery
ID de evento do Windows	`2213`
ID do evento do Kaspersky Security Center	`000008a5`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

A alteração de um arquivo ou pasta foi detectada

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	`2950`
ID do evento do Kaspersky Security Center	`00000b86`
Log de eventos do Windows (padrão)	–

Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

Mudanças de objeto com muita frequência. Iniciada agregação de eventos

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	2955
ID do evento do Kaspersky Security Center	00000b8b
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Relatório sobre mudança de objeto para o período de agregação

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	2956
ID do evento do Kaspersky Security Center	00000b8c
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

A alteração de registro foi detectada

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	2951
ID do evento do Kaspersky Security Center	00000b87
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

Conexão/desconexão do dispositivo detectada

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	2952
ID do evento do Kaspersky Security Center	00000b88

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

O escopo de monitoramento inclui objetos incorretos

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	`2903`
ID do evento do Kaspersky Security Center	`00000b89`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

A operação proibida foi permitida no modo de teste

Status	⚠
Componente	Monitor de integridade do sistema
ID de evento do Windows	`2961`
ID do evento do Kaspersky Security Center	`00000b91`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Não foi possível conectar ao Servidor de integração por mais de 30 minutos. Verifique o status do Servidor de integração e as configurações de rede

Status	⚠
Componente	Light Agent
ID de evento do Windows	`3102`
ID do evento do Kaspersky Security Center	`00000c1e`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Não foi possível conectar ao Servidor de integração por mais de 6 horas. Verifique o status do Servidor de integração e as configurações de rede

Status	⚠
Componente	Light Agent
ID de evento do Windows	`3103`
ID do evento do Kaspersky Security Center	`00000c1f`

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Não foi possível conectar ao Servidor de integração. Verifique o status do Servidor de integração e as configurações de rede

Status	⚠
Componente	Light Agent
ID de evento do Windows	3101
ID do evento do Kaspersky Security Center	00000c1d
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

O modelo de máquina virtual precisa ser atualizado

Status	⚠
Componente	Light Agent
ID de evento do Windows	3181
ID do evento do Kaspersky Security Center	00000c6d
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

A licença Standard encerrou. O aplicativo está sendo executado com a licença Enterprise

Status	⚠
Componente	Light Agent
ID de evento do Windows	3171
ID do evento do Kaspersky Security Center	00000c64
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Status	⚠
Componente	Monitor de Integridade de Arquivos
ID de evento do Windows	2901
ID do evento do Kaspersky Security Center	00000b55
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Status	⚠
Componente	Monitor de integridade de arquivos
ID de evento do Windows	2900
ID do evento do Kaspersky Security Center	00000b54
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Mensagem informativa

Aplicativo iniciado

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	235
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Aplicativo interrompido

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	236
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Acesso restrito ao recurso protegido pela Autodefesa

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	213
ID do evento do Kaspersky Security Center	000000d5
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Relatório apagado

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	217
ID do evento do Kaspersky Security Center	000000d9
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Política do grupo desativada

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	220

ID do evento do Kaspersky Security Center	000000dc
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Configurações de aplicativo alteradas

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	218
ID do evento do Kaspersky Security Center	000000da
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Tarefa iniciada

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	221
ID do evento do Kaspersky Security Center	000000dd
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Tarefa concluída

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	223
ID do evento do Kaspersky Security Center	000000df
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Todos os componentes do aplicativo que são definidos pela licença foram instalados e são executados no modo normal

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	227
ID do evento do Kaspersky Security Center	000000e3
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

As configurações de assinatura foram alteradas

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	238

ID do evento do Kaspersky Security Center	000000ee
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

A assinatura foi renovada

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	239
ID do evento do Kaspersky Security Center	000000ef
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto restaurado do Backup

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	335
ID do evento do Kaspersky Security Center	0000014f
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Entrada de nome de usuário e senha

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	2000
ID do evento do Kaspersky Security Center	000007d0
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

A participação na KSN está ativada

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	2020
ID do evento do Kaspersky Security Center	000007e4
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Servidores da KSN disponíveis

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	2022

ID do evento do Kaspersky Security Center	000007e6
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

O aplicativo funciona e processa dados de acordo com a legislação relevante e utiliza a infraestrutura apropriada

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	2024
ID do evento do Kaspersky Security Center	000007e8
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto restaurado da Quarentena

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	345
ID do evento do Kaspersky Security Center	00000159
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto excluído da Quarentena

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	347
ID do evento do Kaspersky Security Center	0000015b
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Foi criada uma cópia de backup do objeto

Status	ⓘ
Componente	Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças ao Correio Detecção de Comportamento Anticryptor Prevenção de Intrusão do Host Sandbox Verificação de malware
ID de evento do Windows	308
ID do evento do Kaspersky Security Center	00000134
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Substituído por uma cópia que foi desinfectada anteriormente

Status	ⓘ
Componente	Proteção Contra Ameaças ao Arquivo Prevenção de Intrusão do Host Verificação de malware
ID de evento do Windows	327
ID do evento do Kaspersky Security Center	00000147
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Arquivo compactado protegido por senha detectado

Status	ⓘ
Componente	Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças da Web Proteção Contra Ameaças ao Correio Proteção AMSI Prevenção de Intrusão do Host Verificação de malware
ID de evento do Windows	322
ID do evento do Kaspersky Security Center	GNRL_EV_PASSWD_ARCHIVE_FOUND
Parâmetros do evento	• GNRL_EA_PARAM_2 é o nome do objeto. • GNRL_EA_PARAM_3 é a data de criação do objeto (opcional). • GNRL_EA_PARAM_7 é o nome do usuário da sessão. • GNRL_EA_PARAM_9 são as informações adicionais sobre o objeto detectado: Componente de aplicativo (engine). Tecnologia de detecção de ameaça (method). Ameaça detectada pela KSN privada (lista de bloqueio): true ou false.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Informações sobre o objeto detectado

Status	ⓘ
Componente	Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças da Web Proteção Contra Ameaças ao Correio Proteção AMSI Prevenção de Intrusão do Host Verificação de malware
ID de evento do Windows	332
ID do evento do Kaspersky Security Center	0000014c
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

O objeto está na lista de permissão da Kaspersky Private Security Network

Status	ⓘ
Componente	Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças da Web Proteção Contra Ameaças ao Correio Proteção AMSI Prevenção de Intrusão do Host Verificação de malware
ID de evento do Windows	340

ID do evento do Kaspersky Security Center	00000154
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto renomeado

Status	ⓘ
Componente	Proteção Contra Ameaças ao Correio Prevenção de Exploits Detecção de Comportamento Anticryptor Verificação de malware
ID de evento do Windows	329
ID do evento do Kaspersky Security Center	00000149
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto processado

Status	ⓘ
Componente	Prevenção de Intrusão do Host Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças da Web Proteção Contra Ameaças ao Correio Verificação de malware
ID de evento do Windows	301
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Objeto ignorado

Status	ⓘ
Componente	Prevenção de Intrusão do Host Proteção Contra Ameaças ao Arquivo Proteção AMSI Verificação de malware
ID de evento do Windows	315
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Arquivo compactado detectado

Status	ⓘ
Componente	Prevenção de Intrusão do Host Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças da Web Proteção Contra Ameaças ao Correio Proteção AMSI Verificação de malware
ID de evento do Windows	318

ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Objeto empacotado detectado

Status	ⓘ
Componente	Prevenção de Intrusão do Host Proteção Contra Ameaças ao Arquivo Proteção Contra Ameaças da Web Proteção Contra Ameaças ao Correio Proteção AMSI Verificação de malware
ID de evento do Windows	319
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Link processado

Status	ⓘ
Componente	Proteção Contra Ameaças da Web
ID de evento do Windows	361
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Permitida a inicialização do aplicativo

Status	ⓘ
Componente	Controle de aplicativos
ID de evento do Windows	701
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

A fonte de atualização foi selecionada

Status	ⓘ
Componente	Atualização
ID de evento do Windows	1001
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

O servidor proxy foi selecionado

Status	ⓘ
Componente	Atualização
ID de evento do Windows	1002
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

O link está na lista de permissão da Kaspersky Private Security Network

Status	ⓘ
Componente	Proteção Contra Ameaças da Web
ID de evento do Windows	370
ID do evento do Kaspersky Security Center	00000172
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Aplicativo colocado no grupo confiável

Status	ⓘ
Componente	Prevenção de Intrusão do Host
ID de evento do Windows	401
ID do evento do Kaspersky Security Center	00000191
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Aplicativo colocado no grupo restrito

Status	ⓘ
Componente	Prevenção de Intrusão do Host
ID de evento do Windows	402
ID do evento do Kaspersky Security Center	00000192
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

A Prevenção de Intrusão do Host foi acionada

Status	ⓘ
Componente	Prevenção de Intrusão do Host
ID de evento do Windows	403
ID do evento do Kaspersky Security Center	00000193
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Arquivo restaurado

Status	ⓘ
Componente	Detecção de Comportamento Anticryptor Prevenção de Exploits Prevenção de Intrusão do Host
ID de evento do Windows	`457`
ID do evento do Kaspersky Security Center	`000001c9`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Valor do registro restaurado

Status	ⓘ
Componente	Detecção de Comportamento Prevenção de Exploits
ID de evento do Windows	`458`
ID do evento do Kaspersky Security Center	`000001ca`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Valor do registro excluído

Status	ⓘ
Componente	Detecção de Comportamento Prevenção de Exploits
ID de evento do Windows	`459`
ID do evento do Kaspersky Security Center	`000001cb`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Ação do processo ignorada

Status	ⓘ
Componente	Controle Adaptativo de Anomalias
ID de evento do Windows	`2201`
ID do evento do Kaspersky Security Center	`GNRL_EV_ADSEC_DETECT`
Parâmetros do evento	• `GNRL_EA_PARAM_1` é o nome da regra do controle adaptativo de anomalia. • `GNRL_EA_PARAM_2` é o ID da regra heurística. • `GNRL_EA_PARAM_3` é o nome do usuário da sessão. • `GNRL_EA_PARAM_4` está no processo de origem. • `GNRL_EA_PARAM_5` está no objeto de origem. • `GNRL_EA_PARAM_6` está no processo de destino. • `GNRL_EA_PARAM_7` é o objeto de destino. • `GNRL_EA_PARAM_8` são as informações adicionais sobre o objeto detectado: Hashes do processo de origem / objeto e processo de destino / objeto. Processo bloqueado (`verdict_type`): `true` ou `false`. ID de segurança do usuário (SID).
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Teclado autorizado

Status	ⓘ
Componente	Prevenção contra ataque BadUSB
ID de evento do Windows	`2050`
ID do evento do Kaspersky Security Center	`00000802`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Atividade de rede permitida

Status	ⓘ
Componente	Firewall
ID de evento do Windows	`601`
ID do evento do Kaspersky Security Center	`00000259`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Proibida a inicialização do aplicativo em modo de teste

Status	ⓘ
Componente	Controle de aplicativos
ID de evento do Windows	`703`
ID do evento do Kaspersky Security Center	`GNRL_EV_APP_LAUNCH_TESTED_DENIED`
Parâmetros do evento	• `GNRL_EA_PARAM_2` é o nome do usuário da sessão. • `GNRL_EA_PARAM_3` é o identificador de categoria criado manualmente. • `GNRL_EA_PARAM_4` é o identificador de segurança da conta (SID). • `GNRL_EA_PARAM_5` é a informação sobre a assinatura digital do aplicativo. • `GNRL_EA_PARAM_6` é o nome do arquivo executável do aplicativo (por exemplo, chrome.exe). • `GNRL_EA_PARAM_7` é o caminho do arquivo executável. • `GNRL_EA_PARAM_8` é o hash do objeto (SHA256). • `GNRL_EA_PARAM_9` é a versão do aplicativo que o usuário está tentando executar.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Permitida a inicialização do aplicativo em modo de teste

Status	ⓘ
Componente	Controle de aplicativos
ID de evento do Windows	`704`
ID do evento do Kaspersky Security Center	`GNRL_EV_APP_LAUNCH_TESTED_ALLOW`
Parâmetros do evento	• `GNRL_EA_PARAM_2` é o nome do usuário da sessão. • `GNRL_EA_PARAM_3` é o identificador de categoria criado manualmente. • `GNRL_EA_PARAM_4` é o identificador de segurança da conta (SID). • `GNRL_EA_PARAM_5` é a informação sobre a assinatura digital do aplicativo.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Uma página autorizada foi aberta

Status	ⓘ
Componente	Controle da Web
ID de evento do Windows	751
ID do evento do Kaspersky Security Center	000002f4
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Operação com o dispositivo permitida

Status	ⓘ
Componente	Controle de dispositivos
ID de evento do Windows	801
ID do evento do Kaspersky Security Center	00000321
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Operação com arquivo realizada

Status	ⓘ
Componente	Controle de dispositivos
ID de evento do Windows	808
ID do evento do Kaspersky Security Center	GNRL_EV_USB_FILE_OPERATION
Parâmetros do evento	• GNRL_EA_PARAM_1 é a operação do arquivo (gravação ou exclusão). • GNRL_EA_PARAM_2 é o caminho para o arquivo. • GNRL_EA_PARAM_3 é o nome do dispositivo. • GNRL_EA_PARAM_4 é o nome do usuário da sessão. • GNRL_EA_PARAM_5 é o ID do hardware (HWID).
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Nenhuma atualização disponível

Status	ⓘ
Componente	Atualização
ID de evento do Windows	1020
ID do evento do Kaspersky Security Center	000003fc
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Distribuição da atualização concluída com êxito

Status	ⓘ
Componente	Atualização
ID de evento do Windows	1022
ID do evento do Kaspersky Security Center	000003fe

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Baixando arquivos...

Status	ⓘ
Componente	Atualização
ID de evento do Windows	1003
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Arquivo baixado

Status	ⓘ
Componente	Atualização
ID de evento do Windows	1004
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Arquivo instalado

Status	ⓘ
Componente	Atualização
ID de evento do Windows	1005
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Arquivo atualizado

Status	ⓘ
Componente	Atualização
ID de evento do Windows	1006
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Arquivo revertido devido a erro de atualização

Status	ⓘ
Componente	Atualização
ID de evento do Windows	1007
ID do evento do Kaspersky Security Center	–

Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Atualizando arquivos...

Status	ⓘ
Componente	Atualização
ID de evento do Windows	1008
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Distribuindo as atualizações...

Status	ⓘ
Componente	Atualização
ID de evento do Windows	1009
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Revertendo arquivos...

Status	ⓘ
Componente	Atualização
ID de evento do Windows	1010
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Criando a lista de arquivos para baixar...

Status	ⓘ
Componente	Atualização
ID de evento do Windows	1013
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Baixando patches...

Status	ⓘ
Componente	Atualização
ID de evento do Windows	2150
ID do evento do Kaspersky Security Center	–

Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Instalando patch...

Status	ⓘ
Componente	Atualização
ID de evento do Windows	2151
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Patch instalado

Status	ⓘ
Componente	Atualização
ID de evento do Windows	2152
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Revertendo patch...

Status	ⓘ
Componente	Atualização
ID de evento do Windows	2154
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Patch revertido

Status	ⓘ
Componente	Atualização
ID de evento do Windows	2155
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Iniciada a aplicação das regras de criptografia/descriptografia do arquivo

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	901
ID do evento do Kaspersky Security Center	00000385

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Concluída a aplicação das regras de criptografia/descriptografia do arquivo

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	902
ID do evento do Kaspersky Security Center	00000386
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Retomada a aplicação das regras de criptografia/descriptografia

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	905
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Criptografia/descriptografia do arquivo iniciada

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	910
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Criptografia/descriptografia do arquivo concluída

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	911
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

O arquivo não foi criptografado porque é uma exclusão

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	913
ID do evento do Kaspersky Security Center	–

Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Modo portátil ativado

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	950
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Modo portátil desativado

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	952
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Criptografia/descriptografia do dispositivo iniciada

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	1301
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Criptografia/descriptografia do dispositivo concluída

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	1302
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Criptografia/descriptografia do dispositivo retomada

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	1304
ID do evento do Kaspersky Security Center	–

Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

O dispositivo não está criptografado

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	1307
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

O processo de criptografia/descriptografia do dispositivo foi alterado para o modo ativo

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	1308
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

O processo de criptografia/descriptografia do dispositivo foi alterado para o modo passivo

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	1309
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Módulo de criptografia carregado

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	1310
ID do evento do Kaspersky Security Center	0000051e
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Nova conta do Agente de Autenticação criada

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	1330
ID do evento do Kaspersky Security Center	00000532

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Conta do Agente de Autenticação excluída

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	1331
ID do evento do Kaspersky Security Center	00000533
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Senha da conta do Agente de Autenticação alterada

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	1332
ID do evento do Kaspersky Security Center	00000534
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Login no Agente de Autenticação feito com êxito

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	1333
ID do evento do Kaspersky Security Center	00000535
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Falha na tentativa de login no Agente de autenticação

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	1334
ID do evento do Kaspersky Security Center	00000536
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Disco rígido acessado usando o procedimento de solicitação de acesso a dispositivos criptografados

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	1335
ID do evento do Kaspersky Security Center	00000537

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Falha na tentativa de acesso ao disco rígido usando o procedimento de solicitação de acesso a dispositivos criptografados

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	`1336`
ID do evento do Kaspersky Security Center	`00000538`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

A conta não foi adicionada. Esta conta já existe

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	`1337`
ID do evento do Kaspersky Security Center	`00000539`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

A conta não foi modificada. Esta conta não existe

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	`1338`
ID do evento do Kaspersky Security Center	`0000053a`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

A conta não foi excluída. Esta conta não existe

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	`1339`
ID do evento do Kaspersky Security Center	`0000053b`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Atualização de FDE realizada com êxito

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	`1341`
ID do evento do Kaspersky Security Center	`0000053d`

Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Reversão de atualização de FDE realizada com êxito

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	`1343`
ID do evento do Kaspersky Security Center	`0000053f`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Falha ao desinstalar os drivers do Kaspersky Disk Encryption da imagem WinRE

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	`1346`
ID do evento do Kaspersky Security Center	`00000542`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

A chave de recuperação do BitLocker foi alterada

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	`1370`
ID do evento do Kaspersky Security Center	`0000055a`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

A senha / PIN do BitLocker foi alterada

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	`1371`
ID do evento do Kaspersky Security Center	`0000055b`
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

A recuperação da chave do BitLocker foi salva em uma unidade removível

Status	ⓘ
Componente	Criptografia de dados
ID de evento do Windows	`1372`
ID do evento do Kaspersky Security Center	`0000055c`

Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

O processamento de tarefas do servidor da Kaspersky Anti Targeted Attack Platform está inativo

Status	ⓘ
Componente	Endpoint Sensor
ID de evento do Windows	`2103`
ID do evento do Kaspersky Security Center	`00000837`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Endpoint Sensor conectado ao servidor

Status	ⓘ
Componente	Endpoint Sensor
ID de evento do Windows	`2101`
ID do evento do Kaspersky Security Center	`00000835`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

A conexão ao servidor da Kaspersky Anti Targeted Attack Platform foi restaurada

Status	ⓘ
Componente	Endpoint Sensor
ID de evento do Windows	`2102`
ID do evento do Kaspersky Security Center	`00000836`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

O processamento de tarefas do servidor da Kaspersky Anti Targeted Attack Platform está ativo

Status	ⓘ
Componente	Endpoint Sensor
ID de evento do Windows	`2104`
ID do evento do Kaspersky Security Center	`00000838`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto excluído

Status	ⓘ
Componente	Limpar dados
ID de evento do Windows	`2251`
ID do evento do Kaspersky Security Center	`000008cb`

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	–

Estatísticas da tarefa de limpeza

Status	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID de evento do Windows	2853
ID do evento do Kaspersky Security Center	00000b25
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Status	ⓘ
Componente	Limpar dados
ID de evento do Windows	2253
ID do evento do Kaspersky Security Center	000008cd
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto colocado na quarentena (Sandbox)

Status	ⓘ
Componente	Sandbox
ID de evento do Windows	2602
ID do evento do Kaspersky Security Center	00000a2a
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto excluído (Sandbox)

Status	ⓘ
Componente	Sandbox
ID de evento do Windows	2604
ID do evento do Kaspersky Security Center	00000a2c
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Verificação de IOC iniciada

Status	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2652
ID do evento do Kaspersky Security Center	00000a5c
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Verificação de IOC concluída

Status	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2653
ID do evento do Kaspersky Security Center	00000a5d
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto colocado na quarentena (Endpoint Detection and Response)

Status	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2555
ID do evento do Kaspersky Security Center	000009fb
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Objeto excluído (Endpoint Detection and Response)

Status	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2557
ID do evento do Kaspersky Security Center	000009fd
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Componentes do aplicativo modificados com êxito

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	1402
ID do evento do Kaspersky Security Center	0000057a
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Status	ⓘ
Componente	Sandbox
ID de evento do Windows	2606
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Status	ⓘ
Componente	Sandbox
ID de evento do Windows	2609
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Status	ⓘ
Componente	Sandbox
ID de evento do Windows	2610
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

Status	ⓘ
Componente	Sandbox
ID de evento do Windows	2616
ID do evento do Kaspersky Security Center	–
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	–

O Servidor de Administração no qual o dispositivo está conectado está definido como confiável

Status	ⓘ
Componente	Proteção da conexão do Servidor de Administração
ID de evento do Windows	3300
ID do evento do Kaspersky Security Center	00000ce4
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

O dispositivo está conectado a um novo Servidor de Administração confiável

Status	ⓘ
Componente	Proteção da conexão do Servidor de Administração
ID de evento do Windows	3302
ID do evento do Kaspersky Security Center	00000ce6
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

O Servidor de Administração no qual o dispositivo está conectado não está mais definido como confiável

Status	ⓘ
Componente	Proteção da conexão do Servidor de Administração
ID de evento do Windows	3303

ID do evento do Kaspersky Security Center	`00000ce7`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Detecção assíncrona do Sandbox

Status	ⓘ
Componente	Sandbox
ID de evento do Windows	`2619`
ID do evento do Kaspersky Security Center	`GNRL_EV_APP_INCIDENT_OCCURED`
Parâmetros do evento	• `GNRL_EA_PARAM_1` são os parâmetros dos componentes do Sandbox. • `GNRL_EA_PARAM_2` é o caminho para o objeto. • `GNRL_EA_PARAM_3` é o ID do incidente. • `GNRL_EA_PARAM_4` é o hash do objeto (SHA256).
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

A tarefa de verificação foi enviada com sucesso para o Sandbox por um usuário

Status	ⓘ
Componente	Sandbox
ID de evento do Windows	`2622`
ID do evento do Kaspersky Security Center	`00000a3e`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

O dispositivo está conectado

Status	ⓘ
Componente	Controle de dispositivos
ID de evento do Windows	`805`
ID do evento do Kaspersky Security Center	`GNRL_EV_DEVCTRL_DEV_PLUGGED`
Parâmetros do evento	• `GNRL_EA_PARAM_1` é o ID do hardware (HWID). • `GNRL_EA_PARAM_2` é o nome do usuário da sessão.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

O dispositivo está desconectado

Status	ⓘ
Componente	Controle de dispositivos
ID de evento do Windows	`806`
ID do evento do Kaspersky Security Center	`GNRL_EV_DEVCTRL_DEV_UNPLUGGED`
Parâmetros do evento	• `GNRL_EA_PARAM_1` é o ID do hardware (HWID). • `GNRL_EA_PARAM_2` é o nome do usuário da sessão.
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Conexão bem-sucedida com o servidor do EDR Expert

Status	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID de evento do Windows	2853
ID do evento do Kaspersky Security Center	00000b25
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Conexão bem-sucedida com o servidor de resposta da EDR Expert

Status	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID de evento do Windows	2853
ID do evento do Kaspersky Security Center	00000b25
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Conexão bem-sucedida com o servidor de coleta de telemetria da EDR Expert

Status	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID de evento do Windows	2857
ID do evento do Kaspersky Security Center	00000b26
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

Conexão bem-sucedida com o servidor NDR

Status	ⓘ
Componente	Network Detection and Response (KATA)
ID de evento do Windows	3083
ID do evento do Kaspersky Security Center	00000c0b
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

É permitido iniciar o aplicativo cliente de serviços de nuvem

Status	ⓘ
Componente	Cloud Discovery
ID de evento do Windows	2210
ID do evento do Kaspersky Security Center	000008a2

Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Acesso ao serviço de nuvem permitido

Status	ⓘ
Componente	Cloud Discovery
ID de evento do Windows	2211
ID do evento do Kaspersky Security Center	000008a3
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Acesso à área protegida

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	2004
ID do evento do Kaspersky Security Center	000007d4
Log de eventos do Windows (padrão)	✓
Log de eventos do Kaspersky Security Center (padrão)	✓

A alteração de um arquivo ou pasta foi detectada

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	2950
ID do evento do Kaspersky Security Center	00000b86
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

Mudanças de objeto com muita frequência. Iniciada agregação de eventos

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	2955
ID do evento do Kaspersky Security Center	00000b8b
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Relatório sobre mudança de objeto para o período de agregação

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	2956
ID do evento do Kaspersky Security Center	00000b8c
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

A alteração de registro foi detectada

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	2951
ID do evento do Kaspersky Security Center	00000b87
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

Conexão/desconexão do dispositivo detectada

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	2952
ID do evento do Kaspersky Security Center	00000b88
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

O escopo de monitoramento inclui objetos incorretos

Status	ⓘ / ⚠ / ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	2903
ID do evento do Kaspersky Security Center	00000b89
Log de eventos do Windows (padrão)	–

Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

Linha de base criada

Status	ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	`2957`
ID do evento do Kaspersky Security Center	`00000b8d`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Linha de base atualizada

Status	ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	`2958`
ID do evento do Kaspersky Security Center	`00000b8e`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Uma operação está sendo executada pelo usuário confiável

Status	ⓘ
Componente	Monitor de integridade do sistema
ID de evento do Windows	`2962`
ID do evento do Kaspersky Security Center	`00000b92`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção para este evento, vá para a seção **Configuração de eventos** da política e defina o período de retenção para o evento geral de Monitor da integridade do sistema – *A alteração de um arquivo ou pasta foi detectada*.

Conectado ao SVM

Status	ⓘ
Componente	Light Agent
ID de evento do Windows	`3152`
ID do evento do Kaspersky Security Center	`00000c50`
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Uma nova senha temporária foi criada

Status	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	265
ID do evento do Kaspersky Security Center	00000109
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Conectado ao Servidor de integração

Status	ⓘ
Componente	Light Agent
ID de evento do Windows	3105
ID do evento do Kaspersky Security Center	00000c21
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Restaurando a conexão com o Servidor de integração...

Status	ⓘ
Componente	Light Agent
ID de evento do Windows	3104
ID do evento do Kaspersky Security Center	00000c20
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Conexão bem-sucedida com o servidor KUMA

Status	ⓘ
Componente	Integração KUMA
ID de evento do Windows	2857
ID do evento do Kaspersky Security Center	00000b29
Log de eventos do Windows (padrão)	–
Log de eventos do Kaspersky Security Center (padrão)	✓

Apêndice 7. Extensões de arquivo compatíveis com a prevenção de execução

O Kaspersky Endpoint Security é compatível com a prevenção de abertura de arquivos no formato office em certos aplicativos. As informações sobre as extensões de arquivo e aplicativos compatíveis estão indicadas na seguinte tabela.

Extensões de arquivo compatíveis com a prevenção de execução

Nome do aplicativo	Arquivo executável	Extensão do arquivo
Microsoft Word	winword.exe	rtf doc ponto docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Leitor de PDF Foxit STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Yandex Browser Tor Browser	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

Apêndice 8. Interpretadores de script compatíveis com a prevenção de execução

A prevenção de execução é compatível com os seguintes intérpretes de script:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe

- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

A prevenção de execução é compatível com os aplicativos Java no ambiente de tempo de execução Java (processos java.exe e javaw.exe).

Apêndice 9. Escopo da verificação de IOC no registro (RegistryItem)

Quando o tipo de dado **Registro do Windows – RegistryItem** for adicionado ao escopo da verificação de IOC, o Kaspersky Endpoint Security, por padrão, verificará as seguintes chaves do registro:

```
HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile
```

```
HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

Apêndice 10. Requisitos de arquivos IOC

Ao criar as tarefas de Verificação de IOC, considere os seguintes requisitos e limitações de arquivos IOC:

- O aplicativo é compatível com os arquivos IOC com as extensões IOC e XML no padrão aberto OpenIOC versões 1.0 e 1.1 para descrever os indicadores de comprometimento.
- Depois de carregar os arquivos IOC, é possível fazer a edição manual deles no editor integrado, diretamente nas propriedades da tarefa. O Kaspersky Endpoint Security oferece suporte para a edição de arquivos IOC compatíveis com o padrão OpenIOC 1.1. Não é possível modificar o conteúdo de arquivos IOC compatíveis com o OpenIOC versão 1.0.
- Se, ao criar uma tarefa de *Verificação de IOC* na linha de comando, os arquivos IOC forem carregados, alguns dos quais sendo incompatíveis, quando a tarefa for executada, o aplicativo usará somente os arquivos IOC compatíveis. Se, ao criar uma tarefa de *Verificação de IOC* na linha de comando, todos os arquivos IOC carregados forem indicados como incompatíveis, a tarefa ainda pode será executada, mas ela não detectará nenhum indicador de compromisso. Não é possível carregar arquivos IOC incompatíveis usando o Web Console ou Cloud Console.
- Erros semânticos, termos e tags IOC não compatíveis em arquivos IOC não causam falha na execução da tarefa. Nessas seções de arquivos IOC, o aplicativo não detecta nenhuma correspondência.
- Os identificadores de todos os arquivos IOC utilizados em uma única tarefa de Verificação de IOC devem ser únicos. Se houver arquivos IOC com o mesmo identificador, isso poderá afetar os resultados da execução da tarefa.

- Um único arquivo IOC não deve exceder o tamanho de 2 MB. A utilização de arquivos maiores causará erros nas tarefas de Verificação de IOC. O tamanho total de todos os arquivos adicionados à coleção IOC não deve exceder 10 MB. Se o tamanho total de todos os arquivos exceder 10 MB, você precisará dividir a coleção IOC e criar diversas tarefas de *Verificação de IOC*.

- Recomenda-se a criação de um arquivo IOC por ameaça. Isso facilita a análise dos resultados da tarefa de *Verificação de IOC*.

O arquivo que pode ser baixado clicando no link abaixo contém uma tabela com a lista completa dos termos de IOC do padrão OpenIOC.

DOWNLOAD DO ARQUIVO IOC TERMS.XLSX

Os recursos e as limitações de compatibilidade do aplicativo com o padrão OpenIOC são apresentados na tabela a seguir.

Recursos e limitações do compatibilidade do OpenIOC versão 1.0 e 1.1.

Condições de compatibilidade	OpenIOC 1.0:
	
	`is`
	`isnot` (uma exceção a partir do conjunto)
	`contains`
	`containsnot` (uma exceção a partir do conjunto)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	
	Para termos de Email/*, somente as condições `contains` e `is` são compatíveis. Para que a Verificação Retrospectiva de IOC funcione corretamente, ao usar a condição `is`, os endereços de e-mail nos arquivos de IOC devem ser especificados no seguinte formato: `"name@example.org" <SMTP:name@example.org>`. Ao executar a tarefa *Verificação de IOC* normalmente, é suficiente especificar o endereço de e-mail no seguinte formato: `name@example.org`.

Atributos de condições de compatibilidade	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Operadores compatíveis	`AND` `OR`
Tipos de dados compatíveis	`"date"`: data (condições aplicáveis: `is`, `greater-than`, `less-than`) `"int"`: número inteiro (condições aplicáveis: `is`, `greater-than`, `less-than`) `"string"`: string (condições aplicáveis: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: duração em segundos (condições aplicáveis: `is`, `greater-than`, `less-than`)

Características de interpretação de tipos de dados	Os tipos de dados `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"` e `"base64Binary"` são interpretados como string.
	
	O aplicativo é compatível com a interpretação da configuração `Content`, para os tipos de dados `int` e `date` quando definidos na forma de intervalos:
	
	OpenIOC 1.0:
	Uso do operador `TO` no campo `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	Uso das condições `greater-than` e `less-than`
	Uso do operador `TO` no campo `Content`
	O aplicativo é compatível com a interpretação dos tipos de dados `date` e `duration` caso os indicadores sejam definidos no formato `ISO 8601, Zulu time zone, UTC`.

Apêndice 11. Resposta a ameaças da API para EDR

O Kaspersky Endpoint Security 12.9 for Windows apresenta compatibilidade com Ações de Resposta a ameaças do EDR (EDR responses) usando a OpenAPI do Kaspersky Security Center. Ou seja, você pode chamar os métodos OpenAPI para automatizar a resposta a ameaças do EDR usando o Python. Você pode chamar esses métodos quando integrado com soluções SIEM. A *Kaspersky Unified Monitoring and Analysis Platform*, a solução SIEM da Kaspersky, é compatível com a OpenAPI de Resposta a ameaças do EDR a partir da versão 3.4.1. Para scripts de exemplo, consulte a documentação do KUMA.

Para executar ações de resposta a ameaças EDR, é preciso criar uma solicitação e enviá-la usando KSC Open API (`AddIncident`). Após o processamento da solicitação, uma tarefa especial será criada no console do Kaspersky Security Center.

Para criar tarefas ao responder a ameaças EDR, é necessário estabelecer uma conexão em segundo plano entre o Servidor de Administração e o Kaspersky Security Center Web Console. O serviço de conexão em segundo plano está disponível no Kaspersky Security Center Windows 14.2 ou posterior e no Kaspersky Security Center Linux 15.2 ou posterior. Outros consoles, incluindo consoles das soluções Detection and Response da Kaspersky, não são compatíveis.

Para a resposta a ameaças EDR, é necessário especificar parâmetros básicos de solicitação, por exemplo, no formato JSON:

- `task` é o tipo da tarefa (veja abaixo).
- `targetHost` é o ID do computador no qual o script deve ser executado. Argumento necessário. O script obtém esse argumento do evento.
- `responseEventIncidentArea` é o nome do aplicativo que executou o script (por exemplo, `KUMA`). Este parâmetro é adicionado ao nome da tarefa criada.

Para configurar a resposta a ameaças EDR, é preciso especificar as configurações da tarefa no formato JSON no parâmetro `"KLINCDT_BODY": json.dumps(data)`. Como resultado, o aplicativo cria o `[Response][KUMA] <task type> - <Date> <Time> - <ID>` no console do Kaspersky Security Center.

Conectar-se à OpenAPI do Kaspersky Security Center

Como parte da resposta a ameaças EDR, o aplicativo cria tarefas especiais no console do Kaspersky Security Center. A criação de tarefas requer o estabelecimento de uma conexão entre o computador e o Kaspersky Security Center. Para conseguir isso, os parâmetros de conexão do Kaspersky Security Center devem ser especificados na solicitação.

No Kaspersky XDR versão 2.1, o método para autorizar solicitações foi alterado. O Kaspersky XDR usa tokens PAT em vez da autenticação por nome de usuário e senha. Portanto, não é possível executar scripts no Kaspersky XDR. Para obter mais informações sobre a autorização de solicitações, consulte a Ajuda do Kaspersky XDR.

Parâmetros de conexão do Kaspersky Security Center

Parâmetro	Tipo	Descrição
`kscHost`	`string`	Endereço do Servidor de Administração do Kaspersky Security Center. Parâmetro obrigatório.
`kscPort`	`int`	Porta da conexão do Servidor de Administração Parâmetro obrigatório.
`kscCert`	`string`	Caminho para um arquivo de certificado para conexão ao Servidor de Administração do Kaspersky Security Center. Por padrão, o parâmetro é definido como `False`.
`kscUser`	`string`	Nome da conta do usuário. Parâmetro obrigatório.
`kscPassword`	`string`	Senha da conta de usuário. Parâmetro obrigatório.

Exemplo

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
# KSC password, string, required
kscPassword = "kscPassword"

server_url = 'https://' + kscHost + ':' + str(kscPort)
    server = KlAkAdmServer.Create(
        server_url, kscUser, kscPassword, verify=kscCert)

    params = validate(args)

    data = {"targetHost": <MyHost>,
            "task": task,
            "params": params,
            "responseEventIncident": True,
            "responseEventIncidentArea":"Kuma"}

    oHostGroup = KlAkHostGroup(server)

    incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2,
                                     "KLINCDT_ADDED": paramDateTime(datetime.datetime.now()),
                                     "KLINCDT_BODY": json.dumps(data),
                                     "KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal()

    oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False,
                                       "KLHST_WKS_HOSTNAME":  args.targetHost})
```

Os dados da conta do usuário não são protegidos, portanto, é necessário dedicar um usuário separado que será usado para executar somente essas ações.

Obter o arquivo – getFile

Configurações da tarefa Obter o arquivo

Parâmetro	Tipo	Descrição
`md5hash`	`string`	Hash MD5 do arquivo que o usuário deseja obter.
`sha256hash`	`string`	Hash SHA256 do arquivo que o usuário deseja obter.
`path`	`string`	Caminho para o arquivo que o usuário deseja obter.

Exemplo

```
type getFile = {
  task: 'getFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Excluir arquivo – deleteFile

Configurações da tarefa Excluir arquivo

Parâmetro	Tipo	Descrição
`md5hash`	`string`	Hash MD5 do arquivo que o usuário deseja excluir.
`sha256hash`	`string`	Hash SHA256 do arquivo que o usuário deseja excluir.
`path`	`string`	Caminho para o arquivo que o usuário deseja excluir.
`searchInSubfolders?`	`boolean`	Pesquise o arquivo que deseja excluir nas subpastas.

Exemplo

```
type deleteFile = {
  task: 'deleteFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // recursive search for a file (subfolder), optional
    searchInSubfolders?: boolean;
  };
  responseEventIncidentArea: string;
};
```

Mover arquivo para a Quarentena – quarantineFile

Configurações da tarefa Mover arquivo para a Quarentena

Parâmetro	Tipo	Descrição
`md5hash`	`string`	Hash MD5 do arquivo que o usuário deseja colocar em quarentena.
`sha256hash`	`string`	Hash SHA256 do arquivo que o usuário deseja colocar em quarentena.
`path`	`string`	Caminho para o arquivo que o usuário deseja colocar em quarentena.

Exemplo

```
type quarantineFile = {
  task: 'quarantineFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Verificação de IOC – iocScan

Configurações da tarefa Verificação de IOC

Parâmetro	Tipo	Descrição
`ioc`	`string`	Caminho para o arquivo comprimido Zip com arquivos IOC que você deseja usar para verificação.
`isolateHost`	`boolean`	Isole o computador da rede quando um indicador de comprometimento for detectado para impedir que a ameaça se espalhe.
`scanCriticalAreas`	`boolean`	Execute a tarefa *Verificação de áreas críticas* quando um indicador de comprometimento for detectado.
`quarantineObject`	`boolean`	Exclua o objeto malicioso quando um indicador de comprometimento for detectado. Antes de excluir o objeto, o Kaspersky Endpoint Security cria uma cópia de backup, caso o objeto precise ser restaurado posteriormente. O Kaspersky Endpoint Security move a cópia de backup para a quarentena.

Exemplo

```
type iocScan = {
  task: 'iocScan';
  targetHost: string;
  params: {
    // the path to the zip archive with ioc files in base64 encoding
    ioc: string;
    // isolation of the computer from the network
    isolateHost: boolean;
    // critical areas scan
    scanCriticalAreas: boolean;
    // quarantine the file
    quarantineObject: boolean;
  };
  responseEventIncidentArea: string;
};
```

Iniciar processo – startProcess

Configurações da tarefa Iniciar processo

Parâmetro	Tipo	Descrição
executablePath	string	Caminho para o arquivo executável usado para iniciar o processo.
arguments?	string	Argumentos de linha de comando adicionais para iniciar o processo.
workingFolder?	string	Caminho para a pasta de trabalho do processo.

Exemplo

```
type startProcess = {
  task: 'startProcess';
  targetHost: string;
  params: {
    // the path to the file
    executablePath: string;
    // command line arguments, optional
    arguments?: string;
    // a working folder, optional
    workingFolder?: string;
  };
  responseEventIncidentArea: string;
};
```

Encerrar processo – terminateProcess

Configurações da tarefa Encerrar processo

Parâmetro	Tipo	Descrição
md5hash	string	Hash MD5 do arquivo cujo processo o usuário deseja encerrar.
sha256hash	string	Hash SHA256 do arquivo cujo processo o usuário deseja encerrar.
path	string	Caminho para o arquivo que o usuário deseja excluir.
caseSensitive	boolean	Diferenciação entre maiúsculas e minúsculas ao procurar o arquivo.

Exemplo

```
type terminateProcess = {
  task: 'terminateProcess';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Isolamento de rede do computador – isolateHost

Configurações de isolamento de rede do computador

Parâmetro	Tipo	Descrição
`action`	`string`	Modo de operação do Isolamento de rede.

Exemplo

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

Prevenção de execução – preventExecution

Configurações de prevenção de execução

Parâmetro	Tipo	Descrição
`hash`	`string`	Hash MD5 do arquivo do qual o usuário deseja impedir a execução.
`path`	`string`	Caminho para o arquivo do qual o usuário deseja impedir a execução.
`caseSensitive`	`boolean`	Diferenciação entre maiúsculas e minúsculas ao procurar o arquivo.

Exemplo

```
type preventExecution = {
  task: 'preventExecution';
  targetHost: string;
  params: {
    // a valid md5 hash of the file
    hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Verificação de malware – onDemandScan

Configurações da tarefa Verificação de malware

Parâmetro	Tipo	Descrição
`path`	`string`	Lista delimitada por espaços de arquivos e pastas para Verificação personalizada.
`recursive`	`boolean`	Modo de Verificação recursiva.

Parâmetro	Tipo	Descrição
type	number	Escopo da verificação.

```
ScanObjectType = Enum("ScanObjectType",
                      [
                          ("SystemMemory", 14),
                          ("StartupObjectsAndRunningProcesses", 15),
                          ("DiskBootSectors", 16),
                          ("SystemBackupStorage", 17),
                          ("Email", 18),
                          ("Folder", 22),
                          ("AllRemovableDrives", 23),
                          ("AllNetworkDrives", 24),
                          ("AllFixedDrives", 25)])
```

Exemplo

```
type onDemandScan = {
  task: 'onDemandScan';
  targetHost: string;
  // please note, this is an array
  // array of scan object
  params: [{
    // enabling the scan object
    enabled: boolean;
    // an empty string or the path to the folder to scan
    path: string;
    // recursive scan mode
    recursive: boolean;
    // ID scan object
    type: number;
  }];
  responseEventIncidentArea: string;
};
```

Apêndice 12. Contas de usuário em regras de componentes de aplicativos

Para configurar alguns componentes do aplicativo, é preciso adicionar regras especiais. Por exemplo, para o Controle da Web, é preciso adicionar uma regra com uma lista de endereços da Web que você deseja que ele bloqueie. Nas regras de componentes do aplicativo, também é possível configurar um agendamento para o componente ou selecionar usuários para os quais o aplicativo deverá aplicar a regra.

As regras devem ser adicionadas para configurar os seguintes componentes do aplicativo:

- Controle de Aplicativos.
- Controle da Web.
- Controle de Dispositivos.
- Inspeção de Log.
- Controle Adaptativo de Anomalias.
- Monitor de integridade do sistema.

A partir do Kaspersky Endpoint Security for Windows 12.5, é possível selecionar usuários não apenas do Active Directory, mas também da lista de usuários no Kaspersky Security Center. Também é possível inserir os dados da conta de usuário local manualmente. Isso significa que é possível adicionar usuários das seguintes maneiras:

- Active Directory (recomendado)
- Lista de usuários no Kaspersky Security Center
- Conta de usuário local

Para utilizar corretamente todos os métodos de seleção de usuário, você precisa atualizar o aplicativo e o plug-in de gerenciamento do Kaspersky Endpoint Security para a versão 12.5 ou superior.

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 Kaspersky Endpoint Security.

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 aplicativo utiliza nomes NetBIOS para a identificação de contas de usuário adicionadas manualmente nos formatos `<username>` e `<hostname>\<username>`. Um nome NetBIOS pode ter até 16 bytes (15 caracteres) de comprimento. Se o nome do computador tiver mais de 15 caracteres, o aplicativo não poderá identificar o usuário. Em seguida, o aplicativo desativa a regra e gera um erro, por exemplo, *Controle da Web: acionamento de regras desativado para contas de usuários sem identificador de segurança (SID) correspondente*. Para que a regra funcione, você deve alterar manualmente o nome do computador para um mais curto. Você pode adicionar contas de usuário do Active Directory ou do Kaspersky Security Center. Nesse caso, o aplicativo altera manualmente o nome do computador para um mais curto.

O Kaspersky Endpoint Security também é compatível com usuários e grupos integrados (como o grupo "Todos") nas regras. Devido à forma como o SID de um usuário é determinado, o aplicativo permite usar somente contas de usuário incorporadas adicionadas por meio do Active Directory ou da lista de usuários no Kaspersky Security Center. As regras nas quais uma conta de usuário integrada é adicionada localmente não funcionam.

Informações Legais

Provisão de dados

Esta seção contém informações sobre os dados que o aplicativo Kaspersky Endpoint Security pode armazenar no dispositivo e transmitir automaticamente para a Kaspersky durante sua operação.

As informações recebidas são protegidas pela Kaspersky conforme a lei e os requisitos e as regulações aplicáveis da Kaspersky. Os dados são transmitidos por canais de comunicação criptografados.

Provisão de dados segundo o Contrato de Licença do Usuário Final

Se um código de ativação for aplicado para ativar o Kaspersky Endpoint Security, você aceitará enviar periodicamente para o Kaspersky as seguintes informações automaticamente, com a finalidade de verificar o uso correto do aplicativo:

- Tipo, versão e localização do Kaspersky Endpoint Security;
- Versões de atualizações instaladas do Kaspersky Endpoint Security;
- ID do computador e ID da instalação específica do Kaspersky Endpoint Security no computador;
- Número de série e identificador da chave ativa;
- Tipo, versão e taxa de bits do sistema operacional e nome do ambiente virtual (se o Kaspersky Endpoint Security estiver instalado em um ambiente virtual);
- ID de solicitação exclusivo para os serviços do Titular dos direitos;
- IDs dos componentes do Kaspersky Endpoint Security que estão ativos quando as informações são transmitidas.

A Kaspersky também pode usar essas informações para gerar estatísticas sobre a disseminação e o uso do software da Kaspersky.

Ao usar um código de ativação, você concorda em transmitir automaticamente os dados listados acima. Se não concordar em transmitir essas informações à Kaspersky, você deve usar arquivo de chave para ativar o Kaspersky Endpoint Security.

Ao aceitar os termos do Contrato de Licença do Usuário Final, você aceita transmitir automaticamente as seguintes informações:

- Ao atualizar o Kaspersky Endpoint Security:
  - versão do Kaspersky Endpoint Security;
  - ID do Kaspersky Endpoint Security;

- chave ativa;
- ID único de início da tarefa de atualização;
- ID único de instalação do Kaspersky Endpoint Security.

- Ao seguir links da interface do Kaspersky Endpoint Security:
  - versão do Kaspersky Endpoint Security;
  - Versão do sistema operacional;
  - Data de ativação do Kaspersky Endpoint Security;
  - data de expiração da licença;
  - Data de criação da chave;
  - Data de instalação do Kaspersky Endpoint Security;
  - ID do Kaspersky Endpoint Security;
  - ID da vulnerabilidade detectada no sistema operacional;
  - ID da última atualização instalada para o Kaspersky Endpoint Security;
  - Hash da ameaça detectada no arquivo e o nome dessa ameaça segundo a classificação da Kaspersky;
  - Categoria de erro de ativação do Kaspersky Endpoint Security;
  - Código de erro de ativação do Kaspersky Endpoint Security;
  - Número de dias antes da expiração da chave;
  - O número de dias que se passaram desde que a chave foi adicionada;
  - Número de dias que se passaram desde que a licença expirou;
  - Número de computadores nos quais a licença atualmente em uso foi aplicada;
  - chave ativa;
  - Termo de licença do Kaspersky Endpoint Security;
  - Status atual da licença;
  - Tipo de licença atualmente em uso;
  - Tipo de aplicativo;
  - ID único de início da tarefa de atualização;
  - ID único de instalação do Kaspersky Endpoint Security no computador;
  - Idioma de interface do Kaspersky Endpoint Security.

As informações recebidas são protegidas pela Kaspersky conforme a lei e os requisitos e as regulações aplicáveis da Kaspersky. Os dados são transmitidos por canais de comunicação criptografados.

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.

Fornecimento de dados ao usar a Kaspersky Security Network

O conjunto de dados que o Kaspersky Endpoint Security envia ao Kaspersky depende do tipo de licença e das configurações de uso da Kaspersky Security Network.

Uso de KSN sob licença em não mais de 4 computadores

Ao aceitar a Declaração da Kaspersky Security Network, você concorda em transmitir automaticamente as seguintes informações:

- informações sobre atualizações nas configuração da KSN: identificador da configuração ativa, identificador da configuração recebida, código de erro da atualização da configuração;
- informações sobre arquivos e endereços de URL a serem verificados: somas de verificação do arquivo verificado (MD5, SHA2-256, SHA1) e padrões de arquivos (MD5), tamanho do padrão, tipo de ameaça detectada e respectivo nome de acordo com a classificação do Titular dos Direitos, identificador dos bancos de dados de antivírus, endereço URL em que a reputação está sendo solicitada, bem como o endereço URL do solicitante, identificador do protocolo de conexão e número da porta que está sendo utilizada;
- ID da tarefa de verificação que detectou a ameaça;
- informações sobre os certificados digitais que estão sendo utilizados e que são necessárias para verificar a autenticidade deles: as somas de verificação (SHA256) do certificado utilizado para assinar o objeto verificado e a chave pública do certificado;
- identificador do componente de software que está executando a verificação;
- IDs dos bancos de dados de antivírus e dos registros nesses bancos de dados de antivírus;
- informações sobre ativação do Software no Computador: cabeçalho assinado do ticket do serviço de ativação (identificador do centro de ativação regional, soma de verificação do código de ativação, soma de verificação do ticket, data de criação do ticket, identificador único do ticket, versão do ticket, status de licença, data e hora de início/final da validade do ticket, identificador único da licença, versão da licença), identificador do certificado usado para assinar o cabeçalho do ticket, soma de verificação (MD5) do arquivo de chave;
- informações sobre o Software do Titular dos direitos: versão completa, tipo e versão do protocolo usado para conectar-se aos serviços da Kaspersky.

Uso de KSN sob licença em 5 ou mais computadores

Ao aceitar a Declaração da Kaspersky Security Network, você concorda em transmitir automaticamente as seguintes informações:

Se a caixa de seleção **Kaspersky Security Network** estiver marcada e a caixa de seleção **Ativar modo KSN estendido** estiver desmarcada, as seguintes informações serão transmitidas:

- informações sobre atualizações nas configuração da KSN: identificador da configuração ativa, identificador da configuração recebida, código de erro da atualização da configuração;
- informações sobre arquivos e endereços de URL a serem verificados: somas de verificação do arquivo verificado (MD5, SHA2-256, SHA1) e padrões de arquivos (MD5), tamanho do padrão, tipo de ameaça detectada e respectivo nome de acordo com a classificação do Titular dos Direitos, identificador dos bancos de dados de antivírus, endereço URL em que a reputação está sendo solicitada, bem como o endereço URL do solicitante, identificador do protocolo de conexão e número da porta que está sendo utilizada;
- ID da tarefa de verificação que detectou a ameaça;
- informações sobre os certificados digitais que estão sendo utilizados e que são necessárias para verificar a autenticidade deles: as somas de verificação (SHA256) do certificado utilizado para assinar o objeto verificado e a chave pública do certificado;
- identificador do componente de software que está executando a verificação;
- IDs dos bancos de dados de antivírus e dos registros nesses bancos de dados de antivírus;
- informações sobre ativação do Software no Computador: cabeçalho assinado do ticket do serviço de ativação (identificador do centro de ativação regional, soma de verificação do código de ativação, soma de verificação do ticket, data de criação do ticket, identificador único do ticket, versão do ticket, status de licença, data e hora de início/final da validade do ticket, identificador único da licença, versão da licença), identificador do certificado usado para assinar o cabeçalho do ticket, soma de verificação (MD5) do arquivo de chave;
- informações sobre o Software do Titular dos direitos: versão completa, tipo e versão do protocolo usado para conectar-se aos serviços da Kaspersky.

Caso as caixas de seleção **Ativar modo KSN estendido** e **Kaspersky Security Network** estejam marcadas, o aplicativo enviará as seguintes informações, além das informações listadas acima:

- informações sobre os resultados da categorização dos recursos da Web solicitados, que contêm o endereço URL e IP processados do host, a versão do componente do Software que executou a categorização, o método de categorização e o conjunto de categorias definidas para o recursos da Web;
- informações sobre o software instalado no Computador: nomes dos aplicativos de software e fornecedores do software, chaves de registro e respectivos valores, informações sobre arquivos dos componentes de software instalados (somas de verificação (MD5, SHA2-256, SHA1), nome, caminho até o arquivo no Computador, tamanho, versão e assinatura digital);
- informações sobre o estado da proteção antivírus do Computador: as versões e os carimbos de data/hora de lançamento dos bancos de dados de antivírus em uso, o ID da tarefa e o ID do Software que executa a verificação;

- informações sobre arquivos que o Usuário Final esteja baixando: URL e endereços IP dos downloads e páginas de download, identificador do protocolo de download e número da porta de conexão, status dos URLs como malicioso ou não malicioso, atributos, tamanho e somas de verificação (MD5, SHA2-256, SHA1) dos arquivos, informações sobre o processo que baixou o arquivo (somas de verificação (MD5, SHA2-256, SHA1), data e hora da criação/compilação, status de reprodução automática, atributos, nomes dos empacotadores, informações sobre assinaturas, indicador de arquivo executável, identificador de formatos e entropia), nome e caminho do arquivo no Computador, assinatura digital do arquivo e marca de hora de sua geração, endereço URL onde ocorreu a detecção, número do script na página parece suspeita ou nociva, informações sobre solicitações HTTP geradas e respectivas respostas;

- informações sobre os aplicativos em execução e respectivos módulos: dados sobre processos em execução no sistema (ID de processo (PID), nome do processo, informações sobre a conta na qual o processo foi iniciado, aplicativo e comando que iniciaram o processo, sinal de programa ou processo confiável, caminho completo dos arquivos do processo e as respectivas somas de verificação (MD5, SHA2-256, SHA1), e a linha de comando inicial, o grau de integridade do processo, uma descrição do produto ao qual o processo pertence (o nome do produto e informações sobre o editor), além de certificados digitais em uso e informações necessárias para verificar a autenticidade ou informações sobre a ausência de assinatura digital do arquivo) e informações sobre os módulos carregados nos processos (nomes, tamanhos, tipos, datas de criação, atributos, somas de verificação (MD5, SHA2-256, SHA1), respectivos caminhos no Computador), informações do cabeçalho do arquivo PE, nomes dos compactadores (se o arquivo estiver compactado);

- informações sobre todos os objetos e atividades potencialmente maliciosos: nome do objeto detectado e caminho completo para o objeto no computador, somas de verificação de arquivos processados (MD5, SHA2-256, SHA1), data e hora da detecção, nomes e tamanhos de arquivos infectados e caminhos para eles, código de modelo de caminho, indicador de arquivo executável, indicador se o objeto é um contêiner, nomes do compactador (se o arquivo foi compactado), código do tipo de arquivo, identificação do formato do arquivo, lista de ações realizadas pelo malware e a decisão tomada pelo software e o usuário em resposta a elas, IDs dos bancos de dados de antivírus e dos registros nesses bancos de dados de antivírus que foram usados para tomar a decisão, indicador de um objeto potencialmente malicioso, nome da ameaça detectada de acordo com a classificação do Titular de direito, nível de perigo, status de detecção e método de detecção, razão para inclusão no contexto analisado e o número de sequência do arquivo no contexto, somas de verificação (MD5, SHA2-256, SHA1), nome e atributos do arquivo executável do aplicativo por meio do qual a mensagem ou o link infectados foram transmitidos, endereços IP despersonalizados (IPv4 e IPv6) do host do objeto bloqueado, entropia de arquivo, indicador de execução automática do arquivo, hora em que o arquivo foi detectado pela primeira vez no sistema, número de vezes que o arquivo foi executado desde que as últimas estatísticas foram enviadas, informações sobre nome, somas de verificação (MD5, SHA2-256, SHA1) e tamanho do cliente de e-mail por meio do qual o objeto malicioso foi recebido, ID da tarefa de software que realizou a verificação, indicador para a verificação de reputação ou assinatura do arquivo, resultado de processamento de arquivos, soma de verificação (MD5) do padrão coletado para o objeto, tamanho do padrão em bytes e especificações técnicas das tecnologias de detecção aplicadas;

- informações sobre objetos verificados: grupo de confiança atribuído no qual e/ou a partir do qual o arquivo foi colocado, motivo pelo qual o arquivo foi colocado naquela categoria, identificador da categoria, informações sobre a origem das categorias e a versão do banco de dados das categorias, identificador do certificado confiável do arquivo, nome do fornecedor do arquivo, versão do arquivo, nome e versão do aplicativo de software que inclui o arquivo;

- informações sobre vulnerabilidades detectadas: ID da vulnerabilidade no banco de dados de vulnerabilidades, classe de perigo da vulnerabilidade;

- informações sobre a emulação do arquivo executável: tamanho do arquivo e respectivas somas de verificação (MD5, SHA2-256, SHA1), versão do componente de emulação, profundidade da emulação, matriz das propriedades de blocos lógicos e funções dentro dos blocos lógicos obtidos durante a emulação, dados dos cabeçalhos PE do arquivo executável;

- os endereços IP do computador que realiza o ataque (IPv4 e IPv6), o número da porta no computador ao qual o ataque de rede foi direcionado, o identificador do protocolo do pacote IP que contém o ataque, o alvo do ataque (nome da organização, site), o indicador da reação ao ataque, peso do ataque, nível de confiança;

- informações sobre ataques associados a recursos de rede falsificados, DNS e endereços IP (IPv4 e IPv6) dos sites visitados;

- DNS e endereços IP (IPv4 ou IPv6) do recurso da Web solicitado, informações sobre o arquivo e o cliente Web que acessou o recurso da Web, nome, tamanho e checksums (MD5, SHA2-256, SHA1) do arquivo, caminho completo do arquivo e código do modelo do caminho, resultado da verificação da assinatura digital e status de acordo com a KSN;

- informações sobre reversão de ações de Malware: dados no arquivo cuja atividade foi revertida (nome do arquivo, caminho completo para o arquivo, seu tamanho e somas de verificação (MD5, SHA2-256, SHA1)), dados sobre ações bem-sucedidas e malsucedidas a excluir, renomear e copiar arquivos e restaurar os valores no registro (nomes das chaves de registro e seus valores) e informações sobre arquivos de sistema modificados pelo Malware, antes e depois da reversão;

- Informações sobre as exclusões definidas para o componente de Controle Adaptativo de Anomalias: ID e status da regra que foi acionada, ação executada pelo Software quando a regra foi acionada, tipo de conta de usuário sob a qual o processo ou o thread executa atividade suspeita, informações sobre o processo que estava sujeito à atividade suspeita (ID do script ou nome do arquivo de processo, caminho completo do arquivo de processo, código do modelo do caminho, checksums (MD5, SHA2-256, SHA1) do arquivo de processo); informações sobre o objeto que executou as ações suspeitas e sobre o objeto que estava sujeito às ações suspeitas (nome da chave do registro ou nome do arquivo, caminho completo do arquivo, código do modelo de caminho e checksums (MD5, SHA2-256, SHA1) do arquivo).

- informações sobre módulos de software carregados: nome, tamanho e somas de verificação (MD5, SHA2-256, SHA1) do arquivo de módulo, caminho completo e código do modelo do caminho, configurações da assinatura digital do arquivo de módulo, data e hora da geração da assinatura, nomes da pessoa física e jurídica que assinou o arquivo de módulo, ID do processo no qual o módulo foi carregado, nome do fornecedor do módulo e o número de sequência do módulo na fila de carregamento;

- informações sobre a qualidade da interação do Software com os serviços KSN: data e hora inicial e final do período em que as estatísticas foram geradas, informações sobre a qualidade das solicitações e a conexão a cada um dos serviços da KSN usados (ID do serviço da KSN, número de solicitações bem-sucedidas, número de solicitações com respostas do cache, número de solicitações malsucedidas (problemas de rede, desativação da KSN nas configurações do Software, roteamento incorreto), intervalo de tempo das solicitações bem-sucedidas, intervalo de tempo das solicitações canceladas, intervalo de tempo das solicitações com limite de tempo excedido, número de conexões à KSN retiradas do cache, número de conexões bem-sucedidas à KSN, número de conexões malsucedidas à KSN, número de transações bem-sucedidas, número de transações malsucedidas, intervalo de tempo das conexões bem-sucedidas à KSN, intervalo de tempo das conexões malsucedidas à KSN, intervalo de tempo das transações bem-sucedidas, intervalo de tempo das transações malsucedidas);

- se um objeto potencialmente malicioso for detectado, serão fornecidas informações sobre dados na memória dos processos: elementos da hierarquia de objetos do sistema (ObjectManager), dados na memória UEFI-BIOS, nomes das chaves de registro e respectivos valores;

- informações sobre eventos em logs do sistema: marca de hora do evento, nome do log no qual o evento foi encontrado, tipo e categoria do evento, nome da origem do evento e descrição do evento;

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

- informações sobre a data de instalação e ativação do software no computador: o ID do parceiro que vendeu a licença, o número de série da licença, o cabeçalho assinado do tíquete do serviço de ativação (o ID de um centro de ativação regional, o checksum do código de ativação, o checksum do tíquete, a data de criação do tíquete, o ID exclusivo do tíquete, a versão do tíquete, o status da licença, a data e hora de início/término do tíquete, o ID exclusivo da licença, a versão da licença), o ID do certificado usado para assinar o cabeçalho do tíquete, o checksum (MD5) do arquivo de chave, o ID exclusivo de instalação do software no computador, o tipo e ID do aplicativo que é atualizado, o ID da tarefa de atualização;

- informações sobre o conjunto de todas as atualizações instaladas e o conjunto das atualizações instaladas/removidas mais recentemente, tipo de evento que causou o envio das informações de atualização, tempo decorrido desde a instalação da última atualização, informações sobre quaisquer bancos de dados de antivírus instalados;

- informações sobre operação de software no computador: dados sobre uso de CPU, dados sobre uso de memória (bytes privados, Pool não paginado, Pool em páginas) número de ameaças ativas no processo de software e ameaças pendentes e a duração de operação de software antes do erro;

- número de dumps do software e dumps do sistema (BSOD) desde a instalação do Software e desde o momento da última atualização, identificador e versão do módulo do Software que apresentou erro fatal, pilha da memória no processo do Software, e informações sobre os bancos de dados antivírus no momento do erro fatal;

- dados sobre o dump do sistema (BSOD): sinalizador indicando a ocorrência da BSOD no Computador, nome do driver que causou a BSOD, endereço e pilha de memória no driver, sinalizador indicando a duração da sessão no SO antes da ocorrência da BSOD, pilha de memória do driver que apresentou erro fatal, tipo de dump de memória armazenado, sinalizador da sessão do SO anterior à BSOD com duração superior a 10 minutos, identificador exclusivo do dump, carimbo de data/hora da BSOD;

- informações sobre erros ou problemas de desempenho que ocorreram durante a operação dos componentes do Software: ID de status do Software, tipo de erro, código e causa, bem como a hora em que ocorreu o erro, IDs do componente, módulo e processo do produto no qual ocorreu o erro, ID da tarefa ou categoria de atualização durante a qual ocorreu o erro, logs de drivers utilizados pelo Software (código de erro, nome do módulo, nome do arquivo de origem e a linha em que ocorreu o erro);

- informações sobre atualizações de bancos de dados antivírus e componentes de Software: nome, data e hora dos arquivos de índice baixados durante a última atualização e que estão sendo baixados durante a atualização atual;

- informações sobre encerramento anormal da operação do Software: carimbo de data/hora de criação do dump, respectivo tipo, tipo de evento que causou o encerramento anormal da operação do Software (desligamento inesperado, erro fatal em aplicativos de terceiros), data e hora do desligamento inesperado;

- informações sobre a compatibilidade dos drivers de Software com o hardware e o Software: informações sobre propriedades do SO que restringem o funcionamento dos componentes do Software (inicialização segura, KPTI, WHQL Enforce, BitLocker, diferenciação entre maiúsculas e minúsculas), tipo de Software baixado e instalado (UEFI, BIOS), identificador do módulo de plataforma confiável (TPM), versão de especificação do TPM, informações sobre a CPU instalada no Computador, modo de operação e parâmetros de integridade do código e proteção do dispositivo, modo de operação dos drivers e motivo do uso do modo atual, versão dos drivers do Software e status de suporte à virtualização do software e hardware do Computador;

- informações sobre aplicativos de terceiros que tenham causado o erro: nome, versão e localização dos aplicativos, código do erro e informações sobre o erro contidas no log de aplicativos do sistema, endereço do erro e pilha de memória do aplicativo de terceiros, sinalizador indicando a ocorrência do erro no componente do Software, tempo de operação do aplicativo de terceiros antes da ocorrência do erro, somas de verificação (MD5, SHA2-256, SHA1) da imagem do processo do aplicativo no qual ocorreu o erro, caminho da imagem do processo do aplicativo e código do modelo do caminho, informações contidas no log do sistema com descrição do erro associado ao aplicativo, informações sobre o módulo do aplicativo no qual ocorreu o erro (identificador da exceção, endereço da memória afetada pela pane como deslocamento no módulo do aplicativo, nome e versão do módulo, identificador da pene do aplicativo no plug-in e pilha de memória da pane do Titular dos Direitos, duração da sessão do aplicativo antes da pane);

- versão do componente de atualização do Software, número de panes do componente de atualização durante a execução de tarefas de atualização ao longo da vida útil do componente, ID do tipo de tarefa de atualização, número de tentativas fracassadas do componente de atualização para concluir as tarefas de atualização;

- informações sobre a operação dos componentes de monitoramento do sistema de Software: versões completas dos componentes, data e hora em que os componentes foram iniciados, código do evento que sobrecarregou a fila de eventos e número de eventos, número total de eventos de sobrecarga da fila, informações sobre o arquivo do processo do iniciador do evento (nome do arquivo e respectivo caminho no Computador, código do modelo do caminho do arquivo, checksums (MD5, SHA2-256, SHA1) do processo associado ao arquivo, versão do arquivo), identificador da interceptação do evento ocorrida, versão completa do filtro de interceptação, identificador do tipo de evento interceptado, tamanho da fila de eventos e número de eventos entre o primeiro evento da fila e o evento atual, número de eventos atrasados na fila, informações sobre o arquivo do processo do iniciador do evento atual (nome do arquivo e respectivo caminho no Computador, código do modelo do caminho do arquivo, checksums (MD5, SHA2-256, SHA1) do processo associado ao arquivo), duração do processamento do evento, duração máxima do processamento do evento, probabilidade de envio de estatísticas, informações sobre eventos do SO para os quais o limite de tempo de processamento foi excedido (data e hora do evento, número de inicializações repetidas dos bancos de dados antivírus, data e hora da última inicialização repetida dos bancos de dados antivírus após a atualização deles, tempo de atraso no processamento de eventos para cada componente de monitoramento do sistema, número de eventos na fila, número de eventos processados, número de eventos atrasados do tipo atual, tempo total de atraso dos eventos do tipo atual, tempo total de atraso de todos os eventos);

- informações da ferramenta de rastreamento de eventos do Windows (Event Tracing for Windows, ETW) em caso de problemas de desempenho do Software, fornecedores de eventos SysConfig/SysConfigEx/WinSATAssessment da Microsoft: informações sobre o Computador (modelo, fabricante, fator de forma da carcaça, versão), informações sobre métricas de desempenho do Windows (avaliações WinSAT, índice de desempenho do Windows), nome de domínio, informações sobre processadores físicos e lógicos (número de processadores físicos e lógicos, fabricante, modelo, nível de revisão, número de cores, frequência de relógio, CPUID, características do cache, características do processador lógico, indicadores de modos suportados e instruções), informações sobre módulos RAM (tipo, fator de forma, fabricante, modelo, capacidade, granularidade de alocação da memória), informações sobre interfaces de rede (endereços IP e MAC, nome, descrição, configuração de interfaces de rede, discriminação de número e tamanho dos pacotes de rede por tipo, velocidade de troca da rede, discriminação do número de erros de rede por tipo), configuração do controlador IDE, endereços IP de servidores DNS, informações sobre a placa de vídeo (modelo, descrição, fabricante, compatibilidade, capacidade de memória de vídeo, permissão de tela, número de bits por pixel, versão BIOS), informações sobre dispositivos plug-and-play (nome, descrição, identificador de dispositivo [PnP, ACPI], informações sobre discos e dispositivos de armazenamento (número de discos ou flash drives, fabricante, modelo, capacidade de disco, número de cilindros, número de trilhas por cilindro, número de setores por trilha, capacidade dos setores, características do cache, número sequencial, número de partições, configuração do controlador SCSI), informações sobre discos lógicos (número sequencial, capacidade de partição, capacidade de volume, letra do volume, tipo de partição, tipo de sistema de arquivos, número de clusters, tamanho do cluster, número de setores por cluster, número de clusters vazios e ocupados, letra do volume inicializável, endereço de deslocamento da partição em relação ao início do disco), informações sobre a placa-mãe BIOS (fabricante, data de lançamento, versão), informações sobre a placa-mãe (fabricante, modelo, tipo), informações sobre memória física (capacidade compartilhada e livre), informações sobre serviços do sistema operacional (nome, descrição, status, marcação, informações sobre processos [nome e PID]), parâmetros de consumo de energia para o Computador, configuração do controlador de interrupções, caminho das pastas do sistema Windows (Windows e System32), informações sobre o SO (versão, compilação, data de lançamento, nome, tipo, data de instalação), tamanho do arquivo de páginas, informações sobre monitores (número, fabricante, permissão de tela, capacidade de resolução, tipo), informações sobre o driver da placa de vídeo (fabricante, data de lançamento, versão);

- informações do ETW, fornecedores de eventos EventTrace / EventMetadata da Microsoft: informações sobre a sequência de eventos do sistema (tipo, hora, data, fuso horário), metadados sobre o arquivo com os resultados do rastreamento (nome, estrutura, parâmetros de rastreamento, discriminação do número de operações de rastreamento por tipo), informações sobre o SO (nome, tipo, versão, compilação, data de lançamento, hora de início);

- informações do ETW, fornecedores de eventos de Process/Microsoft Windows Kernel Process/Microsoft Windows Kernel Processor Power da Microsoft: informações sobre processos iniciados e concluídos (nome, PID, parâmetros de início, linha de comando, código de retorno, parâmetros de gerenciamento de energia, hora de início e conclusão, tipo de token de acesso, SID, SessionID, número de descritores instalados), informações sobre alterações nas prioridades do thread (TID, prioridade, hora), informações sobre operações de disco do processo (tipo, hora, capacidade, número), histórico de alterações na estrutura e capacidade dos processos de memória utilizáveis;

- informações do ETW, fornecedores de eventos StackWalk/Perfinfo da Microsoft: informações sobre contadores de desempenho (desempenho de seções de código individuais, sequência de chamadas de função, PID, TID, endereços e atributos de ISRs e DPCs);

- informações do ETW, fornecedor de eventos KernelTraceControl-ImageID da Microsoft: informações sobre arquivos executáveise bibliotecas dinâmicas (nome, tamanho da imagem, caminho completo), informações sobre arquivos PDB (nome, identificador), dados de recursos VERSIONINFO para arquivos executáveis (nome, descrição, criador, localização, versão e identificador do aplicativo, versão do arquivo e identificador);

- informações do ETW, fornecedores de eventos FileIo/DiskIo/Image/Windows Kernel Disk da Microsoft: informações sobre operações de arquivo e disco (tipo, capacidade, hora de início, hora de conclusão, duração, status da conclusão, PID, TID, endereços de chamada de funções do driver, pacote de solicitações de E/S (IRP), atributos de objetos de arquivos do Windows), informações sobre arquivos envolvidos em operações de arquivo e disco (nome, versão, tamanho, caminho completo, atributos, deslocamento, checksum de imagem, opções de abertura e acesso);

- informações do ETW, fornecedor de eventos PageFault da Microsoft: informações sobre erros de acesso à página de memória (endereço, hora, capacidade, PID, TID, atributos do objeto de arquivos do Windows, parâmetros de alocação de memória);

- informações do ETW, fornecedor de eventos de Thread da Microsoft: informações sobre criação/conclusão de threads, informações sobre threads iniciados (PID, TID, tamanho da pilha, prioridades e alocação de recursos da CPU, recursos de E/S, páginas de memória entre threads, endereço da pilha, endereço da função init, endereço do Thread Environment Block (TEB), identificador de serviços do Windows);

- informações do ETW, fornecedor de eventos Microsoft Windows Kernel Memory da Microsoft: informações sobre operações de gerenciamento de memória (status de conclusão, hora, quantidade, PID), estrutura de alocação de memória (tipo, capacidade, SessionID, PID);

- informações sobre a operação do Software em caso de problemas de desempenho: identificador da instalação do Software, tipo e valor da queda de desempenho, informações sobre a sequência de eventos dentro do Software (hora, fuso horário, tipo, status de conclusão, identificador de componentes do Software, identificador de cenário operacional do Software, TID, PID, endereços de chamadas de funções), informações sobre conexões de rede a serem verificadas (URL, direção da conexão, tamanho do pacote de rede), informações sobre arquivos PDB (nome, identificador, tamanho da imagem do arquivo executável), informações sobre arquivos a serem verificados (nome, caminho completo, checksum), parâmetros de monitoramento de desempenho do Software;

- informações sobre a última reinicialização do SO: número de reinicializações malsucedidas desde a instalação do SO, dados no dump do sistema (código e parâmetros de um erro, nome, versão e soma de verificação (CRC32) do módulo que causou um erro na operação do SO, endereço do erro como desvio no módulo, somas de verificação (MD5, SHA1, SHA2-256) do dump do sistema);

- informações para verificar a autenticidade de certificados digitais que estão sendo utilizados para assinar arquivos: impressão digital do certificado, algoritmo da soma de verificação, chave pública e número de série do certificado, nome do emissor do certificado, resultado da validação do certificado e identificador do banco de dados do certificado;

- informações sobre o processo que executou o ataque na autodefesa do Software: nome e tamanho do arquivo, respectivas somas de verificação (MD5, SHA2-256, SHA1), caminho completo do arquivo de processo e código do modelo do caminho do arquivo, carimbos de data/hora de criação/compilação, sinalizador de arquivo executável, atributos do arquivo de processo, informações sobre o certificado utilizado para assinar o arquivo de processo, código da conta usada para iniciar o processo, ID das operações executadas para acessar o processo, tipo de recurso com o qual a operação é executada (processo, arquivo, objeto de registro, função de pesquisa FindWindow), nome do recurso com o qual a operação é executada, sinalizador indicando o êxito da operação, status do arquivo do processo e respectiva assinatura de acordo com a KSN;

- informações sobre o Software do Titular dos direitos: versão completa, tipo, localização e estado de operação do Software usado, versões dos componentes de Software instalados e seu estado de operação, informações sobre as atualizações de Software instaladas, o valor do filtro TARGET, a versão do protocolo usado para se conectar aos serviços do Titular dos direitos;

- informações sobre o hardware instalado no Computador: tipo, nome, nome do modelo, versão do firmware, parâmetros dos dispositivos embutidos e conectados, identificador exclusivo do Computador com o Software instalado;

- informações sobre as versões do sistema operacional e atualizações instaladas, tamanho das palavras, edição e parâmetros do modo de execução do SO, versão e somas de verificação (MD5, SHA1, SHA2-256) do arquivo do kernel do SO e data e hora iniciais do SO;
- arquivos executáveis e não executáveis, total ou parcialmente;
- porções da RAM do computador;
- setores envolvidos no processo de inicialização do sistema operacional;
- pacotes de dados de tráfego de rede;
- páginas da web e e-mails que contenham objetos suspeitos e maliciosos;
- descrição das classes e instâncias de classes do repositório do WMI;
- relatórios de atividades dos aplicativos:
  - o nome, tamanho e versão do arquivo que está sendo enviado, sua descrição e checksums (MD5, SHA2-256, SHA1), identificador de formato de arquivo, o nome do fornecedor do arquivo, o nome do produto ao qual o arquivo pertence, caminho completo para o arquivo no computador, o código do modelo do caminho, os carimbos de data/hora de criação e modificação do arquivo;
  - data/hora de início e término do período de validade do certificado (se o arquivo tiver uma assinatura digital), a data e a hora da assinatura, o nome do emissor do certificado, informações sobre o titular do certificado, a impressão digital, a chave pública do certificado e algoritmos apropriados, e o número de série do certificado;
  - o nome da conta na qual o processo está sendo executado;
  - checksums (MD5, SHA2-256, SHA1) do nome do Computador no qual o processo está sendo executado;
  - títulos das janelas de processo;
  - identificador para os bancos de dados do antivírus, nome da ameaça detectada de acordo com a classificação do Titular dos direitos;
  - dados sobre a licença instalada, seu identificador, tipo e data de expiração;
  - hora local do Computador no momento da prestação da informação;
  - nomes e caminhos dos arquivos que foram acessados pelo processo;
  - nomes de chaves de registro e seus valores que foram acessados pelo processo;
  - URL e endereços IP que foram acessados pelo processo;
  - URL e endereços IP dos quais o arquivo em execução foi baixado.

Provisão de dados ao usar as soluções de Detection and Response

Em computadores com o Kaspersky Endpoint Security instalado, os dados preparados para envio automático para servidores do Kaspersky Endpoint Detection and Response, Kaspersky Sandbox e Kaspersky Anti Targeted Attack Platform são armazenados. Os arquivos são armazenados nos computadores de forma simples e não criptografada.

O conjunto específico de dados depende da solução na qual o Kaspersky Endpoint Security é usado.

Kaspersky Endpoint Detection and Response

Todos os dados que o aplicativo armazena localmente são excluídos do computador quando o Kaspersky Endpoint Security é desinstalado.

Dados recebidos como resultado da execução da tarefa Verificação de IOC (tarefa padrão)

O Kaspersky Endpoint Security envia automaticamente dados sobre os resultados da execução da tarefa *Verificação de IOC* para o Kaspersky Security Center.

Os dados nos resultados da execução da tarefa *Verificação de IOC* podem conter as seguintes informações:

- Endereço IP da tabela ARP
- Endereço físico da tabela ARP
- Tipo e nome do registro DNS
- Endereço IP do computador protegido
- Endereço físico (endereço MAC) do computador protegido
- Identificador na entrada do log de eventos
- Nome da fonte de dados no log
- Nome do log
- Hora do evento
- Hashes MD5 e SHA256 do arquivo
- Nome completo do arquivo (inclusive o caminho)
- Tamanho do arquivo

- Porta e endereço IP remotos com os quais a conexão foi estabelecida durante a verificação
- Endereço IP do adaptador local
- Porta aberta no adaptador local
- Protocolo como um número (de acordo com o padrão da IANA)
- Nome do processo
- Argumentos do processo
- Caminho para o arquivo do processo
- Identificador do Windows (PID) do processo
- Identificador do Windows (PID) do processo principal
- Conta de usuário que iniciou o processo
- Data e hora de início do processo
- Nome do serviço
- Descrição do serviço
- Caminho e nome do serviço DLL (para svchost)
- Caminho e nome do arquivo executável do serviço
- Identificador do Windows (PID) do serviço
- Tipo de serviço (por exemplo, um driver ou adaptador de kernel)
- Status do serviço
- Modo de inicialização do serviço
- Nome da conta do usuário.
- Nome do volume
- Letra de volume
- Tipo de volume
- Valores de registro do Windows
- Valor hive do registro
- Caminho da chave do registro (sem hive e nome do valor)
- Configuração do registro
- Sistema (ambiente)

- Nome e versão do sistema operacional instalado no computador
- Nome da rede do computador protegido
- Domínio ou grupo ao qual o computador protegido pertence
- Nome do navegador
- Versão do navegador
- Hora em que o recurso da Web foi acessado pela última vez
- URL a partir da solicitação HTTP
- Nome da conta usada para a solicitação HTTP
- Nome do arquivo do processo que fez a solicitação HTTP
- Caminho completo para o arquivo do processo que fez a solicitação HTTP
- Identificador do Windows (PID) do processo que fez a solicitação HTTP
- Referencial HTTP (URL de origem da solicitação HTTP)
- URI do recurso solicitado por HTTP
- Informações sobre o agente do usuário HTTP (o aplicativo que fez a solicitação HTTP)
- Tempo de execução da solicitação HTTP
- Identificador exclusivo do processo que fez a solicitação HTTP

Dados para criar uma cadeia de evolução de ameaças

Os dados para criar uma cadeia de evolução de ameaças são armazenados por sete dias por padrão. Os dados são enviados automaticamente para o Kaspersky Security Center.

Os dados para criar uma cadeia de evolução de ameaças podem conter as seguintes informações:

- Data e hora do incidente
- Nome da detecção
- Modo de verificação
- Status da última ação relacionada à detecção
- Razão pela qual o processamento de detecção falhou
- Tipo de objeto detectado
- Nome do objeto detectado

- Status da ameaça após o processamento do objeto
- Razão pela qual a execução de ações no objeto falhou
- Ações executadas para reverter ações maliciosas
- Informações sobre o objeto processado:
  - Identificador exclusivo do processo
  - Identificador exclusivo do processo principal
  - Identificador exclusivo do arquivo de processo
  - Identificador do processo do Windows (PID)
  - Linha de comando do processo
  - Conta de usuário que iniciou o processo
  - Código da sessão de logon na qual o processo está sendo executado
  - Tipo da sessão em que o processo está sendo executado
  - Nível de integridade do processo que está sendo processado
  - Associação da conta de usuário que iniciou o processo nos grupos locais e de domínio privilegiados
  - Identificador do objeto processado
  - Nome completo do objeto processado
  - Identificador do dispositivo protegido
  - Nome completo do objeto (nome do arquivo local ou endereço da Web do arquivo baixado)
  - Hash MD5 ou SHA256 do objeto processado
  - Tipo do objeto processado
  - Data de criação do objeto processado
  - Data em que o objeto processado foi modificado pela última vez
  - Tamanho do objeto processado
  - Atributos do objeto processado
  - Organização que assinou o objeto processado
  - Resultado da verificação do certificado digital do objeto processado
  - Identificador de segurança (SID) do objeto processado
  - Identificador de fuso horário do objeto processado

- Endereço da Web do download do objeto processado (somente para arquivos em disco)
- Nome do aplicativo que baixou o arquivo
- Hashes MD5 e SHA256 do aplicativo que baixou o arquivo
- Nome do aplicativo que modificou o arquivo pela última vez
- Hashes MD5 e SHA256 do aplicativo que modificou o arquivo pela última vez
- Número de iniciações de objetos processados
- Data e hora em que o objeto processado foi iniciado pela primeira vez
- Identificadores exclusivos do arquivo
- Nome completo do arquivo (nome do arquivo local ou endereço da Web do arquivo baixado)
- Caminho para a variável processada de registro do Windows
- Nome da variável processada de registro do Windows
- Valor da variável processada de registro do Windows
- Tipo da variável processada de registro do Windows
- Indicador da associação da chave de registro processada no ponto de execução automática
- Endereço da Web da solicitação Web processada
- Origem do link da solicitação Web processada
- Agente do usuário da solicitação Web processada
- Tipo de solicitação Web processada (`GET` ou `POST`)
- Porta IP local da solicitação Web processada
- Porta IP remota da solicitação Web processada
- Direção da conexão (entrada ou saída) da solicitação Web processada
- Identificador do processo no qual o código malicioso foi incorporado

Kaspersky Sandbox

Todos os dados que o aplicativo armazena localmente são excluídos do computador quando o Kaspersky Endpoint Security é desinstalado.

Dados de serviço

O Kaspersky Endpoint Security armazena os seguintes dados processados durante a resposta automática:

- Arquivos processados e dados inseridos pelo usuário durante a configuração do agente integrado do Kaspersky Endpoint Security:
  - Arquivos na Quarentena
  - Chave pública do certificado usado para integração com o Kaspersky Sandbox
- Cache do agente integrado do Kaspersky Endpoint Security:
  - Hora em que os resultados da verificação foram gravados no cache
  - Hash MD5 da tarefa de verificação
  - Identificador da tarefa de verificação
  - Resultado da verificação para o objeto
- Fila de solicitações de objetos verificados:
  - ID do objeto na fila
  - Hora em que o objeto foi colocado na fila
  - Status de processamento do objeto na fila
  - ID da sessão de usuário no sistema operacional onde a tarefa de verificação de objeto foi criada
  - Identificador do sistema (SID) do usuário do sistema operacional cuja conta foi usada para criar a tarefa
  - Hash MD5 da tarefa de verificação de objeto
- Informações sobre as tarefas para as quais o agente integrado do Kaspersky Endpoint Security está aguardando os resultados da verificação do Kaspersky Sandbox:
  - Hora em que a tarefa de verificação de objeto foi recebida
  - Status de processamento de objeto
  - ID da sessão de usuário no sistema operacional onde a tarefa de verificação de objeto foi criada
  - Identificador da tarefa de verificação de objeto
  - Hash MD5 da tarefa de verificação de objeto
  - Identificador do sistema (SID) do usuário do sistema operacional cuja conta foi usada para criar a tarefa
  - Esquema XML do IOC criado automaticamente
  - Hash MD5 ou SHA256 do objeto verificado

- Erros de processamento
- Nomes dos objetos para os quais a tarefa foi criada
- Resultado da verificação para o objeto

Dados em solicitações para o Kaspersky Sandbox

Os seguintes dados de solicitações do agente integrado do Kaspersky Endpoint Security para o Kaspersky Sandbox são armazenados localmente no computador:

- Hash MD5 da tarefa de verificação
- Identificador da tarefa de verificação
- Objeto verificado e todos os arquivos relacionados

Dados recebidos como resultado da execução da tarefa Verificação de IOC (tarefa autônoma)

O Kaspersky Endpoint Security envia automaticamente dados sobre os resultados da execução da tarefa *Verificação de IOC* para o Kaspersky Security Center.

Os dados nos resultados da execução da tarefa *Verificação de IOC* podem conter as seguintes informações:

- Endereço IP da tabela ARP
- Endereço físico da tabela ARP
- Tipo e nome do registro DNS
- Endereço IP do computador protegido
- Endereço físico (endereço MAC) do computador protegido
- Identificador na entrada do log de eventos
- Nome da fonte de dados no log
- Nome do log
- Hora do evento
- Hashes MD5 e SHA256 do arquivo
- Nome completo do arquivo (inclusive o caminho)
- Tamanho do arquivo
- Porta e endereço IP remotos com os quais a conexão foi estabelecida durante a verificação

- Endereço IP do adaptador local
- Porta aberta no adaptador local
- Protocolo como um número (de acordo com o padrão da IANA)
- Nome do processo
- Argumentos do processo
- Caminho para o arquivo do processo
- Identificador do Windows (PID) do processo
- Identificador do Windows (PID) do processo principal
- Conta de usuário que iniciou o processo
- Data e hora de início do processo
- Nome do serviço
- Descrição do serviço
- Caminho e nome do serviço DLL (para svchost)
- Caminho e nome do arquivo executável do serviço
- Identificador do Windows (PID) do serviço
- Tipo de serviço (por exemplo, um driver ou adaptador de kernel)
- Status do serviço
- Modo de inicialização do serviço
- Nome da conta do usuário.
- Nome do volume
- Letra de volume
- Tipo de volume
- Valores de registro do Windows
- Valor hive do registro
- Caminho da chave do registro (sem hive e nome do valor)
- Configuração do registro
- Sistema (ambiente)
- Nome e versão do sistema operacional instalado no computador

- Nome da rede do computador protegido
- Domínio ou grupo ao qual o computador protegido pertence
- Nome do navegador
- Versão do navegador
- Hora em que o recurso da Web foi acessado pela última vez
- URL a partir da solicitação HTTP
- Nome da conta usada para a solicitação HTTP
- Nome do arquivo do processo que fez a solicitação HTTP
- Caminho completo para o arquivo do processo que fez a solicitação HTTP
- Identificador do Windows (PID) do processo que fez a solicitação HTTP
- Referencial HTTP (URL de origem da solicitação HTTP)
- URI do recurso solicitado por HTTP
- Informações sobre o agente do usuário HTTP (o aplicativo que fez a solicitação HTTP)
- Tempo de execução da solicitação HTTP
- Identificador exclusivo do processo que fez a solicitação HTTP

Kaspersky Endpoint Detection and Response Expert (on-premises)

Todos os dados que o aplicativo armazena localmente são excluídos do computador quando o Kaspersky Endpoint Security é desinstalado.

Dados de serviço

O agente integrado do Kaspersky Endpoint Security armazena os seguintes dados localmente:

- Dados necessários para a integração com o componente EDR Expert (on-premises):
  - Endereço e porta para conexão com o servidor KATA Central Node
  - Endereço e porta para conexão com o servidor de transmissão de telemetria
  - Endereço e porta para conexão com o servidor de resposta
  - Informações sobre certificados usados para integração com o KATA Central Node

    - Informações sobre certificados usados para integração com o servidor de transmissão de telemetria
    - Informações sobre certificados usados para integração com o servidor de resposta
- Arquivos na Quarentena

Dados de eventos de telemetria transmitidos

- **Dados de telemetria**
    - Dados nos arquivos:
        - Identificadores exclusivos do arquivo
        - Tipo de arquivo
        - Caminho completo para o arquivo
        - Tamanho do arquivo
        - Atributos do arquivo
        - Identificador de zona
        - Data e hora de criação do arquivo
        - Data e hora em que o arquivo foi modificado pela última vez
        - Nome do arquivo original
        - Nome do aplicativo
        - Versão do aplicativo.
        - Fornecedor do aplicativo
        - Descrição do arquivo
        - Versão do arquivo.
        - Hashes MD5 e SHA256 do objeto
        - Resultado da verificação da assinatura do arquivo
        - Nome do emissor de certificado
        - Nome do titular do certificado
        - Número de série do certificado

- Dados sobre a verificação AMSI:
  - Identificador exclusivo do processo que iniciou a atividade
  - Tipo de conteúdo do objeto enviado à AMSI
  - Conteúdo do objeto enviado à AMSI
  - Nome do objeto
  - Hashes MD5 e SHA256 do objeto
- Dados sobre o bloqueio de aplicativos:
  - Identificador exclusivo do processo que iniciou o bloqueio de aplicativos
  - Identificador exclusivo do processo principal
  - Identificador do sistema exclusivo do processo
  - Comando usado para iniciar um processo
  - ID da sessão de login
  - Nível de integridade do processo
  - Status do processo
  - Identificador exclusivo do arquivo de processo
  - Linha de comando do processo
  - Lista de identificadores exclusivos de arquivos interpretados
- Dados sobre aberturas de arquivos bloqueadas:
  - Identificador exclusivo do processo que iniciou a abertura do arquivo
  - Identificadores exclusivos do arquivo
- Dados sobre o carregamento do driver:
  - Identificador exclusivo do driver carregado
- Dados sobre eventos:
  - Identificador exclusivo do evento
  - Data e hora do evento
- Dados sobre a modificação:
  - Identificador exclusivo do processo que iniciou a modificação de arquivo
  - Identificadores exclusivos do arquivo

    - Tipo da operação de modificação
    - Sinalizador que indica que o arquivo será excluído após o computador ser reiniciado
    - Identificador exclusivo do arquivo modificado
    - Identificador exclusivo do arquivo antes da modificação
    - Conjunto de sinalizadores de bits que determinam como o arquivo foi aberto
    - Dados sobre operações na lista de controle de acesso
    - Dados sobre alterações na propriedade ou no grupo principal do arquivo
- Dados sobre a sessão de login:
    - ID da sessão de login
    - Nome do usuário que fez login
    - Tipo da conta do usuário
    - Tipo de sessão
- Dados sobre as conexões de rede:
    - Identificador exclusivo do processo que iniciou a conexão
    - Endereço IP local usado para iniciar a conexão
    - Endereço IP remoto do endpoint de conexão
    - Direção da conexão
    - Protocolo de transferência de dados
    - Método HTTP
    - Caminho sem o nome do host
    - Nome do host
    - Estado do processo dinâmico no momento da conexão
    - Sinalizador que indica que a conexão está aberta no nível do soquete bruto
    - Versão TLS usada na sessão de conexão
    - Nome do servidor TLS
    - Hashes MD5 e SHA1 do certificado do servidor TLS
    - Lista de Nomes alternativos da entidade (SAN) do certificado
    - Nome do emissor de certificado TSL

    - Número de série do certificado
    - Algoritmo de criptografia usado
    - Datas de início e término do certificado
    - Identificação digital JA3 do cliente TLS
    - Identificação digital JA3S do servidor
- Dados capturados durante a escuta em uma porta de rede:
    - Identificador exclusivo do processo que iniciou a conexão
- Dados de entrada da linha de comando:
    - Identificador exclusivo do processo que iniciou a entrada do console
    - Tipo de entrada do console
    - Texto inserido por um usuário ou um processo
- Dados sobre a criação de processo:
    - Identificador exclusivo do processo
    - Identificador exclusivo do processo principal
    - Identificador do sistema exclusivo do processo
    - Comando usado para iniciar um processo
    - ID da sessão de login
    - Nível de integridade do processo
    - Identificador exclusivo do arquivo de processo
    - Lista de identificadores exclusivos de arquivos interpretados
    - Tipo de processo
- Dados sobre o módulo carregado pelo processo:
    - Identificador exclusivo do processo que iniciou o download
    - Caminho completo para o arquivo que foi carregado no processo
    - Identificador exclusivo do arquivo do módulo
    - Nome qualificado completo do assembly .NET, se o arquivo carregado for um módulo .NET
    - Sinalizadores do assembly .NET definido no seu manifesto

- Dados sobre o encerramento de processo:
  - Identificador exclusivo do processo encerrado
- Dados sobre a modificação do registro:
  - Identificador exclusivo do processo que iniciou a modificação do registro
  - Tipo de operação do registro
  - Caminho completo para a chave do registro
  - Nome do valor dentro de uma chave do registro
  - Tipo de dados armazenados no valor da chave do registro
  - Dados especificados no valor da chave do registro
  - Nome da chave antes de renomear
  - Informações sobre uma alteração na propriedade da chave ou do grupo de chaves principais
  - Lista de alterações na lista de controle de acesso (ACL) da chave
- Dados sobre a ameaça detectada e seu processamento:
  - Sinalizador que indica que a detecção de ameaças foi executada em segundo plano
  - Veredito de ameaça
  - Nome do veredito
  - Identificador exclusivo do registro do banco de dados
  - Hora em que o registro da ameaça foi salvo no banco de dados
  - Modo do processamento de ameaças
  - Tipo de objeto infectado
  - Nome do objeto infectado
  - Hashes MD5 e SHA256 do objeto
  - Identificador exclusivo do objeto infectado
  - Identificador exclusivo do processo que baixou o objeto infectado da Internet
  - URL por meio da qual o objeto infectado foi baixado
  - Endereço de e-mail do remetente que enviou o objeto infectado
  - Protocolo de rede por meio do qual o objeto infectado foi recebido
  - Endereço local por meio do qual o objeto infectado foi recebido

    - Endereço externo por meio do qual o objeto infectado foi recebido
    - Tipo de conteúdo do objeto
    - Conteúdo do objeto
- Dados sobre o acesso aos processos:
    - Identificador exclusivo do processo que tentou fazer o acesso
    - Identificador exclusivo do processo de destino que foi acessado
    - Conjunto de direitos solicitados do processo de destino
    - Tipo de operação
    - Conjunto de chamadas no momento em que um processo foi acessado
    - Descritor do processo de origem
    - Descritor do processo de destino
- Dados sobre o DNS:
    - Identificador exclusivo do processo que iniciou a consulta DNS
    - Endereço IP do servidor DNS
    - Sinalizadores que gerenciam o comportamento de uma consulta DNS
    - Status de conclusão da solicitação
    - Nome de domínio totalmente qualificado especificado na consulta DNS
    - Tipo de dados na consulta DNS
    - Respostas do servidor DNS
- Dados sobre injeção de código:
    - Identificador exclusivo do processo que tentou injetar um código
    - Método de acesso usado
    - Conjunto de chamadas no momento em que o código injetado foi detectado
    - Identificador exclusivo do processo de destino no qual o código foi carregado
    - Dados sobre alterações na sequência de comandos do processo de destino
    - Endereço do processo de destino
    - Nome da biblioteca DLL que foi carregada no processo de destino
    - Caminho completo para o arquivo DDL

- Dados sobre operações com canais nomeados:
  - Identificador exclusivo do processo que criou ou se conectou ao canal
  - Nome completo do canal nomeado
  - Tipo de operação (criação ou conexão)
- Dados sobre consultas WMI:
  - Identificador exclusivo do processo que iniciou a operação WMI
  - Tipo de operação WMI
  - Nome do dispositivo de destino da consulta WMI
  - Conta de usuário que iniciou a consulta WMI
  - Texto da consulta WMI
  - Namespace no qual a consulta WMI é executada
  - Nome do filtro WMI
  - Nome do objeto consumidor
  - Texto que descreve a ação do objeto consumidor
- Dados sobre consultas LDAP:
  - Identificador exclusivo do processo que fez a solicitação LDAP
  - Escopo da pesquisa de consultas LDAP
  - Filtro LDAP
  - Parâmetro que especifica a partição do Active Directory para a qual a consulta foi direcionada
  - Atributos da pesquisa LDAP
- Dados sobre dispositivos USB conectados:
  - Tipo de operação do dispositivo USB
  - Tipo do dispositivo USB
  - Identificador do dispositivo USB
  - Nome do dispositivo USB
  - Caminho para o dispositivo USB
  - Sinalizador que indica que o dispositivo USB é uma unidade do sistema
- Dados sobre criação, exclusão e modificação de uma tarefa agendada

- Dados sobre criação, exclusão e modificação de serviços
- Dados sobre a montagem/desmontagem do sistema de arquivos
- Dados sobre a operação do componente EDR Expert (on-premise):
  - Informações sobre como iniciar/parar o agente
  - Informações sobre como instalar/desinstalar o agente
  - Identificador exclusivo para o início do agente
  - Identificador do sistema do processo do agente
  - Identificador exclusivo do processo do agente
  - Motivo do encerramento do agente
  - Código de encerramento do processo do agente
- Configurações de filtragem de eventos:
  - Nomes dos módulos
  - Caminhos completos para objetos
  - Hashes MD5 e SHA256 dos objetos
  - Identificadores das entradas no log de eventos do Windows
  - Configurações de certificado digital
  - Direção do tráfego, endereços IP, portas, protocolos, caminhos completos para arquivos executáveis
  - Nomes de usuário
  - Tipos de logon de usuário
  - Tipos de eventos de telemetria para os quais os filtros são aplicados

Dados das solicitações do componente do EDR Expert para o agente integrado do Kaspersky Endpoint Security

- Configurações gerais da tarefa:
  - Tipo de tarefa
  - Configurações do agendamento de tarefas
  - Nomes e senhas das contas nas quais as tarefas podem ser executadas
  - Versões de configurações

    - Identificadores de objetos em quarentena
    - Caminhos para o objetos
    - Hashes MD5 e SHA256 dos objetos
    - Linha de comando para iniciar o processo com os argumentos
    - Sinais das ações adicionais realizadas após a conclusão das tarefas
    - Identificadores de arquivo IOC a serem recuperados do servidor
    - Arquivos IOC
    - Nome do serviço
    - Tipo de inicialização do serviço
    - Pastas para as quais os resultados da tarefa *Obter perícia* devem ser recebidos
    - Máscaras dos nomes dos objetos e extensões para a tarefa *Obter perícia*
- Configurações de isolamento de rede:
    - Tipos de configurações
    - Versões de configurações
    - Listas de exclusões de isolamento de rede e configurações de exclusão: direção do tráfego, endereços IP, portas, protocolos e caminhos completos para arquivos executáveis
    - Sinais das ações adicionais
    - Tempo de desativação do isolamento automático
- Configurações de prevenção de execução:
    - Tipos de configurações
    - Versões de configurações
    - Listas de regras de prevenção de execução e configurações de regras: caminhos para objetos, tipos de objetos, hashes MD5 e SHA256 de objetos
    - Sinais das ações adicionais

Dados de solicitações enviadas pelo Kaspersky Endpoint Security ao componente EDR Expert

Ao fazer a integração com a solução EDR Expert (on-premises), os seguintes dados são armazenados localmente nos computadores.

- Em solicitações de sincronização:
  - ID único
  - Parte básica do endereço da Web do servidor
  - Nome do computador
  - Endereço IP do computador
  - Endereço MAC do computador
  - Hora local no computador
  - Status de autodefesa do Kaspersky Endpoint Security
  - Nome e versão do sistema operacional instalado no computador
  - Versão do Kaspersky Endpoint Security
  - Versões das configurações do aplicativo e configurações de tarefas
  - Status de tarefas: identificadores de tarefas, status de execução, códigos de erro
- Nas solicitações de obtenção de arquivos do servidor:
  - Identificadores exclusivos de arquivos
  - Identificador exclusivo do Kaspersky Endpoint Security
  - Identificadores exclusivos de certificados
  - Parte básica do endereço da Web do servidor com o componente Central Node instalado
  - Endereço IP do host
- Nos relatórios sobre os resultados da execução da tarefa:
  - Endereço IP do host
  - Informações sobre os objetos detectados durante uma verificação de IOC ou verificação YARA
  - Sinais das ações adicionais realizadas após a conclusão das tarefas
  - Erros de execução de tarefas e códigos de retorno
  - Status de conclusão da tarefa

    - Tempo de conclusão da tarefa
    - Versões das configurações usadas para a execução de tarefas
    - Informações sobre os objetos enviados ao servidor, objetos em quarentena e objetos restaurados da quarentena: caminhos para objetos, hashes MD5 e SHA256, identificadores de objetos em quarentena
    - Informações sobre os processos iniciados ou interrompidos em um computador na solicitação do servidor: PID e UniquePID, código de erro, hashes MD5 e SHA256 dos objetos
    - Informações sobre os serviços iniciados ou interrompidos em um computador na solicitação do servidor: nome do serviço, tipo de inicialização, código de erro, hashes MD5 e SHA256 de imagens de arquivo dos serviços
    - Informações sobre os objetos para os quais um despejo de memória foi feito por uma verificação YARA (caminhos, identificador de arquivo de despejo)
    - Arquivos solicitados pelo servidor
- Dados sobre processos em execução:
    - Nome do arquivo executável, inclusive caminho completo e extensão
    - Parâmetros de execução automática do processo
    - ID do processo
    - ID da sessão de login
    - Nome da sessão de login
    - Data e hora de início do processo
    - Hashes MD5 e SHA256 do objeto
- Dados nos arquivos:
    - Caminho do arquivo
    - Nome do arquivo.
    - Tamanho do arquivo
    - Atributos do arquivo
    - Data e hora de criação do arquivo
    - Data e hora em que o arquivo foi modificado pela última vez
    - Descrição do arquivo
    - Nome da empresa

    - Hashes MD5 e SHA256 do objeto
    - Chave do registro (para pontos de execução automática)
- Dados de erros que ocorrem quando as informações sobre os objetos foram recuperadas:
    - Nome completo do objeto que foi processado quando ocorreu um erro
    - Código do erro
- Dados nos resultados da verificação YARA:

  O agente integrado do Kaspersky Endpoint Security transfere automaticamente os resultados da verificação YARA para o Kaspersky Anti Targeted Attack Platform para criar uma cadeia de evolução de ameaças.

  Os dados são temporariamente armazenados em fila local para enviar os resultados da execução da tarefa para o servidor da Kaspersky Anti Targeted Attack Platform. Os dados são excluídos do armazenamento temporário depois de enviados.

    - Hashes MD5 e SHA256 do arquivo
    - Nome completo do arquivo
    - Caminho do arquivo
    - Tamanho do arquivo
    - Nome do processo
    - Argumentos do processo
    - Caminho para o arquivo do processo
    - Identificador do Windows (PID) do processo
    - Identificador do Windows (PID) do processo principal
    - Conta de usuário que iniciou o processo
    - Data e hora de início do processo
- Dados nos resultados da verificação IOC:
    - Endereço IP da tabela ARP
    - Endereço físico da tabela ARP
    - Nome do registro DNS
    - Tipo de registro DNS
    - Nome do host
    - Endereço IP
    - ID do evento no registro

- Nome da fonte de dados no log
- Nome do log
- Nome de usuário
- Data e hora em que o evento foi gerado, no formato ISO
- Hashes MD5 e SHA256 do arquivo
- Nome completo do arquivo
- Tamanho do arquivo
- Porta e endereço IP remotos com os quais a conexão foi estabelecida durante a verificação
- Endereço IP e porta do adaptador local
- Protocolo
- Nome do processo
- Argumentos do processo
- Caminho para o arquivo do processo
- Identificador do Windows (PID) do processo
- Identificador do Windows (PID) do processo principal
- Conta de usuário que iniciou o processo
- Data e hora de início do processo
- Caminho para a chave do registro
- Nome da chave de registro
- Valor de texto da chave do registro
- Nome do serviço
- Descrição do serviço
- Caminho e nome do serviço DLL
- Caminho e nome do arquivo executável do serviço
- Identificador do Windows (PID) do serviço
- Tipo de serviço
- Status do serviço
- Modo de inicialização do serviço

- Nome do sistema operacional
- Versão do sistema operacional
- Nome da rede do computador sem domínio
- Domínio ou grupo de trabalho
- Nome de usuário
- Nome do volume
- Letra de volume
- Tipo de volume

Kaspersky Network Detection and Response (KATA)

Todos os dados que o aplicativo armazena localmente são excluídos do computador quando o Kaspersky Endpoint Security é desinstalado.

Dados de telemetria

- **Dados sobre os arquivos**
  - Identificadores exclusivos do arquivo
  - Tipo de arquivo
  - Caminho completo para o arquivo
  - Tamanho do arquivo
  - Atributos do arquivo
  - Identificador de zona
  - Data e hora de criação do arquivo
  - Data e hora em que o arquivo foi modificado pela última vez
  - Nome do arquivo original
  - Nome do aplicativo
  - Versão do aplicativo.
  - Fornecedor do aplicativo

- Descrição do arquivo
- Versão do arquivo.
- Hashes MD5 e SHA256 do objeto
- Resultado da verificação da assinatura do arquivo
- Data e hora em que a assinatura do arquivo foi criada
- Cadeias do certificado usadas no arquivo de assinatura
- Tipo de cadeia do certificado
- Certificados na cadeia
- Nome do emissor de certificado
- Nome do titular do certificado
- Número de série do certificado
- Algoritmo de impressão digital do certificado
- Impressão digital do certificado
- Período de validade do certificado

- **Dados sobre a sessão de login**
  - ID da sessão de login
  - Nome da conta do usuário que fez login
  - Tipo da conta do usuário
  - Tipo de sessão
  - Endereço IP da máquina por meio da qual a tentativa de login foi feita
  - Endereço IP da máquina local para a qual a tentativa de login foi feita
  - Sinalizador que indica que a sessão representada por este evento tem privilégios elevados e direitos administrativos
  - Parâmetro que indica se outras sessões estão vinculadas a esta sessão de login
  - Protocolo usado para a sessão do terminal
  - Protocolo IPv4 usado para a sessão do terminal

- **Dados sobre a comunicação de rede**
  - Início e fim do intervalo de tempo durante o qual os dados foram coletados
  - Lista de conexões
  - Endereço IP local do computador
  - Endereço MAC local do computador
  - Endereço IP remoto do computador
  - Endereço MAC remoto do computador
  - Endereço IP do gateway
  - Número de pacotes de dados transmitidos
  - Número de pacotes de dados recebidos
  - Número total de bytes transferidos
  - Protocolo de transferência de dados
  - Campo EtherType do quadro Ethernet
  - Prefixo da carga útil do primeiro pacote no intervalo
  - Endereço IPv4 da interface da rede por meio da qual a comunicação foi capturada
- **Dados sobre a conexão de rede**
  - Identificador exclusivo do processo que iniciou a conexão
  - Protocolo de transferência de dados
  - Endereço IP local usado para iniciar a conexão
  - Endereço IP remoto do endpoint de conexão
  - Método HTTP
  - Caminho sem o nome do host
  - Nome do host
  - Estado do processo dinâmico no momento da conexão
  - Direção da conexão
  - Estado do processo dinâmico
  - Campo EtherType do quadro Ethernet

- **Dados capturados durante a escuta em uma porta de rede**
  - Identificador exclusivo do processo que iniciou a conexão
  - Protocolo de transferência de dados
  - Endereço local
  - Estado do processo dinâmico no momento da conexão
- **Resultado da verificação da conexão**
  - Configurações de rede do host
  - Descrição da interface da rede
  - Nome de domínio DNS
  - Endereço MAC local do computador
  - Número da métrica da conexão IP
  - Lista de endereços IP
  - Endereço IP
  - Máscara de rede
  - Endereço IP do gateway
  - Endereço MAC do gateway
  - Lista de patches instalados
  - Número do patch
  - Data de instalação do patch
  - Modelo do dispositivo
  - Fornecedor do dispositivo
  - ID do host no Kaspersky Security Center
  - Descrição do antivírus da Kaspersky instalado
  - Nome do componente do antivírus da Kaspersky instalado
  - Versão do componente do antivírus da Kaspersky instalado
  - Versão do banco de dados do componente do antivírus da Kaspersky instalado
  - Data da última atualização do banco de dados do componente do antivírus da Kaspersky instalado
  - Status do componente do antivírus da Kaspersky instalado

    - Lista de chaves da licença
    - Número de série da chave
    - Tipo de chave
    - Data de expiração da chave
    - Status da chave
- **Dados sobre a criação de processo no host**
    - Identificador exclusivo do processo
    - Identificador exclusivo do processo principal
    - Identificador do sistema exclusivo do processo
    - Comando usado para iniciar um processo
    - ID da sessão de login
    - ID de sessão do terminal
    - Identificador exclusivo do arquivo de processo
    - Nível de integridade do processo
    - Lista de tokens de direitos de processo
    - Atribuir direitos
    - Lista de identificadores exclusivos de arquivos interpretados
    - Status do processo
    - Comando usado para iniciar um processo
- **Dados sobre o encerramento de processo**
    - Identificador exclusivo do processo
- **Dados sobre a ameaça detectada**
    - Informações sobre ameaças
    - Veredito de ameaça
    - Número do registro AMR
    - Versão do banco de dados do antivírus
    - Modo de detecção de ameaças
    - Identificador exclusivo da ameaça

    - Tecnologia de proteção
    - Informações sobre o objeto infectado
    - Tipo de objeto infectado
    - Nome do objeto infectado
    - Hashes MD5 e SHA256 do objeto
    - Identificador exclusivo do processo infectado
    - Identificador exclusivo do objeto infectado
    - Identificador exclusivo do processo que baixou o objeto infectado da Internet
    - URL por meio da qual o objeto infectado foi baixado
    - Endereço de e-mail do remetente que enviou o objeto infectado
    - Protocolo de rede por meio do qual o objeto infectado foi recebido
    - Endereço local por meio do qual o objeto infectado foi recebido
    - Endereço externo por meio do qual o objeto infectado foi recebido
    - Tipo de conteúdo do objeto
    - Contexto da ameaça detectada
    - Conteúdo do objeto
    - Sinalizador que indica que a detecção de ameaças foi executada em segundo plano
- **Dados sobre o processamento de ameaças**
    - Informações sobre ameaças
    - Veredito de ameaça
    - Número do registro AMR
    - Versão do banco de dados do antivírus
    - Modo de detecção de ameaças
    - Nome do objeto infectado
    - Hashes MD5 e SHA256 do objeto
    - Identificador exclusivo do processo infectado
    - Identificador exclusivo do objeto infectado
    - Protocolo de rede por meio do qual o objeto infectado foi recebido

- Endereço local por meio do qual o objeto infectado foi recebido
- Endereço externo por meio do qual o objeto infectado foi recebido
- Status do processamento de ameaças
- Motivo pelo qual a ameaça não pôde ser remediada
- Endereço físico local

- **Dados sobre usuários**
  - SID do usuário
  - ID do usuário
  - Nome de usuário
  - Nome completo do usuário
  - Descrição do usuário
  - Se a conta está ativa ou bloqueada
  - Se a senha expirou
  - Se uma alteração de senha é necessária
  - Se a alteração da senha é permitida
  - Tipo da conta do usuário
  - Se o login automático está ativado para esta conta
  - Lista de grupos aos quais o usuário pertence

Integração com Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Todos os dados que o aplicativo armazena localmente são excluídos do computador quando o Kaspersky Endpoint Security é desinstalado.

Ao integrar com o Kaspersky Unified Monitoring and Analysis Platform (KUMA), os dados das configurações de conexão são transferidos, assim como todos os eventos registrados nos Logs do Windows.

Os principais Logs de eventos do Windows são Sistema, Segurança, Aplicativo, ForwardedEvents e HardwareEvents. Os usuários também podem criar e trabalhar com logs personalizados para atender a seus requisitos específicos.

Conformidade com a legislação da União Europeia (GDPR)

O Kaspersky Endpoint 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.
- Seguir links na interface 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 Endpoint Security, leia com atenção a descrição dos dados transmitidos no Contrato de Licença do Usuário Final e na Declaração da Kaspersky Security Network. Se dados específicos transmitidos do Kaspersky Endpoint 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. Para mais detalhes sobre a KPSN, consulte a documentação do Kaspersky Private Security Network.

Ativar o aplicativo com um código de ativação

Ao usar um código de ativação, você concorda em fornecer automaticamente os dados listados 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 Endpoint Security.

Atualizar módulos de aplicativos e bancos de dados de antivírus

Ao usar os servidores da Kaspersky, você concorda em fornecer automaticamente os dados listados no Contrato de Licença do Usuário Final. A Kaspersky requer essas informações para verificar se o Kaspersky Endpoint Security está sendo usado de forma legítima. Se você não concordar em fornecer essas informações à Kaspersky, use o Kaspersky Security Center para atualizações do banco de dados ou o Utilitário de atualização da Kaspersky.

Seguir links na interface do aplicativo

Ao usar links na interface do aplicativo, você concorda em fornecer automaticamente os dados listados no Contrato de Licença do Usuário Final. A lista precisa de dados transmitidos em cada link específico depende de onde o link está localizado na interface do aplicativo e qual problema ele pretende resolver. Se você não concordar em fornecer esses dados à Kaspersky, use a interface de aplicativo simplificada ou oculte a interface do aplicativo.

Armazenar despejos

Se você ativou a gravação do dump, o Kaspersky Endpoint Security criará um arquivo de dump que conterá todos os dados da memória dos processos do aplicativo no momento em que esse arquivo de dump foi criado.

Avisos de marcas registradas

As marcas comerciais e as marcas de serviço registradas são de propriedade de seus respectivos proprietários.

Adobe, Acrobat, Flash, Reader e Shockwave são marcas registradas ou marcas comerciais da Adobe nos Estados Unidos e em outros países.

Amazon, Amazon Web Services e AWS são marcas comerciais da Amazon.com, Inc. ou de suas afiliadas.

Apple, FireWire, iTunes, Mac e Safari são marcas comerciais da Apple Inc.

Arm é uma marca registrada da Arm Limited (ou de subsidiárias) nos EUA e/ou em outros lugares.

AutoCAD é uma marca comercial ou a marca registrada da Autodesk, Inc. e/ou as suas subsidiárias e/ou afiliadas nos EUA e em outros países.

A palavra, marca e logotipos do Bluetooth são de propriedade da Bluetooth SIG, Inc.

Borland é marca comercial ou registrada da Borland Software Corporation.

Cisco e Cisco AnyConnect, IOS são marcas registradas ou marcas comerciais registradas da Cisco Systems, Inc. e/ou de suas afiliadas nos Estados Unidos e em alguns outros países.

Citrix, Citrix Provisioning, Citrix Provisioning Services, Citrix Virtual Apps and Desktop, XenDesktop, e XenServer são marcas registradas ou marcas comerciais do Cloud Software Group, Inc., e/ou de suas subsidiárias nos Estados Unidos e/ou em outros países.

Cloudflare, Cloudflare Workers e o logotipo da Cloudflare são marcas comerciais e/ou marcas registradas da Cloudflare, Inc. nos Estados Unidos e em outras jurisdições.

Core é a marca comercial da Intel Corporation ou de suas subsidiárias.

dBase é uma marca comercial da dataBased Intelligence, Inc.

Dell Technologies, Dell, EMC e outras marcas comerciais são marcas comerciais da Dell Inc. ou de suas subsidiárias.

Docker e o logotipo Docker são marcas comerciais ou marcas registradas de Docker, Inc. nos Estados Unidos e/ou em outros países. A Docker, Inc. e outras partes também podem ter direitos de marca registrada em outros termos aqui usados.

ESET é uma marca comercial ou marca registrada da ESET spol. s r.o. ou respectiva entidade ESET.

Foxit é uma marca registrada da Foxit Corporation.

Radmin é uma marca registrada da Famatech.

Google, Android, Google Public DNS, Google Chrome e Chrome são marcas comerciais da Google LLC.

HUAWEI, FusionCompute e FusionSphere são marcas comerciais da Huawei Technologies Co., Ltd.

ICQ é uma marca registrada e/ou marca de serviço da ICQ LLC.

Intel é a marca comercial da Intel Corporation ou de suas subsidiárias.

IBM é uma marca comercial da International Business Machines Corporation registrada em muitas jurisdições em todo o mundo.

Lenovo e Lenovo ThinkPad são marcas comerciais da Lenovo nos Estados Unidos e/ou em outros lugares.

Linux é uma marca registrada da Linus Torvalds nos EUA e em outros países.

Logitech é uma marca registrada ou comercial da Logitech nos Estados Unidos e/ou em outros países.

LogMeIn Pro e Remotely Anywhere são marcas registradas da LogMeIn, Inc.

Mail.ru é uma marca registrada da Mail.Ru, LLC.

McAfee é marca comercial ou marca registrada da McAfee LLC ou de suas subsidiárias nos Estados Unidos e/ou em outros países.

Microsoft, Access, Active Directory, ActiveSync, Bing, BitLocker, Excel, Hyper-V, Internet Explorer, JScript, LifeCam Cinema, Microsoft Edge, MSDN, MS-DOS, MultiPoint, Office 365, Outlook, PowerPoint, PowerShell, Skype, SQL Server, Surface, Visual Basic, Visual FoxPro, Windows, Windows Live, Windows PowerShell, Windows Server e Windows Store são marcas registradas do grupo de empresas Microsoft.

Mozilla, Firefox e Thunderbird são marcas comerciais da Mozilla Foundation nos Estados Unidos e em outros países.

NetApp é uma marca comercial ou registrada da NetApp, Inc. nos Estados Unidos e em outros países.

OpenSSL é uma marca registrada da OpenSSL Software Foundation.

OpenStack é uma marca registrada da OpenStack Foundation nos Estados Unidos e em outros países.

Oracle, Java e JavaScript são marcas registradas da Oracle Corporation e/ou suas afiliadas.

Python é uma marca comercial ou marca registrada da Python Software Foundation.

Realtek é uma marca comercial da Realtek Semiconductor Corporation.

SAMSUNG é uma marca comercial da SAMSUNG nos Estados Unidos ou em outros países.

Thawte é uma marca comercial ou registrada da Symantec Corporation ou de duas afiliadas nos EUA e em outros países.

Trend Micro é uma marca comercial ou marca registrada da Trend Micro Incorporated.

VERISIGN é uma marca comercial registrada nos Estados Unidos e em outros lugares ou uma marca comercial não registrada da VeriSign, Inc. e suas subsidiárias.

VMware, VMware ESXi, VMware Horizon, VMware Workstation, VMware Tools e VMware vSphere são marcas registradas ou comerciais da VMware, Inc. nos Estados Unidos e/ou em outros países.

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.