kaspersky

Kaspersky Endpoint Security 14.2 for Windows

© 2026 AO Kaspersky Lab

Conteúdos

Ajuda do Kaspersky Endpoint Security for Windows
- O que há de novo
- Problemas resolvidos
- Perguntas frequentes

Kaspersky Endpoint Security for Windows
- Modos da aplicação: Standard, EDR Agent, Light Agent
- Kit de distribuição
- Requisitos de hardware e de software
- Comparação das características de aplicação disponíveis dependendo do tipo de sistema operativo
- Comparação de funções da aplicação, dependendo das ferramentas de gestão
- Compatibilidade com outras aplicações

Instalar e remover a aplicação
- Implementação através do Kaspersky Security Center
  - Instalação padrão da aplicação
  - Criar um pacote de instalação
  - A atualizar bases de dados no pacote de instalação
  - Criar uma tarefa de instalação remota
- Instalar a aplicação localmente utilizando o Assistente
- Instalação remota da aplicação que utiliza o System Center Configuration Manager
- Descrição das configurações de instalação do ficheiro setup.ini
- Processos do Kaspersky Endpoint Security for Windows
- Change application components
- Atualização a partir de uma versão anterior da aplicação
  - Atualização da aplicação sem um reinício
  - Atualização SMU da aplicação
- Remover a aplicação

Licenciamento da aplicação
- Acerca do Contrato de Licença do Utilizador Final
- Sobre a licença
- Sobre o certificado de licença
- Sobre a subscrição
- Sobre a chave de licença
- Sobre o código de ativação
- Sobre o ficheiro-chave
- Comparação de funcionalidade da aplicação dependendo do tipo de licença para estações de trabalho
- Comparação da funcionalidade da aplicação dependendo do tipo de licença para servidores
- Ativar a aplicação
- Remover uma chave de licença
- Ver informação sobre a licença
- Comprar uma licença
- Renovar a subscrição

Como Começar
- Sobre o Management Plug-in do Kaspersky Endpoint Security for Windows
- Considerações especiais ao trabalhar com versões diferentes dos plug-ins de administração
- Considerandos especiais ao usar protocolos encriptados para interagir com serviços externos
- Interface da aplicação
  - Ícone da aplicação na área de notificação da barra de tarefas
  - Interface simplificada da aplicação
  - Configurar a apresentação da interface da aplicação
- Preparar a aplicação para utilização
- Gerir políticas
  - Criar uma política
  - Exportar e importar uma política
  - Indicador de nível de segurança
- Gestão de tarefas
- Configurar definições da aplicação locais
- Iniciar e parar o Kaspersky Endpoint Security
- Pausar e retomar a proteção e controlo do computador
- Criar e utilizar um ficheiro de configuração
- Restaurar as predefinições da aplicação
- Desempenho do Kaspersky Endpoint Security e compatibilidade com outras aplicações
  - Ativar ou desativar o modo de poupança de energia
  - Ativar ou desativar a concessão de recursos para outras aplicações
  - Melhores práticas para otimizar o desempenho do Kaspersky Endpoint Security

Verificação de software malicioso
- Verificar o computador
- Verificar unidades amovíveis quando forem ligadas ao computador
- Verificação de fundo
- Verificar a partir do menu de contexto
- Verificação de integridade das aplicações
- Editar o âmbito de verificação
- Execução de uma verificação agendada
- Executar uma verificação com outra conta de utilizador
- Optimização da verificação

Atualização de bases de dados e módulos de software de aplicação
- Cenários de atualização do módulo da aplicação e base de dados
  - Atualizar a partir do armazenamento de um servidor
  - Atualizar a partir de uma pasta partilhada
  - Atualizar utilizando o Utilitário Kaspersky Update
  - Atualizar no modo móvel
- Iniciar e parar uma tarefa de atualização
- Iniciar uma tarefa de atualização com os direitos de outra conta de utilizador
- Selecionar o modo de execução da tarefa de atualização
- Adicionar uma origem de atualização
- Atualizar módulos de aplicação
- Utilizar um servidor proxy para atualizações
- Reverter última atualização

Tecnologia de desinfeção avançada
Desinfeção de ameaças ativas em computadores
Desinfeção de ameaças ativas em servidores
Eliminar ameaças não processadas
Proteção do computador
Estado da Proteção em Tempo Real
Proteção contra ameaças de ficheiros
Ativar e desativar a Proteção contra ameaças de ficheiros
Pausa automática da Proteção contra ameaças de ficheiros
Alterar a ação a executar em ficheiros infetados pelo componente Proteção contra ameaças de ficheiros
Formar o âmbito de proteção do componente Proteção contra ameaças de ficheiros
Utilizar métodos de verificação
Utilizar tecnologias de verificação no funcionamento do componente Proteção contra ameaças de ficheiros
Otimizar a verificação de ficheiros
Verificação de ficheiros compostos
Alterar o modo de verificação
Verificação de Contentores
Prevenção contra invasões
Ativar e desativar a Prevenção contra invasões
Gerir grupos fiáveis da aplicação
Alterar o grupo fiável de uma aplicação
Configurar os direitos do grupo fiável
Selecionar um grupo fiável para aplicações iniciadas antes do Kaspersky Endpoint Security
Selecionar um grupo fiável de aplicações desconhecidas
Selecionar um grupo fiável para aplicações assinadas digitalmente
Gerir direitos da aplicação
Proteção dos recursos do sistema operativo e de dados pessoais
Eliminar informações acerca de aplicações não utilizadas
Monitorizar a Prevenção contra invasões
Proteger o acesso a áudio e vídeo
Prevenção de ataques BadUSB
Ativar e desativar Prevenção de ataques BadUSB
Utilizar o teclado no ecrã para autorização de dispositivos USB
Autorização do leitor de código de barras
Proteção AMSI
Ativar e desativar a Proteção AMSI
Otimizar a verificação de ficheiros pela Proteção AMSI
Proteção contra ameaças da Web
Ativar e desativar a Proteção contra ameaças da Web
Configurar métodos de deteção de endereços da Web maliciosos
Anti-Phishing
Criar a lista de URL fiáveis
Exportar e importar a lista de endereços Web fiáveis
Proteção contra ameaças de correio
Ativar e desativar a Proteção contra ameaças de correio
Alterar a ação a executar em mensagens de e-mail infetadas
Formar o âmbito de proteção do componente Proteção contra ameaças de correio

- Verificação de ficheiros compostos anexados a mensagens de e-mail
- Filtrar 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, R7-Office

Proteção contra ameaças de Rede
- Ativar e desativar a Proteção contra ameaças de Rede
- Bloquear um computador atacante
- Configurar moradas de exclusões de bloqueio
- Exportar e importar a lista de exclusões a partir do bloqueio
- Configurar a Proteção contra ameaças de rede por tipo

Firewall
- Ativar ou desativar a Firewall
- Alterar o tipo da ligação de rede
- Gerir regras de pacotes de rede
  - Criar uma regra de pacotes de rede
  - Ativar ou desativar uma regra de pacotes de rede
  - Alterar a ação da 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 de regras de pacotes de rede em XML
- Gerir regras de rede de aplicações
  - Criar uma regra de rede de aplicações
  - Ativar e desativar uma regra de rede de aplicações
  - Alterar a ação da Firewall para uma regra de rede de aplicações
  - Alterar a prioridade de uma regra de rede de aplicações
- Monitor de Rede

Prevenção de explorações
- Ativar e desativar a prevenção de explorações
- Proteção da memória de processos do sistema

Deteção de comportamento

Anti-Cryptor
- Ativar ou desativar a proteção de pastas partilhadas contra encriptação externa
- Configurar o período de bloqueio de um computador não fiável
- Editar o âmbito da proteção
- Adicionar computadores fiáveis para encriptação de dados externos
- Exportar e importar uma lista de exclusões da proteção de pastas partilhadas contra encriptação externa

Motor de remediação

Kaspersky Security Network
- Ativar e desativar a utilização da Kaspersky Security Network
- Limitações do Kaspersky Private Security Network
- Ativar e desativar o modo de nuvem para componentes de proteção
- Definições do KSN Proxy
- Verificar a reputação de um ficheiro na Kaspersky Security Network

Verificação de ligações encriptadas
- Ativar a verificação de ligações encriptadas
- Instalar certificados de raiz fiáveis

Verificar ligações encriptadas com um certificado não fiável
Adicionar um certificado Kaspersky ao próprio armazenamento de certificados
Excluir ligações encriptadas da verificação
Bloquear o acesso a domínios com certificados não fidedignos
Eliminar dados
Controlo de computador
Controlo de Internet
Adicionar uma regra de acesso a recursos da Internet
Filtro por endereços de recursos da Internet
Filtro por conteúdo de recursos da Internet
Testar regras de acesso a recursos da Internet
Exportar e importar regras de Controlo de Internet
Exportar e importar endereços de recursos da Internet da regra de Controlo de Internet
Monitorizar atividade da Internet do utilizador
Editar modelos de mensagens de Controlo de Internet
Editar máscaras para endereços de recursos da Internet
Controlo de Internet para máquinas virtuais
Configure os modelos de mensagens do Controlo de Internet:
Controlo de Dispositivos
Sobre as regras de acesso
Obter informações sobre os dispositivos instalados
Gerir o acesso aos dispositivos por tipo
Gerir o acesso aos dispositivos pelo barramento de ligação
Diferenciação de direitos de acesso do utilizador aos dispositivos
Gerir o acesso a dispositivos móveis
Gerir o acesso a dispositivos Bluetooth
Controlo de impressão
Controlo de ligações Wi-Fi
Monitorizar o uso de unidades amovíveis
Alterar a duração da cache
Ações com dispositivos fiáveis
Adicionar um dispositivo à lista fiável
Exportar e importar a lista de dispositivos fiáveis
Obter acesso a um dispositivo bloqueado
Modo online para conceder acesso
Modo offline para conceder acesso
Editar modelos de mensagens de Controlo de Dispositivos
Anti-Bridging
Ativar Anti-Bridging
Alterar o estado de uma regra de ligação
Alterar a prioridade de uma regra de ligação
Controlo de Anomalias Adaptativo
Formação do Controlo de Anomalias Adaptativo
Ativar e desativar uma regra de Controlo de Anomalias Adaptativo
Modificar a ação efetuada quando uma regra de Controlo de Anomalias Adaptativo é acionada
Criar uma exclusão para uma regra do Controlo de Anomalias Adaptativo
Exportar e importar exclusões para regras do Controlo de Anomalias Adaptativo

- Aplicar atualizações para regras de Controlo de Anomalias Adaptativo
- Editar modelos de mensagem do Controlo de Anomalias Adaptativo
- Monitorização de operações de Controlo de Anomalias Adaptativo

Controlo das Aplicações

- Limitações da funcionalidade de Controlo das Aplicações
- Obter informações sobre as aplicações instaladas
- Como ativar o modo de Aplicações bloqueadas
- Controlo das Aplicações com base num computador de linha de base
- Gerir as regras de Controlo das aplicações
  - Adicionar uma condição de ativação para a Regra de Controlo das aplicações
  - Adicionar ficheiros executáveis da pasta de Ficheiros executáveis à categoria de aplicações
  - Adicionar ficheiros executáveis relacionados a eventos à categoria de aplicações
  - Adicionar uma Regra de Controlo das Aplicações
  - Alterar o estado de uma Regra de Controlo das aplicações utilizando o Kaspersky Security Center
  - Exportar e importar Regras de Controlo das Aplicações
  - Ver eventos que resultam da operação do componente de Controlo das Aplicações
  - Ver um relatório sobre aplicações bloqueadas
- Testar Regras de Controlo das Aplicações
  - Ativar e desativar teste de regras do Controlo das Aplicações
  - Ver um relatório sobre as aplicações bloqueadas no modo de teste
  - Ver eventos que resultam de operação de teste do componente de Controlo das Aplicações
- Monitor de atividade das aplicações
- Regras para criar máscaras de nome para ficheiros ou pastas
- Editar modelos de mensagens do Controlo das Aplicações
- Variáveis em modelos de mensagens do Controlo das aplicações
- Melhores práticas para efetuar um inventário de ficheiros executáveis
- Melhores práticas para implementar uma lista de aplicações permitidas
  - Configurar o modo de lista de permissão para aplicações
  - Testar o modo de lista de permissão
  - Suporte para o modo de lista de permissão

Monitorização de portas de rede

- Ativar a monitorização de todas as portas de rede
- Criar uma lista de portas de rede monitorizadas
- Criar uma lista das aplicações para as quais todas as portas de rede são monitorizadas
- Exportar e importar listas de portas monitorizadas

Inspeção do Registo

- Configurar regras predefinidas
- Adicionar regras personalizadas

Monitorização da integridade do sistema

- Sobre as regras da Monitorização da integridade do sistema
- Monitorização da integridade do sistema em tempo real
- Verificação de integridade do sistema mediante pedido
- Exportar e importar as regras da Monitorização da integridade do sistema
- Visualizar os relatórios da Monitorização da integridade do sistema
- Redefinição do estado de integridade do sistema

Cloud Discovery

Zona fiável
Criar uma exclusão de verificação
Criar uma exclusão por tipo de objetos detetados
Editar a lista de aplicações fiáveis
Criar uma zona local fiável
Exportar e importar a zona fiável
Tratamento de aplicações com uma assinatura digital fiável
Anexo. Exclusões de verificação predefinidas e aplicações fiáveis
Microsoft SQL Server
Microsoft Exchange Server
Microsoft System Center Configuration Manager
Citrix
VMware
Desduplicação de dados no Microsoft Windows Server
Gerir Cópias de segurança
Configurar o período de armazenamento máximo dos ficheiros na Cópia de segurança
Configure o tamanho máximo da Cópia de segurança
Restaurar ficheiros a partir da Cópia de segurança
Apagar cópias de segurança de ficheiros da Cópia de segurança
Serviço de notificação
Configurar as definições do registo de eventos
Configurar a apresentação e o envio de notificações
Configurar a apresentação de avisos sobre o estado da aplicação na área de notificação
Mensagens entre utilizadores e o administrador
Gerir relatórios
Visualizar relatórios
Configurar o prazo máximo de armazenamento de relatórios
Configurar o tamanho máximo do ficheiro de relatório
Guardar um relatório em ficheiro
Limpar relatórios
Autodefesa do Kaspersky Endpoint Security
Ativar e desativar a Autodefesa
Ativar e desativar o Suporte AM-PPL
Proteção dos serviços da aplicação contra gestão externa
Disponibilizar apoio para aplicações de administração remota
Proteção por password
Ativar proteção por password
Conceder permissões a utilizadores ou grupos individuais
Usar uma password temporária para conceder permissões
Revogar password temporária
Aspetos especiais de permissões de proteção por password
Redefinir a password do KLAdmin
Proteção da ligação do Servidor de Administração
Encriptação de dados
Limitações da funcionalidade de encriptação
Alterar o comprimento da chave de encriptação (AES56 / AES256)

Encriptação de disco Kaspersky
- Funcionalidades especiais de encriptação de unidade SSD
- A iniciar a encriptação de disco Kaspersky
- Criar uma lista de unidades de disco rígido excluídas da encriptação
- Exportar e importar uma lista de discos rígidos excluídos da encriptação
- Ativação da tecnologia de autenticação única (SSO)
- Gestão de contas do agente de autenticação
- Utilizar um token e um smart-card com o Agente de Autenticação
- Desencriptação de unidade de disco rígido
- Restaurar acesso a uma unidade protegida pela tecnologia Encriptação de disco Kaspersky
- Iniciar sessão com a conta de serviço do Agente de Autenticação
- Atualizar o sistema operativo
- A eliminar erros da atualização da funcionalidade de encriptação
- Rastrear o Agente de Autenticação
- Editar as mensagens de ajuda do Agente de Autenticação
- Remover objetos e dados restantes após testar o funcionamento do Agente de Autenticação

Gestão de BitLocker
- Iniciar a Encriptação de Unidade BitLocker
- Desencriptar um disco rígido protegido por BitLocker
- Restaurar acesso a uma unidade protegida por BitLocker
- Pausar a proteção por BitLocker para atualizar o software

Encriptação ao nível dos ficheiros em unidades locais do computador
- Encriptar ficheiros nas unidades locais do computador
- Formar regras de acesso a ficheiros encriptados para aplicações
- Encriptar ficheiros criados ou alterados por aplicações específicas
- Criar uma regra de desencriptação
- Desencriptar ficheiros nas unidades locais do computador
- Criar pacotes encriptados
- Restaurar o acesso aos ficheiros encriptados
- Restaurar o acesso a dados encriptados após uma falha do sistema operativo
- Editar modelos de mensagens de acesso a ficheiros encriptados

Encriptação de unidades amovíveis
- Iniciar a encriptação de unidades amovíveis
- Adicionar uma regra de encriptação para unidades amovíveis
- Exportar e importar uma lista de regras de encriptação para unidades amovíveis
- Modo portátil para aceder a ficheiros encriptados em unidades amovíveis
- Desencriptação de unidades amovíveis

Ver detalhes da encriptação de dados
- Visualizar o estado de encriptação
- Ver estatísticas de encriptação nos painéis do Kaspersky Security Center
- Visualizar os erros de encriptação de ficheiros em unidades do computador locais
- Ver o relatório de encriptação de dados

Trabalhar com dispositivos encriptados quando não existe acesso aos mesmos
- Recuperar dados utilizando Utilitário de Restauro FDERT
- Criar um disco de recuperação do sistema operativo

- Soluções Detection and Response
  - Licenciamento MDR e EDR Optimum
  - Compatibilidade com soluções da EDR de terceiros
  - Kaspersky Endpoint Agent
    - Migrar a configuração [KES+KEA] para a configuração [KES+agente incorporado]
    - Migração de Política e Tarefa para o Kaspersky Endpoint Agent
  - Endpoint Detection and Response Agent (EDR Agent)
    - Instalar o EDR Agent
    - Integrar o EDR Agent com MDR
    - Integrar o EDR Agent com EDR (KATA)
    - Integrar o EDR Agent com NDR (KATA)
    - Integrar o EDR Agent com EDR Expert (on-premises)
    - Compatibilidade com aplicações da EPP de terceiros
  - Managed Detection and Response
    - Integração do agente integrado com MDR
    - Guia de migração de KEA para o KES para MDR
  - Endpoint Detection and Response
    - Integração do agente integrado com EDR Optimum / EDR Expert
    - Verificar os indicadores de compromisso (tarefa padrão)
    - Telemetria estendida para Verificação IOC
    - Mover ficheiro para Quarentena
    - Obter ficheiro
    - Delete file
    - Início do Processo
    - Terminação de Processo
    - Prevenção da execução
    - Isolamento da rede do computador
    - Cloud Sandbox
    - Guia de migração de KEA para o KES para EDR Optimum
  - Kaspersky Sandbox
    - Integração do agente integrado com o Kaspersky Sandbox
    - Verifique se há indicadores de compromisso (tarefa autónoma)
    - Guia de migração de KEA para o KES para Kaspersky Sandbox
  - Kaspersky Anti Targeted Attack Platform
    - Integração do agente integrado com EDR/NDR (KATA)
    - Configurar a telemetria EDR (KATA)
    - Exclusões de telemetria EDR (KATA)
      - Exemplo 1. Processos excluídos
      - Exemplo 2. Comunicações de rede excluídas
      - Exemplo 3. Operações de ficheiro excluídas
      - Exemplo 4. Modificações de registo excluídas
    - KATA Sandbox
      - Integração do agente integrado com o KATA Sandbox
      - Configuração de ações de Resposta a ameaças
    - Guia de migração de KEA para o KES para EDR (KATA)

- Endpoint Detection and Response Expert (on-premises)
  - Integração do agente integrado com EDR Expert (on-premises)
  - Configurar as definições 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 de política para configurar a integração com o EDR Expert (on-premises) e o EDR (KATA)
- Endpoint Detection and Response Expert (cloud)
  - Integração do agente integrado com EDR Expert (cloud)
  - Configurar as definições de telemetria do EDR Expert (cloud)
  - Exclusões de telemetria do EDR Expert (cloud)
  - Como exportar ou importar filtros de eventos do EDR Expert (cloud)
- Gerir a Quarentena
  - Configurar o tamanho máximo da Quarentena
  - Enviar dados sobre ficheiros da Quarentena para o Kaspersky Security Center
  - Restaurar ficheiros a partir da Quarentena
- Monitorização de ações de EDR

Kaspersky Unified Monitoring and Analysis Platform (KUMA)
- Integração do Kaspersky Endpoint Security com o KUMA
  - Preparação para a integração do KES com o KUMA
  - Ligação do KES ao KUMA
- Filtrar eventos a serem enviados para o KUMA
- Exportar e importar filtros de eventos do KUMA

Guia de Migração do KSWS para o KES
- Correspondência dos componentes KSWS e KES
- Correspondência das definições KSWS e KES
- Migrar componentes do KSWS
- Migrar tarefas e políticas do KSWS
- Migrar a zona fiável do KSWS
- Migrar regras do Controlo de Execução de Aplicações do KSWS
- Instalar o KES em vez do KSWS
- Migrar a configuração [KSWS+KEA] para a configuração [KES+agente incorporado]
- Certificar-se de que o Kaspersky Security for Windows Server foi removido com sucesso
- Ativar o KES com uma chave KSWS
- Considerações especiais para migrar servidores de alta carga
- Gerir a aplicação num servidor no modo Server Core
- Migrar de [KSWS+KEA] para [KES+agente incorporado]

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
- A instalar o Light Agent
- A ligar o Light Agent à SVM
  - Descoberta de SVM
  - Configurar o algoritmo de seleção de SVM para Light Agent

Distribuir as ligações de Light Agents para SVM (etiquetas)
Proteger a ligação entre um Light Agent e a SVM
A ativar o Light Agent
Guia de migração do KSVLA Light Agent para o KES Light Agent
Instalar o KES Light Agent, em vez do KSVLA Light Agent
Correspondência dos componentes do KSVLA Light Agent e do KES Light Agent
Migrar tarefas e políticas do KSVLA Light Agent
Migrar a configuração [KSVLA Light Agent+KEA] para a configuração [KES Light Agent+agente incorporado]
Gerir a aplicação a partir da command line
Setup. Instalar a aplicação
Setup /x. Remover a aplicação
msiexec /i. Recuperar a aplicação
Comandos AVP
SCAN. Verificação de software malicioso
UPDATE. Atualização de bases de dados e módulos de software de aplicação
ROLLBACK. Reverter última atualização
TRACES. Rastreio
START. Iniciar um perfil
STOP. Interromper um perfil
STATUS. Estado do perfil
STATISTICS. Estatísticas da operação do perfil
RESTORE. Restaurar ficheiros a partir da Cópia de segurança
EXPORT. Exportar definições da aplicação
IMPORT. Importar definições da aplicação
ADDKEY. Aplicar um ficheiro de chave
LICENSE. Licenciamento
RENEW. Comprar uma licença
PBATESTRESET. Repor os resultados da verificação do disco antes de encriptar o disco
EXIT. Sair da aplicação
EXITPOLICY. Desativar política
STARTPOLICY. Ativar a política
DISABLE. Desativar a proteção
SPYWARE. Deteção de spyware
KSN. Alternar entre KSN/KPSN
SERVERBINDINGDISABLE. Desativar a proteção da ligação do servidor
Comandos KESCLI
Scan. Verificação de software malicioso
GetScanState. Estado de conclusão da verificação
GetLastScanTime. Determinar a hora de conclusão da verificação
GetThreats. Obter dados sobre ameaças detetadas
UpdateDefinitions. Atualização de bases de dados e módulos de software de aplicação
GetDefinitionState. Determinação da última data e hora de atualização das bases de dados
EnableRTP. Ativar proteção
GetRealTimeProtectionState. Estado da Proteção contra ameaças de ficheiros
GetEncryptionState. Estado da encriptação do disco
Version. Identificar a versão da aplicação

- Comandos Managed Detection and Response
  - SANDBOX. Gestão do Sandbox
  - PREVENTION. Gestão de prevenção de execução
  - ISOLATION. Gerir o isolamento da rede
  - RESTORE. Restaurar ficheiros a partir da Quarentena
  - IOCSCAN. Verificar indicadores de comprometimento (IOC)
  - MDRLICENSE. Ativação MDR
  - EDRKATA. Integração com o EDR (KATA)
  - EDRExpertOnPrem. Integração com o EDR Expert (on-premises)
  - KUMA. Integração do KUMA
  - YARA. Executar verificação YARA
  - TELEMETRYFILTERS. Filtrar eventos a serem enviados para o KUMA
- Comandos de gestão do Light Agent
  - KSVLAINFO. Determinar o modo Light Agent
  - VIISINFO. Estado da ligação do Light Agent ao Servidor de Integração
  - SVMINFO. Estado da ligação do Light Agent ao Servidor de Proteção
- Códigos de erro
- Anexo. Perfis da aplicação

Gerir a aplicação com API REST
- Instalar a aplicação com API REST
- Trabalhar com API

Fontes de informação sobre a aplicação

Contactar o Suporte Técnico
- Conteúdos e armazenamento de ficheiros de rastreio
- Rastreios da operação da aplicação
- Rastreios de desempenho da aplicação
- Gravação de descarga
- Proteger ficheiros de descarga e ficheiros de rastreio
- Obter dados do sistema operativo (Kaspersky Get System Info)

Limitações e avisos

Glossário
- Agente de Autenticação
- Agente de Rede
- Âmbito de Proteção
- Âmbito de verificação
- Arquivo
- Autenticação Kerberos
- Base de dados de endereços de phishing
- Base de dados de endereços web maliciosos
- Bases de dados de antivírus
- Certificado de licença
- Chave ativa
- Cloud Discovery
- Desinfeção
- Emissor do certificado
- Falso alarme
- Ficheiro infetado

- Ficheiro infetável
- Ficheiro IOC
- Forma normalizada do endereço de um recurso da Internet
- Gestor de ficheiros portátil
- Grupo de administração
- IOC
- Light Agent
- Máscara
- Objeto OLE
- OpenIOC
- Servidor de Integração
- SVM
- Tarefa
- Trusted Platform Module

Apêndices

- Anexo 1. Definições da aplicação
  - Proteção contra ameaças de ficheiros
  - Proteção contra ameaças da Web
  - Proteção contra ameaças de correio
  - Proteção contra ameaças de Rede
  - Firewall
  - Prevenção de ataques BadUSB
  - Proteção AMSI
  - Prevenção de explorações
  - Deteção de comportamento
  - Prevenção contra invasões
  - Motor de remediação
  - Kaspersky Security Network
  - Inspeção do Registo
  - Anti-Cryptor
  - Controlo de Internet
  - Controlo de Dispositivos
  - Controlo das Aplicações
  - Controlo de Anomalias Adaptativo
  - Monitorização da 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 do KUMA
  - Encriptação de disco completa
  - Encriptação ao nível dos ficheiros
  - Encriptação de unidades amovíveis
  - Modelos (encriptação de dados)
  - Exclusões

Definições da aplicação
Relatórios e armazenamento
Definições de Rede
Interface
Gerir definições
Atualização de bases de dados e módulos de software de aplicação
Anexo 2. Grupos fiáveis da aplicação
Anexo 3. Extensões de ficheiro para verificação rápida de unidades removíveis
Anexo 4. Tipos de ficheiros para o filtro de anexo Proteção contra ameaças de correio
Anexo 5. Definições de rede para interação com serviços externos
Anexo 6. Eventos da aplicação
Crítico
Falha funcional
Aviso
Mensagens informativas
Anexo 7. Extensões de ficheiros suportadas para a prevenção da execução
Anexo 8. Interpretadores de script suportados para Prevenção da execução
Anexo 9. Âmbito de verificação IOC no registo (RegistryItem)
Anexo 10. Requisitos para IOC file
Anexo 11. API para Resposta a Ameaças EDR
Anexo 12. Contas de utilizador em regras de componentes de aplicação
Informações legais
Fornecimento de dados
Fornecimento de dados ao abrigo do Contrato de Licença do Utilizador Final
Fornecimento de dados ao utilizar a Kaspersky Security Network
Fornecimento de dados ao usar 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 (RGPD)
Avisos de marcas comerciais
Informação acerca de código de terceiros

Ajuda do Kaspersky Endpoint Security for Windows

O que há de novo na versão 14.2

Foi adicionado suporte para autenticação baseada em tokens na Proteção por password

O que há de novo em cada versão do Kaspersky Endpoint Security for Windows

Como começar

Implementação do Kaspersky Endpoint Security for Windows

Arranque inicial do Kaspersky Endpoint Security for Windows

Licenciamento do Kaspersky Endpoint Security for Windows

Fornecimento de dados

Sob o Contrato de Licença do Utilizador Final

Ao utilizar o KSN

RGPD

Eliminar ameaças

Em estações de trabalho

Em servidores

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

Melhores práticas

Otimização do desempenho das aplicações

Implementação do modo de rejeição predefinido no Controlo das Aplicações

Migração do KEA para o KES com o agente integrado

Utilizar o KES como parte de outras soluções

Kaspersky EDR

Kaspersky Sandbox

Kaspersky MDR

O que há de novo

Atualização 14.2

O Kaspersky Endpoint Security for Windows 14.2 apresenta as seguintes funcionalidades e melhorias:

1. Alterado o conjunto de componentes instalados por predefinição. A configuração predefinida da aplicação inclui agora a Prevenção de ataques BadUSB, a Gestão do BitLocker e o agente incorporado do EDR Optimum.

2. Foi adicionado suporte para autenticação baseada em tokens (Proteção por password). Agora, para aceder à aplicação, pode utilizar o seu nome de utilizador e password, uma password temporária emitida pelo administrador ou um token. A autenticação baseada em tokens pode ser utilizada, por exemplo, para contas de utilizador de serviço que não necessitem de password.

3. Foi adicionado um novo critério de robustez da password para o BitLocker: verificação do histórico de passwords. A aplicação impede os utilizadores de definirem uma password que já tenham utilizado anteriormente.

4. Foi adicionado suporte para alterar o idioma da interface do Kaspersky Endpoint Security ao atualizar a aplicação através da tarefa *Instalar aplicação remotamente*. Agora, não é necessário reinstalar a aplicação caso tenha escolhido o idioma de interface errado.

5. Foram adicionados novos eventos de telemetria para os utilizadores das soluções Kaspersky Endpoint Detection and Response: GPO Change, SCCM Local Config Mismatch, SCCM Config Change, SCCM Deployment Task, Smb Connection Open. Estes novos eventos reforçam as capacidades de deteção de ameaças das soluções EDR.

6. Foi adicionado suporte para uma nova ação de resposta a ameaças, *Colocar ficheiro*, para os utilizadores do Kaspersky Endpoint Detection and Response Expert (on-premise). Esta tarefa permite enviar ficheiros de configuração, scripts de resposta a ameaças, utilitários para mitigar os efeitos de ataques, etc., para os computadores. A tarefa *Colocar ficheiro* está disponível na consola OSMP com a versão 9.0 da solução Kaspersky EDR Expert (on-premises) implementada.

7. Foi melhorado o comportamento das ações de resposta a ameaças para os utilizadores do Kaspersky Endpoint Detection and Response Optimum. Agora, antes de executar a ação (*Eliminar ficheiro*, *Mover ficheiro para a Quarentena* ou *Prevenção de execução*), a aplicação verifica se o objeto é crítico para o sistema (System Critical Object, SCO) e avisa sobre o potencial impacto na estabilidade do sistema. Não é recomendável aplicar estas ações a ficheiros de Objetos Críticos do Sistema (SCO).

8. Foi adicionado suporte para que os utilizadores do Kaspersky Security for Virtualization Light Agent utilizem a aplicação como parte de um cluster de alta disponibilidade de Servidores de Integração. Um cluster de alta disponibilidade de Servidores de Integração assegura a proteção ininterrupta do ambiente virtual graças à comutação pós-falha das SVM e dos Light Agents para um Servidor de Integração de reserva sempre que o Servidor de Integração principal falha.

9. Ao desenvolver esta versão do Kaspersky Endpoint Security, incorporámos as alterações incluídas nos 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 for Windows 14.1 apresenta as seguintes funcionalidades e melhorias:

1. Foi adicionado suporte para o sistema operativo do Windows Server 2025.

2. O limite para o número de regras de filtragem de eventos de telemetria para o Endpoint Detection and Response Expert (on-premises) e o Kaspersky Endpoint Detection and Response Expert (cloud) foi aumentado. O Kaspersky Endpoint Security agora suporta até 10 000 regras de filtragem, incluindo e excluindo regras específicas.

3. Agora pode configurar tarefas para serem executadas apenas em dias específicos da semana, num intervalo de semanas especificado. O agendamento está disponível no Kaspersky Security Center 16.1 ou posterior.

4. Para a *Verificação de software malicioso*, agora pode especificar um intervalo durante o qual a tarefa será pausada, por exemplo, para minimizar o impacto no desempenho do computador durante períodos de carga aumentada.

5. O desempenho do subsistema de disco rígido no computador protegido foi otimizado através da redução do número de operações de E/S.

6. Ao desenvolver esta versão do Kaspersky Endpoint Security, incorporámos as alterações incluídas nos 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, PF25019.

Atualização 14.0

O Kaspersky Endpoint Security for Windows 14.0 apresenta as seguintes funcionalidades e melhorias:

1. Agora há suporte para computadores baseados em Arm. Pode instalar a aplicação no modo padrão ou no modo EDR Agent. No entanto, a aplicação apresenta várias limitações (por exemplo, entre as tecnologias de encriptação de dados, apenas o BitLocker é suportado).

2. A auditoria de políticas alargada é suportada na versão 15.0 ou posterior do Kaspersky Security Center Web Console. Agora pode visualizar as revisões das políticas e guardá-las num ficheiro. Uma *revisão* é um conjunto de parâmetros modificados guardados pelo utilizador. As revisões permitem comparar e reverter alterações nos parâmetros da política.

3. Estão agora disponíveis novos eventos de telemetria para os utilizadores do Kaspersky Endpoint Detection and Response. Estes novos eventos reforçam as capacidades de deteção de ameaças através das soluções Kaspersky EDR.

4. Ao desenvolver esta versão do Kaspersky Endpoint Security for Windows, incorporámos as alterações incluídas nos 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 for Windows 12.12 apresenta as seguintes funcionalidades e melhorias:

1. A proteção de pastas partilhadas contra encriptação externa, que antes fazia parte do componente Deteção de Comportamento, passou a ser um componente separado, o Anti-Cryptor.

2. Foi adicionado suporte ao protocolo Kerberos para autenticar a aplicação por meio de um servidor proxy para acesso à Internet.

3. Agora pode especificar um hash de ficheiro para uma aplicação fiável e não apenas um caminho completo.

4. Estão disponíveis mais funcionalidades da tarefa *Verificação IOC* para utilizadores de soluções Detection and Response (EDR). A funcionalidade Verificação retrospetiva IOC já está disponível. A *Verificação retrospetiva dos IOC* é um modo da tarefa *Verificação IOC* na qual o Kaspersky Endpoint Security verifica indicadores de comprometimento usando dados de um determinado período de tempo. Este modo destina-se à deteção de indicadores de comprometimento nos dados da atividade de rede do computador. O Kaspersky Endpoint Security analisa os dados nos registos do sistema operativo e nos registos do navegador no computador.

5. Os utilizadores do Kaspersky Endpoint Detection and Response (EDR) podem remover o limite de tamanho de quarentena. Isto pode ser necessário para a verificação YARA porque a aplicação pode guardar um ficheiro de despejo de memória de grande dimensão. Agora pode usar todo o seu espaço livre no disco para a quarentena.

6. Agora é possível utilizar a compressão HTTPS para otimizar a exportação de eventos para a Kaspersky Unified Monitoring and Analysis Platform (KUMA). Isto ajuda a reduzir o tráfego de saída.

7. Ao desenvolver esta versão do Kaspersky Endpoint Security for Windows, incorporámos as alterações incluídas nos 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 for Windows 12.11 disponibiliza as seguintes funcionalidades e melhorias:

1. A aplicação verifica a configuração dos componentes de controlo antes de guardar as definições. A verificação foi adicionada para os componentes Controlo das Aplicações, Controlo de Dispositivos e Monitorização da Integridade do Sistema. A aplicação agora exibe um aviso se as definições atuais do componente de controlo puderem aumentar a carga no computador ou causar falhas no sistema. Por exemplo, no caso do Controlo das Aplicações, se tiver selecionado o modo que bloqueia todas as aplicações, exceto as permitidas, e não tiver adicionado nenhuma regra de permissão, a aplicação exibe um aviso, porque essa configuração pode causar falhas no sistema.

2. Adicionado suporte para envio automático de ficheiros para o KATA Sandbox para revisão. O *KATA Sandbox* é um componente da Kaspersky Anti Targeted Attack Platform que executa ficheiros em imagens virtuais de sistemas operativos. O Sandbox analisa o comportamento do objeto para detetar atividades maliciosas e atividades características de ataques direcionados à infraestrutura de TI da organização. O Sandbox analisa e verifica objetos em servidores especiais com imagens virtuais implementadas de sistemas operativos Microsoft Windows (servidores do Sandbox). Para que o KATA Sandbox funcione no modo automático, o Kaspersky Anti Targeted Attack Platform 8.0 ou versão posterior tem de ser implementado.

3. Envio otimizado de telemetria EDR. Agora pode especificar o comprimento máximo do pacote.

4. Diagnóstico de ligação melhorado para a Kaspersky Security Network. Detalhes adicionais sobre erros de ligação para a Kaspersky Security Network para resolver potenciais problemas.

5. Adicionado suporte para configurar listas de eventos a serem enviadas para a Kaspersky Unified Monitoring and Analysis Platform (KUMA). Agora, além das listas de eventos predefinidas no KUMA, pode adicionar manualmente eventos à telemetria ou excluir eventos pelo seu ID no Registo de Eventos do Windows.

6. Atualizou a interface da política na Consola Web. O layout das secções da política foi alterado para permitir um acesso mais rápido às funcionalidades essenciais.

7. Suporte para Windows 11 25H2.

8. Ao desenvolver esta versão do Kaspersky Endpoint Security for Windows, incorporámos as alterações incluídas nos 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 for Windows 12.10 disponibiliza as seguintes funcionalidades e melhorias:

1. Para o componente Prevenção de ataques BadUSB, foi adicionada a opção de autorizar leitores de código de barras lendo um código de barras no monitor. Agora não precisa digitar um código utilizando o teclado no ecrã para autorizar leitores de código de barras.

2. As seguintes funcionalidades e melhorias estão disponíveis para os utilizadores das soluções de Endpoint Detection and Response (EDR) da Kaspersky:

   - Agora pode gerir o Isolamento de Rede do computador nos detalhes do alerta. Além disso, nos detalhes do alerta, pode especificar o período de Isolamento da Rede do computador e adicionar exclusões.

   - Preenchimento dos detalhes do alerta com novos dados. Agora, os detalhes do alerta contêm mais informações sobre a ameaça, incluindo o comportamento da aplicação ao responder a ameaças EDR.

   - O processamento de ficheiros IOC foi melhorado. Agora pode ver e editar o conteúdo dos ficheiros IOC na interface da Consola Web do Kaspersky Security Center. Após carregar um ficheiro IOC, a aplicação apresenta um relatório sobre a aplicação dos termos do IOC.

   - Resposta melhorada aos IOCs detetados. Agora pode colocar em quarentena os ficheiros detetados pela tarefa de *verificação IOC* diretamente nos resultados de deteção de IOC nas propriedades da tarefa. Também pode isolar computadores da rede nas propriedades da tarefa.

   - Agora pode criar ficheiros IOC diretamente nas propriedades da tarefa de *Verificação IOC*, com base em listas de hashes de arquivos, endereços IP ou nomes DNS gerados num ficheiro TXT.

   - Âmbito de verificação expandido para a tarefa de *verificação IOC*. Agora pode definir um âmbito para a verificação IOC do registo (**Registo do Windows – Registryltem**). Em versões anteriores da aplicação, só podia utilizar um âmbito de verificação IOC predefinido no registo.

3. Nova permissão de proteção por password adicionada, *Exportar definições*. Por defeito, apenas o utilizador do KLAdmin pode criar um ficheiro de configuração com as definições do Kaspersky Endpoint Security na interface da aplicação. Para conceder acesso a outros utilizadores, precisa de lhes fornecer a permissão correspondente.

4. Ao desenvolver esta versão do Kaspersky Endpoint Security for Windows, incorporamos as alterações incluídas nas seguintes correções privadas: 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 for Windows 12.9 disponibiliza as seguintes funcionalidades e melhorias:

1. Foi adicionada a nova funcionalidade de *gestão de passwords temporárias*. A password temporária permite-lhe fornecer acesso ao Kaspersky Endpoint Security com a Proteção por password ativada para um computador separado. A gestão de passwords temporárias permite guardar o histórico de passwords (até 30 dias), monitorizar o estado das passwords temporárias (*Ativo*, *Expirado*, *Revogado*) e revogar passwords temporárias.

2. Foi adicionada a opção de terminar a ligação a recursos Web proibidos pelas regras de Controlo de Internet imediatamente após a aplicação da política. Nas versões anteriores da aplicação, o Controlo de Internet restringia apenas as novas ligações a recursos da Web proibidos.

3. Para os utilizadores da Kaspersky Anti Targeted Attack Platform, foi adicionada uma opção para executar a verificação YARA localmente no computador. Para o fazer, tem de descarregar um ficheiro com regras YARA e executar o comando em CMD.

4. Foi corrigido o comportamento da aplicação quando o BitLocker é ativado em computadores nos quais as unidades já estão protegidas pelo BitLocker utilizando ferramentas de terceiros. O Kaspersky Endpoint Security inicia o procedimento de recuperação para enviar a chave de recuperação para o Kaspersky Security Center. Assim, a gestão do BitLocker é transferida para a consola Kaspersky Security Center.

5. Uma nova secção, **Response history**, está disponível para utilizadores de soluções de Detection and Response da Kaspersky. Esta secção contém informações sobre as ações de resposta a ameaças executadas no computador. Estas ações incluem, por exemplo, a execução da tarefa *Terminar processo* ou o isolamento do computador da rede. O histórico de respostas só está disponível para os utilizadores das seguintes soluções da Kaspersky: MDR, EDR, KATA.

6. Para os utilizadores de Kaspersky Unified Monitoring and Analysis Platform, o suporte para ações de resposta a ameaças EDR está agora disponível. Ao responder a ameaças, o KUMA executa scripts que criam tarefas EDR correspondentes. Para executar tarefas EDR, tem de criar uma regra de resposta para o script personalizado na consola KUMA e selecionar eventos.

7. Ao desenvolver esta versão do Kaspersky Endpoint Security for Windows, incorporamos as alterações incluídas nas seguintes correções privadas: 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 for Windows 12.8 disponibiliza as seguintes funcionalidades e melhorias:

1. A aplicação agora suporta o modo Light Agent para proteger ambientes virtuais. Agora pode implementar a aplicação como Light Agent como parte da solução Kaspersky Security for Virtualization Light Agent 6.2.

2. A interceção de operações de ficheiros em contentores Docker nos servidores é agora suportada. Um *contentor* é um ambiente isolado no qual uma aplicação pode ser executada sem interagir diretamente com o sistema operativo. O Kaspersky Endpoint Security verifica os ficheiros dentro dos contentores aos quais o utilizador obtém acesso. Quando uma ameaça é detetada, as aplicações bloqueiam esta atividade maliciosa e tentam desinfetar o ficheiro dentro do contentor. Se o ficheiro não puder ser desinfetado, a aplicação interrompe o contentor.

3. Agora pode definir um âmbito de proteção para a proteção de pastas partilhadas contra encriptação externa (componente Deteção de comportamento). Agora pode especificar as pastas partilhadas que a aplicação tem de monitorizar quanto à atividade dos ficheiros. Também pode excluir ficheiros do âmbito de proteção. Nas versões anteriores da aplicação, o componente de Deteção de Comportamento monitorizava todas as pastas partilhadas quanto à atividade dos ficheiros.

4. Agora pode configurar diferentes conjuntos de componentes para diferentes tipos de sistemas operativos no pacote de instalação. Ou seja, pode implementar a aplicação em estações de trabalho e servidores utilizando o mesmo pacote de instalação. Os componentes que não estão disponíveis para um determinado tipo de sistema operativo são automaticamente excluídos nas propriedades do pacote de instalação.

5. Foi adicionada a opção de selecionar exclusões de verificação predefinidas e aplicações fiáveis. As exclusões de verificação predefinidas e as aplicações de confiança permitem configurar rapidamente a zona fiável para a aplicação num ambiente virtual (Citrix, VMware). Estas exclusões incluem, por exemplo, ficheiros de máquinas virtuais VHD e VHDX. As exclusões podem ser adicionadas ao criar um pacote de instalação de aplicações, ao criar uma política ou ao instalar o Kaspersky Endpoint Security.

6. A telemetria EDR agora inclui eventos para operações com dispositivos ligados via USB. Também pode adicionar estes eventos às exclusões da telemetria EDR.

7. Foi adicionada a opção de bloquear ligações de rede através do protocolo obsoleto TLS 1.0. O TLS 1.0 tem um nível de segurança baixo, pelo que se recomenda a desativação deste protocolo e a utilização de versões mais recentes do TLS 1.2 ou do TLS 1.3. Por padrão, o Kaspersky Endpoint Security bloqueia ligações do TLS 1.0. Depois de atualizar a versão da aplicação, o funcionamento de serviços de terceiros que utilizam o protocolo TLS 1.0 pode falhar. Para evitar problemas no funcionamento de serviços de terceiros, pode permitir a utilização do protocolo TLS 1.0 na política de grupo antes de atualizar a versão da aplicação.

8. Ao desenvolver esta versão do Kaspersky Endpoint Security for Windows, incorporamos as alterações incluídas nas seguintes correções privadas: 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 for Windows 12.7 disponibiliza as seguintes funcionalidades e melhorias:

1. Agora pode limitar a utilização de recursos da CPU para as tarefas de *Verificação de software malicioso*. Para o fazer, nas definições da aplicação, especifique a percentagem máxima de carga da CPU para todos os núcleos que podem ser utilizados durante a verificação do computador.

2. Agora pode enviar manualmente ficheiros para serem verificados no KATA Sandbox. O *KATA Sandbox* é um componente da Kaspersky Anti Targeted Attack Platform que executa ficheiros em imagens virtuais de sistemas operativos. O Sandbox analisa o comportamento do objeto para detetar atividades maliciosas e atividades características de ataques direcionados à infraestrutura de TI da organização. O Sandbox analisa e verifica objetos em servidores especiais com imagens virtuais implementadas de sistemas operativos Microsoft Windows (servidores do Sandbox). Para enviar um ficheiro para a verificação para o KATA Sandbox, selecione o comando relevante no menu de contexto do ficheiro.

3. Agora pode configurar a integração com a solução que protege a LAN empresarial, *Kaspersky Network Detection and Response*. O Kaspersky Network Detection and Response (NDR) faz parte da Kaspersky Anti Targeted Attack Platform. Pode configurar a interação com o NDR no modo padrão, bem como no modo EDR Agent.

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

5. Ao desenvolver esta versão do Kaspersky Endpoint Security for Windows, incorporámos as alterações incluídas nas seguintes correções privadas: PF10049, PF10355, PF12114, PF13109, PF14056, PF15038, PF15045, PF16037, PF16042, PF16047, PF17014, PF17018, PF17021, PF17024, PF18006, PF18007.

Atualização 12.6

O Kaspersky Endpoint Security for Windows 12.6 disponibiliza as seguintes funcionalidades e melhorias:

1. A funcionalidade de integração com a solução Kaspersky SIEM - *Kaspersky Unified Monitoring and Analysis Platform; KUMA* - foi adicionada. Agora é possível enviar eventos dos registos de eventos do Windows para o coletor KUMA. Isto permite ao KUMA receber eventos do Windows (é suportado um conjunto limitado de EventIDs) de todos os computadores nos quais o Kaspersky Endpoint Security está instalado, sem instalar agentes KUMA nestes computadores.

2. Um novo componente *Monitorização da integridade do sistema* foi adicionado para substituir o componente Monitorização de integridade do ficheiro. O componente Monitorização da integridade do sistema inclui todas as funcionalidades do Monitor de integridade do ficheiro e, adicionalmente, permite monitorizar alterações de registo e conexão de dispositivos externos. O componente Monitorização da integridade do sistema monitoriza as alterações no sistema operativo que podem indicar violações da segurança informática. Quando essas alterações são detetadas, o Kaspersky Endpoint Security gera eventos correspondentes e alerta o administrador. O Monitor de integridade do ficheiro já não faz parte da aplicação. As definições do Monitor de integridade do ficheiro migram automaticamente para o Monitor de integridade do ficheiro quando atualiza a aplicação. Para assegurar o correto funcionamento da Monitorização da integridade do sistema, tanto a aplicação Kaspersky Endpoint Security como o plug-in de gestão devem ser atualizados para a versão 12.6.

3. O estado do EDR Agent (KATA) incorporado instalado foi adicionado às propriedades do computador na consola do Kaspersky Security Center. Agora, se tiver um EDR Agent (KATA) incorporado instalado, a coluna do **estado do Endpoint Sensor** apresenta o estado atual do componente (por exemplo, *Em execução*, *Parado*, *Não suportado pela licença*, etc.).

4. Foi adicionada a opção de selecionar exclusões de verificação predefinidas e aplicações fiáveis. Exclusões de verificação predefinidas e aplicações fiáveis ajudam a configurar rapidamente a zona fiável ao utilizar a aplicação em servidores SQL, servidores Microsoft Exchange e System Center Configuration Manager. Estas exclusões incluem, por exemplo, ficheiros de bases de dados MDF e LDF. As exclusões podem ser adicionadas ao criar uma nova política, modificar uma política existente ou ao instalar o Kaspersky Endpoint Security.

5. A exibição dos detalhes de alerta para o Kaspersky Endpoint Detection and Response Optimum foi movida do plug-in de gestão do Kaspersky Endpoint Security para um plug-in de gestão separado do Kaspersky Endpoint Detection and Response. O plug-in de gestão do EDR é um plug-in único para trabalhar com agentes nos sistemas operativos Windows, Mac e Linux. Agora, ao trabalhar com o EDR Optimum, irá precisar do plug-in de gestão do Kaspersky Endpoint Security para criar tarefas de resposta a ameaças e do plug-in de gestão EDR para ver detalhes de alertas.

6. Suporte para Windows 11 24H2.

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

Atualização 12.5

O Kaspersky Endpoint Security for Windows 12.5 disponibiliza as seguintes funcionalidades e melhorias:

1. A opção de 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 monitorizar e proteger a infraestrutura informática 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 recolha de Telemetria.

2. A interface da zona fiável da aplicação foi melhorada. O Kaspersky Endpoint Security oculta agora objetos de zona fiável do utilizador se o administrador tiver proibido o utilizador de adicionar as suas próprias exclusões de verificação (locais) e aplicações fiáveis. Isto impede o acesso não autorizado à zona fiável por parte de um intruso, aumentando o nível de segurança do computador.

3. Foi adicionada a opção para analisar o tráfego dos clientes de e-mail MyOffice Mail e R7-Office Organizer. O componente Proteção contra ameaças de correio analisa agora não só os anexos das mensagens quando são descarregados, mas também as mensagens enviadas e recebidas.

4. Foi adicionada uma nova categoria de recursos Web *Ferramentas de IA generativa*. Pode configurar o acesso a sites da nova categoria utilizando o Controlo Web.

5. Agora pode selecionar a localização de uma regra de pacote de rede na lista Firewall. A localização de uma regra de pacote de rede na lista determina a sua prioridade. Nas versões anteriores da aplicação, só podia ser adicionada uma nova regra ao fim da lista, depois era necessário deslocar manualmente a regra pela lista para lhe dar prioridade. Agora, ao adicionar uma regra, pode escolher se a regra deve ser colocada no início, no fim da lista ou ao lado da regra selecionada.

6. Nas regras dos componentes do Kaspersky Endpoint Security, agora pode selecionar utilizadores não só a partir do Active Directory, mas também a partir da lista de utilizadores no Kaspersky Security Center. Também pode introduzir manualmente os dados da conta de utilizador local. Esta possibilidade foi adicionada para as regras dos seguintes componentes: Controlo das Aplicações, Controlo de Dispositivos, Controlo de Internet, Controlo de Anomalias Adaptativo e Inspeção de Registo.

7. O relatório de deteção de ataque à rede agora inclui uma coluna com o Endereço MAC do computador atacante (o componente Proteção contra ameaças de Rede). Agora pode ver o endereço MAC do computador atacante no relatório, além de seu endereço IP. Isto é útil para a investigação de incidentes. Os relatórios que contêm o endereço MAC do computador atacante também estarão disponíveis na consola Linux do Kaspersky Security Center versão 15.1 e superiores.

8. O nível dos requisitos de proteção do computador foi aumentado. O elevado nível de proteção exige agora a ativação da Proteção dos serviços da aplicação contra a gestão externa. Verifique o indicador do nível de segurança na parte superior da janela da política. Se tiver um nível de segurança médio ou baixo, pode ativar a opção Proteção dos serviços da aplicação contra gestão externa na janela de recomendação do indicador do nível de segurança.

9. Foi adicionado suporte para novos eventos de deteção de objetos quando a aplicação está a executar a Configuração do Endpoint Detection and Response Agent (EDR Agent). Estes eventos já eram suportados na configuração do [KES+agente incorporado].

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

Atualização 12.4

O Kaspersky Endpoint Security for Windows 12.4 disponibiliza as seguintes funcionalidades e melhorias:

1. Adicionada nova funcionalidade para proteger a ligação do computador ao Kaspersky Security Center. Nova tarefa de *Proteção da ligação do Servidor de Administração* permite definir uma password para a ligação a um servidor fiável. Isto significa que não é possível voltar a ligar o computador e executar comandos a partir de outro servidor sem esta password.

2. Para o componente de Proteção por password, foi adicionada a capacidade de selecionar utilizadores manualmente e não apenas do Active Directory. Ou seja, pode especificar manualmente um nome de utilizador e uma password e atribuir direitos de acesso ao Kaspersky Endpoint Security para esta conta. Desta forma, não é necessário partilhar a sua password do KLAdmin com outros utilizadores ou criar novas contas do Active Directory para controlar o acesso à aplicação.

3. Suporte para Windows 11 23H2.

Atualização 12.3

O Kaspersky Endpoint Security for Windows 12.3 disponibiliza as seguintes funcionalidades e melhorias:

1. Agora pode instalar a aplicação na configuração do Endpoint Detection and Response Agent. Esta configuração permite instalar a aplicação com um conjunto de componentes exigidos pelas soluções Detection and Response da Kaspersky: Kaspersky Managed Detection and Response e Kaspersky Anti Targeted Attack Platform (EDR). Pode instalar a aplicação nesta configuração em conjunto com soluções de terceiros (por exemplo, Dr.Web, Dallas Lock, ESET). Isso permite que use ferramentas de segurança de infraestrutura de terceiros em conjunto com o Detection and Response da Kaspersky.

2. O funcionamento do Kaspersky Endpoint Security com dispositivos Bluetooth foi melhorado. Agora pode configurar exclusões e restringir o acesso a todos os dispositivos Bluetooth, exceto dispositivos de entrada (teclados sem fio, ratos, etc.).

3. O funcionamento do componente Controlo de Aplicações com a base de dados de ficheiros executáveis foi otimizado. O Kaspersky Endpoint Security agora remove automaticamente as informações do ficheiro da base de dados se o ficheiro for removido do computador. Isto permite manter a base de dados atualizada e poupar recursos do Kaspersky Security Center.

4. O nível dos requisitos de proteção do computador foi aumentado. O elevado nível de proteção requer agora que ative a proteção por password. Verifique o indicador do nível de segurança na parte superior da janela da política. Se tiver um nível de proteção médio ou baixo, poderá ativar a Proteção por password na janela de recomendações do indicador de nível de segurança.

5. Foi adicionado o suporte ao protocolo HTTPS para permitir que a aplicação funcione com o Kaspersky Security Network. Ative a utilização de HTTPS nas propriedades do servidor de administração nas definições do servidor proxy KSN.

Atualização 12.2

O Kaspersky Endpoint Security for Windows 12.2 disponibiliza as seguintes funcionalidades e melhorias:

1. Foi adicionado suporte ao protocolo WPA3 para controlar as ligações a redes Wi-Fi (Controlo de Dispositivos). Agora pode optar por usar o protocolo WPA3 nas definições de rede Wi-Fi fiável e negar ligações à rede que usam um protocolo menos seguro.

2. Agora pode escolher um protocolo e portas para exclusões de proteção contra ameaças de rede. Agora, além de especificar endereços IP de dispositivos fiáveis, também pode selecionar uma porta e um protocolo. Isto permite excluir fluxos de dados individuais e prevenir ataques de rede de endereços IP fiáveis.

3. Diferente ordem de fontes de atualização para a *Atualização das bases de dados e módulos da aplicação tarefa* local se uma política for aplicada ao computador. O servidor Kaspersky Security Center é agora usado por defeito como a primeira fonte de atualizações em vez dos servidores Kaspersky. Isto ajuda a economizar tráfego quando o utilizador executa a tarefa *Atualização das bases de dados e módulos da aplicação* local.

Atualização 12.1

O Kaspersky Endpoint Security for Windows 12.1 disponibiliza as seguintes funcionalidades e melhorias:

1. Foi adicionado um agente integrado para a solução Kaspersky Anti Targeted Attack Platform. Já não é preciso o Kaspersky Endpoint Agent para 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, utilize o Assistente de migração. Depois de atualizar a aplicação, o Kaspersky Endpoint Security troca para a utilização do agente incorporado e remove o Kaspersky Endpoint Agent. O Kaspersky Endpoint Agent foi adicionado à lista de software incompatível. O Kaspersky Endpoint Security agora possui agentes integrados para todas as soluções Detection and Response, portanto, já não é necessário instalar o Kaspersky Endpoint Agent para integração com estas soluções.

2. Agora é suportado o modo de compatibilidade do Azure WVD. Esta funcionalidade garante a exibição correta do estado da máquina virtual do Azure na consola da Kaspersky Anti Targeted Attack Platform. O modo de compatibilidade do Azure WVD permite atribuir um ID do Sensor único permanente a estas máquinas virtuais.

3. Agora pode configurar o acesso do utilizador a dispositivos móveis no iTunes ou aplicações semelhantes. Ou seja, pode, por exemplo, permitir que o dispositivo móvel seja usado apenas no iTunes e bloquear o uso do dispositivo móvel como uma unidade amovível. A aplicação também suporta estas regras para a aplicação Android Debug Bridge (ADB).

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

Problemas resolvidos

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 Controlo de Dispositivos permite o acesso a um dispositivo MTD (cartão SD) quando a ação **Bloquear** está selecionada para o tipo de dispositivo **Unidades amovíveis**.
10068496	Num dispositivo protegido, é possível alterar o modo de Proteção contra falsificação de MAC quando as definições da Proteção contra ameaças de Rede estão bloqueadas na política principal.
10095087	Quando a Análise de ligações encriptadas está ativada, o acesso a qualquer website através de uma firewall de próxima geração (NGFW) com um certificado revogado aciona uma notificação sobre o redirecionamento para um domínio com um certificado não fidedigno.
10140912	Com a aplicação instalada, o computador não deteta o dispositivo PDA BHT1100B com o Windows Mobile.
10141009	Se o componente Encriptação de Ficheiros estiver instalado, poderá não ser possível iniciar a aplicação Anthropic Claude.
10610853	Após a atualização para a nova versão, não é possível abrir a política porque as definições do Controlo de Dispositivos na nova versão incluem dispositivos que não são suportados na versão anterior.

Identificador	Descrição
10720516	Os anexos em ficheiros de formatos do Office poderão não ser abertos com a aplicação instalada.
10421967	Não é possível iniciar sessão numa caixa de correio partilhada se esta tiver sido adicionada como uma conta separada.

Lista de problemas corrigidos no plug-in da aplicação web 14.2.0.8289

Identificador	Descrição
9946286	Ao adicionar o endereço de um website a uma regra do Controlo de Internet, não é possível utilizar uma máscara que não inclua um ponto entre o domínio e a zona do domínio.
10054657 10507166	Após a migração para a nova versão, determinados componentes (como Controlo de Dispositivos e Application Control) não podem ser geridos através da política.
10084390	Nas definições do componente Controlo de Dispositivos, o tipo de dispositivo **Disco rígido** está duplicado, o que faz com que os discos rígidos dos utilizadores sejam bloqueados.
10113718	Em alguns casos, as regras personalizadas da Firewall não são apresentadas.
10311613	Nas definições do componente Host Intrusion Prevention, não é possível adicionar um recurso protegido por máscara utilizando o caráter `*`.
10391923	No Controlo das Aplicações, ao criar uma categoria de aplicações com base num hash MD5 de um ficheiro, não é apresentado qualquer aviso a indicar que essa categoria é inválida e não funcionará.
10571790	No componente Application Control, foi corrigido o título da lista de regras de bloqueio no modo **Allow all except the rules list**.
10592891 10689065	Na Zona fidedigna, o campo **Comment** não é apresentado para as exclusões na secção **Malware Scan exclusions**.
10613015 10689049 10592534	No componente Controlo de Dispositivos, o campo **Comment** não é apresentado para os dispositivos fiáveis.
10645068 10689057	A tarefa *Remove key* não é executada se for selecionado um ficheiro de chave de licença no formato KEY.
10685370 10685422	No componente Controlo de Dispositivos, não é possível adicionar um novo dispositivo à lista de dispositivos fiáveis se já existir na lista um dispositivo com esse nome.
10721136	Não é possível guardar as tarefas de grupo se não for especificada uma data de conclusão nas definições de agendamento.
10753509	A alteração da lista de utilizadores e grupos para dispositivos fiáveis no componente Controlo de Dispositivos pode alterar os tipos de registo, fazendo com que as definições deixem de se aplicar ao dispositivo.
10773402	Em alguns casos, as alterações às definições da política poderão não ser guardadas devido a perfis corrompidos.
10822620	As definições do componente Anti-Cryptor não são apresentadas na política e as alterações às definições de notificações não são guardadas.
10817035	Numa política subordinada, é possível adicionar um dispositivo fiável mesmo que esta definição esteja desativada na política principal («cadeado» fechado). No entanto, o dispositivo adicionado não é guardado.
10678009	No plug-in da aplicação web do Kaspersky Endpoint Security, não é possível adicionar uma nova regra da Firewall a uma política se tiver sido criada anteriormente uma regra utilizando um intervalo de endereços IP.

Lista de problemas corrigidos na versão 14.1

Identificador	Descrição
10140523	A ativação do NVMe nativo no Windows 11 pode resultar num comportamento instável da aplicação.
9340076	Num dispositivo em que a aplicação esteja instalada e o componente de encriptação de ficheiros esteja ativado, o Explorador do Windows não atualiza automaticamente o conteúdo de uma pasta de rede após esta ter sido alterada a partir de outro dispositivo.
9722863	O relatório Controlo de Dispositivos não inclui eventos de desconexão de tokens USB.

Identificador	Descrição
10006481	Após aplicar uma regra que bloqueia o tráfego de entrada, as ligações TCP ativas a serviços externos poderão ser encerradas prematuramente devido a um cálculo incorreto do tempo de espera.
10140912	A aplicação não deteta o dispositivo PDA BHT1100B.
10157563	Folder Redirection pode não funcionar após o reinício em estações de trabalho VDI.
10158494	O Controlo de Dispositivos regista vários eventos de ligação e desconexão de um dispositivo amovível sem que este seja fisicamente ligado novamente.

Perguntas frequentes

GERAL

Em que computadores funciona o Kaspersky Endpoint Security?

O que mudou desde a última versão?

Com que outras aplicações da Kaspersky é que o Kaspersky Endpoint Security pode funcionar?

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

IMPLEMENTAÇÃO

Como é que instalo o Kaspersky Endpoint Security em todos os computadores de uma organização?

Que definições de instalação podem ser configuradas na command line?

Como é que desinstalo remotamente o Kaspersky Endpoint Security?

ATUALIZAÇÃO

Que métodos estão disponíveis para atualizar as bases de dados?

O que devo fazer se surgirem problemas após uma atualização?

Como é que atualizo bases de dados fora da rede empresarial?

É possível utilizar um servidor proxy para atualizações?

SEGURANÇA

Como é que o Kaspersky Endpoint Security verifica o email?

Como é que excluo um ficheiro fiável das verificações?

Como é que protejo um computador contra vírus de unidades USB?

Como é que executo uma verificação de software malicioso oculta do utilizador?

Como é que coloco em pausa temporariamente a proteção do Kaspersky Endpoint Security?

Como é que restauro um ficheiro que o Kaspersky Endpoint Security eliminou erroneamente?

Como é que protejo o Kaspersky Endpoint Security de ser desinstalado por um utilizador?

INTERNET

O Kaspersky Endpoint Security verifica ligações encriptadas (HTTPS)?

Como é que permito que os utilizadores se liguem apenas a redes Wi-Fi fiáveis?

Como é que bloqueio redes sociais?

APLICAÇÕES

Como é que descubro que aplicações estão instalados no computador de um utilizador (inventário)?

Como é que evito que jogos de computador sejam executados?

Como é que verifico se o Controlo da Aplicação foi configurado corretamente?

Como é que adiciono uma aplicação à lista fiável?

DISPOSITIVOS

Como é que bloqueio o uso de unidades USB?

Como é que adiciono um dispositivo à lista fiável?

É possível obter acesso a um dispositivo bloqueado?

ENCRIPTAÇÃO

Em que condições é impossível a encriptação?

Como é que uso uma password para restringir o acesso a um ficheiro?

É possível usar cartões inteligentes e tokens com encriptação?

É possível obter acesso a dados encriptados sem uma ligação ao Kaspersky Security Center?

O que devo fazer se o sistema operativo do computador falhar, mas os dados permanecerem encriptados?

SUPORTE

Onde é armazenado o ficheiro do relatório?

Como é que crio um ficheiro de rastreio?

Como é que ativo a gravação de descarga?

Kaspersky Endpoint Security for Windows

O Kaspersky Endpoint Security for Windows (doravante designado como Kaspersky Endpoint Security) fornece proteção abrangente para o computador cotra vários tipos de ameaças, ataques à rede e de phishing.

A aplicação não se destina a ser utilizada em processos tecnológicos que envolvam sistemas de controlo automatizados. Para proteger dispositivos nesses sistemas, recomendamos a aplicação Kaspersky Industrial CyberSecurity for Nodes.

Tecnologias de deteção de ameaças



Aprendizagem automática

O Kaspersky Endpoint Security utiliza um modelo baseado em aprendizagem automática. O modelo foi desenvolvido pelos especialistas da Kaspersky. Posteriormente, o modelo é continuamente alimentado com dados de ameaças do KSN (formação de modelo).



Análise da nuvem

O Kaspersky Endpoint Security recebe dados sobre ameaças da Kaspersky Security Network. *A Kaspersky Security Network (KSN)* é uma infraestrutura de serviços na nuvem que fornece o acesso à Base de Conhecimento online da Kaspersky, que contém informações sobre a reputação de ficheiros, recursos da Internet e software.



Análise especializada

O Kaspersky Endpoint Security utiliza dados sobre ameaças adicionados pelos analistas de vírus da Kaspersky. Os analistas de vírus avaliam os objetos, se a reputação de um objeto não puder ser determinada automaticamente.



Análise comportamental

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



Análise automática

O Kaspersky Endpoint Security recebe dados do sistema automático de análise de objetos. O sistema processa todos os objetos enviados para a Kaspersky. Depois, o sistema determina a reputação do objeto e adiciona os dados às bases de dados de antivírus. Se o sistema não puder determinar a reputação do objeto, o sistema consulta os analistas de vírus da Kaspersky.



Sandbox

O Kaspersky Endpoint Security verifica o objeto numa máquina virtual. O Kaspersky Sandbox analisa o comportamento do objeto e toma uma decisão sobre a sua reputação. Esta tecnologia só está disponível se estiver a utilizar a solução Kaspersky Sandbox.



Cloud Sandbox

O Kaspersky Endpoint Security verifica objetos num ambiente isolado fornecido pela Kaspersky. A tecnologia Cloud Sandbox está permanentemente ativa e está disponível para todos os utilizadores da Kaspersky Security Network, independentemente do tipo de licença que estejam a utilizar. Se já tiver implementado a solução Endpoint Detection and Response, pode ativar um contador separado para as ameaças detetadas pelo Cloud Sandbox.

Árvore de seleções

Cada tipo de ameaça é processado por um componente dedicado. Os componentes podem ser ativados ou desativados de forma independente e as respetivas definições configuradas.

Secção	Componente
Proteção essencial contra ameaças 	**Proteção contra ameaças de ficheiros** O componente Proteção contra ameaças de ficheiros permite-lhe impedir a infeção do sistema de ficheiros de um computador. Por predefinição, o componente de Proteção contra ameaças de ficheiros reside permanentemente na RAM do computador e verifica todos os ficheiros abertos, guardados ou executados em tempo real. Este componente verifica ficheiros em todas as unidades do computador, incluindo unidades conectadas. O componente fornece proteção ao computador com a ajuda das bases de dados antivírus, o serviço de nuvem da Kaspersky Security Network e análise heurística. **Proteção contra ameaças da Web** O componente Proteção contra ameaças da Web impede a transferência de ficheiros maliciosos da Internet e também bloqueia a ligação a sites maliciosos e de phishing. O componente fornece proteção ao computador com a ajuda das bases de dados antivírus, o serviço de nuvem da Kaspersky Security Network e análise heurística. **Proteção contra ameaças de correio** O componente Proteção contra ameaças de correio verifica a existência de vírus e outras ameaças nos anexos das mensagens de e-mail recebidas e enviadas. O componente fornece proteção ao computador com a ajuda das bases de dados antivírus, o serviço de nuvem da Kaspersky Security Network e análise heurística. A proteção contra ameaças ao correio verifica as mensagens recebidas e enviadas. A aplicação suporta POP3, SMTP, IMAP e NNTP nos seguintes clientes de e-mail: • Microsoft Office Outlook • Mozilla Thunderbird • Windows Mail • MyOffice Mail • R7-Office Organizer Para verificar o tráfego nos clientes de e-mail Mozilla Thunderbird, MyOffice Mail e R7-Office Organizer, tem de adicionar um certificado Kaspersky ao armazenamento de certificados e selecionar o próprio armazenamento de certificados. A Proteção contra ameaças de correio não oferece suporte a outros protocolos e clientes de e-mail. A Proteção contra ameaças de correio pode nem sempre ser capaz de obter acesso de *nível de protocolo* a mensagens (por exemplo, ao usar a solução Microsoft Exchange). Por este motivo, a Proteção contra ameaças de correio inclui uma extensão para Microsoft Office Outlook. A extensão permite verificar mensagens ao *nível do cliente de e-mail*. A extensão Proteção contra ameaças de correio suporta as versões de 32 bits e 64 bits do Outlook 2010, 2013, 2016, 2019, 2021, 2024 e 365. Em computadores baseados em Arm, a extensão Proteção contra ameaças de correio suporta as versões de 32 bits e 64 bits do Outlook 2016, Outlook 2021, Outlook 2024 e Outlook 365 para Arm64. **Proteção contra ameaças de rede** O componente *Proteção contra ameaças de Rede* (também chamado de Intrusion Detection System, IDS) monitoriza o tráfego de entrada da rede quanto à existência de atividade característica de ataques à rede. Quando a aplicação deteta uma tentativa de ataque à rede no computador do utilizador, bloqueia a ligação da rede a o computador atacante. As bases de dados da aplicação fornecem descrições dos tipos de ataques de rede conhecidos e das formas utilizadas para os combater. A lista de ataques à rede que o componente Proteção contra ameaças de Rede deteta é atualizada durante as atualizações da base de dados e do módulo da aplicação. **Firewall** O componente da Firewall bloqueia ligações não autorizadas a um computador enquanto trabalha na Internet ou numa rede local. A Firewall controla também a atividade de rede das aplicações no computador. Isto permite-lhe proteger a sua LAN empresarial contra roubo de identidade e outros ataques. O componente fornece proteção ao computador com a ajuda das bases de dados antivírus, o serviço de nuvem da Kaspersky Security Network e *regras de rede* predefinidas. **Prevenção de ataques BadUSB** O componente "Prevenção de ataques BadUSB" bloqueia a ligação de dispositivos USB infetados que emulam um teclado ao computador. **Proteção AMSI** O componente de Proteção AMSI destina-se a fins de suporte da Antimalware Scan Interface da Microsoft. A *Antimalware Scan Interface (AMSI)* permite às aplicações de terceiros com suporte AMSI enviar objetos (por exemplo, scripts PowerShell) ao Kaspersky Endpoint Security para uma verificação adicional e receber depois os resultados de verificação destes objetos.

Secção	Componente
Proteção avançada contra ameaças 	**Kaspersky Security Network** *A Kaspersky Security Network (KSN)* é uma infraestrutura de serviços na nuvem que fornece o acesso à Base de Conhecimento online da Kaspersky, que contém informações sobre a reputação de ficheiros, recursos da Internet e software. A utilização de dados da Kaspersky Security Network permite uma resposta mais rápida do Kaspersky Endpoint Security a novas ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos diagnósticos positivos. Se participar na Kaspersky Security Network, os serviços da KSN irão fornecer ao Kaspersky Endpoint Security informações sobre a reputação dos endereços Web verificados, bem como informações sobre a categoria e a reputação dos ficheiros verificados. **Deteção de comportamento** O componente Deteção de comportamento recebe dados sobre as ações das aplicações no computador e transmite essas informações para outros componentes de proteção, de modo a melhorar o respetivo desempenho. O componente Deteção de comportamento utiliza Assinaturas de Fluxos de Comportamento (BSS) para aplicações. Se a atividade das aplicações corresponder uma assinatura de fluxo de comportamento, o Kaspersky Endpoint Security irá executar a ação de resposta selecionada. A funcionalidade do Kaspersky Endpoint Security é baseado em assinaturas de fluxos de comportamento e proporciona defesa proativa ao computador. O componente Deteção de comportamento também monitoriza portas de rede em busca de processos de aplicações que podem ameaçar a segurança do computador. A aplicação obtém informações sobre tais processos com bases de dados de antivírus. **Anti-Cryptor** O componente Anti-Cryptor analisa a atividade em pastas partilhadas. Se esta atividade corresponder a uma assinatura de fluxo de comportamento que seja comum para encriptação externa, o Kaspersky Endpoint Security executa a ação selecionada. **Prevenção de explorações** O componente Prevenção de explorações deteta o código de programa que aproveita vulnerabilidades no computador para explorar privilégios de administrador ou realizar atividades maliciosas. Por exemplo, as explorações podem utilizar um ataque de capacidade da memória intermédia excedida. Para tal, a exploração envia uma grande quantidade de dados para uma aplicação vulnerável. Ao processar estes dados, a aplicação vulnerável executa código malicioso. Como resultado deste ataque, a exploração pode iniciar uma instalação não autorizada de software malicioso. Ao detetar que uma tentativa para executar um ficheiro executável a partir de uma aplicação vulnerável não foi executada pelo utilizador, o Kaspersky Endpoint Security bloqueia a execução desse ficheiro ou notifica o utilizador. O componente Prevenção de explorações também monitoriza portas de rede em busca de processos de aplicações que podem ameaçar a segurança do computador. A aplicação obtém informações sobre tais processos com bases de dados de antivírus. **Prevenção contra invasões** O componente Prevenção contra invasões impede as aplicações de executarem ações que possam ser perigosas para o sistema operativo e garante o controlo do acesso aos recursos do sistema operativo e a dados pessoais. O componente fornece proteção ao computador com a ajuda das bases de dados antivírus e o serviço de nuvem da Kaspersky Security Network. **Motor de remediação** O componente Motor de remediação permite que o Kaspersky Endpoint Security reverta ações que foram executadas por software malicioso no sistema operativo.

Secção	Componente
Controlos de segurança 	**Controlo das aplicações** O Controlo das Aplicações gere a inicialização de aplicações nos computadores dos utilizadores. Isso permite-lhe implementar uma política de segurança empresarial ao usar aplicações. O Controlo das Aplicações reduz também o risco de infeção do computador, restringindo o acesso às aplicações. **Controlo de Dispositivos** O Controlo de Dispositivos gere o acesso de utilizador a dispositivos que são instalados no ou ligados ao computador (por exemplo, discos rígidos, câmaras ou módulos Wi-Fi). Tal permite proteger o computador da infeção quando os dispositivos são ligados, e impede a perda ou fuga de dados. **Controlo de Internet** O Controlo de Internet gere o acesso do utilizador aos recursos da Web. Isto ajuda a reduzir o tráfego e o uso inadequado do tempo de trabalho. Quando um utilizador tenta abrir um website restrito pelo Controlo de Internet, o Kaspersky Endpoint Security bloqueia o acesso ou apresenta um aviso. **Controlo de Anomalias Adaptativo** O componente Controlo de Anomalias Adaptativo monitoriza e bloqueia ações que não são típicas dos computadores na rede de uma empresa. O Controlo de Anomalias Adaptativo usa um conjunto de regras para rastrear comportamento invulgar (por exemplo, a regra *Início da Microsoft PowerShell da aplicação de ambiente de trabalho*). As regras são criadas pelos especialistas da Kaspersky com base em cenários típicos de atividade maliciosa. Pode configurar o modo como o Controlo de Anomalias Adaptativo manuseia cada regra e, por exemplo, permitir a execução de scripts do PowerShell que automatizam determinadas tarefas do fluxo de trabalho. O Kaspersky Endpoint Security atualiza o conjunto de regras a par das bases de dados da aplicação. **Inspeção de Registo** A Inspeção de Registo monitoriza a integridade do ambiente protegido com base na análise do registo de eventos do Windows. Quando a aplicação deteta sinais de comportamento atípico no sistema, ela informa o administrador, visto que este comportamento pode indicar uma tentativa de ciberataque. **Monitorização da integridade do sistema** O componente Monitorização da integridade do sistema monitoriza as alterações no sistema operativo que podem indicar violações da segurança informática. Quando essas alterações são detetadas, o Kaspersky Endpoint Security gera eventos correspondentes e alerta o administrador.
Tarefas 	**Verificação de software malicioso** O Kaspersky Endpoint Security verifica o computador à procura de vírus e outras ameaças. A Verificação de software malicioso ajuda a excluir a possibilidade de espalhar software malicioso que não tenha sido detetado por componentes de proteção, por exemplo, devido a um baixo nível de segurança. **Atualização das bases de dados e módulos da aplicação** O Kaspersky Endpoint Security transfere bases de dados e módulos da aplicação atualizados. A atualização mantém o computador protegido contra vírus e outras ameaças. A aplicação é atualizada automaticamente por predefinição, mas se necessário, pode atualizar as bases de dados e os módulos da aplicação manualmente. **Reverter última atualização** O Kaspersky Endpoint Security reverte a última atualização de bases de dados e módulos. Isto permite-lhe reverter as bases de dados e módulos da aplicação para as suas versões anteriores quando necessário, por exemplo, quando a nova versão da base de dados contém uma assinatura inválida que faz com que o Kaspersky Endpoint Security bloqueie uma aplicação segura. **Verificação de integridade da aplicação** O Kaspersky Endpoint Security verifica se os módulos de aplicação na pasta de instalação de aplicações foram corrompidos ou modificados. Se um módulo de aplicação tiver uma assinatura digital incorreta, o módulo é considerado corrupto.
Encriptação de dados 	**Encriptação ao nível dos ficheiros** O componente permite a criação de regras de encriptação de ficheiros. Pode selecionar pastas predefinidas para encriptação, selecionar uma pasta manualmente ou selecionar ficheiros por extensão. **Encriptação de disco completa** O componente permite a encriptação do disco rígido com a tecnologia de Encriptação de disco Kaspersky ou Encriptação de Unidade BitLocker. **Encriptação de unidades amovíveis** O componente permite a proteção de dados em unidades amovíveis. Pode usar Encriptação de disco completa (FDE) ou Encriptação ao nível dos ficheiros (FLE).

Secção	Componente
Detection and Response 	**Endpoint Detection and Response Optimum** Agente integrado para a solução Kaspersky Endpoint Detection and Response Optimum (doravante também referida como "EDR Optimum"). O *Kaspersky Endpoint Detection and Response* é uma solução para proteger a infraestrutura de TI corporativa contra ciberameaças avançadas. A funcionalidade da solução combina a deteção automática de ameaças com a capacidade de reagir a tais ameaças para neutralizar ataques avançados, incluindo novas explorações, ransomware, ataques sem ficheiros, bem como métodos que utilizam ferramentas legítimas do sistema. Para obter mais informações sobre a solução, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum. **Endpoint Detection and Response Expert** Agente integrado para a solução Kaspersky Endpoint Detection and Response Expert (doravante também referida como "EDR Expert"). O EDR Expert oferece mais funcionalidades de monitorização de ameaças e 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 gerir os componentes Endpoint Detection and Response e Network Detection and Response que fazem parte da solução Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* é uma solução criada para a deteção atempada de ameaças sofisticadas, como ataques direcionados, ameaças persistentes avançadas (APT), ataques de dia zero e outras. 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)*) Pode adquirir todas as unidades funcionais ou unidades funcionais individuais separadamente. Para obter mais informações sobre a solução, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform. **Sandbox** Agente integrado para o Sandbox. O componente *Sandbox* deteta e bloqueia automaticamente ameaças avançadas em computadores. O Sandbox analisa o comportamento do objeto para detetar atividades maliciosas e atividades características de ataques direcionados à infraestrutura de TI da organização. O Sandbox analisa e verifica objetos em servidores especiais com imagens virtuais implementadas de sistemas operativos Microsoft Windows (servidores do Sandbox). Para obter mais informações 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 suportar a operação da solução Kaspersky Managed Detection and Response. A solução *Kaspersky Managed Detection and Response (MDR)* deteta e analisa automaticamente os incidentes de segurança na sua infraestrutura. Para tal, o MDR utiliza dados de telemetria recebidos de terminais e aprendizagem automática. O MDR envia os dados de incidentes aos especialistas da Kaspersky. Os especialistas podem então processar o incidente e, por exemplo, adicionar uma nova entrada às bases de dados de antivírus. Em alternativa, os especialistas podem emitir recomendações sobre o processamento do incidente e, por exemplo, sugerir que o computador seja isolado da rede. Para obter mais informações sobre a utilização da solução, consulte a Ajuda do Kaspersky Managed Detection and Response.

Modos da aplicação: Standard, EDR Agent, Light Agent

O Kaspersky Endpoint Security for Windows faz parte de muitas soluções da Kaspersky. Dependendo da solução, precisa de selecionar um modo para a aplicação.



Modo Padrão

Este é o modo principal e predefinido da aplicação. Pode instalar a aplicação neste modo como parte das soluções Kaspersky EPP (Endpoint Protection Platform). Por exemplo, o Kaspersky Endpoint Security no modo Padrão faz parte do Kaspersky Endpoint Security for Business. O Kaspersky Endpoint Security oferece proteção abrangente de estações de trabalho e servidores contra diversas ameaças, ataques de rede e fraudes. No modo padrão, os agentes integrados também estão disponíveis para integração com as soluções Kaspersky Detection and Response, incluindo EDR, MDR, KUMA e outras.



EDR Agent

Este modo permite implementar soluções Kaspersky Detection and Response juntamente com soluções EPP de terceiros. As soluções Detection and Response incluem o Kaspersky Managed Detection and Response (MDR) e a Kaspersky Anti Targeted Attack Platform (KATA). O Agente EDR também oferece suporte à solução Kaspersky SIEM, Kaspersky Unified Monitoring and Analysis Platform (KUMA).

Neste modo, os componentes de proteção padrão, como a Proteção contra ameaças de ficheiros ou a Proteção contra ameaças da Web, não estão disponíveis. A proteção padrão do computador é fornecida pela solução EPP de terceiros. O Agente EDR monitoriza continuamente os processos em execução nestes computadores, as ligações de rede abertas e os ficheiros que são modificados, além de interagir com as soluções Detection and Response.



Light Agent

Este modo é utilizado 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 operativos convidados para estações de trabalho e servidores. Os mesmos componentes de proteção e controlo estão disponíveis neste modo, tal como no modo Padrão. A diferença é que os objetos são verificados em busca de vírus e outros softwares maliciosos por um componente de solução especial instalado numa máquina virtual separada, SVM (Secure Virtual Machine). Desta forma, o Light Agent utiliza os recursos da 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**

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

- **AES56**

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

- **Arm64**

  Este pacote de distribuição destina-se à instalação em computadores baseados em Arm. Este pacote de distribuição não se destina à instalação em servidores.

Antes da instalação, certifique-se de que o pacote de distribuição corresponde à arquitetura do seu processador. Se o pacote de distribuição não for compatível com a arquitetura do processador, o instalador encerrará a instalação com um erro.

O pacote de distribuição é um arquivo auto-extraível em formato EXE. Para visualizar o conteúdo do pacote de distribuição, tem de extrair o arquivo para uma pasta separada. Cada pacote de distribuição contém os seguintes ficheiros:

`kes_win.msi`	Pacote de instalação do Kaspersky Endpoint Security.
`setup_kes.exe`	Os ficheiros necessários para instalar a aplicação utilizando qualquer um dos métodos disponíveis.
`kes_win.kud`	Ficheiro para criar pacotes de instalação do Kaspersky Endpoint Security.
`klcfginst.msi`	Pacote de instalação para o plug-in de gestão de aplicações na Consola Kaspersky Security Center Administration.
`bases.cab`	Os ficheiros do pacote de atualização que são usados durante a instalação.
`cleaner_v2.cab` `cleanerapi_v2.cab`	Ficheiros para remover o software incompatível.
`incompatible.txt`	Ficheiro que contém a lista de software que pode causar problemas de compatibilidade com o Kaspersky Endpoint Security. A Kaspersky não garante a compatibilidade do Kaspersky Endpoint Security com software da lista.
`ksn_<language ID>.txt`	O ficheiro onde pode ler os termos de participação na Kaspersky Security Network.
`license.txt`	O ficheiro onde pode ler o Contrato de Licença do Utilizador Final e a Privacy Policy.
`installer.ini`	Ficheiro que contém as definições internas do kit de distribuição.
`kes.cab`	Ficheiros para a interface gráfica da aplicação.
`aes256.cab` / `aes56.cab`	Ficheiros para o algoritmo criptográfico AES (não incluídos no pacote de distribuição Arm64).
`package.kcat`	Ficheiro com assinaturas do kit de distribuição da aplicação. A assinatura digital garante a autenticidade e a integridade do kit de distribuição da aplicação.

Não recomendamos a alteração dos valores destas definições. Se quiser alterar as opções de instalação, utilize o ficheiro setup.ini.

Requisitos de hardware e de software

Este artigo enumera as versões de software nas quais a aplicação foi testada e para as quais se garante o seu funcionamento correto. A aplicação poderá também funcionar com outras versões do software, mas essas configurações não foram submetidas a um ciclo completo de testes e não estão incluídas na lista de versões com suporte garantido.

Para garantir o funcionamento correto do Kaspersky Endpoint Security, o computador tem de ter os requisitos seguintes:

Para instalar a aplicação, necessita de direitos de administrador no computador.

Requisitos gerais mínimos

Requisitos mínimos	Estação de trabalho (x86/x64)	Servidor (x86/x64)	Arm
Armazenamento	2 GB	2 GB	2 GB
CPU	Suporte a instruções SSE2 de 1 GHz	Suporte a instruções SSE2 de 1,4 GHz	Arquitetura Armv8.1 de 1 GHz
RAM	Estação de trabalho (x86): 1 GB Estação de trabalho (x64): 2 GB	2 GB Nota: o servidor necessita de 8 GB de memória para instalar a aplicação com um agente incorporado 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 operativos suportados para as estações de trabalho:

- 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 multi-sessão
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-sessão
- Windows 11 for Arm64 Home / Pro / Pro for Workstations / Education / Enterprise

Os sistemas operativos Windows, a partir da versão 11 24H2, suportam a tecnologia UDP Receive Segment Coalescing Offload (URO). A tecnologia é ativada por predefinição se estiver instalada no computador uma placa de rede e controladores compatíveis. A desativação da URO no computador de um utilizador pode reduzir significativamente o desempenho da aplicação.

Para garantir que o Kaspersky Endpoint Security funciona corretamente, o serviço Windows Security Center (wscsvc) tem de estar em execução no computador do utilizador.

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

Para obter detalhes sobre o suporte do sistema operativo do Microsoft Windows 10, por favor refira-se ao Conhecimento de Suporte Técnico.

Para obter detalhes sobre o suporte do sistema operativo do Microsoft Windows 11, por favor refira-se ao Conhecimento de Suporte Técnico.

Servidores

O Kaspersky Endpoint Security suporta os principais componentes da aplicação em computadores com o sistema operativo Windows para servidores. Pode usar o Kaspersky Endpoint Security for Windows em vez do Kaspersky Security for Windows Server em servidores e clusters da sua organização (Cluster Mode). A aplicação também suporta o Server Core Mode (consulte os problemas conhecidos).

Sistemas operativos suportados para servidores:

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

  O Microsoft Small Business Server 2011 Standard (64 bits) só é compatível 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 Foundation/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 as atualizações do sistema operativo instaladas: KB4490628 (12 de março de 2019) e KB4474419 (23 de setembro de 2019).

Para obter detalhes sobre o suporte para o sistema operativo Microsoft Windows Server 2016 e o Microsoft Windows Server 2019, consulte o Base de conhecimento de Suporte Técnico.

Para obter detalhes sobre o suporte do sistema operativo do Microsoft Windows Server 2022, por favor refira-se ao Conhecimento de Suporte Técnico.

Sistemas operativos não suportados 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 suportadas para operação de aplicações no modo padrão:

- VMware Workstation Pro 15.5.2
- Versão de patch do VMware ESXi 7.0 ESXi 7.0b
- Windows Hyper-V Server 2019
- Citrix Virtual Apps and Desktops 7 2009
- Citrix Provisioning 2009
- Citrix Hypervisor 8.2 LTSR

A aplicação suporta máquinas virtuais com o Windows 11 Pro Arm64 criadas através do Hyper-V.

Máquinas virtuais para instalar o Light Agent

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

A BIOS em máquinas virtuais tem de suportar a especificação SMBIOS versão 2.1 ou posterior.

Os seguintes pacotes e utilitários têm de ser instalados nas máquinas virtuais:

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

Consulte a Ajuda do Kaspersky Security for Virtualization Light Agent para conhecer os requisitos de infraestrutura virtual para executar a aplicação no modo Light Agent.

Para que a aplicação funcione corretamente, utilize uma interface de rede virtualizada com uma largura de banda de, pelo menos, 100 Mbit/s.

Servidores terminais

Tipos de servidor de terminal suportados:

- Serviços de Ambiente de Trabalho Remoto da Microsoft baseados no Windows Server 2008 R2 SP1
- Serviços de Ambiente de Trabalho Remoto da Microsoft baseados no Windows Server 2012
- Serviços de Ambiente de Trabalho Remoto da Microsoft baseados no Windows Server 2012 R2
- Serviços de Ambiente de Trabalho Remoto da Microsoft baseados no Windows Server 2016
- Serviços de Ambiente de Trabalho Remoto da Microsoft baseados no Windows Server 2019
- Serviços de Ambiente de Trabalho Remoto da Microsoft baseados no Windows Server 2022
- Serviços de Ambiente de Trabalho Remoto da Microsoft baseados no Windows Server 2025
- Citrix RDSH from Citrix Virtual Apps and Desktops 7 2507 LTSR

Suporte do Kaspersky Security Center

O Kaspersky Endpoint Security suporta o funcionamento 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 das características de aplicação disponíveis dependendo do tipo de sistema operativo

O conjunto de funcionalidades disponíveis no Kaspersky Endpoint Security depende do tipo de sistema operativo: estação de trabalho ou servidor (consulte a tabela abaixo).

A partir do Kaspersky Endpoint Security12.8 for Windows, pode configurar diferentes conjuntos de componentes para diferentes tipos de sistemas operativos no pacote de instalação. Ou seja, pode implementar a aplicação em estações de trabalho e servidores utilizando o mesmo pacote de instalação.

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

Funcionalidade	Estação de trabalho	Estação de trabalho baseada em Arm	Servidor	Modo Server Core
Proteção avançada contra ameaças				
Kaspersky Security Network	✓	✓	✓	✓
Deteção de comportamento	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓
Prevenção de explorações	✓	✓	✓	✓
Prevenção contra invasões	✓	✓	–	–
Motor de remediação	✓	✓	✓	✓
Proteção essencial contra ameaças				
Proteção contra ameaças de ficheiros	✓	✓	✓	✓
Proteção contra ameaças da web	✓	✓	✓	–
Proteção contra ameaças de correio	✓	✓	✓	–
Firewall	✓	✓	✓	✓
Proteção contra ameaças de rede	✓	✓	✓	✓
Prevenção de ataques BadUSB	✓	✓	✓	–
Proteção AMSI	✓	✓	✓	✓
Controlos de segurança				
Inspeção de Registo	–	–	✓	–
Controlo das Aplicações	✓	✓	✓	✓
Controlo de Dispositivos	✓	✓	✓	✓
Controlo de Internet	✓	✓	✓	–
Controlo de Anomalias Adaptativo	✓	✓	–	–
Monitorização da integridade do sistema	–	–	✓	–
Cloud Discovery	✓	✓	–	–
Encriptação de dados				
Encriptação de disco Kaspersky	✓	–	–	–
Encriptação BitLocker de Unidade	✓	✓	✓	✓
Encriptação ao nível dos ficheiros	✓	–	–	–
Encriptação de unidades amovíveis	✓	–	–	–
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 da aplicação, dependendo das ferramentas de gestão

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

Pode gerir a aplicação, utilizando as seguintes consolas do Kaspersky Security Center:

- Consola de Administração. Snap-in da Consola de Gestão Microsoft (MMC) instalado na estação de trabalho do administrador.
- Consola Web. Componente do Kaspersky Security Center instalado no Servidor de Administração. Pode trabalhar na Web Console utilizando um navegador em qualquer computador.

Pode gerir a aplicação, utilizando a Consola de Nuvem do Kaspersky Security Center. A *consola de nuvem do Kaspersky Security Center* é a versão de nuvem do Kaspersky Security Center. Isso significa que o Servidor de Administração e outros componentes do Kaspersky Security Center estão instalados na infraestrutura de nuvem da Kaspersky. Para obter mais informações sobre a gestão da aplicação utilizando a Cloud Console do Kaspersky Security Center, consulte a Ajuda da Cloud Console do Kaspersky Security Center.

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

Comparação das funcionalidades do Kaspersky Endpoint Security

Funcionalidade	Kaspersky Security Center		Kaspersky Security Center
	Consola de Administração	Consola Web	Consola de Nuvem
Proteção avançada contra ameaças			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Deteção de comportamento	✓	✓	✓
Anti-Cryptor			
Prevenção de explorações	✓	✓	✓
Prevenção contra invasões	✓	✓	✓
Motor de remediação	✓	✓	✓
Proteção essencial contra ameaças			
Proteção contra ameaças de ficheiros	✓	✓	✓
Proteção contra ameaças da web	✓	✓	✓
Proteção contra ameaças de correio	✓	✓	✓
Firewall	✓	✓	✓
Proteção contra ameaças de rede	✓	✓	✓
Prevenção de ataques BadUSB	✓	✓	✓
Proteção AMSI	✓	✓	✓

Funcionalidade	Kaspersky Security Center		Kaspersky Security Center
	Consola de Administração	Consola Web	Consola de Nuvem
Controlos de segurança			
Inspeção de Registo	✓	✓	✓
Controlo das Aplicações	✓	✓	✓
Controlo de Dispositivos	✓	✓	✓
Controlo de Internet	✓	✓	✓
Controlo de Anomalias Adaptativo	✓	✓	✓
Monitorização da integridade do sistema	✓	✓	✓
Cloud Discovery	–	–	✓
Encriptação de dados			
Encriptação de disco Kaspersky	✓	✓	–
Encriptação BitLocker de Unidade	✓	✓	✓
Encriptação ao nível dos ficheiros	✓	✓	–
Encriptação de unidades amovíveis	✓	✓	–
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 da aplicação	✓	✓	✓
Inventário	✓	✓	✓
Atualizar	✓	✓	✓
Reverter atualização	✓	✓	✓
Verificação de software malicioso	✓	✓	✓
Verificação de integridade da aplicação	✓	✓	–
Eliminar dados	✓	✓	✓
Gestão das contas de Agente de Autenticação (Encriptação de disco Kaspersky)	✓	✓	–
Verificação IOC (EDR)	–	✓	✓
Mover ficheiro para a Quarentena (EDR)	–	✓	✓
Obter ficheiro (EDR)	–	✓	✓
Eliminar ficheiro (EDR)	–	✓	✓
Iniciar processo (EDR)	–	✓	✓
Terminar processo (EDR)	–	✓	✓

Compatibilidade com outras aplicações

O Kaspersky Endpoint Security é incompatível com algumas aplicações da Kaspersky, bem como com algumas aplicações de terceiros. Assim, antes de instalar, atualizar a versão da aplicação e alterar os componentes da aplicação, o Kaspersky Endpoint Security verifica o computador para ver se alguma destas aplicações está presente.

Compatibilidade com aplicações de terceiros

O Kaspersky Endpoint Security é incompatível com aplicações que fazem parte de sistemas de proteção de pontos finais de terceiros (Endpoint Protection Platform, EPP). O Kaspersky Endpoint Security também pode ter problemas de compatibilidade com outras aplicações. Para determinar a compatibilidade, o Kaspersky Endpoint Security consulta uma lista de software preparada pela Kaspersky. Esta lista encontra-se no ficheiro incompatible.txt. O ficheiro está incluído no kit de distribuição.

A Kaspersky não garante a compatibilidade do Kaspersky Endpoint Security com software da lista. Se uma aplicação da lista for descoberta, o instalador interrompe a implementação do Kaspersky Endpoint Security. O instalador pode eliminar automaticamente algumas aplicações da lista. Se estiver disposto a desconsiderar os riscos e quiser instalar o Kaspersky Endpoint Security e um software da lista no mesmo computador, poderá ignorar a verificação do computador (consulte as instruções abaixo).

TRANSFERIR O FICHEIRO INCOMPATIBLE.TXT

Compatibilidade com aplicações da Kaspersky

O Kaspersky Endpoint Security não é compatível com as seguintes aplicações 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 a trocar todo o 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, a aplicação suporta todas as soluções de Detection and Response.

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

  A partir do Kaspersky Endpoint Security 12.0, pode migrar do Kaspersky Security for Windows Server para o Kaspersky Endpoint Security for Windows e utilizar uma única solução para proteger estações de trabalho e servidores.

- Kaspersky Embedded Systems Security.

Se as aplicações da Kaspersky desta lista estiverem instaladas no computador, o Kaspersky Endpoint Security remove-as. Aguarde pela conclusão deste processo antes de continuar a instalação do Kaspersky Endpoint Security.

Ignorar a verificação de software que pode causar problemas de compatibilidade

Se o Kaspersky Endpoint Security detetar software da lista incompatible.txt, a instalação da aplicação será terminada. Para continuar a instalação, tem de remover essa aplicação. Contudo, se o fornecedor de software de terceiros tiver indicado na sua documentação que o seu software é compatível com a Endpoint Protection Platform (EPP), pode instalar o Kaspersky Endpoint Security num computador que tenha uma aplicação deste fornecedor. Por exemplo, o fornecedor da solução Endpoint Detection and Response (EDR) pode declarar a sua compatibilidade com sistemas EPP de terceiros. Se for este o caso, tem de iniciar a instalação do Kaspersky Endpoint Security sem executar uma verificação de software instalado. Para o fazer, passe 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 ficheiro incompatible.txt que está incluído no kit de distribuição. Se nenhum valor for definido para este parâmetro e for detetado software da lista, a instalação do Kaspersky Endpoint Security será cancelada.

- `SKIPPRODUCTUNINSTALL=1` Desative a remoção automática de software detetado 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 das aplicações encontradas pelo cheque. Se este parâmetro não for definido, a verificação de assinaturas digitais será desativada ao implementar a aplicação através do Kaspersky Security Center. Quando a aplicação é instalada localmente, a verificação da assinatura digital é ativada por defeito.

Pode passar parâmetros na linha de comandos ao instalar localmente a aplicação.

Se durante o processo de instalação tiver ignorado a verificação de software que pode causar problemas de compatibilidade, o Kaspersky Endpoint Security pode realizar esta verificação novamente quando os componentes da aplicação forem alterados. Para ignorar a verificação de software instalado, tem de configurar a tarefa *Alterar componentes da aplicação*.

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, tem de adicionar os parâmetros apropriados ao ficheiro de geração do pacote de instalação com o nome `kes_win.kud` em `[Setup]` (veja abaixo). O ficheiro `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 a aplicação

O Kaspersky Endpoint Security pode ser instalado num computador de várias formas:

- localmente, usando o Assistente de Configuração.
- localmente a partir da command line.
- remotamente, usando o Kaspersky Security Center.
- remotamente, através do Microsoft Windows Group Policy Management Editor (para obter mais detalhes, visite o Website de Suporte Técnico da Microsoft).
- remotamente, usando o System Center Configuration Manager.

Pode definir as definições de instalação da aplicação de várias maneiras. Se usar simultaneamente vários métodos para configurar as definições, o Kaspersky Endpoint Security aplicará as definições com a prioridade mais elevada. O Kaspersky Endpoint Security usa a seguinte ordem de prioridades:

1. Definições recebidas do ficheiro setup.ini.
2. Definições recebidas do ficheiro installer.ini.
3. Definições recebidas da linhas de comandos.
4. Definições recebidas do ficheiro de configuração (install.cfg).

Recomendamos que feche todas as aplicações em funcionamento antes de iniciar a instalação do Kaspersky Endpoint Security (incluindo a instalação remota).

Ao instalar o Kaspersky Endpoint Security, o sistema operativo pode mostrar as suas próprias mensagens. As ligações à rede e à Internet também podem ser interrompidas quando a aplicação está a ser instalada.

Ao instalar, se atualizar ou desinstalar o Kaspersky Endpoint Security, poderão ocorrer erros. Para obter mais informações sobre como solucionar esses erros, consulte o Base de conhecimento de Suporte Técnico.

Implementação através do Kaspersky Security Center

O Kaspersky Endpoint Security pode ser implementado em computadores numa rede corporativa de vários modos. Pode escolher o cenário de implementação mais adequado para a sua organização ou combinar vários cenários de implementação simultaneamente. Antes de instalar a aplicação, tem de se certificar de que o Kaspersky Security Center Network Agent está instalado no computador. O *Agente de Rede* facilita a interação entre o Servidor de administração e um computador do cliente.

O Kaspersky Security Center suporta os seguintes principais métodos de implementação:

- Instalar a aplicação utilizando o Assistente de Implementação da Proteção.

  O método de instalação padrão é conveniente se estiver satisfeito com as predefinições Kaspersky Endpoint Security e a sua organização tem uma infraestrutura simples que não necessita configurações especiais.

- Instalar a aplicação utilizando a tarefa de instalação remota.

  O método de instalação universal que permite configurar as definições do Kaspersky Endpoint Security e gira flexivelmente as tarefas de instalação remota. A instalação do Kaspersky Endpoint Security é constituído pelos seguintes passos:

  1. Create installation package.
  2. Criar uma tarefa de instalação remota.

O Kaspersky Security Center suporta também outros métodos de instalação do Kaspersky Endpoint Security, como a implementação numa imagem do sistema operativo. Para obter mais informações sobre a hierarquia da política, consulte o Guia de Ajuda do Kaspersky Security Center.

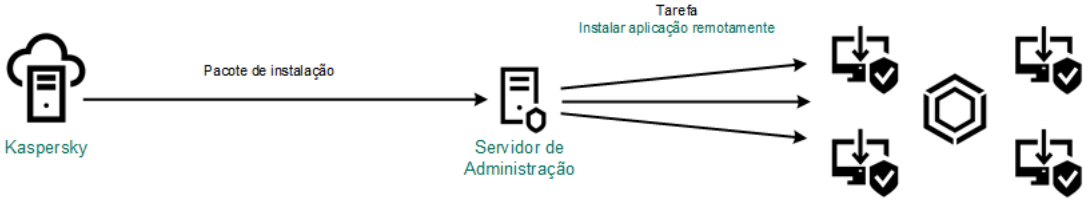
Instalação padrão da aplicação

O Kaspersky Security Center disponibiliza um Assistente de Implementação da Proteção para instalar a aplicação em computadores corporativos. O Assistente de Implementação da Proteção inclui as seguintes ações principais:

1. Selecionar um pacote de distribuição do Kaspersky Endpoint Security.

   Um *pacote de instalação* é um conjunto de ficheiros criados para a instalação remota de uma aplicação da Kaspersky através do Kaspersky Security Center. O pacote de instalação contém uma gama de definições necessárias para instalar a aplicação e colocá-la em funcionamento imediatamente após a instalação. O pacote de instalação é criado utilizando ficheiros com as extensões .kpd e .kud incluídas no kit de distribuição da aplicação. O pacote de instalação do Kaspersky Endpoint Security é comum para todas as versões suportadas de sistemas operativos Windows e tipos de arquitetura de processador.

2. Criar a tarefa *Install application remotely* do Servidor de administração do Kaspersky Security Center.



Implementação do Kaspersky Endpoint Security

Como executar o Assistente de Implementação da Proteção na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Advanced** → **Remote installation**.
3. Clique na hiperligação **Deploy installation package on managed devices (workstations)**.

Isto iniciará o Assistente de Implementação da Proteção. Siga as instruções do Assistente.

As portas TCP 139 e 445 e as portas UDP 137 e 138 devem estar abertas num computador do cliente.

Passo 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, pode criar o pacote no Assistente.

Pode configurar as definições do pacote de instalação no Kaspersky Security Center. Por exemplo, pode selecionar os componentes da aplicação que serão instalados num computador.

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

Passo 2. Selecionar a origem do pacote de instalação

Selecione a origem **Deploy Kaspersky Security Center package**.

Passo 3. Selecionar dispositivos para instalação

Selecione os computadores para instalar o Kaspersky Endpoint Security. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. O Agente de Rede não é instalado em Install application remotely. Neste caso, a tarefa é atribuída a dispositivos específicos. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 4. Definir as definições da tarefa de instalação remota

Configure as seguintes definições adicionais da aplicação:

- **Force installation package download**. Selecionar o método de instalação da aplicação:
  - **Using Network Agent**. O Agente de Rede é responsável por entregar o pacote de instalação do Kaspersky Endpoint Security aos computadores clientes. Se o Agente de Rede não estiver instalado, a tarefa será terminada com um erro. Neste caso, adicione o pacote de instalação do Agente de Rede à tarefa *Install application remotely* e ative a entrega de ficheiros através dos recursos do sistema operativo. Em seguida, o Agente de Rede será instalado utilizando recursos do sistema operativo. O Kaspersky Endpoint Security é então instalada pelas ferramentas do Agente de Rede.
  - **Using operating system resources through distribution points**. O pacote de instalação é transmitido aos computadores do cliente utilizando recursos do sistema operativo através de pontos de distribuição. Pode selecionar esta opção se houver pelo menos um ponto de distribuição na rede. Para obter mais informação detalhadas sobre os pontos de distribuição, consulte a Ajuda do Kaspersky Security Center.
  - **Using operating system resources through Administration Server**. Os ficheiros serão entregues o computadores cliente utilizando os recursos do sistema operativo através do Servidor de administração. Pode selecionar esta opção se nenhum Agente de Rede for instalado no computador cliente, mas o computador cliente está na mesma rede que o Servidor de administração.
- **Behavior for devices managed through other Administration Servers**. Selecionar o método de instalação do Kaspersky Endpoint Security. Se a rede tiver mais do que um Servidor de administração instalado, estes Servidores de administração podem ver os mesmos computadores do cliente. Isto pode levar a que, por exemplo, uma aplicação seja instalada remotamente no mesmo computador do cliente múltiplos vezes através de diferentes Servidores de administração ou outros conflitos.
- **Do not re-install application if it is already installed**. Limpe esta caixa de verificação se quiser instalação uma versão anterior da aplicação, por exemplo.
- **Assign Network Agent installation in Active Directory group policies**. Instalar manualmente o Agente de Rede utilizando recursos do Diretório Ativo. Para instalar o Agente de Rede, a tarefa de instalação remota deve ser executada com privilégios de administrador de domínio.

Passo 5. Selecionar uma chave de licença

Adicione uma chave ao pacote de instalação para ativar a aplicação. Este passo é opcional. Se o Servidor de administração tiver uma chave de licença com a funcionalidade de distribuição automática, a chave será adicionada automaticamente posteriormente. Pode também ativar a aplicação posteriormente utilizando a tarefa *Add key*.

Passo 6. Selecionar a definição de reinicialização do sistema operativo

Selecione a ação que deve ser executada se for necessário um reinício de computador. Reinicio não é necessário ao instalar o Kaspersky Endpoint Security. O reinicio é necessário apenas se precisar de remover aplicações incompatíveis antes da instalação. Reinício pode também ser necessário ao atualizar a versão da aplicação.

Passo 7. Remover aplicações incompatíveis antes de instalar a aplicação

Leia cuidadosamente a lista de aplicações incompatíveis e permita a remoção destas aplicações. Se forem instaladas aplicações incompatíveis no computador, a instalação do Kaspersky Endpoint Security termina com um erro.

Passo 8. Selecionar uma conta para aceder a dispositivos

Selecione a conta para instalar o Agente de Rede utilizando as ferramentas do sistema operativo. Neste caso, os direitos de administrador são necessitados para o acesso do computador. Pode adicionar múltiplas contas. Se uma conta não tiver direitos suficientes, o Assistente de Instalação utiliza a conta seguinte. Não tem de selecionar uma conta se instalar o Kaspersky Endpoint Security utilizando ferramentas do Agente de Rede.

Passo 9. Iniciar a instalação

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa.

Como iniciar o Assistente de Implementação de Proteção na Consola da Web e na Consola da Nuvem

Na janela principal da Consola Web, selecione **Discovery & deployment** → **Deployment & assignment** → **Protection deployment wizard**.

Isto iniciará o Assistente de Implementação da Proteção. Siga as instruções do Assistente.

As portas TCP 139 e 445 e as portas UDP 137 e 138 devem estar abertas num computador do cliente.

Passo 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, pode criar o pacote no Assistente. Para criar o pacote de instalação, não precisa procurar o pacote de distribuição e guardá-lo na memória do computador. No Kaspersky Security Center, pode consultar a lista de pacotes de distribuição existentes nos servidores da Kaspersky, e o pacote de instalação é criado automaticamente. A Kaspersky atualiza a lista após o lançamento de novas versões de aplicações.

Pode configurar as definições do pacote de instalação no Kaspersky Security Center. Por exemplo, pode selecionar os componentes da aplicação que serão instalados num computador.

Passo 2. Selecionar uma chave de licença

Adicione uma chave ao pacote de instalação para ativar a aplicação. Este passo é opcional. Se o Servidor de administração tiver uma chave de licença com a funcionalidade de distribuição automática, a chave será adicionada automaticamente posteriormente. Pode também ativar a aplicação posteriormente utilizando a tarefa *Add key*.

Passo 3. Selecionar um Agente de Rede

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

Passo 4. Selecionar dispositivos para instalação

Selecione os computadores para instalar o Kaspersky Endpoint Security. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. O Agente de Rede não é instalado em Install application remotely. Neste caso, a tarefa é atribuída a dispositivos específicos. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 5. Configurar definições avançadas

Configure as seguintes definições adicionais da aplicação:

- **Force installation package download**. Selecionar o método de instalação da aplicação:
  - **Using Network Agent**. O Agente de Rede é responsável por entregar o pacote de instalação do Kaspersky Endpoint Security aos computadores clientes. Se o Agente de Rede não estiver instalado, a tarefa será terminada com um erro. Neste caso, adicione o pacote de instalação do Agente de Rede à tarefa *Install application remotely* e ative a entrega de ficheiros através dos recursos do sistema operativo. Em seguida, o Agente de Rede será instalado utilizando recursos do sistema operativo. O Kaspersky Endpoint Security é então instalada pelas ferramentas do Agente de Rede.
  - **Using operating system resources through distribution points**. O pacote de instalação é transmitido aos computadores do cliente utilizando recursos do sistema operativo através de pontos de distribuição. Pode selecionar esta opção se houver pelo menos um ponto de distribuição na rede. Para obter mais informação detalhadas sobre os pontos de distribuição, consulte a Ajuda do Kaspersky Security Center.
  - **Using operating system resources through Administration Server**. Os ficheiros serão entregues o computadores cliente utilizando os recursos do sistema operativo através do Servidor de administração. Pode selecionar esta opção se nenhum Agente de Rede for instalado no computador cliente, mas o computador cliente está na mesma rede que o Servidor de administração.
- **Do not re-install application if it is already installed**. Limpe esta caixa de verificação se quiser instalação uma versão anterior da aplicação, por exemplo.
- **Assign package installation in Active Directory group policies**. O Kaspersky Endpoint Security é instalado através do Agente de Rede ou manualmente através do Diretório Ativo. Para instalar o Agente de Rede, a tarefa de instalação remota deve ser executada com privilégios de administrador de domínio.

Passo 6. Selecionar a definição de reinicialização do sistema operativo

Selecione a ação que deve ser executada se for necessário um reinício de computador. Reinicio não é necessário ao instalar o Kaspersky Endpoint Security. O reinicio é necessário apenas se precisar de remover aplicações incompatíveis antes da instalação. Reinício pode também ser necessário ao atualizar a versão da aplicação.

Passo 7. Remover aplicações incompatíveis antes de instalar a aplicação

Leia cuidadosamente a lista de aplicações incompatíveis e permita a remoção destas aplicações. Se forem instaladas aplicações incompatíveis no computador, a instalação do Kaspersky Endpoint Security termina com um erro.

Passo 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 de ser movidos para um grupo de administração para que as políticas e tarefas de grupo possam ser aplicadas. Se um computador já estiver num qualquer grupo de administração, o computador não será movido. Se não selecionar um grupo de administração, os computadores serão adicionados ao grupo de **Unassigned devices**.

Passo 9. Selecionar uma conta para aceder a dispositivos

Selecione a conta para instalar o Agente de Rede utilizando as ferramentas do sistema operativo. Neste caso, os direitos de administrador são necessitados para o acesso do computador. Pode adicionar múltiplas contas. Se uma conta não tiver direitos suficientes, o Assistente de Instalação utiliza a conta seguinte. Não tem de selecionar uma conta se instalar o Kaspersky Endpoint Security utilizando ferramentas do Agente de Rede.

Passo 10. Iniciar instalação

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa.

Criar um pacote de instalação

Um *pacote de instalação* é um conjunto de ficheiros criados para a instalação remota de uma aplicação da Kaspersky através do Kaspersky Security Center. O pacote de instalação contém uma gama de definições necessárias para instalar a aplicação e colocá-la em funcionamento imediatamente após a instalação. O pacote de instalação é criado utilizando ficheiros com as extensões .kpd e .kud incluídas no kit de distribuição da aplicação. O pacote de instalação do Kaspersky Endpoint Security é comum para todas as versões suportadas de sistemas operativos Windows e tipos de arquitetura de processador.

Como criar um pacote de instalação na Consola de Administração (MMC)

1. Na Consola de administração, aceda à pasta **Administration Server** → **Advanced** → **Remote installation** → **Installation packages**.

   Isto abre uma lista de pacotes de instalação que foram transferidos para o Kaspersky Security Center.

2. Clique em **Create installation package**.

O Assistente de Novo Pacote é iniciado. Siga as instruções do Assistente.

Passo 1. Selecionar o tipo de pacote de instalação

selecione a opção **Create an installation package for a Kaspersky application**.

Passo 2. Definir o nome do pacote de instalação

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

Passo 3. Selecionar o pacote de distribuição para instalação

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

Se necessário, atualize as bases de dados antivírus no pacote de instalação utilizando a caixa de verificação **Copy updates from repository to installation package**.

Passo 4. Contrato de Licença do Utilizador Final e Política de Privacidade

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

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

Nas definições do pacote de instalação, pode selecionar componentes de aplicação para diferentes tipos de sistemas operativos. Ou seja, o pacote de instalação inclui dois conjuntos de componentes: para estações de trabalho e para servidores. Antes de implementar o pacote de instalação, o instalador deteta o tipo de sistema operativo e instala apenas os componentes de aplicação que selecionou para esse tipo de sistema operativo. Desta forma, pode utilizar o mesmo pacote de instalação para estações de trabalho e servidores.

O pacote de instalação inclui bases de dados de antivírus do repositório do Servidor de Administração. Pode atualizar as bases de dados no pacote de instalação para reduzir o consumo de tráfego quando atualizar as bases de dados depois de instalar o Kaspersky Endpoint Security.

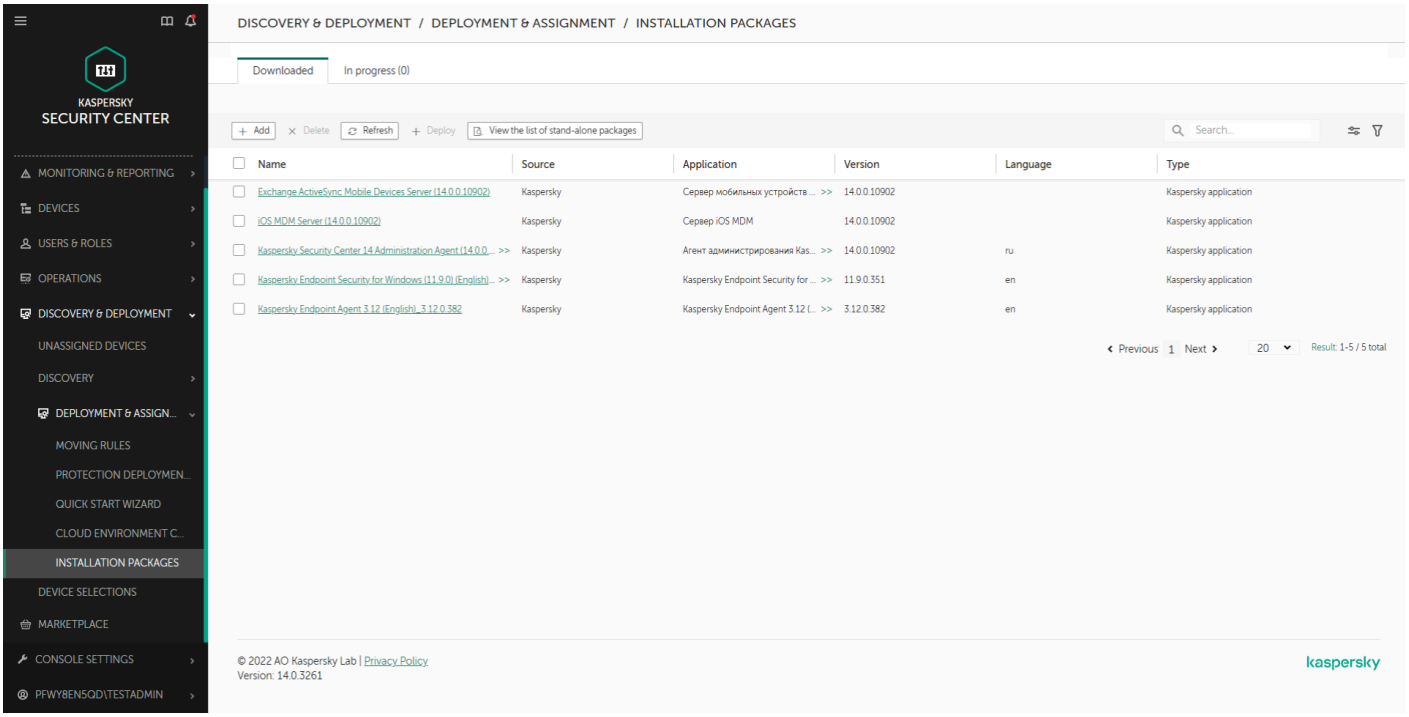
Como criar um pacote de instalação na Web Console

1. Na janela principal da Consola Web, selecione **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.

   Isto abre uma lista de pacotes de instalação que foram transferidos para o Kaspersky Security Center.

2. Clique em **Add**.

O Assistente de Novo Pacote é iniciado. Siga as instruções do Assistente.



Lista de pacotes de instalação

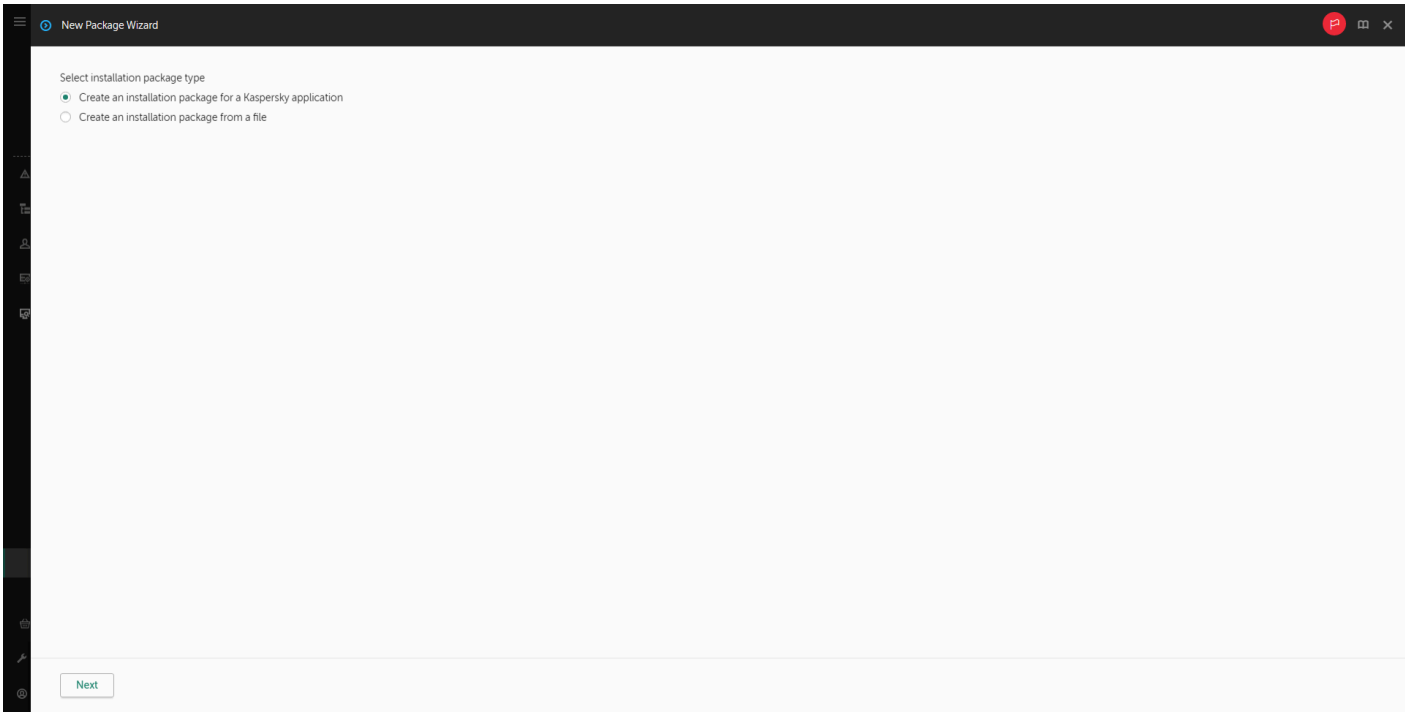
Passo 1. Selecionar o tipo de pacote de instalação

selecione a opção **Create an installation package for a Kaspersky application**.

O Assistente criará um pacote de instalação a partir do pacote de distribuição existente nos servidores da Kaspersky. A lista é atualizada automaticamente à medida que são lançadas novas versões das aplicações. Recomenda-se a seleção desta opção para a instalação do Kaspersky Endpoint Security.

Pode também criar um pacote de instalação a partir de um ficheiro.

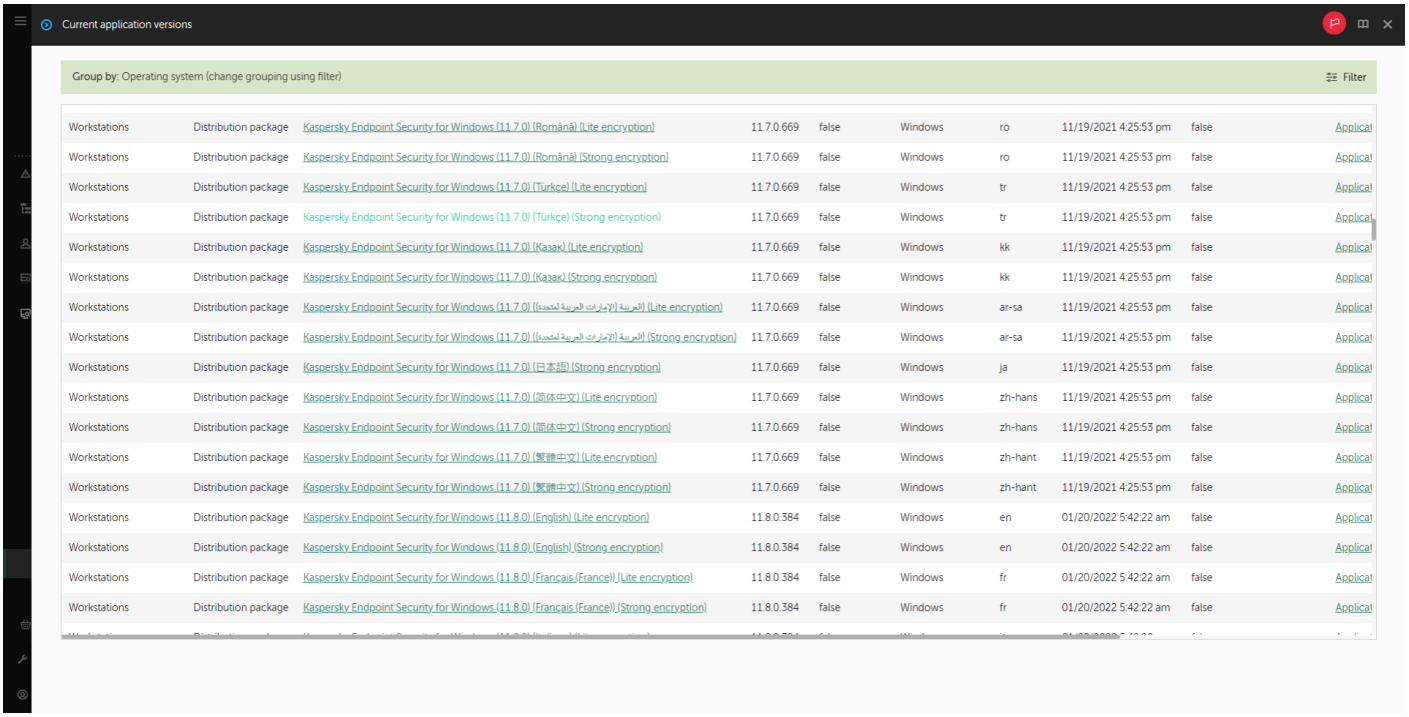
A criação de um pacote de instalação do Kaspersky Endpoint Security a partir de um ficheiro apenas está disponível no Kaspersky Security Center Web Console.



Tipos de pacotes de instalação

Passo 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, deve aceitar os termos do Contrato de Licença do Utilizador Final e da Privacy Policy.



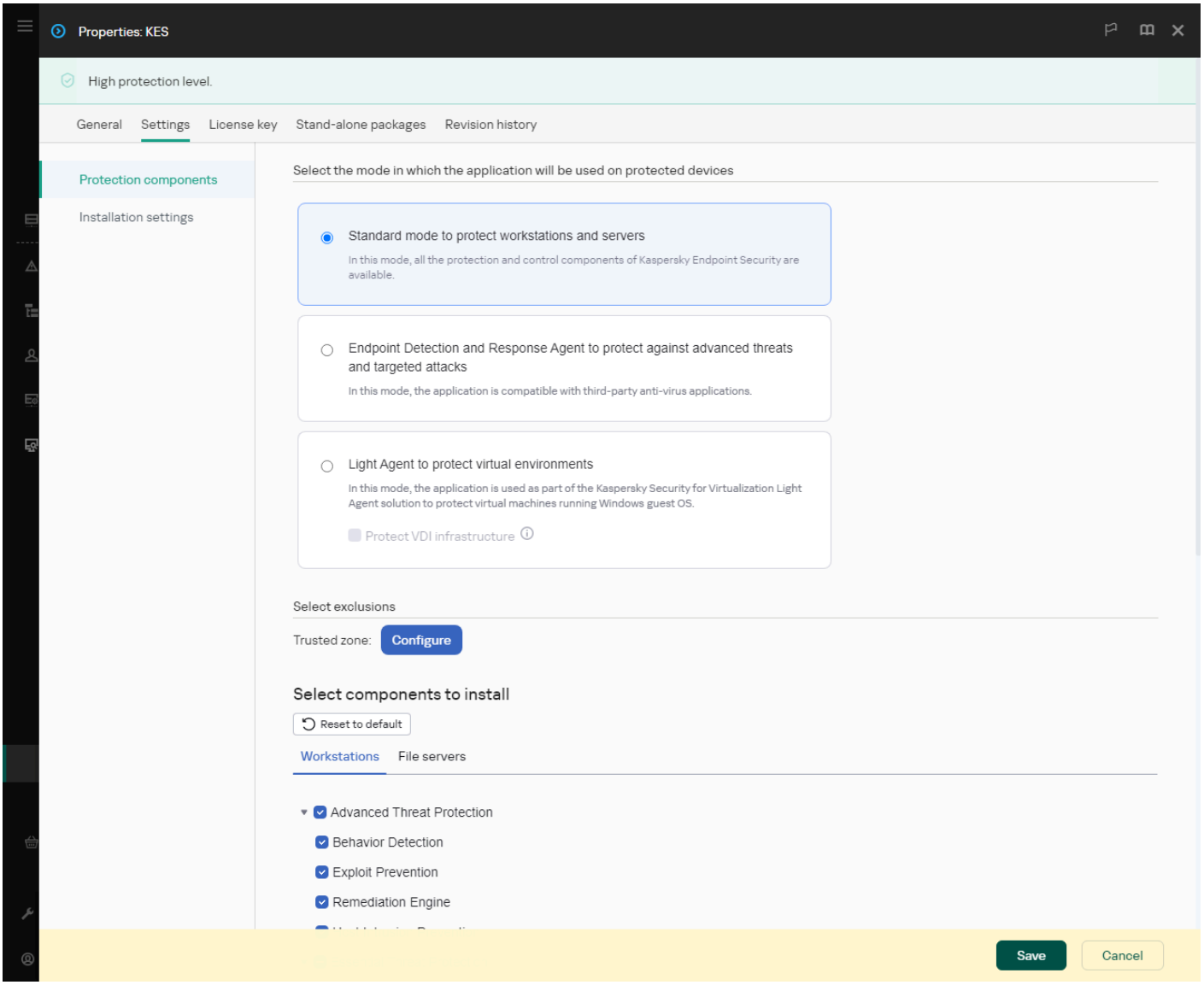
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Română) (Lite encryption)	11.7.0.669	false	Windows	ro	11/19/2021 4:25:53 pm	false
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Română) (Strong encryption)	11.7.0.669	false	Windows	ro	11/19/2021 4:25:53 pm	false
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
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
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Қазақ) (Lite encryption)	11.7.0.669	false	Windows	kk	11/19/2021 4:25:53 pm	false
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Қазақ) (Strong encryption)	11.7.0.669	false	Windows	kk	11/19/2021 4:25:53 pm	false
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
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
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
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
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
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
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
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
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
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
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

Lista de pacotes de instalação nos servidores da Kaspersky

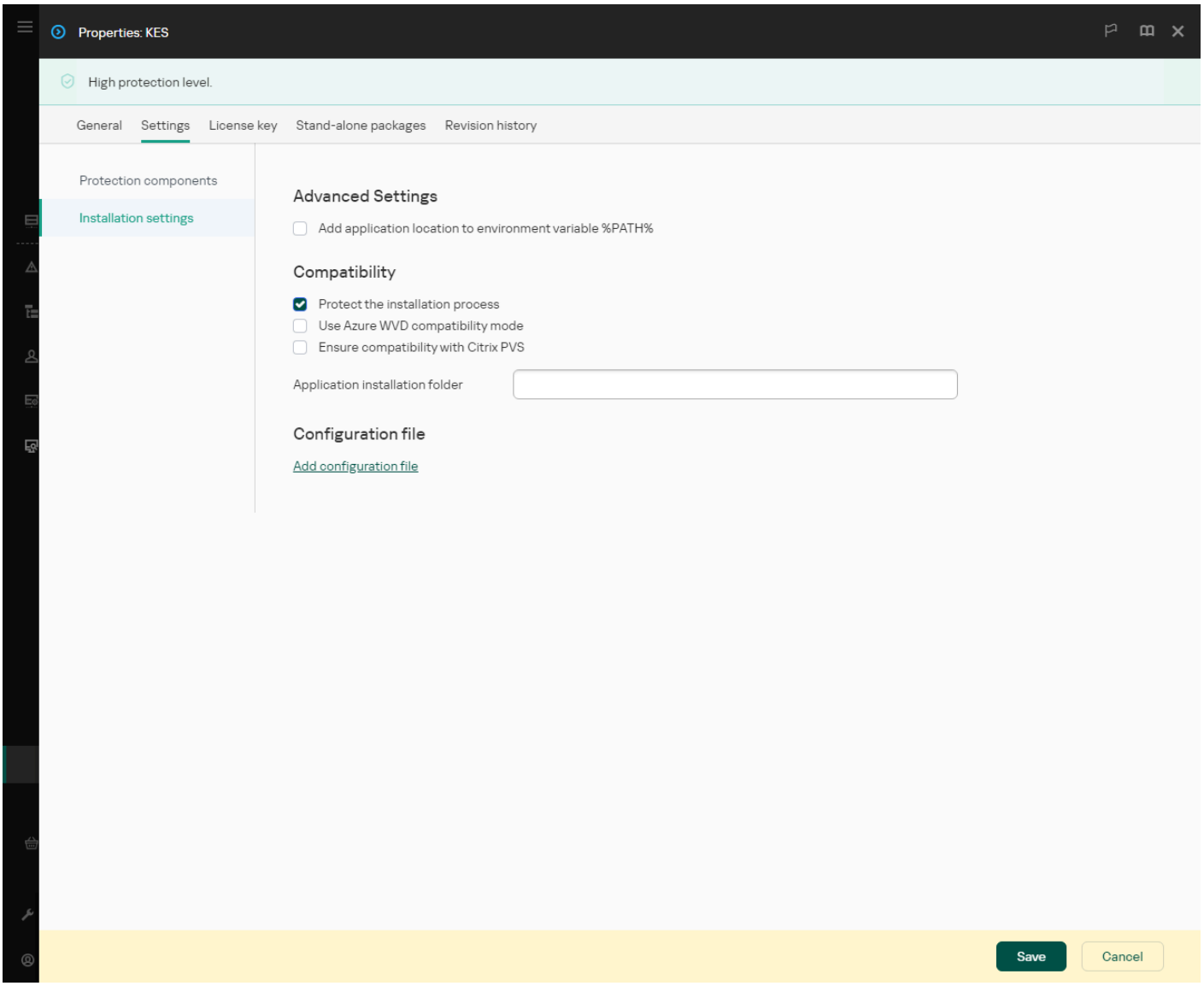
O pacote de instalação será criado e adicionado ao Kaspersky Security Center. Utilizando o pacote de instalação, pode instalar o Kaspersky Endpoint Security em computadores da rede corporativa ou atualizar a versão da aplicação.

Nas definições do pacote de instalação, pode selecionar componentes de aplicação para diferentes tipos de sistemas operativos. Ou seja, o pacote de instalação inclui dois conjuntos de componentes: para estações de trabalho e para servidores. Antes de implementar o pacote de instalação, o instalador deteta o tipo de sistema operativo e instala apenas os componentes de aplicação que selecionou para esse tipo de sistema operativo. Desta forma, pode utilizar o mesmo pacote de instalação para estações de trabalho e servidores.

O pacote de instalação inclui bases de dados de antivírus do repositório do Servidor de Administração. Pode atualizar as bases de dados no pacote de instalação para reduzir o consumo de tráfego quando atualizar as bases de dados depois de instalar o Kaspersky Endpoint Security.



Componentes incluídos no pacote de instalação



Definições de instalação do pacote de instalação

Definições do pacote de instalação

Secção	Descrição
Componentes de proteção	**Modo Padrão**. A configuração predefinida. Esta configuração permite utilizar todos os componentes da aplicação, incluindo componentes que fornecem suporte para soluções de Detection and Response. Esta configuração é utilizada para proteção abrangente do computador contra diversas ameaças, ataques de rede e fraudes. **Endpoint Detection and Response Agent**. Nesta configuração, só é possível instalar os componentes que fornecem suporte para soluções Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) e KUMA. Esta configuração será necessária se uma Endpoint Protection Platform (EPP) de terceiros for implementada na sua organização em conjunto com uma solução de Detection and Response da Kaspersky. Isso torna o Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent compatível com aplicações EPP de terceiros. **Light Agent para proteger ambientes virtuais**. Esta configuração destina-se à aplicação que é usada como parte da solução Kaspersky Security for Virtualization Light Agent. O Light Agent tem de ser instalado em cada máquina virtual que precisa de ser protegida usando a solução. Nesta configuração, não pode utilizar componentes de Encriptação de Dados ou Controlo de Anomalias Adaptativo. Se estiver a instalar o Light Agent num modelo de máquina virtual que será usado para criar *máquinas virtuais não persistentes*, selecione a caixa de verificação **Proteger a 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. Neste modo, o Light Agent recusa atualizações de aplicações que exigem o reinício da máquina virtual. Ao receber atualizações de aplicações que exigem um reinício, o Light Agent gera um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas.
Exclusões	A partir do Kaspersky Endpoint Security 12.6 para Windows, as exclusões de verificação e as aplicações fiáveis são adicionadas à zona fiável. Exclusões de verificação predefinidas e aplicações fiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e System Center Configuration Manager. Isto significa que não é necessário configurar manualmente uma zona fiável para a aplicação nos servidores. A partir do Kaspersky Endpoint Security 12.8 para Windows, pode instalar aplicação no modo Light Agent para proteger ambientes virtuais. As exclusões de verificação predefinidas e as aplicações fiáveis podem ajudá-lo a configurar rapidamente o Kaspersky Endpoint Security em ambientes virtuais Citrix e VMware. Também pode configurar a zona fiável mais tarde nas propriedades da política: exclusões de verificação e aplicações fiáveis.

Secção	Descrição
Selecionar componentes a instalar	Nesta secção, pode selecionar os componentes da aplicação que estarão disponíveis. Pode alterar o conjunto de componentes da aplicação mais tarde utilizando a tarefa *Alterar componentes da aplicação*. Pode criar conjuntos de componentes separados para estações de trabalho e servidores. Antes de implementar o pacote de instalação, o instalador deteta o tipo de sistema operativo e instala apenas os componentes de aplicação que selecionou para esse tipo de sistema operativo. Desta forma, pode utilizar o mesmo pacote de instalação para estações de trabalho e servidores. O conjunto de componentes disponíveis depende da configuração da aplicação: **Modo Padrão** A Encriptação de dados da Kaspersky, a Encriptação ao nível dos ficheiros e todos os agentes incorporados, exceto o EDR Optimum, não são instalados por predefinição. Estes componentes podem ser adicionados nas definições do pacote de instalação. **Endpoint Detection and Response Agent** Nesta definição, estão disponíveis apenas agentes integrados para soluções Kaspersky Detection and Response. **Light Agent para proteger ambientes virtuais** Nesta configuração, pode utilizar quase todos os componentes de aplicação que estão disponíveis na configuração **Modo Padrão**, exceto os componentes de encriptação de dados e o Controlo de Anomalias Adaptativo.
License key	Nesta secção, pode ativar a aplicação. Para ativar a aplicação, deve selecionar uma chave da licença. Antes de fazer isso, deve adicionar a chave ao Servidor de Administração. Para obter informações detalhadas adicionais sobre a adição de chaves do Servidor de administração do Kaspersky Security Center, consulte a Ajuda do Kaspersky Security Center.
Incompatible applications	Leia cuidadosamente a lista de aplicações incompatíveis e permita a remoção destas aplicações. Se forem instaladas aplicações incompatíveis no computador, a instalação do Kaspersky Endpoint Security termina com um erro.
Installation settings	**Adicione o caminho para o ficheiro avp.com à variável de sistema %PATH%**. Pode adicionar o caminho de instalação à variável %PATH% para utilização conveniente da interface da linha de comando. **Protect the installation process**. A proteção de instalação inclui a proteção contra a substituição do pacote de distribuição com aplicações maliciosas, bloqueando o acesso à pasta de instalação do Kaspersky Endpoint Security, e bloqueando o acesso à secção do registo do sistema contendo as chaves da aplicação. Contudo, se não for possível instalar a aplicação (por exemplo, ao executar uma instalação remota com a ajuda do Windows Remote Desktop), recomendamos que desative a proteção do processo de instalação. **Garanta a compatibilidade com Citrix PVS**. Pode ativar o suporte dos Citrix Provisioning Services para instalar o Kaspersky Endpoint Security numa máquina virtual. **Utilizar o modo de compatibilidade do Azure WVD**. Esta funcionalidade garante a exibição correta do estado da máquina virtual do Azure na consola da Kaspersky Anti Targeted Attack Platform. Para monitorizar o desempenho do computador, o Kaspersky Endpoint Security envia telemetria aos servidores KATA. A telemetria inclui um ID do computador (Sensor ID). O modo de compatibilidade do Azure WVD permite atribuir um Sensor ID único permanente a estas máquinas virtuais. Se o modo de compatibilidade estiver desativado, o Sensor ID poderá mudar depois de o computador ser reiniciado devido ao funcionamento das máquinas virtuais do Azure. Isto pode fazer com que os duplicados das máquinas virtuais apareçam na consola. **Application installation folder**. Pode alterar o caminho de instalação do Kaspersky Endpoint Security num computador de cliente. Por predefinição, a aplicação é instalada na pasta `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.2`. **Configuration file**. Instalar a aplicação com configurações predefinidas. Para o fazer, tem de carregar um ficheiro que define as definições do Kaspersky Endpoint Security. Pode criar um ficheiro de configuração na interface local da aplicação. O Assistente de novo pacote não suporta ficheiros de configuração encriptados. Ao exportar o ficheiro de configuração, ignore o passo de encriptação do ficheiro.

A atualizar bases de dados no pacote de instalação

O pacote de instalação contém bases de dados antivírus do repositório do Servidor de Administração atualizados quando o pacote de instalação é criado. Depois de criar o pacote de instalação, pode atualizar as bases de dados antivírus no pacote de instalação. Isto permite reduzir o consumo de tráfego quando atualizar as bases de dados antivírus depois de instalar o Kaspersky Endpoint Security.

Para atualizar as bases de dados antivírus no repositório do Servidor de Administração, execute a tarefa *Download updates to the Administration Server repository* do Servidor de Administração. Para obter mais informações sobre a atualização das bases de dados antivírus no repositório do Administration Server, consulte a Ajuda do Kaspersky Security Center.

Só pode atualizar as bases de dados no pacote de instalação na Consola de Administração e na Consola da Web do Kaspersky Security Center. Não é possível atualizar as bases de dados no pacote de instalação na Consola de Nuvem do Kaspersky Security Center.

Como atualizar as bases de dados antivírus no pacote de instalação através da Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione a pasta **Remote installation** → **Advanced** → **Installation packages**.

   Isto abre uma lista de pacotes de instalação que foram transferidos para o Kaspersky Security Center.
3. Abra as propriedades do pacote de instalação.
4. Na secção **General**, clique **Update databases**.

Como resultado, as bases de dados antivírus no pacote de instalação serão atualizadas a partir do repositório do Servidor de Administração. O ficheiro `bases.cab` incluído no kit de distribuição será substituído pela pasta `bases`. Os ficheiros do pacote de atualização estarão dentro da pasta.

Como atualizar as bases de dados antivírus no pacote de instalação através da Consola da Web

1. Na janela principal da Consola Web, selecione **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.

   Isto abre uma lista de pacotes de instalação transferidos para Consola Web.
2. Clique no nome do pacote de instalação do Kaspersky Endpoint Security no qual pretende atualizar as bases de dados antivírus.

   A janela de propriedades do pacote de instalação abre-se.
3. No separador **General information**, clique na ligação **Update databases**.

Como resultado, as bases de dados antivírus no pacote de instalação serão atualizadas a partir do repositório do Servidor de Administração. O ficheiro `bases.cab` incluído no kit de distribuição será substituído pela pasta `bases`. Os ficheiros do pacote de atualização estarão dentro da pasta.

Criar uma tarefa de instalação remota

A tarefa *Install application remotely* foi criada para a instalação remota do Kaspersky Endpoint Security. A tarefa *Install application remotely* permite implementar o pacote de instalação da aplicação em todos os computadores da organização. Antes de implementar o pacote de instalação, pode atualizar as bases de dados antivírus dentro do pacote e selecionar os componentes de aplicações disponíveis nas propriedades do pacote de instalação.

Como criar uma tarefa de instalação remota na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Tasks**.

   A lista de tarefas é aberta.
3. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

Selecione **Kaspersky Security Center Administration Server → Install application remotely**.

Passo 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, pode criar o pacote no Assistente.

Pode configurar as definições do pacote de instalação no Kaspersky Security Center. Por exemplo, pode selecionar os componentes da aplicação que serão instalados num computador.

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

Passo 3. Adicional

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

Passo 4. Definições

Configure as seguintes definições adicionais da aplicação:

- **Force installation package download**. Selecionar o método de instalação da aplicação:
  - **Using Network Agent**. O Agente de Rede é responsável por entregar o pacote de instalação do Kaspersky Endpoint Security aos computadores clientes. Se o Agente de Rede não estiver instalado, a tarefa será terminada com um erro. Neste caso, adicione o pacote de instalação do Agente de Rede à tarefa *Install application remotely* e ative a entrega de ficheiros através dos recursos do sistema operativo. Em seguida, o Agente de Rede será instalado utilizando recursos do sistema operativo. O Kaspersky Endpoint Security é então instalada pelas ferramentas do Agente de Rede.
  - **Using operating system resources through distribution points**. O pacote de instalação é transmitido aos computadores do cliente utilizando recursos do sistema operativo através de pontos de distribuição. Pode selecionar esta opção se houver pelo menos um ponto de distribuição na rede. Para obter mais informação detalhadas sobre os pontos de distribuição, consulte a Ajuda do Kaspersky Security Center.
  - **Using operating system resources through Administration Server**. Os ficheiros serão entregues o computadores cliente utilizando os recursos do sistema operativo através do Servidor de administração. Pode selecionar esta opção se nenhum Agente de Rede for instalado no computador cliente, mas o computador cliente está na mesma rede que o Servidor de administração.
- **Behavior for devices managed through other Administration Servers**. Selecionar o método de instalação do Kaspersky Endpoint Security. Se a rede tiver mais do que um Servidor de administração instalado, estes Servidores de administração podem ver os mesmos computadores do cliente. Isto pode levar a que, por exemplo, uma aplicação seja instalada remotamente no mesmo computador do cliente múltiplos vezes através de diferentes Servidores de administração ou outros conflitos.
- **Do not re-install application if it is already installed**. Limpe esta caixa de verificação se quiser instalação uma versão anterior da aplicação, por exemplo.

Passo 5. Selecionar a definição de reinicialização do sistema operativo

Selecione a ação que deve ser executada se for necessário um reinício de computador. Reinicio não é necessário ao instalar o Kaspersky Endpoint Security. O reinicio é necessário apenas se precisar de remover aplicações incompatíveis antes da instalação. Reinício pode também ser necessário ao atualizar a versão da aplicação.

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

Selecione os computadores para instalar o Kaspersky Endpoint Security. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. O Agente de Rede não é instalado em Install application remotely. Neste caso, a tarefa é atribuída a dispositivos específicos. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 7. Selecionar a conta para executar a tarefa

Selecione a conta para instalar o Agente de Rede utilizando as ferramentas do sistema operativo. Neste caso, os direitos de administrador são necessitados para o acesso do computador. Pode adicionar múltiplas contas. Se uma conta não tiver direitos suficientes, o Assistente de Instalação utiliza a conta seguinte. Não tem de selecionar uma conta se instalar o Kaspersky Endpoint Security utilizando ferramentas do Agente de Rede.

Passo 8. Configurar um agendamento de início de uma tarefa

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

Passo 9. Definir o nome da tarefa

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

Passo 10. Concluir a criação da tarefa

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa. A aplicação será instalada no modo não assistido. Após a instalação, o ícone será adicionado à área de notificação do computador do utilizador. Se o ícone tiver o seguinte aspeto , certifique-se de que ativou a aplicação.

Como criar uma tarefa de instalação remota na Consola da Web e na Consola da Nuvem

1. Na janela principal da Consola Web, selecione **Asset management → Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

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

Passo 1. Configurar definições da tarefa geral

Configurar definições da tarefa geral:

1. Na lista pendente **Application**, selecione **Kaspersky Security Center**.
2. Na lista pendente **Task type**, selecione **Install application remotely**.
3. No campo **Task name**, introduza uma breve descrição, por exemplo, *Installation of Kaspersky Endpoint Security for Managers*.
4. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

Passo 2. Selecionar computadores para instalação

Neste passo, selecione os computadores nos quais o Kaspersky Endpoint Security será instalado de acordo com a opção do âmbito da tarefa selecionada.

Passo 3. Configurar um pacote de instalação

Neste passo, 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 instalado em conjunto com o Kaspersky Endpoint Security. O *Agente de Rede* facilita a interação entre o Servidor de administração e um computador do cliente. Se o Agente de Rede já estiver instalado no computador, não será instalado novamente.

3. No bloco **Force installation package download**, selecione o método de instalação de aplicação:

   - **Using Network Agent**. O Agente de Rede é responsável por entregar o pacote de instalação do Kaspersky Endpoint Security aos computadores clientes. Se o Agente de Rede não estiver instalado, a tarefa será terminada com um erro. Neste caso, adicione o pacote de instalação do Agente de Rede à tarefa *Install application remotely* e ative a entrega de ficheiros através dos recursos do sistema operativo. Em seguida, o Agente de Rede será instalado utilizando recursos do sistema operativo. O Kaspersky Endpoint Security é então instalada pelas ferramentas do Agente de Rede.

   - **Using operating system resources through distribution points**. O pacote de instalação é transmitido aos computadores do cliente utilizando recursos do sistema operativo através de pontos de distribuição. Pode selecionar esta opção se houver pelo menos um ponto de distribuição na rede. Para obter mais informação detalhadas sobre os pontos de distribuição, consulte a Ajuda do Kaspersky Security Center.

   - **Using operating system resources through Administration Server**. Os ficheiros serão entregues o computadores cliente utilizando os recursos do sistema operativo através do Servidor de administração. Pode selecionar esta opção se nenhum Agente de Rede for instalado no computador cliente, mas o computador cliente está na mesma rede que o Servidor de administração.

4. No campo **Maximum number of concurrent downloads**, defina um número limite de pedidos de transferência do pacote de instalação enviados para o Administration Server. Um número limite de pedidos ajudará a impedir uma sobrecarga na rede.

5. No campo **Maximum number of installation attempts**, defina um número limite de tentativas de instalação da aplicação. Se instalação do Kaspersky Endpoint Security terminar com um erro, a tarefa iniciará automaticamente a instalação novamente.

6. Se necessário, desmarque a caixa de verificação **Do not re-install application if it is already installed**. Permite, por exemplo, instalar uma das versões prévias da aplicação.

7. Se necessário, desmarque a caixa de verificação **Verify operating system type before downloading**. Isto permite-lhe evitar a transferência de um pacote de distribuição da aplicação se o sistema operativo do computador não cumprir os requisitos do software. Pode ignorar esta verificação se tiver a certeza que o sistema operativo do computador cumpre os requisitos do software.

8. Se necessário, selecione a caixa de verificação **Assign package installation in Active Directory group policies**. O Kaspersky Endpoint Security é instalado através do Agente de Rede ou manualmente através do Diretório Ativo. Para instalar o Agente de Rede, a tarefa de instalação remota deve ser executada com privilégios de administrador de domínio.

9. Se necessário, selecione a caixa de verificação **Prompt users to close running applications**. A instalação do Kaspersky Endpoint Security usa recursos do computador. Para fins de conveniência do utilizador, o Assistente de Instalação da Aplicação recomenda o encerramento das aplicações em funcionamento antes de iniciar a instalação. Isto ajuda a impedir perturbações no funcionamento de outras aplicações bem como possíveis avarias do computador.

10. Selecione o método de instalação do Kaspersky Endpoint Security no bloco **Behavior for devices managed through other Administration Servers**. Se a rede tiver mais do que um Servidor de administração instalado, estes Servidores de administração podem ver os mesmos computadores do cliente. Isto pode levar a que, por exemplo, uma aplicação seja instalada remotamente no mesmo computador do cliente múltiplos vezes através de diferentes Servidores de administração ou outros conflitos.

Passo 4. Selecionar a conta para executar a tarefa

Selecione a conta para instalar o Agente de Rede utilizando as ferramentas do sistema operativo. Neste caso, os direitos de administrador são necessitados para o acesso do computador. Pode adicionar múltiplas contas. Se uma conta não tiver direitos suficientes, o Assistente de Instalação utiliza a conta seguinte. Não tem de selecionar uma conta se instalar o Kaspersky Endpoint Security utilizando ferramentas do Agente de Rede.

Passo 5. Completar a criação da tarefa

Termine o assistente clicando no botão **Finish**. Será apresentada uma nova tarefa na lista de tarefas. Para executar uma tarefa, selecione a caixa de seleção em frente da tarefa e clique no botão **Start**. A aplicação será instalada no modo não assistido. Após a instalação, o ícone será adicionado à área de notificação do computador do utilizador. Se o ícone tiver o seguinte aspeto , certifique-se de que ativou a aplicação.

Instalar a aplicação localmente utilizando o Assistente

A interface do Assistente de Instalação da aplicação consiste numa sequência de janelas que correspondem aos passos de instalação da aplicação. Certifique-se de que a conta de utilizador com a qual está a executar o Assistente de Configuração pertence ao grupo de administradores.

Para instalar a aplicação ou para atualizar a aplicação a partir de uma versão anterior utilizando o Assistente de Instalação:

1. Copie a pasta do kit de distribuição para o computador do utilizador.
2. Execute o ficheiro setup_kes.exe.

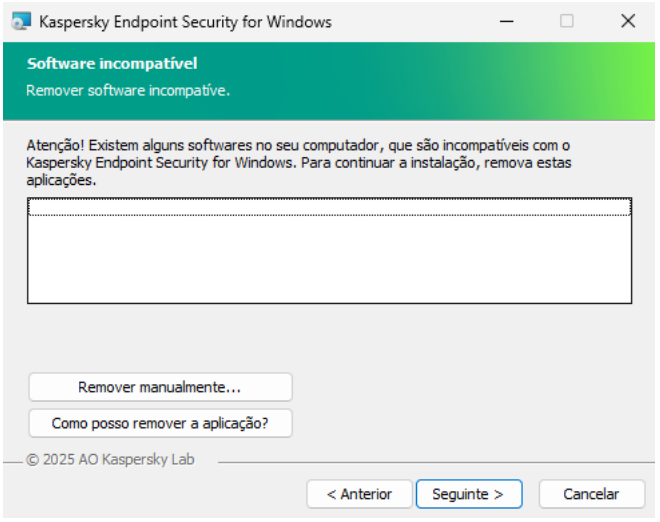
   O Assistente de configuração é iniciado.

Preparação para instalação

Antes de instalar o Kaspersky Endpoint Security num computador ou de atualizar uma versão anterior da aplicação, são verificadas as condições seguintes:

- Verifique se existe algum software instalado que possa apresentar problemas de compatibilidade com o Kaspersky Endpoint Security (a lista de software está disponível no ficheiro incompatible.txt que está incluído no kit de distribuição).
- Se o hardware e os requisitos de software são cumpridos.
- Se o Microsoft .NET Framework estiver presente.
- Se o utilizador dispõe ou não dos direitos necessários para instalar o produto de software.

Se qualquer um dos requisitos anteriores não for cumprido, é apresentada uma notificação relevante no ecrã. Por exemplo, uma notificação sobre software incompatível (veja a figura abaixo).



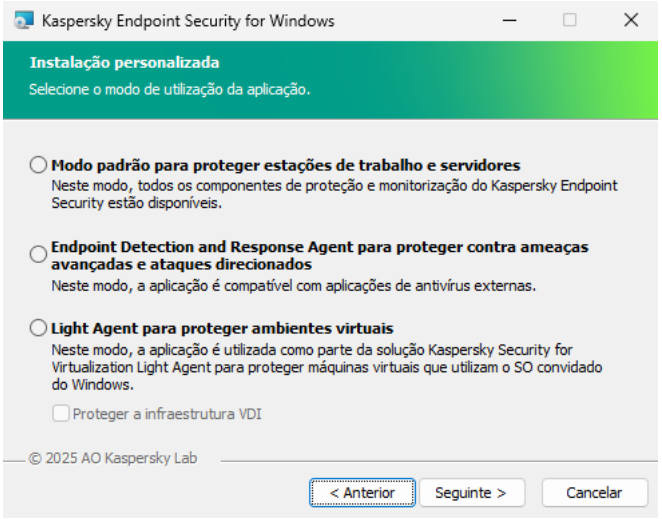
Remover software incompatível

Se o computador cumpre os requisitos indicados, o Assistente de Instalação procura aplicações do Kaspersky que poderão provocar conflitos ao executar em simultâneo com a instalação da aplicação. Se essas aplicações forem encontradas, ser-lhe-á pedido que as remova manualmente.

Se as aplicações detetadas incluírem versões anteriores do Kaspersky Endpoint Security, todos os dados que podem ser migrados (como dados de ativação e definições da aplicação) são conservados e utilizados durante a instalação do Kaspersky Endpoint Security 14.2 for Windows, e a versão anterior da aplicação é automaticamente removida. Isto aplica-se às seguintes versões da aplicação:

- 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



Escolher a configuração da aplicação

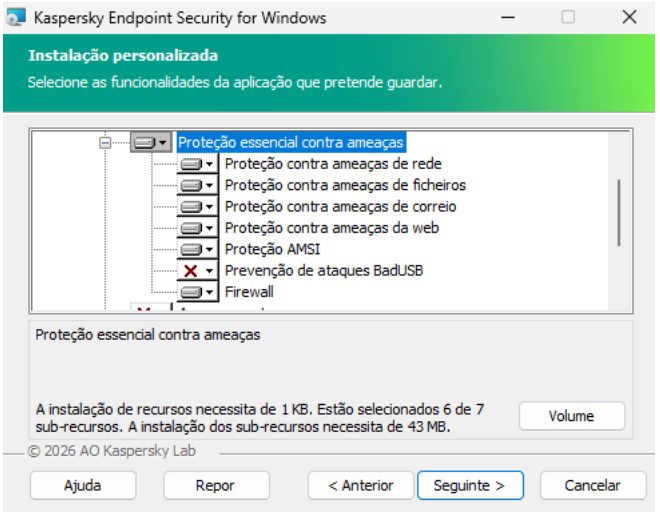
Modo Padrão. A configuração predefinida. Esta configuração permite utilizar todos os componentes da aplicação, incluindo componentes que fornecem suporte para soluções de Detection and Response. Esta configuração é utilizada para proteção abrangente do computador contra diversas ameaças, ataques de rede e fraudes.

Endpoint Detection and Response Agent. Nesta configuração, só é possível instalar os componentes que fornecem suporte para soluções Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) e KUMA. Esta configuração será necessária se uma Endpoint Protection Platform (EPP) de terceiros for implementada na sua organização em conjunto com uma solução de Detection and Response da Kaspersky. Isso torna o Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent compatível com aplicações EPP de terceiros.

Light Agent para proteger ambientes virtuais. Esta configuração destina-se à aplicação que é usada como parte da solução Kaspersky Security for Virtualization Light Agent. O Light Agent tem de ser instalado em cada máquina virtual que precisa de ser protegida usando a solução. Nesta configuração, não pode utilizar componentes de Encriptação de Dados ou Controlo de Anomalias Adaptativo. Se estiver a instalar o Light Agent num modelo de máquina virtual que será usado para criar *máquinas virtuais não persistentes*, selecione a caixa de verificação **Proteger a 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. Neste modo, o Light Agent recusa atualizações de aplicações que exigem o reinício da máquina virtual. Ao receber atualizações de aplicações que exigem um reinício, o Light Agent gera um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas.

Componentes do Kaspersky Endpoint Security

Durante o processo de instalação, pode selecionar os componentes do Kaspersky Endpoint Security que pretende instalar (veja a figura abaixo). O componente Proteção contra ameaças de ficheiros é um componente obrigatório que tem de ser instalado. Não pode cancelar a sua instalação.



Selecionar os componentes da aplicação a instalar

Por predefinição, todos os componentes da aplicação estão selecionados para instalação, exceto os seguintes componentes:

- Encriptação de disco Kaspersky
- Encriptação ao nível dos ficheiros
- 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 o KUMA

Pode alterar os componentes da aplicação disponíveis após instalar a aplicação. Para o fazer, deve executar o Assistente de Instalação novamente e selecionar a alteração dos componentes disponíveis.

Se precisar de instalar os componentes Detection and Response components, o Kaspersky Endpoint Security suporta as seguintes configurações:

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

- Network Detection and Response (KATA) apenas
- Sandbox apenas
- 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 dos componentes antes de instalar a aplicação. Se a configuração selecionada dos componentes Detection and Response não for suportada, o Kaspersky Endpoint Security não pode ser instalado.

Selecionar a pasta para instalar a aplicação

Pode alterar o caminho de instalação do Kaspersky Endpoint Security num computador de cliente. Por predefinição, a aplicação é instalada na pasta `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.2`.

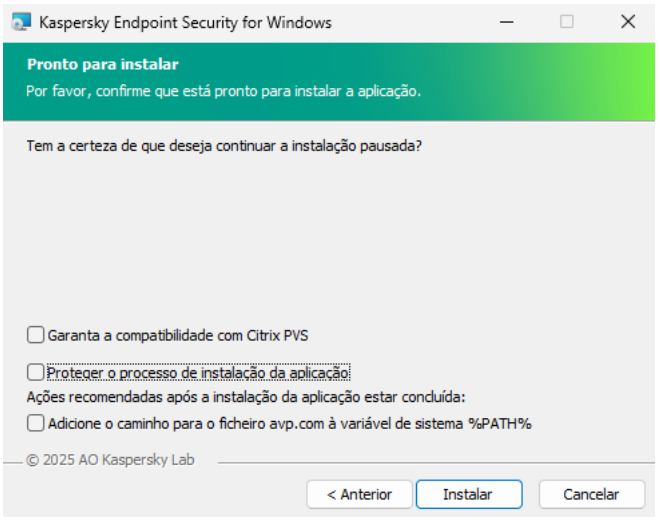
Configurar a zona fiável

A partir do Kaspersky Endpoint Security 12.6 para Windows, as exclusões de verificação e as aplicações fiáveis são adicionadas à zona fiável. Exclusões de verificação predefinidas e aplicações fiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e System Center Configuration Manager. Isto significa que não é necessário configurar manualmente uma zona fiável para a aplicação nos servidores.

A partir do Kaspersky Endpoint Security 12.8 para Windows, pode instalar aplicação no modo Light Agent para proteger ambientes virtuais. As exclusões de verificação predefinidas e as aplicações fiáveis podem ajudá-lo a configurar rapidamente o Kaspersky Endpoint Security em ambientes virtuais Citrix e VMware.

Também pode configurar a zona fiável mais tarde nas propriedades da política: exclusões de verificação e aplicações fiáveis.

Definições avançadas



Definições avançadas de instalação da aplicação

Proteger o processo de instalação da aplicação. A proteção de instalação inclui a proteção contra a substituição do pacote de distribuição com aplicações maliciosas, bloqueando o acesso à pasta de instalação do Kaspersky Endpoint Security, e bloqueando o acesso à secção do registo do sistema contendo as chaves da aplicação. Contudo, se não for possível instalar a aplicação (por exemplo, ao executar uma instalação remota com a ajuda do Windows Remote Desktop), recomendamos que desative a proteção do processo de instalação.

Garanta a compatibilidade com Citrix PVS. Pode ativar o suporte dos Citrix Provisioning Services para instalar o Kaspersky Endpoint Security numa máquina virtual.

Adicione o caminho para o ficheiro avp.com à variável de sistema %PATH%. Pode adicionar o caminho de instalação à variável %PATH% para utilização conveniente da interface da linha de comando.

Instalação remota da aplicação que utiliza o System Center Configuration Manager

Estas instruções são aplicáveis ao System Center Configuration Manager 2012 R2.

Instalar remotamente uma aplicação utilizando o System Center Configuration Manager:

1. Abrir a consola do Gerente de Configuração.
2. Na parte direita da consola, no bloco **Gestão de aplicações**, selecione **Pacotes**.
3. Na parte superior da consola, no painel de controlo, clique no botão **Create package**.
   Isto inicia o *Assistente de Novo Pacote e Aplicações*.

4. No Assistente de Novo Pacote e Aplicações:

   a. Na secção **Pacote**:

   - No campo **Nome**, introduza o nome do pacote de instalação.
   - No campo **Pasta de origem**, especifique o caminho da pasta que contém o pacote de distribuição do Kaspersky Endpoint Security.

   b. Na secção **Application type**, selecione a opção **Programa padrão**.

   c. Na secção **Programa padrão**:

   - No campo **Nome**, introduza o nome único do pacote de instalação (por exemplo, o nome da aplicação incluindo a versão).
   - No campo **command line**, especifique as opções de instalação do Kaspersky Endpoint Security da command line.
   - Clique no botão **Procurar** para especificar o caminho para o ficheiro executável da aplicação.
   - Certifique-se de que a lista **Modo de execução** tem o item **Executar com direitos administrativos** selecionado.

   d. Na secção **Requisitos**:

   - Selecione a caixa de verificação **Executar primeiro outro programa** se pretender que seja iniciada uma aplicação diferente antes de instalar o Kaspersky Endpoint Security.

     Selecione a aplicação na lista pendente **Aplicação** ou especifique o caminho para o ficheiro executável desta aplicação clicando no botão **Procurar**.
   - Selecione a opção **Este programa só pode ser executado em plataformas especificadas** no bloco **Requisitos da plataforma** se pretender que a aplicação seja instalada apenas nos sistemas operativos especificados.

     Na lista seguinte, selecione as caixas de verificação à frente dos sistemas operativos nos quais o Kaspersky Endpoint Security será instalado.

   Este passo é opcional.

   e. Na secção **Resumo**, verifique todos os valores introduzidos das definições e clique em **Seguinte**.

   O pacote de instalação criado é apresentado na secção **Pacotes** na lista de pacotes de instalação disponíveis.

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

   Esta ação inicia o *Assistente de Implementação*.

6. No Assistente de Implementação:

   a. Na secção **Geral**:

   - No campo **Software**, introduza o nome único do pacote de instalação ou selecione o pacote de instalação da lista clicando no botão **Procurar**.
   - No campo **Coleção**, introduza o nome da coleção de computadores nos quais a aplicação será instalada ou selecione a coleção clicando no botão **Procurar**.

b. Na secção **Contém**, adicione os pontos de distribuição (para obter informações mais detalhadas, consulte a documentação de ajuda do System Center Configuration Manager).

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

d. Na secção **Resumo**, verifique todos os valores introduzidos das definições e clique em **Seguinte**.

Após a conclusão do Assistente de Implementação, será criada uma tarefa para a instalação remota do Kaspersky Endpoint Security.

Descrição das configurações de instalação do ficheiro setup.ini

O ficheiro setup.ini é utilizado ao instalar a aplicação a partir da command line ou utilizando o Editor da Política de Grupo do Microsoft Windows. Para aplicar as configurações do ficheiro setup.ini, coloque esse ficheiro na pasta que contém o pacote de distribuição do Kaspersky Endpoint Security.

Utilize o ficheiro setup.ini apenas quando instalar a aplicação em modo silencioso.

Não pode adicionar um caminho ao ficheiro de configuração install.cfg no ficheiro setup.ini. A aplicação também ignora o ficheiro de configuração install.cfg se estiver colocado na mesma pasta que o kit de distribuição do Kaspersky Endpoint Security. Para aplicar as definições do ficheiro de configuração install.cfg, tem de especificar o caminho para o ficheiro no comando de instalação da aplicação que se segue: `CONFIGPATH=<path to the configuration file>`.

TRANSFERIR O FICHEIRO SETUP.INI

O ficheiro setup.ini consiste nas seguintes secções:

- `[Setup]` - configurações gerais da instalação da aplicação.
- `[Components]` — seleção de componentes da aplicação a instalar no modo Padrão. Se nenhum dos componentes estiver especificado, são instalados todos os componentes disponíveis para o sistema operativo. A Proteção contra ameaças de ficheiros é um componente obrigatório que é instalado no computador, independentemente das definições indicadas nesta secção.
- `[Tasks]` – seleção das tarefas a incluir na lista de tarefas do Kaspersky Endpoint Security. Se não for especificada qualquer tarefa, todas as tarefas são incluídas na lista de tarefas do Kaspersky Endpoint Security.

As alternativas ao valor `1` são os valores `yes`, `on`, `enable`, `enabled` e `true`. As alternativas ao valor `0` são os valores `no`, `off`, `disable`, `disabled` e `false`.

Secção	Parâmetro	Descrição
[Setup]	InstallDir	Caminho para a pasta de instalação da aplicação.
	ActivationCode	Código de ativação do Kaspersky Endpoint Security.
	Eula	Aceitação dos termos do Contrato de Licença do Utilizador Final. O texto do Contrato de Licença está incluído no kit de distribuição do Kaspersky Endpoint Security. É necessário aceitar os termos do Contrato de Licença do Utilizador Final para instalar a aplicação ou para atualizar a versão da aplicação.
	PrivacyPolicy	Aceitação da Política de Privacidade. O texto da Privacy Policy encontra-se incluído no kit de distribuição do Kaspersky Endpoint Security. Para instalar a aplicação ou atualizar a versão da aplicação, tem de aceitar a Privacy Policy.
	KSN	Aceitar ou recusar participar na 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 na KSN, quando o Kaspersky Endpoint Security for iniciado pela primeira vez. Valores disponíveis: • 1 - acordo para participar na KSN. • 0 – recusar participar na KSN (valor predefinido). O pacote de distribuição do Kaspersky Endpoint Security está otimizado para utilização com a Kaspersky Security Network. Se optou por não participar na Kaspersky Security Network, deve atualizar o Kaspersky Endpoint Security imediatamente após concluir a instalação.
	CLEANERSIGNCHECK	Verificação das assinaturas digitais dos ficheiros de software detetados a partir da lista incompatible.txt. Para remover o software, o Kaspersky Endpoint Security executa o ficheiro do instalador do software. Se o ficheiro de instalação não tiver uma assinatura digital, o Kaspersky Endpoint Security considera o ficheiro não fiável e interrompe a remoção de software para evitar a execução de código potencialmente malicioso. Se a aplicação não puder verificar a assinatura digital do ficheiro de software detetado, a instalação do Kaspersky Endpoint Security é interrompida com um erro. O valor predefinido é diferente dependendo do método de instalação do software: • 0 significa que a verificação da assinatura digital está desativada (valor predefinido se for implementado através do Kaspersky Security Center). • 1 significa que a verificação de assinatura digital está ativada (valor predefinido se a aplicação estiver a ser instalada localmente).
	Login	Defina o nome de utilizador para aceder aos recursos e configurações do Kaspersky Endpoint Security (o componente Proteção de password). O nome do utilizador é definido com as definições de Password e PasswordArea. O nome de utilizador KLAdmin é usado por definição.
	Password	Especificar uma password para aceder às funcionalidades e definições do Kaspersky Endpoint Security (a password é especificada juntamente com os parâmetros Login de sessão e PasswordArea). Se tiver especificado uma password mas não especificou um nome de utilizador com o parâmetro Login, o nome de utilizador KLAdmin é utilizado por predefinição.
	PasswordArea	Especificar o âmbito da password para aceder às funcionalidades e definições do Kaspersky Endpoint Security. Quando um utilizador tenta executar uma ação incluída neste âmbito, o Kaspersky Endpoint Security solicita as credenciais da conta do utilizador (parâmetros Login e Password). Utilize o caráter ; para especificar vários valores. Valores disponíveis: • SET - modificar as configurações da aplicação. • EXIT - sair da aplicação. • DISPROTECT – desativar componentes de proteção e parar tarefas de verificação. • DISPOLICY — desativar a política do Kaspersky Security Center. • UNINST – remover a aplicação do computador. • DISCTRL - desativar os componentes de controlo. • REMOVELIC - remover a chave. • REPORTS - visualizar relatórios. • EXPORT – exportar definições da aplicação. Por exemplo, PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT.

Secção	Parâmetro	Descrição
	`SelfProtection`	Ativação ou desativação do mecanismo de proteção de instalação da aplicação. Valores disponíveis: • `1` – o mecanismo de proteção de instalação de aplicação é ativado (valor predefinido). • `0` – o mecanismo de proteção de instalação de aplicação é desativado. A proteção de instalação inclui a proteção contra a substituição do pacote de distribuição com aplicações maliciosas, bloqueando o acesso à pasta de instalação do Kaspersky Endpoint Security, e bloqueando o acesso à secção do registo do sistema contendo as chaves da aplicação. Contudo, se não for possível instalar a aplicação (por exemplo, ao executar uma instalação remota com a ajuda do Windows Remote Desktop), recomendamos que desative a proteção do processo de instalação.
	`PROTECTOSSERVICES`	Proteção da funcionalidade dos serviços do sistema operativo. A proteção dos serviços do sistema operativo impede que aplicações de terceiros interfiram com o funcionamento dos serviços do sistema operativo. Esses serviços incluem, por exemplo, o serviço de inicialização automática de aplicações. • `1` significa que a proteção dos serviços do sistema operativo está ativada (valor padrão). • `0` significa que a proteção dos serviços do sistema operativo está desativada.
	`EnableAzureSupport`	Ativar ou desativar o modo de compatibilidade do 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). Esta funcionalidade garante a exibição correta do estado da máquina virtual do Azure na consola da Kaspersky Anti Targeted Attack Platform. Para monitorizar o desempenho do computador, o Kaspersky Endpoint Security envia telemetria aos servidores KATA. A telemetria inclui um ID do computador (Sensor ID). O modo de compatibilidade do Azure WVD permite atribuir um Sensor ID único permanente a estas máquinas virtuais. Se o modo de compatibilidade estiver desativado, o Sensor ID poderá mudar depois de o computador ser reiniciado devido ao funcionamento das máquinas virtuais do Azure. Isto pode fazer com que os duplicados das máquinas virtuais apareçam na consola.
	`Reboot`	Reinício automático do computador, se necessário após a instalação ou atualização da aplicação. Se nenhum valor for definido para este parâmetro, a reinicialização automática do computador será bloqueada. Reinicio não é necessário ao instalar o Kaspersky Endpoint Security. O reinicio é necessário apenas se precisar de remover aplicações incompatíveis antes da instalação. Reinício pode também ser necessário ao atualizar a versão da aplicação.
	`AddEnvironment`	Complementar a variável de sistema %PATH% com o caminho para os ficheiros executáveis localizados na pasta de instalação do Kaspersky Endpoint Security. Valores disponíveis: • `1` – a variável de sistema %PATH% é complementada com o caminho para os ficheiros executáveis localizados na pasta de instalação do Kaspersky Endpoint Security. • `0` – a variável de sistema %PATH% não é complementada com o caminho para os ficheiros executáveis localizados na pasta de instalação do Kaspersky Endpoint Security.
	`AMPPL`	Ativa ou desativa a proteção do serviço Kaspersky Endpoint Security utilizando a tecnologia AM-PPL (Antimalware Protected Process Light). Para obter mais informações sobre a tecnologia AM-PPL, visite o website 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` – a proteção do serviço Kaspersky Endpoint Security com a tecnologia AM-PPL é ativada. • `0` – a proteção do serviço Kaspersky Endpoint Security utilizando a tecnologia AM-PPL é desativada.

Secção	Parâmetro	Descrição
	UPGRADEMODE	Modo de atualização das aplicações: • Seamless significa atualizar a aplicação com um reinício do computador (valor padrão). • Force significa atualizar a aplicação sem um reinício. Pode atualizar a aplicação sem reiniciar a aplicação a partir da versão 11.10.0. Para atualizar uma versão anterior da aplicação, tem de reiniciar o computador. Também pode instalar correções sem reiniciar a aplicação a partir da versão 11.11.0. Reinicio não é necessário ao instalar o Kaspersky Endpoint Security. Assim, o modo de atualização da aplicação será especificado nas definições da aplicação. Pode alterar este parâmetro nas definições da aplicação ou na política. Ao atualizar a aplicação já instalada, a prioridade do parâmetro especificado no ficheiro setup.ini é superior à do parâmetro especificado nas definições da aplicação ou na linha de comandos. Por exemplo, se o modo Force atualização for especificado no ficheiro setup.ini e o modo Seamless for especificado nas definições da aplicação, a atualização será instalada sem reiniciar Force). Se estiver a utilizar o ficheiro setup.ini, onde o parâmetro UPGRADEMODE não está especificado, o instalador utilizará um valor predefinido Seamless) e instalará a atualização com um reinício do computador.
	SetupReg	Ativa a escrita das chaves de registo do ficheiro setup.reg para o registo. Valor do parâmetro SetupReg: setup.reg.
	EnableTraces	Ativar ou desativar os rastreios da aplicação. Depois de iniciado, o Kaspersky Endpoint Security guarda os ficheiros de rastreio na pasta %ProgramData%\Kaspersky Lab\KES.14.2\Traces. Valores disponíveis: • 1 – os rastreios estão ativados. • 0 – os rastreios estão desativados (valor padrão).
	TracesLevel	Nível de detalhe do rastreio. 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 da aplicação no modo normal (predefinição). • 600 (baixo). Todas as mensagens.
	RESTAPI	Gestão da aplicação com API REST. Para gerir a aplicação com API REST, deve especificar o nome do utilizador (parâmetro RESTAPI_User). Valores disponíveis: • 1 - a gestão com API REST é permitida. • 0 - a gestão com API REST é bloqueada (valor predefinido). Para gerir a aplicação com API REST, a gestão com sistemas administrativos deve ser permitida. Para tal, defina o parâmetro AdminKitConnector=1. Se gerir a aplicação com API REST, não é possível gerir a aplicação com os sistemas de administração da Kaspersky.
	RESTAPI_User	Nome do utilizador da conta de domínio do Windows usada para gerir a aplicação com API REST. A gestão da aplicação com API REST está disponível apenas para este utilizador. Introduza o nome de utilizador no formato <DOMAIN>\<UserName> (por exemplo, RESTAPI_User=COMPANY\Administrator). Só pode selecionar um utilizador para trabalhar com API REST. Adicionar um nome de utilizador é um pré-requisito para gerir a aplicação com API REST.
	RESTAPI_Port	Porta usada para gerir a aplicação com API REST. A porta 6782 é usada por defeito. 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 de solicitação. Para tal, deve instalar um certificado e, posteriormente, assinar o payload de cada solicitação.

Secção	Parâmetro	Descrição
	`StandaloneMode`	Instalar a aplicação no modo Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* é uma aplicação instalada em estações de trabalho e servidores individuais na infraestrutura de TI da organização para dar suporte às soluções Kaspersky Managed Detection and Response e Kaspersky Anti Targeted Attack Platform. O EDR Agent é compatível com aplicações EPP de terceiros. Isso permite que use ferramentas de segurança de infraestrutura de terceiros em conjunto com o Detection and Response da Kaspersky. Para instalar o EDR Agent, na secção `[Components]`, selecione os componentes `StandaloneKATA`, `StandaloneNDR` ou `StandaloneMDR`. O EDR Agent não suporta outros componentes da aplicação. Valores disponíveis: • `1` para instalar a aplicação no modo EDR Agent. • `0` para instalar a aplicação no modo Padrão (predefinição).
	`KSVLAMode`	Instalar a aplicação no modo Light Agent. Esta configuração destina-se à aplicação que é usada como parte da solução Kaspersky Security for Virtualization Light Agent. O Light Agent tem de ser instalado em cada máquina virtual que precisa de ser protegida usando a solução. Valores disponíveis: • `1` para instalar a aplicação no modo Light Agent. • `0` para instalar a aplicação no modo Padrão (predefinição).
	`InstallOnVDI`	Ativar o modo de proteção VDI ao instalar a aplicação 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. Neste modo, o Light Agent recusa atualizações de aplicações que exigem o reinício da máquina virtual. Ao receber atualizações de aplicações que exigem um reinício, o Light Agent gera 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 (predefinição).
	`KESExclusions`	Adicionar exclusões de verificação predefinidas e aplicações fiáveis ao instalar a aplicação no servidor. Exclusões de verificação predefinidas e aplicações fiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e System Center Configuration Manager. Por exemplo, exclusões de verificação predefinidas para servidores SQL incluem ficheiros de base de dados MDF e LDF. Isto significa que não é necessário configurar manualmente uma zona fiável para a aplicação nos servidores. Valores disponíveis: • `1` ativa exclusões de verificação predefinidas e aplicações fiáveis. • `0` desativa exclusões de verificação predefinidas e aplicações fiáveis (predefinição).
	`LAExclusions`	Adicionar exclusões de verificação predefinidas e aplicações fiáveis ao instalar a aplicação numa máquina virtual (modo Light Agent). As exclusões de verificação predefinidas e as aplicações fiáveis podem ajudá-lo a configurar rapidamente o Kaspersky Endpoint Security em ambientes virtuais Citrix e VMware. Valores disponíveis: • `1` ativa exclusões de verificação predefinidas e aplicações fiáveis. • `0` desativa exclusões de verificação predefinidas e aplicações fiáveis (predefinição).
	`EnableUniqueSensorID`	Criação de um identificador de computador exclusivo (Sensor ID) durante a instalação ou atualização da aplicação. O Sensor ID é usado na solução Kaspersky Anti Targeted Attack Platform para identificar computadores que enviam telemetria para o servidor. Ao criar o Sensor ID, a aplicação usa um algoritmo que tem em consideração a configuração do computador, como o número de série da placa-mãe. Em alguns casos, por exemplo, quando se utiliza a aplicação num 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 único, tem de definir o parâmetro `EnableUniqueSensorID=1`. Como resultado, a aplicação utilizará um algoritmo diferente para criar o Sensor ID, que tem em conta outros dados sobre o computador. Isto garante um Sensor ID exclusivo. Por defeito, o parâmetro não está definido. A aplicação herda o Sensor ID nos seguintes casos: • Atualizar a versão da aplicação; • migrar a configuração [KES+KEA] para a configuração [KES+agente incorporado]. Como parte da reparação da aplicação, o instalador tenta herdar o Sensor ID. Se o Sensor ID não puder ser restaurado, a aplicação cria um novo Sensor ID.

Secção	Parâmetro	Descrição
	`CitrixCompatibility`	Ativar o suporte dos Citrix Provisioning Services para instalar o Kaspersky Endpoint Security numa máquina virtual.
`[Components]`	`ALL`	Instalação de todos os componentes. Se o valor do parâmetro `1` for especificado, todos os componentes serão instalados independentemente das definições de instalação dos componentes individuais. Devido à forma como as soluções Detection and Response são suportadas, os componentes Endpoint Detection and Response Optimum e Sandbox estão instalados no computador. O componente Endpoint Detection and Response Expert (cloud) não é compatível com esta configuração.
	`MailThreatProtection`	Proteção contra ameaças de correio.
	`WebThreatProtection`	Proteção contra ameaças da Web.
	`AMSI`	Proteção AMSI.
	`HostIntrusionPrevention`	Prevenção contra invasões.
	`BehaviorDetection`	Deteção de comportamento.
	`ExploitPrevention`	Prevenção de explorações.
	`RemediationEngine`	Motor de remediação.
	`Firewall`	Firewall.
	`NetworkThreatProtection`	Proteção contra ameaças de Rede.
	`WebControl`	Controlo de Internet.
	`DeviceControl`	Controlo de Dispositivos.
	`ApplicationControl`	Controlo das aplicações.
	`AdaptiveAnomaliesControl`	Controlo de Anomalias Adaptativo.
	`CloudDiscovery`	Cloud Discovery.
	`LogInspector`	Inspeção do Registo
	`AntiCryptor`	Anti-Cryptor
	`FileThreatProtection`	Proteção contra ameaças de ficheiros.
	`SystemIntegrityMonitor`	Monitorização da integridade do sistema.
	`FileEncryption`	Bibliotecas de encriptação ao nível dos ficheiros.
	`DiskEncryption`	Bibliotecas de Encriptação Completa do Disco.
	`MSBitLocker`	Bibliotecas de gestão de Encriptação do BitLocker.
	`BadUSBAttackPrevention`	Prevenção de ataques BadUSB.
	`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`).

Secção	Parâmetro	Descrição
	`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 Detection and Response autónoma 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`	Gestão de aplicações com sistemas de administração. Os sistemas de administração incluem, por exemplo, o Kaspersky Security Center. Para além dos sistemas de administração da Kaspersky, pode usar soluções de terceiros. O Kaspersky Endpoint Security fornece uma API para esta finalidade. Valores disponíveis: • `1` - a gestão de aplicações com sistemas de administração é permitida (valor predefinido). • `0` - a gestão de aplicações é permitida apenas com a interface local.
	`KUMAIntegration`	Integração com o KUMA.
	`StandaloneKATA`	Instalar a aplicação no modo Endpoint Detection and Response Agent (EDR Agent) para integração com a Kaspersky Anti Targeted Attack Platform (EDR).
	`StandaloneMDR`	Instalar a aplicação no modo do Endpoint Detection and Response Agent (EDR Agent) para integração com o Kaspersky Managed Detection and Response.
	`StandaloneNDR`	Instalar a aplicação no modo Endpoint Detection and Response Agent (EDR Agent) para integração com a Kaspersky Anti Targeted Attack Platform (NDR).
	`StandaloneSiemTelemetry`	Instalar a aplicação no modo do Endpoint Detection and Response Agent (EDR Agent) para integração com o KUMA.
`[Tasks]`	`ScanMyComputer`	Tarefa de Verificação Completa. Valores disponíveis: • `1` – A tarefa não é incluída na lista de tarefas do Kaspersky Endpoint Security. • `0` – A tarefa não é incluída na lista de tarefas do Kaspersky Endpoint Security.
	`ScanCritical`	Tarefa de Verificação de Áreas Críticas. Valores disponíveis: • `1` – A tarefa não é incluída na lista de tarefas do Kaspersky Endpoint Security. • `0` – A tarefa não é incluída na lista de tarefas do Kaspersky Endpoint Security.
	`Updater`	Tarefa de atualização. Valores disponíveis: • `1` – A tarefa não é incluída na lista de tarefas do Kaspersky Endpoint Security. • `0` – A tarefa não é 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.

Nome do ficheiro	Finalidade
avp.exe	Processo de trabalho do Kaspersky Endpoint Security for Windows.
avpsus.exe	Este processo permite instalar e reverter atualizações críticas e aprovadas dos módulos da aplicação.

Change application components

Durante a instalação da aplicação, pode selecionar os componentes que estarão disponíveis. Pode alterar os componentes da aplicação disponíveis do seguinte modo:

- Localmente, usando o Assistente de Configuração.

  Pode alterar os componentes da aplicação com o método habitual do sistema operativo Windows, ou seja, através do Painel de Controlo. Execute o Assistente de Configuração da Aplicação e selecione a opção para alterar os componentes da aplicação que estão disponíveis. Siga as instruções apresentadas no ecrã.

  > Este método não está disponível se a aplicação tiver sido instalada através do Kaspersky Security Center. Só é possível alterar a seleção de componentes da aplicação no Painel de Controlo depois de instalar a aplicação localmente.

- Remotamente, utilizando o Kaspersky Security Center.

  A tarefa *Alterar componentes da aplicação* permite-lhe alterar os componentes do Kaspersky Endpoint Security após a aplicação ser instalada.

Tenha em conta as seguintes considerações especiais quando alterar os componentes da aplicação:

- Em computadores com Windows Server, não pode instalar todos os componentes do Kaspersky Endpoint Security (por exemplo, o componente Controlo de Anomalias Adaptativo não está disponível).
- Se os discos rígidos do seu computador estiverem protegidos pelo Encriptação Completa do Disco (FDE), não poderá remover o componente Encriptação Completa do Disco. Para remover o componente Encriptação Completa do Disco, desencripte todos os discos rígidos do computador.
- Se o computador tiver arquivos encriptados (FLE) ou se o utilizador usar unidades removíveis encriptadas (FDE ou FLE), não será possível aceder aos ficheiros e às unidades removíveis depois de remover os componentes de encriptação de dados. Pode aceder aos ficheiros e às unidades removíveis reinstalando os componentes de Encriptação de Dados.
- Se a aplicação estiver instalada no modo Light Agent numa infraestrutura VDI, não é possível alterar os componentes do conjunto.

Como adicionar ou remover componentes de aplicações na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

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

Passo 2. Definições da tarefa para alterar os componentes da aplicação

Selecione a configuração da aplicação:

- **Modo padrão para proteger anfitriões**. A configuração predefinida. Esta configuração permite utilizar todos os componentes da aplicação, incluindo componentes que fornecem suporte para soluções de Detection and Response. Esta configuração é utilizada para proteção abrangente do computador contra diversas ameaças, ataques de rede e fraudes.

- **Endpoint Detection and Response Agent para proteger contra ameaças avançadas e ataques direcionados**. Nesta configuração, só é possível instalar os componentes que fornecem suporte para soluções Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) e KUMA. Esta configuração será necessária se uma Endpoint Protection Platform (EPP) de terceiros for implementada na sua organização em conjunto com uma solução de Detection and Response da Kaspersky. Isso torna o Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent compatível com aplicações EPP de terceiros.

  Ao alterar a configuração da aplicação para que o Agente EDR funcione com o MDR, certifique-se de que os componentes responsáveis por receber telemetria estão ativados.

- **Light Agent para proteger ambientes virtuais**. Esta configuração destina-se à aplicação que é usada como parte da solução Kaspersky Security for Virtualization Light Agent. O Light Agent tem de ser instalado em cada máquina virtual que precisa de ser protegida usando a solução. Nesta configuração, não pode utilizar componentes de Encriptação de Dados ou Controlo de Anomalias Adaptativo. Se estiver a instalar o Light Agent num modelo de máquina virtual que será usado para criar *máquinas virtuais não persistentes*, selecione a caixa de verificação **Proteger a 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. Neste modo, o Light Agent recusa atualizações de aplicações que exigem o reinício da máquina virtual. Ao receber atualizações de aplicações que exigem um reinício, o Light Agent gera um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas.

Selecione os componentes da aplicação que estarão disponíveis no computador do utilizador.

Passo 3. Definições avançadas

Configure as definições avançadas para a tarefa (consulte a tabela abaixo).

Passo 4. Selecionar os dispositivos aos quais a tarefa será atribuída

Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 5. Configurar um agendamento de início de uma tarefa

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

Passo 6. Definir o nome da tarefa

Digite um nome para a tarefa, por exemplo, *Adicionar o componente Controlo das Aplicações*.

Passo 7. Completar a criação da tarefa

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa.

Como adicionar ou remover componentes de aplicações na Consola da Web e Consola da Nuvem

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

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

Passo 1. Configurar definições da tarefa geral

Configurar definições da tarefa geral:

1. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2.0**.
2. Na lista pendente **Task type**, selecione **Change application components**.
3. No campo **Task name**, introduza uma breve descrição, por exemplo, *Adicione o componente Controlo de Aplicações*.
4. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

Passo 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 compile uma seleção.

Passo 3. Completar a criação da tarefa

Selecione a caixa de verificação **Open task details when creation is complete** e termine o assistente.

Na janela de propriedades da tarefa, selecione a secção **Application settings**. Em seguida, selecione a configuração da aplicação:

- **Standard mode to protect workstations and servers**. A configuração predefinida. Esta configuração permite utilizar todos os componentes da aplicação, incluindo componentes que fornecem suporte para soluções de Detection and Response. Esta configuração é utilizada para proteção abrangente do computador contra diversas ameaças, ataques de rede e fraudes.

- **Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks**. Nesta configuração, só é possível instalar os componentes que fornecem suporte para soluções Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) e KUMA. Esta configuração será necessária se uma Endpoint Protection Platform (EPP) de terceiros for implementada na sua organização em conjunto com uma solução de Detection and Response da Kaspersky. Isso torna o Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent compatível com aplicações EPP de terceiros.

  Ao alterar a configuração da aplicação para que o Agente EDR funcione com o MDR, certifique-se de que os componentes responsáveis por receber telemetria estão ativados.

- **Light Agent to protect virtual environments**. Esta configuração destina-se à aplicação que é usada como parte da solução Kaspersky Security for Virtualization Light Agent. O Light Agent tem de ser instalado em cada máquina virtual que precisa de ser protegida usando a solução. Nesta configuração, não pode utilizar componentes de Encriptação de Dados ou Controlo de Anomalias Adaptativo. Se estiver a instalar o Light Agent num modelo de máquina virtual que será usado para criar *máquinas virtuais não persistentes*, selecione a caixa de verificação **Protect VDI infrastructure** (VDI significa Virtual Desktop Infrastructure). O modo de proteção VDI ajuda a otimizar o desempenho do Kaspersky Endpoint Security em máquinas virtuais não persistentes. Neste modo, o Light Agent recusa atualizações de aplicações que exigem o reinício da máquina virtual. Ao receber atualizações de aplicações que exigem um reinício, o Light Agent gera um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas.

Selecione os componentes da aplicação que estarão disponíveis no computador do utilizador. Configure as definições avançadas para a tarefa (consulte a tabela abaixo).

Deste modo, será alterado o conjunto de componentes do Kaspersky Endpoint Security nos computadores dos utilizadores. As definições de componentes disponíveis serão exibidas na interface local da aplicação. Os componentes que não foram incluídos na aplicação são desativadas e as definições destes componentes não estão disponíveis.

Ao instalar, se atualizar ou desinstalar o Kaspersky Endpoint Security, poderão ocorrer erros. Para obter mais informações sobre como solucionar esses erros, consulte o Base de conhecimento de Suporte Técnico.

Parâmetro	Descrição
Definições da tarefa	**Verificar a existência de aplicações de terceiros incompatíveis**. Por padrão, o Kaspersky Endpoint Security verifica a compatibilidade das aplicações instaladas. A lista de softwares que podem causar problemas de compatibilidade está disponível no ficheiro incompatible.txt. O ficheiro está incluído no kit de distribuição. Se a verificação do software instalado estiver ativada, o Kaspersky Endpoint Security interromperá a tarefa quando for detetada uma aplicação da lista. Pode desativar a verificação de software instalado se a documentação do fornecedor do software de terceiros afirmar compatibilidade com a Endpoint Protection Platform (EPP). **Remover aplicações de terceiros incompatíveis**. Remoção automática de aplicações listadas no ficheiro incompatible.txt antes de alterar o conjunto de componentes. Se esta funcionalidade estiver ativada, o Kaspersky Endpoint Security tentará remover as aplicações que possam causar problemas de compatibilidade para continuar a tarefa. **Utilizar o modo de compatibilidade do Azure WVD**. Esta funcionalidade garante a exibição correta do estado da máquina virtual do Azure na consola da Kaspersky Anti Targeted Attack Platform. Para monitorizar o desempenho do computador, o Kaspersky Endpoint Security envia telemetria aos servidores KATA. A telemetria inclui um ID do computador (Sensor ID). O modo de compatibilidade do Azure WVD permite atribuir um Sensor ID único permanente a estas máquinas virtuais. Se o modo de compatibilidade estiver desativado, o Sensor ID poderá mudar depois de o computador ser reiniciado devido ao funcionamento das máquinas virtuais do Azure. Isto pode fazer com que os duplicados das máquinas virtuais apareçam na consola.
Exclusões	A partir do Kaspersky Endpoint Security 12.6 para Windows, as exclusões de verificação e as aplicações fiáveis são adicionadas à zona fiável. Exclusões de verificação predefinidas e aplicações fiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e System Center Configuration Manager. Isto significa que não é necessário configurar manualmente uma zona fiável para a aplicação nos servidores. A partir do Kaspersky Endpoint Security 12.8 para Windows, pode instalar aplicação no modo Light Agent para proteger ambientes virtuais. As exclusões de verificação predefinidas e as aplicações fiáveis podem ajudá-lo a configurar rapidamente o Kaspersky Endpoint Security em ambientes virtuais Citrix e VMware. Também pode configurar a zona fiável mais tarde nas propriedades da política: exclusões de verificação e aplicações fiáveis.
Modo separado/Modo combinado	Pode criar conjuntos de componentes separados para estações de trabalho e servidores – **Modo separado**. Antes de implementar o pacote de instalação, o instalador deteta o tipo de sistema operativo e instala apenas os componentes de aplicação que selecionou para esse tipo de sistema operativo. Desta forma, pode utilizar o mesmo pacote de instalação para estações de trabalho e servidores. **Modo combinado** oferece uma lista comum de componentes para estações de trabalho e servidores. A disponibilidade dos componentes individuais depende do tipo de sistema operativo. Neste modo, recomendamos criar um pacote de instalação separado para estações de trabalho e um pacote de instalação separado para servidores. Pode configurar a lista comum de componentes no pacote de instalação apenas no modo Padrão.
Usar a password para modificar o conjunto de componentes da aplicação	Os administradores geralmente ativam a Proteção por password para restringir o Kaspersky Endpoint Security. Ou seja, para modificar a seleção dos componentes da aplicação, tem de inserir credenciais de um utilizador que tenha a permissão **Remover/modificar/restaurar a aplicação**. Por exemplo, pode usar a conta KLAdmin.
Usar a password para desinstalar o Kaspersky Endpoint Agent e o Kaspersky Security for Windows Server	Os administradores geralmente ativam a Proteção por password nas definições destas tarefas para restringir o acesso ao Kaspersky Endpoint Agent (KEA) e ao Kaspersky Security for Windows Server (KSWS). Ou seja, se estiver a migrar da configuração [KES+KEA] para [KES+agente integrado] ou se estiver a migrar do KSWS para o KES, tem de inserir uma password para remover estas aplicações.

Atualização a partir de uma versão anterior da aplicação

Quando atualiza uma versão anterior da aplicação para uma versão mais recente, considere o seguinte:

- Recomendamos que encerre todas as aplicações ativas antes de iniciar a atualização.
- Antes de atualizar, o Kaspersky Endpoint Security bloqueia a funcionalidade de Encriptação de disco completa. Se não for possível bloquear a Encriptação de disco completa, a instalação da atualização não será iniciada. Depois de atualizar a aplicação, a funcionalidade de Encriptação de disco completa será restaurada.
- Para alterar o idioma da aplicação, na tarefa *Install application remotely*, selecione o pacote de instalação com a versão localizada pretendida e atualize a aplicação. A possibilidade de alterar o idioma da aplicação ficou disponível pela primeira vez no Kaspersky Endpoint Security for Windows 14.2.

O Kaspersky Endpoint Security suporta atualizações para as seguintes versões da aplicação:

- 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, se atualizar ou desinstalar o Kaspersky Endpoint Security, poderão ocorrer erros. Para obter mais informações sobre como solucionar esses erros, consulte o Base de conhecimento de Suporte Técnico.

Métodos de atualização da aplicação

O Kaspersky Endpoint Security pode ser atualizado no computador de várias formas:

- Usar o serviço de atualização da Kaspersky (Seamless Update – SMU).
- localmente, usando o Assistente de Configuração.
- localmente a partir da command line.
- remotamente, usando o Kaspersky Security Center.
- remotamente, através do Microsoft Windows Group Policy Management Editor (para obter mais detalhes, visite o Website de Suporte Técnico da Microsoft).
- remotamente, usando o System Center Configuration Manager.

Se a aplicação implementada na rede empresarial tiver um conjunto de componentes diferente do conjunto predefinido, a atualização da aplicação através da Administration Console (MMC) será diferente da atualização através da Web Console. Quando atualizar o Kaspersky Endpoint Security, tenha em atenção o seguinte:

- Consola Web do Kaspersky Security Center.

  Se criou um pacote de instalação para a nova versão da aplicação com o conjunto de componentes predefinidos, o conjunto de componentes no computador do utilizador não será alterado. Para usar o Kaspersky Endpoint Security com o conjunto de componentes predefinidos, é necessário abrir as propriedades do pacote de instalação, alterar o conjunto de componentes e, em seguida, repor o conjunto de componentes original e guardar as alterações.

- Consola de Administração do Kaspersky Security Center.

  O conjunto de componentes da aplicação após a atualização vai corresponder ao conjunto de componentes no pacote de instalação. Ou seja, se a nova versão da aplicação tiver o conjunto predefinido de componentes, o agente MDR incorporado, por exemplo, será removido do computador, uma vez que este componente não está incluído no conjunto predefinido. Para continuar a usar a aplicação com o mesmo conjunto de componentes anterior à atualização, selecione os componentes necessários nas definições do pacote de instalação.

Atualização da aplicação sem um reinício

A atualização da aplicação sem um reinício fornece o funcionamento ininterrupto do servidor quando a versão da aplicação é atualizada.

A atualização da aplicação sem um reinício tem as seguintes limitações:

- Pode atualizar a aplicação sem reiniciar a aplicação a partir da versão 11.10.0. Para atualizar uma versão anterior da aplicação, tem de reiniciar o computador.

- Pode instalar correções sem reiniciar a aplicação a partir da versão 11.11.0. Para instalar correções em versões anteriores da aplicação, pode ser necessário reiniciar o computador.

- A atualização da aplicação sem um reinício não está disponível em computadores com encriptação de dados ativada (Encriptação de Disco Kaspersky (FDE), BitLocker, Encriptação ao nível dos ficheiros (FLE)). Para atualizar a aplicação em computadores com a encriptação de dados ativada, o computador tem de ser reiniciado.

- A aplicação não pode ser atualizada numa máquina virtual sem ser reiniciada. Para atualizar a aplicação numa máquina virtual, tem de reiniciar a máquina virtual.

Após atualizar a aplicação, instalar uma correção, alterar o conjunto de componentes da aplicação ou restaurar, o Kaspersky Endpoint Security reinicia para começar a usar a nova versão. Reiniciar o Kaspersky Endpoint Security pode demorar até um minuto. Durante este período, o nível de proteção do computador é reduzido. Após reiniciar a aplicação, o nível de proteção do computador será restaurado.

Como selecionar o modo de atualização da aplicação na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.

2. Na árvore da consola, selecione **Policies**.

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

4. Na janela de política, selecione **Definições gerais** → **Definições da aplicação**.

5. No bloco **Definições avançadas**, selecione ou desmarque a caixa de verificação **Instalar atualizações da aplicação sem reiniciar** para configurar o modo de atualização da aplicação.

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

Como selecionar o modo de atualização da aplicação na Consola Web

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **General Settings** → **User Interaction**.

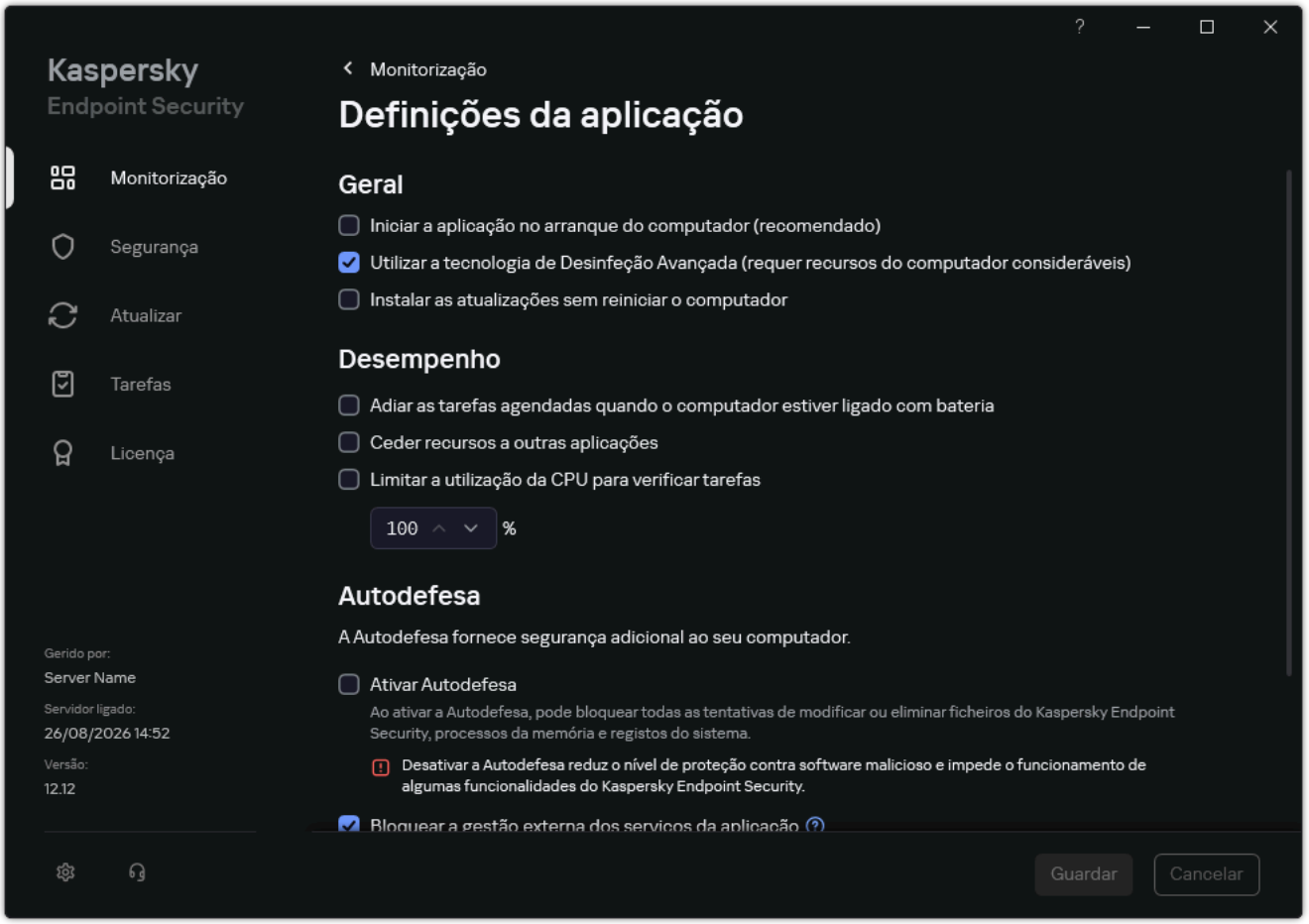
5. No bloco **Application update settings**, selecione ou desmarque a caixa de verificação **Install application updates without restart** para configurar o modo de atualização da aplicação.

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

Como selecionar o modo de atualização da aplicação na interface da aplicação

1. Na janela principal da aplicação, clique no botão .

2. Na janela Application settings, selecione **Definições gerais** → **Definições da aplicação**.



Definições do Kaspersky Endpoint Security for Windows

3. No bloco **Geral**, selecione ou desmarque a caixa de verificação **Instalar as atualizações sem reiniciar o computador** para configurar o modo de atualização da aplicação.

4. Guarde as suas alterações.

Também pode selecionar o modo de atualização da aplicação ao instalar a aplicação a partir da linha de comandos (utilizando a opção `UPGRADEMODE`).

Após a conclusão do processo de atualização da aplicação sem um reinício, a nova versão do Kaspersky Endpoint Security estará instalada no computador. A versão anterior da aplicação é eliminada automaticamente.

Não é possível iniciar uma atualização da aplicação antes de a atualização anterior estar totalmente concluída.

Pode verificar o estado da atualização do Kaspersky Endpoint Security utilizando o relatório da versão da aplicação da Kaspersky na consola do Kaspersky Security Center.

Atualização SMU da aplicação

Para atualizar a aplicação utilizando o serviço de atualização da Kaspersky (Seamless Update; SMU), não tem de executar o instalador, ao contrário de outros métodos de atualização. O Kaspersky Endpoint Security obtém a nova versão da aplicação juntamente com bases de dados de antivírus da mesma fonte.

Uma atualização do SMU permite atualizar a aplicação em todos os computadores da sua organização para a versão mais recente. Antes de aplicar uma atualização do SMU, recomendamos que teste a nova versão da aplicação em alguns computadores. Para o fazer, tem de atualizar manualmente a aplicação nestes computadores (por exemplo, localmente, utilizando o Assistente de Configuração). Não pode selecionar computadores individuais ao realizar uma atualização do SMU.

O calendário de atualização da aplicação é determinado pelo pessoal da Kaspersky. Para se certificar de que a nova versão da aplicação está a funcionar sem problemas, a Kaspersky disponibiliza atualizações regularmente. Isto significa que pode receber a sua atualização do SMU até dois meses depois do lançamento de uma nova versão.

Pode gerir a atualização do SMU da aplicação utilizando a tarefa *Atualização das bases de dados e módulos da aplicação*. Para que a nova versão da aplicação seja incluída no mesmo pacote que as bases de dados de antivírus, tem de permitir a atualização dos *módulos da aplicação* nas definições da tarefa *Atualização das bases de dados e módulos da aplicação*. Também nas definições da tarefa *Atualização das bases de dados e módulos da aplicação* pode permitir atualização da aplicação sem reinicialização.

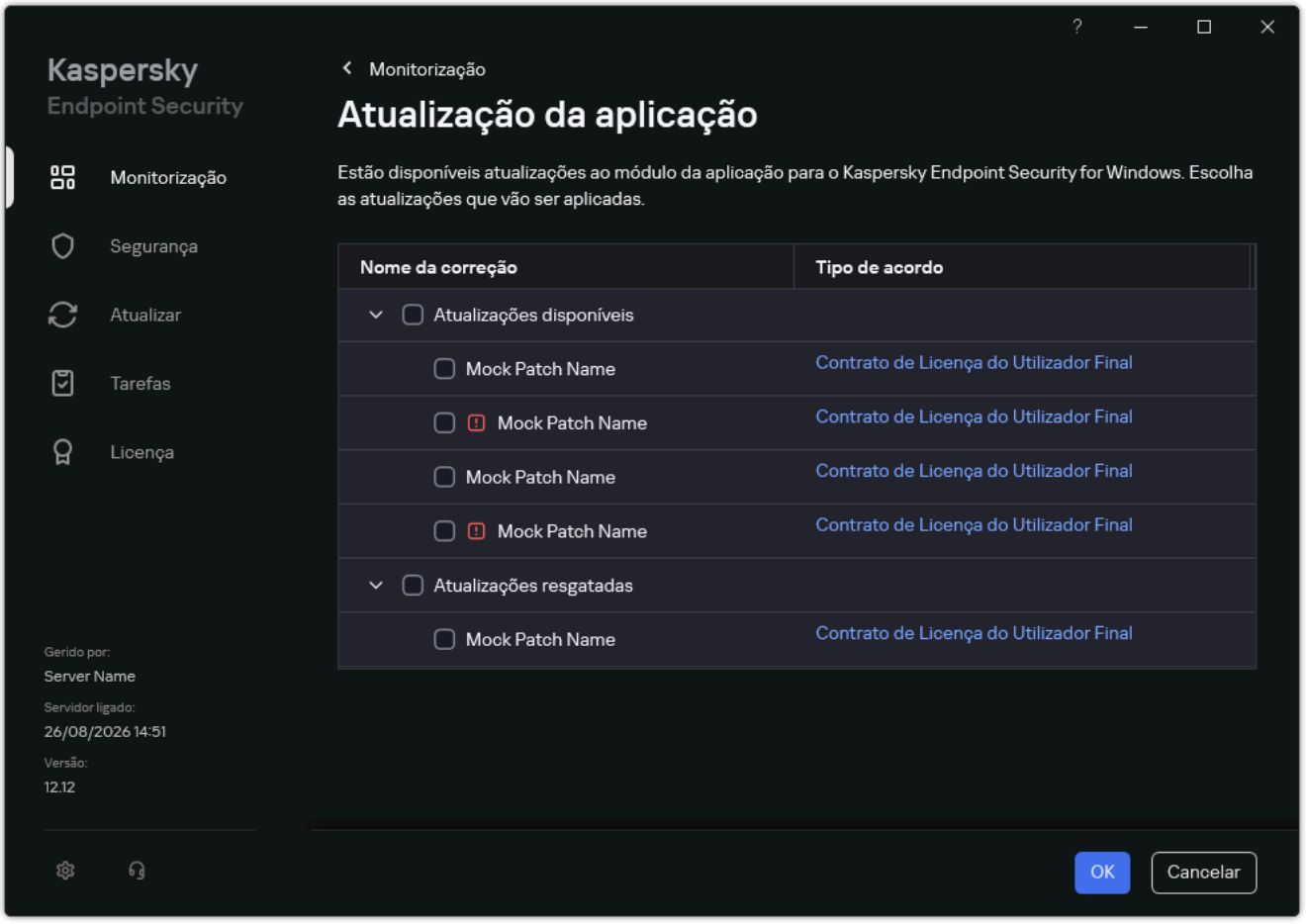
Passos de uma atualização do SMU da aplicação

1. **Depois de uma nova versão da aplicação ser lançada, a Kaspersky distribui a atualização.**
2. **O utilizador aprova a atualização da aplicação.**

   Se o computador estiver associado ao Kaspersky Security Center, a atualização está disponível no Kaspersky Security Center, na secção **Update of Kaspersky databases and application modules**. Para obter mais informações sobre as atualizações de aprovação, consulte a Ajuda do Kaspersky Security Center.

   Se o computador não estiver associado ao Kaspersky Security Center, a atualização está disponível na secção de notificações da interface da aplicação: . Para aprovar a atualização, selecione uma versão da aplicação e aceite os termos e condições dos acordos (consulte a figura abaixo).
3. **O Kaspersky Endpoint Security executa a tarefa *Atualização das bases de dados e módulos da aplicação* de acordo com o agendamento configurado.**

Deste modo, o Kaspersky Endpoint Security atualiza a aplicação em modo "silencioso".



Atualizações de aplicações disponíveis

Remover a aplicação

Remover o Kaspersky Endpoint Security deixa o computador e os dados do utilizador desprotegidos relativamente a ameaças.

Ao instalar, se atualizar ou desinstalar o Kaspersky Endpoint Security, poderão ocorrer erros. Para obter mais informações sobre como solucionar esses erros, consulte o Base de conhecimento de Suporte Técnico.

Remover a aplicação remotamente através do Kaspersky Security Center

Pode desinstalar remotamente a aplicação usando a tarefa *Uninstall application remotely*. Ao executar a tarefa, o Kaspersky Endpoint Security transfere a utilitário de desinstalação da aplicação para o computador do utilizador. O utilitário será removido automaticamente após a conclusão da desinstalação da aplicação.

Como remover a aplicação através da Consola de administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Tasks**.
   A lista de tarefas é aberta.
3. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

Selecione **Kaspersky Security Center Administration Server → Advanced → Uninstall application remotely**.

Passo 2. Selecionar a aplicação a remover

Selecione **Uninstall application supported by Kaspersky Security Center**.

Passo 3. Definições da tarefa para desinstalação da aplicação

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

Passo 4. Desinstalar definições de utilitários

Configure as seguintes definições adicionais da aplicação:

- **Force download of the uninstallation utility**. Selecionar o método de entrega do utilitário:
  - **Using Network Agent**. Se o Agente de Rede não tiver sido instalado no computador, o primeiro Agente de Rede será instalado utilizando as ferramentas do sistema operativo. O Kaspersky Endpoint Security é então desinstalado pelas ferramentas do Agente de Rede.
  - **Using operating system resources through Administration Server**. O utilitário será entregue a computadores do cliente utilizando os recursos do sistema operativo através do Servidor de administração. Pode selecionar esta opção se nenhum Agente de Rede for instalado no computador cliente, mas o computador cliente está na mesma rede que o Servidor de administração.
  - **Using operating system resources through distribution points**. O utilitário é transmitido aos computadores do cliente utilizando recursos do sistema operativo através de pontos de distribuição. Pode selecionar esta opção se houver pelo menos um ponto de distribuição na rede. Para obter mais informação detalhadas sobre os pontos de distribuição, consulte a Ajuda do Kaspersky Security Center.
- **Verify operating system type before downloading**. Se necessário, desmarque esta caixa de verificação. Isto permite-lhe evitar a transferência do utilitário de desinstalação se o sistema operativo do computador não cumprir os requisitos do software. Pode ignorar esta verificação se tiver a certeza que o sistema operativo do computador cumpre os requisitos do software.

Se a operação de desinstalação da aplicação estiver protegida por password, faça o seguinte:

1. Selecione a caixa de verificação **Use uninstallation password**.
2. Selecione o botão **Edit**.
3. Introduza a password da conta do KLAdmin.

Passo 5. Selecionar a definição de reinicialização do sistema operativo

Após a desinstalação da aplicação, é necessário uma reinicialização. Selecione a ação que será executada para reiniciar o computador.

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

Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 7. Selecionar a conta para executar a tarefa

Selecione a conta para instalar o Agente de Rede utilizando as ferramentas do sistema operativo. Neste caso, os direitos de administrador são necessitados para o acesso do computador. Pode adicionar múltiplas contas. Se uma conta não tiver direitos suficientes, o Assistente de Instalação utiliza a conta seguinte. Não tem de selecionar uma conta se desinstalar o Kaspersky Endpoint Security utilizando ferramentas do Agente de Rede.

Passo 8. Configurar um agendamento de início de uma tarefa

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

Passo 9. Definir o nome da tarefa

Introduza um nome para a tarefa, por exemplo, *Desinstalar o Kaspersky Endpoint Security 14.2*.

Passo 10. Concluir a criação da tarefa

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa.

A aplicação será desinstalada no modo não assistido.

Como remover aplicações através da Consola Web e Consola de Nuvem

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

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

Passo 1. Configurar definições da tarefa geral

Configurar definições da tarefa geral:

1. Na lista pendente **Application**, selecione **Kaspersky Security Center**.
2. Na lista pendente **Task type**, selecione **Uninstall application remotely**.
3. No campo **Task name**, introduza uma breve descrição, por exemplo, *Desinstale o Kaspersky Endpoint Security dos computadores da Assistência Técnica*.
4. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

Passo 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 compile uma seleção.

Passo 3. Configurar as definições de desinstalação da aplicação

Neste passo, configure as definições de desinstalação da aplicação:

1. Selecione o tipo de **Uninstall managed application**.
2. Selecione **Kaspersky Endpoint Security for Windows**.

3. **Force download of the uninstallation utility**. Selecionar o método de entrega do utilitário:

   - **Using Network Agent**. Se o Agente de Rede não tiver sido instalado no computador, o primeiro Agente de Rede será instalado utilizando as ferramentas do sistema operativo. O Kaspersky Endpoint Security é então desinstalado pelas ferramentas do Agente de Rede.

   - **Using operating system resources through Administration Server**. O utilitário será entregue a computadores do cliente utilizando os recursos do sistema operativo através do Servidor de administração. Pode selecionar esta opção se nenhum Agente de Rede for instalado no computador cliente, mas o computador cliente está na mesma rede que o Servidor de administração.

   - **Using operating system resources through distribution points**. O utilitário é transmitido aos computadores do cliente utilizando recursos do sistema operativo através de pontos de distribuição. Pode selecionar esta opção se houver pelo menos um ponto de distribuição na rede. Para obter mais informação detalhadas sobre os pontos de distribuição, consulte a Ajuda do Kaspersky Security Center.

4. No campo **Maximum number of concurrent downloads**, defina um limite no número de pedidos enviados ao Administration Server para transferir o utilitário de desinstalação da aplicação. Um número limite de pedidos ajudará a impedir uma sobrecarga na rede.

5. No campo **Maximum number of uninstallation attempts**, defina um número limite de tentativas de desinstalação da aplicação. Se desinstalação do Kaspersky Endpoint Security terminar com um erro, a tarefa iniciará automaticamente a desinstalação novamente.

6. Se necessário, desmarque a caixa de verificação **Verify operating system type before downloading**. Isto permite-lhe evitar a transferência do utilitário de desinstalação se o sistema operativo do computador não cumprir os requisitos do software. Pode ignorar esta verificação se tiver a certeza que o sistema operativo do computador cumpre os requisitos do software.

Passo 4. Selecionar a conta para executar a tarefa

Selecione a conta para instalar o Agente de Rede utilizando as ferramentas do sistema operativo. Neste caso, os direitos de administrador são necessitados para o acesso do computador. Pode adicionar múltiplas contas. Se uma conta não tiver direitos suficientes, o Assistente de Instalação utiliza a conta seguinte. Não tem de selecionar uma conta se desinstalar o Kaspersky Endpoint Security utilizando ferramentas do Agente de Rede.

Passo 5. Completar a criação da tarefa

Termine o assistente clicando no botão **Finish**. Será apresentada uma nova tarefa na lista de tarefas.

Para executar uma tarefa, selecione a caixa de seleção em frente da tarefa e clique no botão **Start**. A aplicação será desinstalada no modo não assistido. Após a conclusão da desinstalação, o Kaspersky Endpoint Security apresenta um aviso para reiniciar o computador.

Se a operação de desinstalação da aplicação estiver protegida por password, introduza a password da conta KLAdmin nas propriedades da tarefa *Uninstall application remotely*. Sem a password, a tarefa não será executada.

Para usar a password da conta KLAdmin na tarefa Uninstall application remotely:

1. Na janela principal da Consola Web, selecione **Asset management** → **Tasks**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Uninstall application remotely** do Kaspersky Security Center.

   É apresentada a janela de propriedades da tarefa.

3. Selecione o separador **Application settings**.

4. Selecione a caixa de verificação **Use uninstallation password**.

5. Introduza a password da conta do KLAdmin.

6. Guarde as suas alterações.

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

Remover a aplicação remotamente através do Active Directory

Pode desinstalar remotamente a aplicação utilizando uma política de grupo do Microsoft Windows. Para desinstalar a aplicação, tem de abrir a Consola de Gestão da Política de Grupo (gpmc.msc) e utilizar o Editor da Política de Grupo para criar uma tarefa de remoção da aplicação (para mais detalhes, visite o site de suporte técnico da Microsoft).

Se a operação de desinstalação da aplicação estiver protegida por password, tem de fazer o seguinte:

1. Criar um ficheiro BAT com o seguinte conteúdo:

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

   `<GUID>` é a ID única da aplicação. Pode consultar o GUID da aplicação na Base de conhecimento de Suporte Técnico ou utilizando o 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 na Consola de Gestão da Política do Grupo (gpmc.msc).

3. Utilize a nova política para executar o ficheiro BAT criado nos computadores.

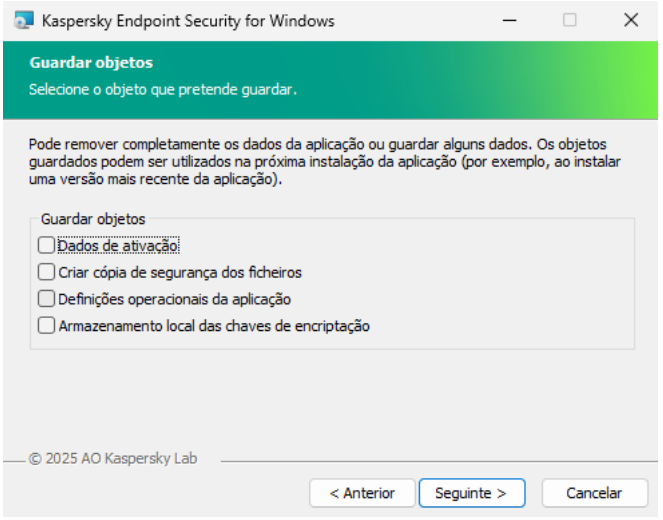
Remover a aplicação localmente

Também pode remover a aplicação localmente, usando o Assistente de Configuração. O Kaspersky Endpoint Security é removido usando o método normal para um sistema operativo Windows, que é através do Painel de Controlo. O Assistente de configuração é iniciado. Siga as instruções apresentadas no ecrã.



Selecionar a operação de remoção da aplicação

Pode especificar que dados são utilizados pela aplicação que quer guardar para uso futuro, durante a próxima instalação da aplicação (por exemplo, ao atualizar para uma versão mais recente da aplicação). Se não especificar quaisquer dados, a aplicação será totalmente removida (veja a figura abaixo).



Guardar dados após a remoção

Pode guardar os seguintes dados:

- **Dados de ativação**, que lhe permite evitar a ativação da aplicação novamente. O Kaspersky Endpoint Security adiciona automaticamente uma chave de licença se a validade da licença não tiver expirado antes da instalação.
- **Criar cópia de segurança dos ficheiros** – ficheiros verificados pela aplicação e colocados na Cópia de Segurança.

Os ficheiros de Cópia de segurança que são guardados após a remoção da aplicação podem ser acedidos apenas a partir da mesma versão da aplicação que foi utilizada para guardá-los.

Se pretender utilizar os objetos de Cópia de Segurança após a remoção da aplicação, tem de restaurar esses objetos antes de remover a aplicação. Contudo, os peritos da Kaspersky não recomendam restaurar os ficheiros de Cópia de segurança, uma vez que tal pode prejudicar o computador.

- **Definições operacionais da aplicação** – valores das definições da aplicação selecionados durante a configuração da aplicação.
- **Armazenamento local das chaves de encriptação** – dados que fornecem acesso a ficheiros e unidades que foram encriptados antes da remoção da aplicação. Para garantir o acesso a ficheiros e unidades encriptados, certifique-se de que selecionou a funcionalidade de encriptação dos dados ao reinstalar o Kaspersky Endpoint Security. Nenhuma ação adicional é necessária para acesso a ficheiros e unidades encriptados anteriormente.

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

Também pode eliminar a aplicação localmente utilizando a command line.

Licenciamento da aplicação

Esta secção fornece informações sobre conceitos gerais relativos às licenças do Kaspersky Endpoint Security.

Acerca do Contrato de Licença do Utilizador Final

O *Contrato de Licença do Utilizador Final* constitui um acordo vinculativo entre o utilizador e a AO Kaspersky Lab, que estabelece os termos nos quais a aplicação pode ser utilizada.

É recomendada a leitura atenta dos termos do Contrato de Licença antes de utilizar a aplicação.

Pode consultar os termos do Contrato de Licença das seguintes formas:

- Ao instalar o Kaspersky Endpoint Security em modo interativo.
- Lendo o ficheiro license.txt. Este documento está incluído no kit de distribuição de aplicações e também se encontra na pasta de instalação da aplicação `%ProgramFiles(x86)%\Kaspersky Lab\KES\Doc\<locale>\KES`.

Ao confirmar que concorda com o Contrato de Licença do Utilizador Final na instalação da aplicação, está a reconhecer a sua aceitação dos termos do Contrato de Licença do Utilizador Final. Caso não aceite os termos do Contrato de Licença do Utilizador Final, deverá abortar a instalação.

Sobre a licença

Uma *licença* consiste num direito de duração limitada de utilização da aplicação, concedido nos termos do Contrato de Licença do Utilizador Final.

A licença dá-lhe o direito de utilizar a aplicação em conformidade com os termos do Contrato de Licença do Utilizador Final e de receber suporte técnico. A lista de funcionalidades disponíveis e o termo de utilização da aplicação dependem do tipo de licença utilizado para ativar a aplicação.

São fornecidos os seguintes tipos de licença:

- *Avaliação* – licença gratuita destinada a uma utilização experimental da aplicação.

  Uma licença de avaliação tem normalmente um período de validade curto. Quando a licença de avaliação expirar, todas as funcionalidades do Kaspersky Endpoint Security são desativadas. Para continuar a utilizar a aplicação, tem de adquirir uma licença comercial.

  Pode ativar a aplicação sob uma licença de avaliação apenas uma vez. A aplicação não pode ser ativada com uma licença de avaliação depois de ter sido ativada com uma licença comercial.

- *Comercial* – uma licença paga fornecida ao adquirir o Kaspersky Endpoint Security.

  As funcionalidades da aplicação disponíveis com a licença comercial dependem da escolha do produto. O produto selecionado é indicado no Certificado de Licença. As informações acerca dos produtos disponíveis encontram-se no website da Kaspersky.

Quando a licença comercial expira, as principais funcionalidades da aplicação são desativadas. Para continuar a utilizar a aplicação, tem de renovar a sua licença comercial. Se não estiver a planear renovar a sua licença, tem de remover a aplicação do seu computador.

Sobre o certificado de licença

Um *certificado de licença* é um documento transferido para o utilizador em conjunto com um ficheiro-chave ou um código de ativação.

O certificado de licença contém as seguintes informações sobre a licença:

- ID de licença ou número de ordem.
- Os detalhes do utilizador a quem a licença é concedida.
- Os detalhes da aplicação que pode ser ativada através da licença.
- A limitação do número de unidades licenciadas (por exemplo, o número de dispositivos nos quais a aplicação pode ser utilizada de acordo com a licença).
- Data de início da validade da licença.
- Data de expiração da licença ou validade da licença.
- Tipo de licença.

Sobre a subscrição

A *Subscrição para o Kaspersky Endpoint Security* é uma ordem de compra para a aplicação com parâmetros específicos (como a data de validade da subscrição e o número de dispositivos protegidos). Pode solicitar uma subscrição para o Kaspersky Endpoint Security ao seu fornecedor de serviços (por exemplo, ao seu ISP). Uma subscrição pode ser renovada manual ou automaticamente ou pode também ser cancelada. Pode gerir a subscrição no site do fornecedor de serviços.

A subscrição pode ser limitada (um ano, por exemplo) ou ilimitada (sem data de validade). Para manter o Kaspersky Endpoint Security a funcionar após o fim da validade da subscrição limitada, tem de renovar a subscrição. A subscrição ilimitada é renovada automaticamente se os serviços do fornecedor tiverem sido atempadamente pré-pagos.

Quando uma subscrição limitada expira, pode ser-lhe concedido um período de carência da renovação da subscrição, durante o qual a aplicação continua a funcionar. A disponibilidade e a duração de tal período de carência são decididas pelo fornecedor de serviços.

Para utilizar o Kaspersky Endpoint Security com subscrição, tem de aplicar o código de ativação recebido do fornecedor de serviços. Após aplicar o código de ativação, a chave ativa é adicionada. A chave ativa determina a licença para utilizar a aplicação com subscrição. Não é possível ativar a aplicação com a subscrição utilizando um ficheiro-chave. O prestador de serviços apenas pode fornecer um código de ativação. Não é possível adicionar uma chave de reserva ao abrigo de uma subscrição.

Os códigos de ativação adquiridos com subscrição podem não ser utilizados para ativar versões anteriores do Kaspersky Endpoint Security.

Sobre a chave de licença

Uma *chave de licença* é uma sequência de bits que pode utilizar para ativar e, em seguida, utilizar a aplicação de acordo com os termos do Contrato de Licença do Utilizador Final.

Um certificado de licença não é fornecido para uma chave adicionada ao abrigo de uma subscrição.

Pode adicionar uma chave de licença à aplicação aplicando um ficheiro de chave ou introduzindo um código de ativação.

A chave pode ser bloqueada pela Kaspersky se os termos do Contrato de Licença do Utilizador Final forem violados. Se a chave foi bloqueada, deve adicionar uma chave diferente para continuar a utilizar a aplicação.

Existem dois tipos de chave: ativa e de reserva.

Uma *chave ativa* é uma chave que está a ser atualmente utilizada pela aplicação. É possível adicionar uma chave de licença de avaliação ou comercial como chave ativa. A aplicação não pode ter mais de uma chave ativa.

Uma *chave de reserva* é uma chave que permite ao utilizador utilizar a aplicação, mas que não está atualmente a ser utilizada. Na altura da expiração da chave ativa, uma chave de reserva torna-se automaticamente ativa. Só é possível adicionar uma chave de reserva se a chave ativa estiver disponível.

Pode ser adicionada uma chave para uma licença de avaliação apenas como chave ativa. Não pode ser adicionada como a chave de reserva. Uma chave de 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 da aplicação definida pela licença usada para ativar a aplicação permanecerá disponível por oito dias. A aplicação notifica o utilizador de que a chave foi adicionada à lista de chaves proibidas. Após oito dias, a funcionalidade da aplicação fica limitada ao nível de funcionalidade disponível após a expiração da licença. Pode utilizar componentes de proteção e controlo e executar uma verificação utilizando as bases de dados das aplicações que foram instaladas antes da licença expirar. A aplicação também continua a encriptar os ficheiros modificados e encriptados antes de a licença expirar, mas não encripta novos ficheiros. A utilização do Kaspersky Security Network não está disponível.

Sobre o código de ativação

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

Para ativar a aplicação com um código de ativação, é necessário ter acesso à Internet para se ligar aos servidores de ativação da Kaspersky.

Quando a aplicação é ativada utilizando um código de ativação, a chave ativa é adicionada. Uma chave de reserva pode ser adicionada apenas através da utilização de um código de ativação e não pode ser adicionada utilizando um ficheiro-chave.

Se o código de ativação tiver sido perdido depois de ativar a aplicação, pode restaurar o código de ativação. Pode precisar de um código de ativação, por exemplo, para registar uma Kaspersky CompanyAccount. Se o código de ativação foi perdido após a ativação da aplicação, contacte o parceiro da Kaspersky a quem adquiriu a licença.

Sobre o ficheiro-chave

Um *ficheiro-chave* é um ficheiro com a extensão .key que recebe da Kaspersky. O objetivo de um ficheiro-chave é adicionar uma chave de licença que ativa a aplicação.

Recebe um ficheiro-chave no e-mail fornecido quando comprou o Kaspersky Endpoint Security ou encomendou a versão de avaliação do Kaspersky Endpoint Security.

Não precisa de se ligar a servidores de ativação da Kaspersky para ativar a aplicação com um ficheiro-chave.

Pode recuperar um ficheiro-chave, caso ele tenha sido apagado acidentalmente. Pode precisar de um ficheiro-chave para registar um Kaspersky CompanyAccount, por exemplo.

Para recuperar um ficheiro-chave, efetue um dos seguintes procedimentos:

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

Quando a aplicação é ativada utilizando um ficheiro-chave, é adicionada uma chave ativa. Uma chave de reserva pode ser adicionada apenas através da utilização de um ficheiro-chave e não pode ser adicionada utilizando um código de ativação.

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

A funcionalidade do Kaspersky Endpoint Security disponível para estações de trabalho depende do tipo de licença (ver tabela abaixo).

Ver também a comparação da funcionalidade da aplicação para servidores.

Comparação da funcionalidade da aplicação dependendo do tipo de licença do Kaspersky Next, consulte em Ajuda do Kaspersky Next.

Comparação das funcionalidades do Kaspersky Endpoint Security

Funcionalidade	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	✓	✓	✓	✓	✓	✓	✓	✓
Deteção de comportamento	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓	✓	✓	✓	✓
Prevenção de explorações	✓	✓	✓	✓	✓	✓	✓	✓
Prevenção contra invasões	✓	✓	✓	✓	✓	✓	✓	✓
Motor de remediação	✓	✓	✓	✓	✓	✓	✓	✓
Proteção essencial contra ameaças								
Proteção contra ameaças de ficheiros	✓	✓	✓	✓	✓	✓	✓	✓
Proteção contra ameaças da Web	✓	✓	✓	✓	✓	✓	✓	✓
Proteção contra ameaças de correio	✓	✓	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓	✓	✓
Proteção contra ameaças de Rede	✓	✓	✓	✓	✓	✓	✓	✓
Prevenção de ataques BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
Proteção AMSI	✓	✓	✓	✓	✓	✓	✓	✓
Controlos de segurança								

Funcionalidade	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 Registo	–	–	–	–	–	–	–	–
Controlo das aplicações	✓	✓	✓	✓	✓	✓	✓	✓
Controlo de Dispositivos	✓	✓	✓	✓	✓	✓	✓	✓
Controlo de Internet	✓	✓	✓	✓	✓	✓	✓	✓
Controlo de Anomalias Adaptativo	–	✓	✓	✓	✓	✓	–	✓
Monitorização da integridade do sistema	–	–	–	–	–	–	–	–
Encriptação de dados								
Encriptação de disco Kaspersky	–	✓	✓	✓	✓	✓	–	✓
Encriptação de Unidade BitLocker	–	✓	✓	✓	✓	✓	–	✓
Encriptação ao nível dos ficheiros	–	✓	✓	✓	✓	✓	–	✓
Encriptação de unidades amovíveis	–	✓	✓	✓	✓	✓	–	✓
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(A licença do Kaspersky Sandbox tem de ser comprada em separado)*	✓	✓	✓	✓	✓	✓	✓	✓
Integração com o KUMA *(a licença para a Integração do KUMA tem de ser adquirida separadamente)*	✓	✓	✓	✓	✓	✓	✓	✓
Modo Light Agent *(para ativar a aplicação, tem de adicionar uma chave de licença à SVM ao qual o Light Agent está ligado)*	–	–	–	–	–	–	✓	✓

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

A funcionalidade do Kaspersky Endpoint Security disponível nos servidores depende do tipo de licença (ver tabela abaixo)

Ver também a comparação da funcionalidade da aplicação para estações de trabalho

Comparação da funcionalidade da aplicação dependendo do tipo de licença do Kaspersky Next, consulte em Ajuda do Kaspersky Next.

Comparação das funcionalidades do Kaspersky Endpoint Security

Funcionalidade	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	✓	✓	✓	✓	✓	✓	✓	✓
Deteção de comportamento	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓	✓	✓	✓	✓
Prevenção de explorações	✓	✓	✓	✓	✓	✓	✓	✓
Prevenção contra invasões	–	–	–	–	–	–	–	–
Motor de remediação	✓	✓	✓	✓	✓	✓	✓	✓
Proteção essencial contra ameaças								
Proteção contra ameaças de ficheiros	✓	✓	✓	✓	✓	✓	✓	✓
Proteção contra ameaças da Web	–	✓	✓	✓	✓	✓	✓	✓
Proteção contra ameaças de correio	–	✓	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓	✓	✓
Proteção contra ameaças de Rede	✓	✓	✓	✓	✓	✓	✓	✓
Prevenção de ataques BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
Proteção AMSI	✓	✓	✓	✓	✓	✓	✓	✓
Controlos de segurança								
Inspeção do Registo	–	–	–	–	–	–	–	✓

Funcionalidade	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
Controlo das aplicações	–	✓	✓	✓	✓	✓	–	✓
Controlo de Dispositivos	–	✓	✓	✓	✓	✓	✓	✓
Controlo de Internet	–	✓	✓	✓	✓	✓	✓	✓
Controlo de Anomalias Adaptativo	–	–	–	–	–	–	–	–
Monitorização da integridade do sistema	–	–	–	–	–	–	–	✓
Encriptação de dados								
Encriptação de disco Kaspersky	–	–	–	–	–	–	–	–
Encriptação BitLocker de Unidade	–	✓	✓	✓	✓	✓	–	✓
Encriptação ao nível dos ficheiros	–	–	–	–	–	–	–	–
Encriptação de unidades amovíveis	–	–	–	–	–	–	–	–
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(A licença do Kaspersky Sandbox tem de ser comprada em separado)*	✓	✓	✓	✓	✓	✓	✓	✓
Integração com o KUMA *(a licença para a Integração do KUMA tem de ser adquirida separadamente)*	✓	✓	✓	✓	✓	✓	✓	✓
Modo Light Agent *(para ativar a aplicação, tem de adicionar uma chave de licença à SVM ao qual o Light Agent está ligado)*	–	–	–	–	–	–	✓	✓

Ativar a aplicação

A *Ativação* é o processo de ativação de uma licença, que permite utilizar uma versão totalmente funcional da aplicação até a licença expirar. Ativação da aplicação implica a adição de uma chave de licença.

Pode ativar a aplicação através de uma das seguintes formas:

- Localmente na interface da aplicação, usando o Assistente de Ativação. É possível adicionar a chave ativa e a chave de reserva desta forma.
- Usando remotamente o pacote de software Kaspersky Security Center.
  - Utilizar a tarefa *Adicionar chave*.

    Este método permite-lhe adicionar uma chave para um computador específico ou para computadores que fazem parte de um grupo de administração. É possível adicionar a chave ativa e a chave de reserva desta forma.
  - Ao distribuir uma chave armazenada no Servidor de administração do Kaspersky Security Center aos computadores.

    Este método permite adicionar automaticamente uma chave aos computadores que já estão ligados ao Kaspersky Security Center e também a novos computadores. Para utilizar este método, tem de primeiro adicionar a chave ao Servidor de Administração do Kaspersky Security Center. Para obter informações detalhadas adicionais sobre a adição de chaves do Servidor de administração do Kaspersky Security Center, consulte a Ajuda do Kaspersky Security Center.

    O código de ativação adquirido com subscrição é distribuído em primeiro lugar.
  - Ao adicionar a chave ao pacote de instalação do Kaspersky Endpoint Security.

    Este método permite que adicione a chave em Propriedades do pacote de instalação durante a implementação do Kaspersky Endpoint Security. A aplicação é ativada automaticamente após a instalação.
- Utilização da linha de comandos.

Poderá demorar algum tempo a ativar a aplicação com um código de ativação (durante a instalação remota ou não interativa) devido à distribuição de carga entre os servidores de ativação do Kaspersky. Se for necessário ativar a aplicação imediatamente, pode interromper o processo de ativação em curso e iniciar a ativação utilizando o Assistente de Ativação.

Se o Kaspersky Endpoint Security estiver a ser usado no modo Light Agent para proteger ambientes virtuais, não será necessário ativar a aplicação separadamente.

Ativar a aplicação

Como ativar a aplicação na Consola de administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Tasks**.

   A lista de tarefas é aberta.
2. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

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

Passo 2. Adicionar uma chave

Introduza um código de ativação ou selecione um ficheiro de chave.

Para obter informações detalhadas adicionais sobre a adição de chaves ao Kaspersky Security Center, consulte a Ajuda do Kaspersky Security Center.

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

Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 4. Configurar um agendamento de início de uma tarefa

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

Passo 5. Definir o nome da tarefa

Digite um nome para a tarefa, como *Activate Kaspersky Endpoint Security for Windows*.

Passo 6. Completar a criação da tarefa

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa. Como resultado, o Kaspersky Endpoint Security será ativado nos computadores dos utilizadores no modo silencioso.

Como ativar a aplicação na Consola da Web e na Consola da Nuvem

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

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

Passo 1. Configurar definições da tarefa geral

Configurar definições da tarefa geral:

1. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.
2. Na lista pendente **Task type**, selecione **Add key**.
3. No campo **Task name**, introduza uma breve descrição, por exemplo, *Activation of Kaspersky Endpoint Security for Windows*.
4. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa. Avance para o passo seguinte.

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

Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 3. Selecionar numa licença

Selecione a licença que pretende utilizar para ativar a aplicação. Avance para o passo seguinte.

Pode adicionar chaves à Consola Web (**Operations → Licensing**).

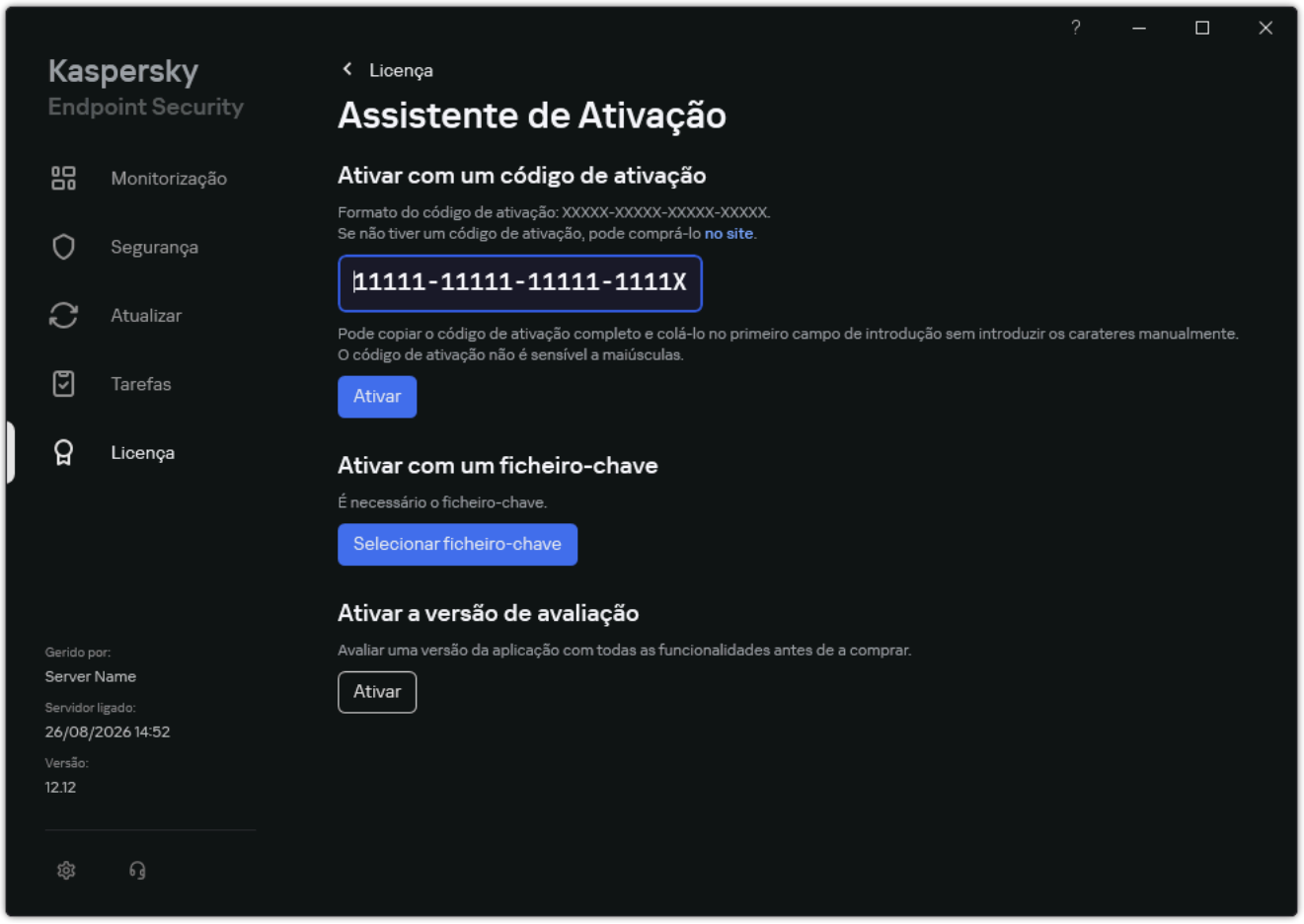
Passo 4. Completar a criação da tarefa

Termine o assistente clicando no botão **Finish**. Será apresentada uma nova tarefa na lista de tarefas. Para executar uma tarefa, selecione a caixa de seleção em frente da tarefa e clique no botão **Start**. Como resultado, o Kaspersky Endpoint Security será ativado nos computadores dos utilizadores no modo silencioso.

Como ativar a aplicação na interface da aplicação

1. Na janela principal da aplicação, aceda à secção **Licença**.
2. Clique em **Ativar a aplicação com uma licença nova**.

   Arranque do Assistente de Ativação da Aplicação. Siga as instruções do Assistente de Ativação.



Ativar a aplicação

Nas propriedades da tarefa *Adicionar chave*, pode adicionar uma chave de reserva ao computador. Uma *chave de reserva* é ativada quando a chave ativa expira. A disponibilidade de uma chave de reserva permite evitar limitações da funcionalidade da aplicação quando uma licença expira.

Como adicionar automaticamente uma chave de licença aos computadores através da Consola de Administração (MMC)

1. Na Consola de Administração, dirija-se à pasta **Kaspersky Licenses**.

   Uma lista de chaves de licença surge.

2. Abra as propriedades da chave de licença.

3. Na secção **General**, marque a caixa de verificação **Automatically distribute license key to managed devices**.

4. Guarde as suas alterações.

Deste modo, a chave será automaticamente distribuída aos computadores apropriados. Durante a distribuição automática de uma chave como uma chave ativa ou uma chave de reserva, é considerado o limite de licenças (definido nas propriedades da chave) no número de computadores. Se o limite de licenças for atingido, a distribuição desta chave aos computadores é automaticamente interrompida. Pode ver o número de computadores aos quais a chave foi adicionada e outros dados sobre as propriedades da chave na secção **Devices**.

Como adicionar automaticamente uma chave de licença aos computadores através da Consola da Web e da Consola da Nuvem

1. Na janela principal da Consola Web, selecione **Operations → Licensing → Licenses**.

   Uma lista de chaves de licença surge.

2. Abra as propriedades da chave de licença.

3. No separador **General**, ative o botão de alternar **Automatically distribute license key to managed devices**.

4. Guarde as suas alterações.

Deste modo, a chave será automaticamente distribuída aos computadores apropriados. Durante a distribuição automática de uma chave como uma chave ativa ou uma chave de reserva, é considerado o limite de licenças (definido nas propriedades da chave) no número de computadores. Se o limite de licenças for atingido, a distribuição desta chave aos computadores é automaticamente interrompida. Pode ver o número de computadores aos quais a chave foi adicionada e outros dados sobre as propriedades da chave no separador **Devices**.

Se estiver a ativar a aplicação com um *código de ativação*, é necessário ter acesso à Internet para se ligar aos servidores de ativação da Kaspersky. Se estiver a ativar a aplicação com um *ficheiro-chave*, o acesso à Internet não é necessário. Se os computadores estiverem num segmento de rede isolado sem acesso à Internet, para ativar a aplicação com um código, tem de permitir a utilização do Kaspersky Security Center Administration Server como um servidor proxy. Ou seja, a aplicação pode obter acesso aos servidores de ativação através do Servidor de Administração que possui acesso à Internet.

Como permitir a utilização do Servidor de Administração como um servidor proxy para ativar a aplicação na Administration Console (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Definições gerais → Definições da aplicação**.

4. Selecione a caixa de verificação **Utilizar o Kaspersky Security Center como servidor de proxy para ativação**.

5. Guarde as suas alterações.

Como permitir a utilização do Servidor de Administração como um servidor proxy para ativar a aplicação na Web Console e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **KSC Integration**.
5. Selecione a caixa de verificação **Use Kaspersky Security Center as proxy server for activation**.
6. Guarde as suas alterações.

Se não for possível ativar a aplicação com um *código de ativação*, pode tentar obter um *ficheiro-chave* ao utilizar o solução da Kaspersky e tentar ativar novamente a aplicação através de um método diferente.

Monitorização de utilização de licença

Pode monitorizar a utilização de licenças dos seguintes modos:

- Ver o *Report on usage of license keys* para a infraestrutura da organização (**Monitoring** → **Reports**).
- Ver os estados dos computadores no separador **Managed devices** → **Devices**. Se a aplicação não estiver ativada, o computador apresenta o estado ⚠ *A aplicação não está ativada*.
- Ver informações da licença nas propriedades do computador.
- Ver propriedades da chave (**Operations** → **Licensing**).

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

É fornecida uma versão de avaliação para a Consola de Nuvem do Kaspersky Security Center. A *versão de avaliação* é uma versão especial da Consola de Nuvem do Kaspersky Security Center criada para familiarizar o utilizador com as funcionalidades da aplicação. Nesta versão, pode executar ações num espaço de trabalho por um período de 30 dias. Todas as aplicações geridas são automaticamente executadas com a licença de avaliação da Consola de Nuvem do Kaspersky Security Center, incluindo o Kaspersky Endpoint Security. No entanto, não pode ativar o Kaspersky Endpoint Security com a sua própria licença de avaliação quando a licença de avaliação da Cloud Console do Kaspersky Security Center expirar. Para obter mais informações sobre o licenciamento do Kaspersky Security Center, consulte a Ajuda da Consola de Nuvem do Kaspersky Security Center.

> A versão de avaliação da Consola de Nuvem do Kaspersky Security Center não permite mudar posteriormente para uma versão comercial. Qualquer espaço de trabalho de avaliação será eliminado automaticamente com todo o seu conteúdo após expirar o período de 30 dias.

Remover uma chave de licença

Para remover uma chave de licença, tem de executar uma tarefa especial nos seus computadores. Pode 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. Se adicionou uma chave de licença com um prazo curto para testar a aplicação (por exemplo, o Suplemento do EDR Optimum), pode remover esta chave de licença para se livrar das notificações e corrigir o estado do seu computador.

A tarefa *Remover chave* permite remover quaisquer chaves de licença do computador. Pode remover chaves de licença ativas, bem como chaves de licença de reserva. Além da chave de licença de ativação do Kaspersky Endpoint Security, pode remover chaves de licença individuais de soluções do Kaspersky Detection and Response (por exemplo, o Suplemento do EDR Optimum).

Como remover uma chave de licença na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

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

Passo 2. Selecionar numa licença

Selecione a chave de licença que pretende eliminar. Pode selecionar uma chave de licença no armazenamento de chaves do Kaspersky Security Center ou selecionar um ficheiro-chave.

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

Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 4. Configurar um agendamento de início de uma tarefa

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

Passo 5. Definir o nome da tarefa

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

Passo 6. Completar a criação da tarefa

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa.

Como remover uma chave de licença na Consola Web

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

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

Passo 1. Configurar definições da tarefa geral

Configurar definições da tarefa geral:

1. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.
2. Na lista pendente **Task type**, selecione **Remove key**.
3. No campo **Task name**, introduza uma breve descrição, por exemplo, *Remover chave para beta*.
4. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa. Avance para o passo seguinte.

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

Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 3. Selecionar numa licença

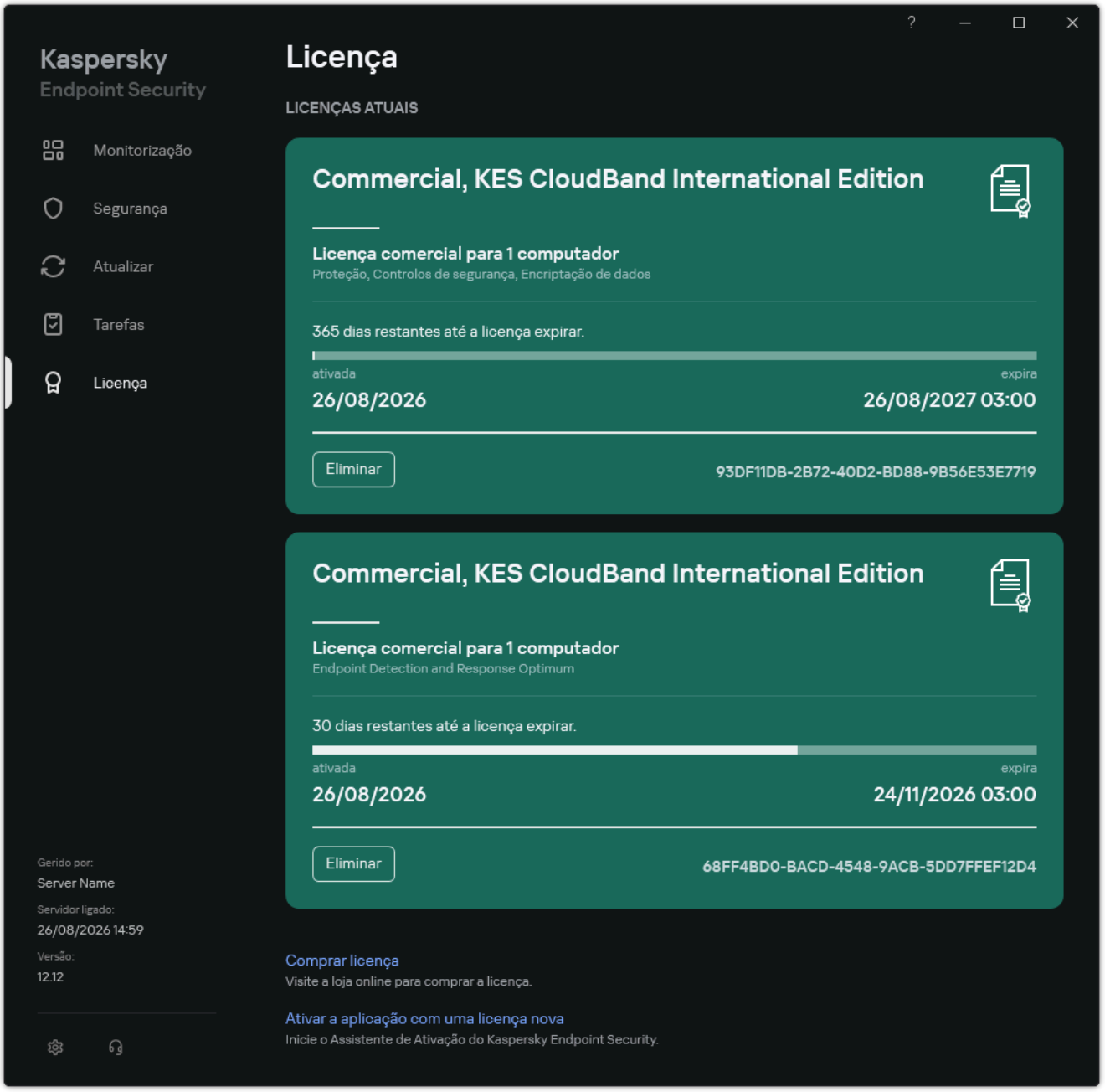
Selecione a chave de licença que pretende eliminar. Pode selecionar uma chave de licença no armazenamento de chaves do Kaspersky Security Center ou selecionar um ficheiro-chave. Avance para o passo seguinte.

Passo 4. Completar a criação da tarefa

Termine o assistente clicando no botão **Finish**. Será apresentada uma nova tarefa na lista de tarefas. Para executar uma tarefa, selecione a caixa de seleção em frente da tarefa e clique no botão **Start**.

Como remover uma chave de licença na interface da aplicação

1. Na janela principal da aplicação, aceda à secção **Licença**.
2. Selecione a chave que pretende eliminar e clique em **Eliminar**.



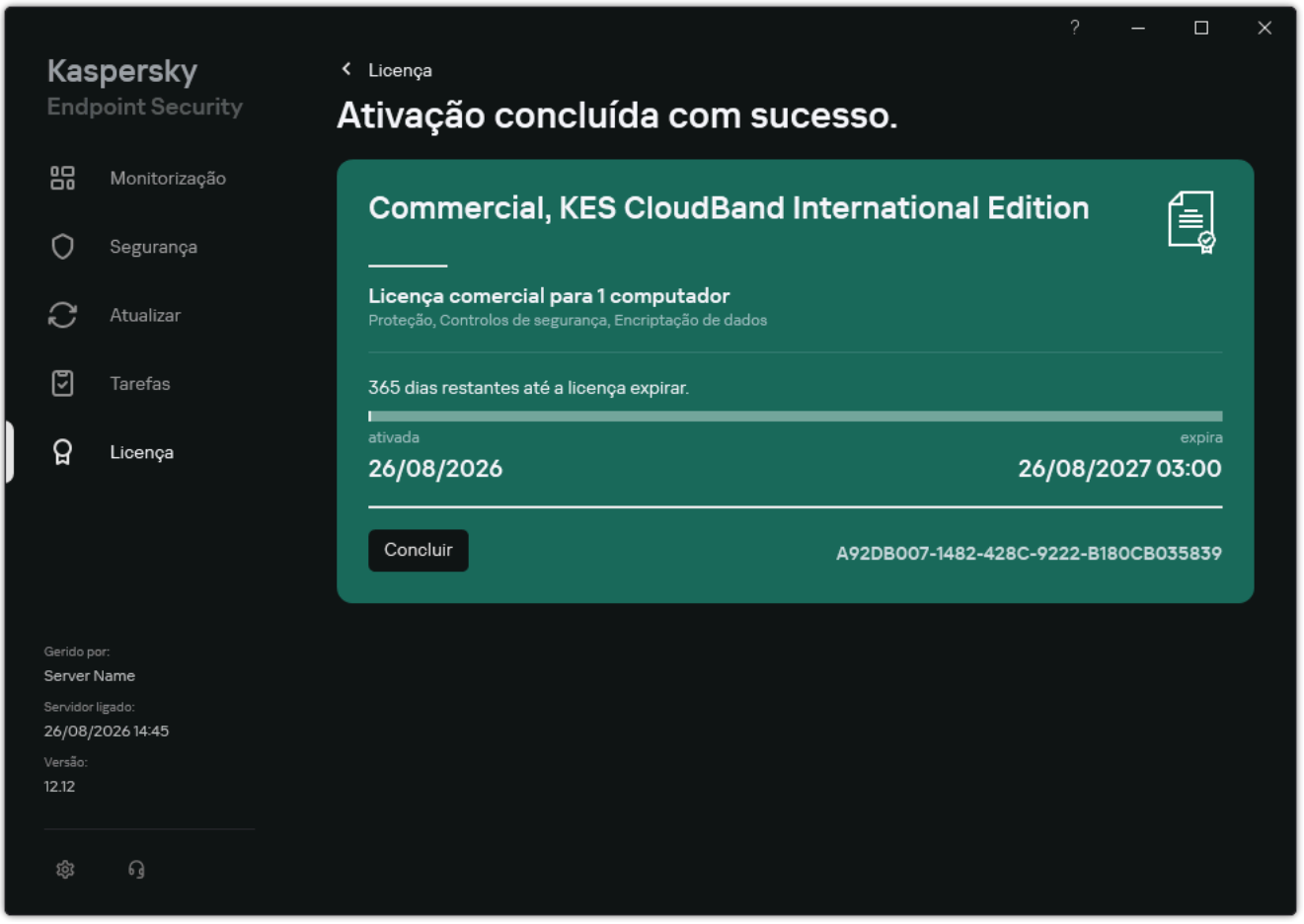
Janela Licenciamento

Também pode remover uma chave de licença na linha de comandos.

Ver informação sobre a licença

Para ver as informações sobre uma licença:

Na janela principal da aplicação, aceda à secção **Licença** (ver a figura abaixo).



Janela Licenciamento

A secção apresenta os seguintes detalhes:

- *Estado da chave*. Pode armazenar várias chaves num computador. Existem dois tipos de chave: ativa e de reserva. A aplicação não pode ter mais de uma chave ativa. Apenas é possível ativar uma chave de reserva após a chave ativa expirar ou eliminar a chave ativa com o botão **Eliminar**.
- *Nome da aplicação*. Nome completo da aplicação Kaspersky comprada.
- *Tipo de licença*. Os seguintes tipos de licenças estão disponíveis: de avaliação e comercial.
- *Funcionalidade*. As funcionalidades da aplicação que estão disponíveis de acordo com a sua licença. As funcionalidades podem incluir Proteção, Controlos de segurança, Encriptação de dados e outras. A lista de funcionalidades disponíveis também é fornecida no Certificado de Licença.

- *Informação adicional acerca da licença*. Data de início e de fim da validade da licença (apenas para a chave ativa), restante período da validade da licença.

  A hora de expiração da licença é apresentada de acordo com o fuso horário configurado no sistema operativo.

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

Na janela Licenciamento, também pode executar uma das seguintes ações:

- **Comprar licença/Renovar licença**. Abre o site de loja online da Kaspersky, onde pode comprar ou renovar uma licença. Para o fazer, introduza as informações sobre a empresa e paga a encomenda.

- **Ativar a aplicação com uma licença nova**. Inicia o Assistente de Ativação da Aplicação. Neste Assistente pode adicionar uma chave utilizando um código de ativação ou um ficheiro-chave. O Assistente de Ativação da Aplicação permite-lhe adicionar uma chave ativa e apenas uma chave de reserva.

Comprar uma licença

Pode adquirir uma licença depois de instalar a aplicação. Ao comprar uma licença, recebe um código de ativação ou um ficheiro-chave para ativar a aplicação.

Para adquirir uma licença:

1. Na janela principal da aplicação, aceda à secção **Licença**.

2. Execute uma das ações seguintes:

   - Se não foram adicionadas quaisquer chaves ou se foi adicionada uma chave para licença de avaliação, clique no botão **Comprar licença**.

   - Se estiver adicionada uma chave para uma licença comercial, clique no botão **Renovar licença**.

   É aberta uma janela no site da loja online da Kaspersky, onde poderá adquirir uma licença.

Renovar a subscrição

Quando utiliza a aplicação com subscrição, o Kaspersky Endpoint Security contacta automaticamente o servidor de ativação em intervalos específicos até que a sua subscrição expire.

Se utilizar a aplicação com subscrição ilimitada, o Kaspersky Endpoint Security verifica automaticamente o servidor de ativação quanto à existência de chaves renovadas, em segundo plano. Se uma chave estiver disponível no servidor de ativação, a aplicação adiciona a mesma substituindo a chave anterior. Desta forma, a subscrição ilimitada para o Kaspersky Endpoint Security é renovada sem intervenção do utilizador.

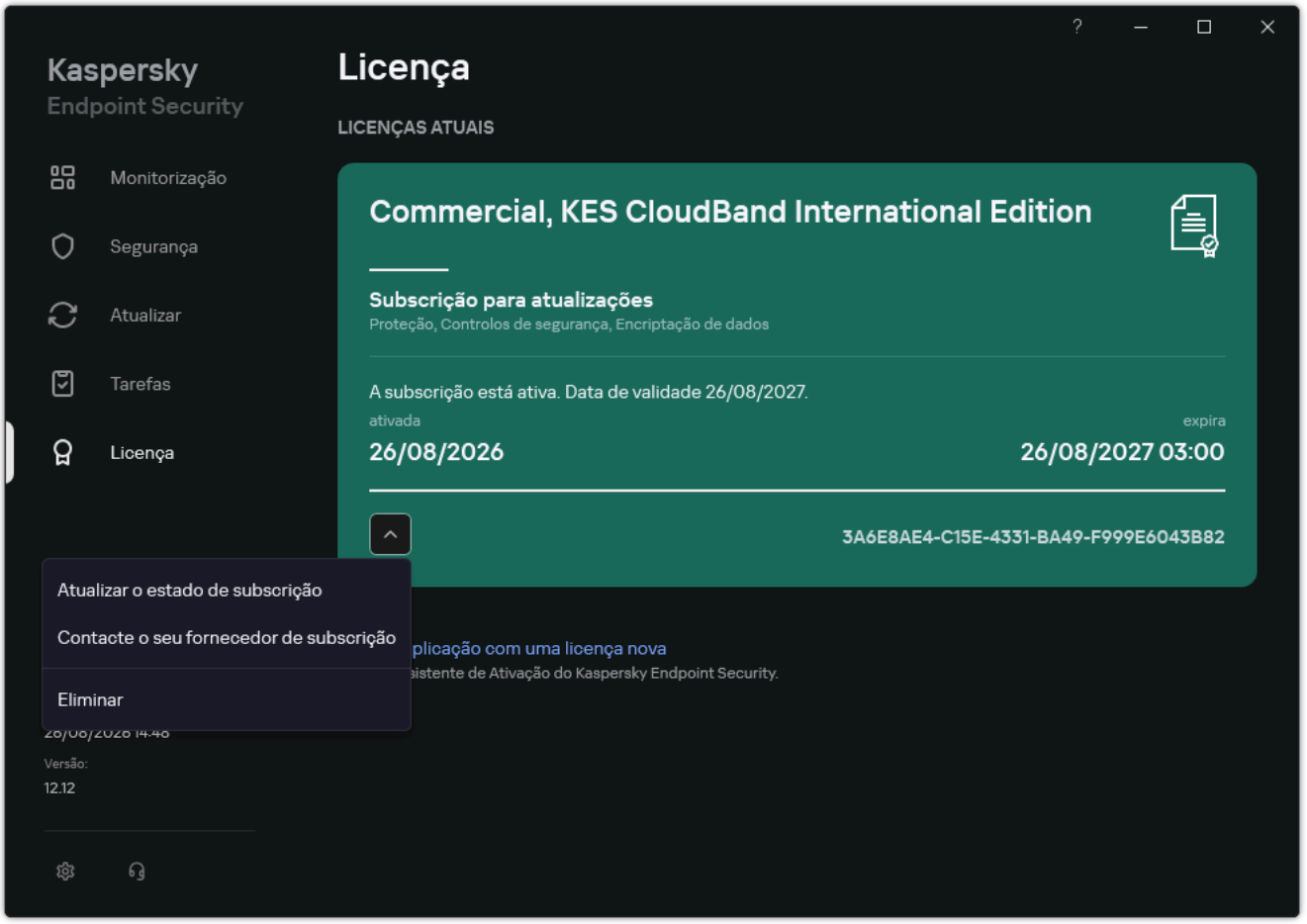
Se estiver a utilizar a aplicação com subscrição limitada, na data de validade da subscrição (ou na data de validade do período de carência da renovação da subscrição), o Kaspersky Endpoint Security notifica-o sobre esta situação e deixa de tentar renovar a subscrição automaticamente. Neste caso, o Kaspersky Endpoint Security tem um comportamento semelhante ao do termo da licença comercial para a aplicação: a aplicação é executada sem atualizações e o Kaspersky Security Network fica indisponível.

Pode renovar a subscrição no site do fornecedor de serviços.

Para visitar o site do fornecedor de serviços a partir da interface da aplicação:

1. Na janela principal da aplicação, aceda à secção **Licença**.
2. Clique em **Contacte o seu fornecedor de subscrição**.

Pode atualizar o estado da subscrição manualmente. Tal poderá ser necessário se a subscrição tiver sido renovada após o período de carência e a aplicação não tiver atualizado o estado da subscrição automaticamente.



Renovar a subscrição

Como Começar

Após a instalação do Kaspersky Endpoint Security, pode gerir a aplicação utilizando as seguintes interfaces:

- Interface local da aplicação.
- Consola de Administração do Kaspersky Security Center.
- Consola Web do Kaspersky Security Center.
- Consola de Nuvem do Kaspersky Security Center.

Consola de Administração do Kaspersky Security Center

O Kaspersky Security Center permite-lhe instalar e desinstalar, iniciar e parar o Kaspersky Endpoint Security, configurar as definições da aplicação, modificar o conjunto de componentes da aplicação disponíveis, adicionar chaves, iniciar atualizações e tarefas de verificação.

A aplicação pode ser gerida através do Kaspersky Security Center utilizando o Management Plug-in do Kaspersky Endpoint Security.

Para obter mais informações na gestão da aplicação através do Kaspersky Security Center, consulte a Ajuda do Kaspersky Security Center.

Consola Web do Kaspersky Security Center e Cloud Console do Kaspersky Security Center

Kaspersky Security Center Web Console (doravante também designada por *Web Console*). Esta é uma interface Web para gerir um sistema de proteção baseado em aplicações da Kaspersky. Pode trabalhar na Kaspersky Security Center Web Console utilizando um navegador em qualquer dispositivo. Para obter informações detalhadas sobre a Consola Web do Kaspersky Security Center, consulte a Ajuda do Kaspersky Security Center.

A Consola de Nuvem do Kaspersky Security Center (doravante também denominada "*Consola de Nuvem*") é uma solução baseada em nuvem para proteger e gerir a rede de uma organização. Para obter mais informações sobre a Consola da Nuvem do Kaspersky Security Center, consulte a Ajuda do Kaspersky Security Center.

Consola de Web e Consola de Nuvem permitem fazer o seguinte:

- Monitorizar o estado do sistema de segurança da sua organização.
- Instalar aplicações da Kaspersky em dispositivos na sua rede.
- Gerir aplicações instaladas.
- Ver relatórios do estado do sistema de segurança.

A gestão do Kaspersky Endpoint Security com a Consola de Web, Consola de Nuvem e a Consola de Administração do Kaspersky Security Center oferecem recursos de gestão diferentes. Os componentes e tarefas disponíveis também variam para as diferentes consolas.

Sobre o Management Plug-in do Kaspersky Endpoint Security for Windows

O Kaspersky Endpoint Security for Windows Management Plug-in permite a interação entre o Kaspersky Endpoint Security e o Kaspersky Security Center. O Management Plug-in permite gerir o Kaspersky Endpoint Security utilizando as políticas, tarefas e definições da aplicação locais. A interação com a Consola Web do Kaspersky Security Center é fornecida pelo plug-in da Web.

A versão do Management Plug-in pode ser diferente da versão da aplicação Kaspersky Endpoint Security instalada no computador cliente. Se a versão do Management Plug-in instalada tiver menos funcionalidade do que a versão instalada do Kaspersky Endpoint Security, as definições das funções ausentes não são reguladas pelo Management Plug-in. Estas definições podem ser modificadas pelo utilizador na interface local do Kaspersky Endpoint Security.

O plug-in Web não é instalado por predefinição no Kaspersky Security Center Web Console. O plug-in Web tem de ser instalado num computador que tenha a consola Web do Kaspersky Security Center instalada. A funcionalidade do plug-in Web está disponível a todos os administradores que têm acesso à Consola Web num navegador. Pode examinar a lista de plug-ins Web instalados na interface da Consola Web (**Console settings** → **Web plug-ins**).

Se estiver a utilizar o Kaspersky Endpoint Security como parte da solução Kaspersky Endpoint Detection and Response Optimum, tem de instalar o plug-in de gestão do Kaspersky Endpoint Detection and Response. Precisa do plug-in de gestão para apresentar os detalhes do alerta. As *informações da deteção* é uma ferramenta para visualizar todas as informações recolhidas sobre uma ameaça detetada. As informações da deteção incluem, por exemplo, o histórico dos ficheiros que aparecem no computador. Assim, para criar tarefas de resposta a ameaças, precisa do plug-in de gestão do Kaspersky Endpoint Security e, para ver detalhes de alertas, precisa do plug-in de gestão do EDR.

Instalar o plug-in Web

Pode instalar o plug-in Web do seguinte modo:

- Instale o plug-in Web utilizando o Quick Start Wizard da Consola Web do Kaspersky Security Center.

  A Consola Web solicita automaticamente que execute o Quick Start Wizard quando liga a Consola Web ao Administration Server pela primeira vez. Também pode executar o Quick Start Wizard na interface da Consola Web (**Discovery & deployment** → **Deployment & assignment** → **Quick start wizard**). O Quick Start Wizard também pode verificar se os plug-ins Web instalados estão atualizados e transferem as atualizações necessárias. Para obter mais informações sobre o Quick Start Wizard da Consola Qeb do Kaspersky Security Center, consulte a Ajuda do Kaspersky Security Center.

- Instale o Plug-in Web a partir da lista de pacotes de distribuição disponíveis na Consola Web.

  Para instalar o plug-in Web, selecione o pacote de distribuição do plug-in da web do Kaspersky Endpoint Security na interface Consola Web (**Console settings** → **Web plug-ins**). A lista de pacotes de distribuição disponíveis é atualizada automaticamente depois das novas versões das aplicações do Kaspersky serem lançadas.

- Transfira o pacote de distribuição da Consola Web a partir de uma fonte externa.

  Para instalar o plug-in Web, adicione o arquivo ZIP do pacote de distribuição do plug-in Web do Kaspersky Endpoint Security na interface da Consola Web (**Console settings** → **Web plug-ins**). Pode transferir o pacote de distribuição do plug-in da web no site da Kaspersky, por exemplo.

A partir da versão 12.11 do Kaspersky Endpoint Security 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*. Isto deve-se à transição para um único plug-in da Web unificado para a gestão de aplicações da Kaspersky. O plug-in da Web unificado permite a criação de uma única política para gerir várias aplicações da Kaspersky (por exemplo, Kaspersky Endpoint Security for Windows, macOS e Linux). A transição para o plug-in da Web unificado pode levar várias versões. Após a conclusão da transição, o pacote de distribuição irá incluir apenas o *Unified Protection and Management Plug-in*.

Atualizar o Management Plug-in

Para atualizar o Management Plug-in do Kaspersky Endpoint Security for Windows, transfira a 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 Web ficar disponível, a Consola Web apresentará a notificação *Estão disponíveis atualizações para os plug-ins utilizados*. Pode atualizar a versão de plug-in Web desta notificação de Consola Web. Pode também verificar manualmente se existem novas atualizações de plug-in Web na interface da Consola Web (**Console settings** → **Web plug-ins**). A versão anterior do plug-in Web será automaticamente removida durante a atualização.

Quando o plug-in Web é atualizado, os itens já existentes (por exemplo, políticas ou tarefas) são guardados. As novas definições de itens que implementam novas funções do Kaspersky Endpoint Security aparecem em itens existentes e têm os valores predefinidos.

Pode atualizar o plug-in Web da seguinte forma:

- Atualizar o plug-in Web a partir da lista de plug-ins Web no modo online.

  Para atualizar o plug-in Web, tem de selecionar o pacote de distribuição do plug-in da web do Kaspersky Endpoint Security na interface Consola Web (**Console settings** → **Web plug-ins**). A Consola Web verifica a existência de atualizações disponíveis nos servidores da Kaspersky e transfere as atualizações relevantes.

- Atualizar o plug-in Web a partir de um ficheiro.

  Para atualizar o plug-in Web, tem de selecionar o arquivo ZIP do pacote de distribuição do plug-in Web do Kaspersky Endpoint Security na interface da Consola Web (**Console settings** → **Web plug-ins**). Pode transferir o pacote de distribuição do plug-in da web no site da Kaspersky, por exemplo. Pode atualizar o plug-in Web do Kaspersky Endpoint Security para uma versão mais recente. O plug-in Web não pode ser atualizado para uma versão anterior.

Se um item for aberto, (como uma política ou tarefa), o plug-in Web verifica a sua informação de compatibilidade. Se a versão do plug-in Web for igual ou posterior à versão especificada na informação de compatibilidade, pode alterar as definições deste item. Caso contrário, não pode utilizar o plug-in Web para alterar as definições do item selecionado. É recomendada a atualização do plug-in Web.

Considerações especiais ao trabalhar com versões diferentes dos plug-ins de administração

Pode gerir o Kaspersky Endpoint Security através do Kaspersky Security Center apenas se tiver um Management Plug-in cuja versão é igual a ou posterior à versão especificada na informação relativa à compatibilidade do Kaspersky Endpoint Security com o Management Plug-in. Pode visualizar a versão mínima necessária do Management Plug-in no ficheiro installer.ini incluído no kit de distribuição.

Se um item for aberto (como a política ou a tarefa), o Management Plug-in verifica a sua informação de compatibilidade. Se a versão do Management Plug-in for igual ou posterior à versão especificada na informação de compatibilidade, pode alterar as definições deste item. Caso contrário, não pode utilizar o Management Plug-in para alterar as definições do item selecionado. É recomendada a atualização do Management Plug-in.

Se o plug-in de gestão do Kaspersky Endpoint Security for instalado na Consola de Administração, considere o seguinte quando instalar uma nova versão do plug-in de gestão:

- A versão anterior do plug-in de gestão do Kaspersky Endpoint Security será removida.
- A nova versão do plug-in de gestão do Kaspersky Endpoint Security suporta a gestão da versão anterior do Kaspersky Endpoint Security for Windows em computadores.
- Pode utilizar a nova versão do plug-in de gestão para alterar as definições em políticas, tarefas e outros itens criados pela versão anterior do plug-in de gestão.
- Para novas definições, a nova versão do plug-in de gestão atribui os valores predefinidos quando uma política, perfil de política ou tarefa são guardados pela primeira vez.

  Depois de atualizar o plug-in de gestão, recomenda-se que os valores das novas definições de políticas e perfis de políticas sejam verificados e guardados. Se não o fizer, os novos grupos das definições do Kaspersky Endpoint Security no computador do utilizador irão assumir os valores predefinidos e poderão ser editados (o atributo ). Recomenda-se que as definições sejam verificadas, começando pelas políticas e perfis de políticas no nível superior da hierarquia. Também recomendamos que utilize a conta de utilizador que tem direitos de acesso em todas as áreas funcionais do Kaspersky Security Center.

  Para saber mais sobre as novas capacidades da aplicação, consulte as Notas de Versão ou a ajuda de aplicação.

- Se um novo parâmetro tiver sido adicionado a um grupo de definições na nova versão do plug-in de gestão, o estado anteriormente definido do atributo  deste grupo de definições não é alterado.

Considerandos especiais ao usar protocolos encriptados para interagir com serviços externos

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

- Atualização das bases de dados e módulos de software da aplicação;
- Ativação da aplicação com um código de ativação (ativação 2.0)
- Utilização da Kaspersky Security Network.

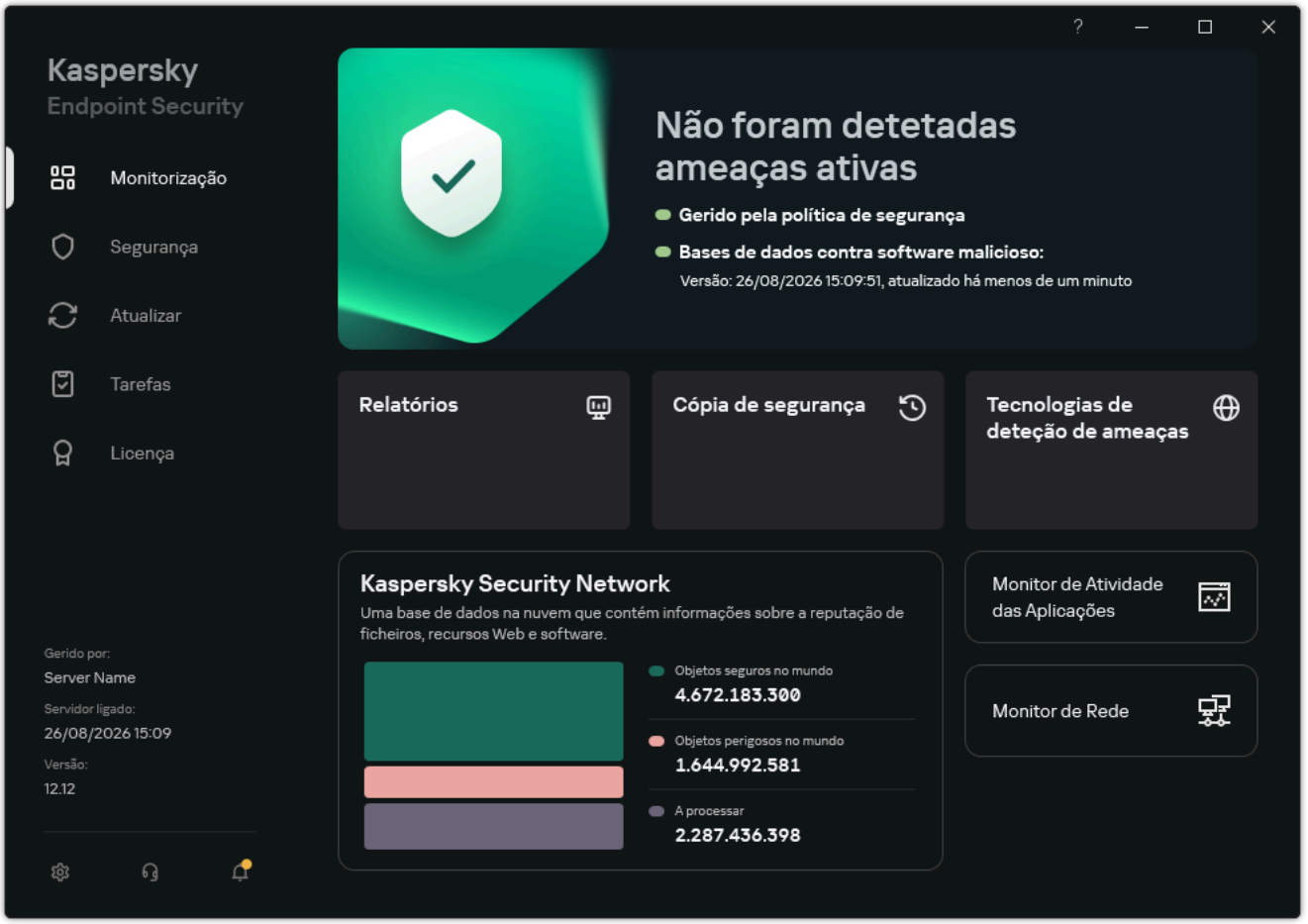
O uso de TLS protege a aplicação, fornecendo as seguintes funcionalidades:

- Encriptação. Os conteúdos das mensagens são confidenciais e não são divulgados a terceiros utilizadores.
- Integridade. O destinatário da mensagem tem a certeza de que o conteúdo da mensagem não foi modificado desde que a mensagem foi encaminhada pelo remetente.
- Autenticação. O destinatário tem a certeza de que a comunicação é estabelecida apenas com um servidor fiável da Kaspersky.

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

Ambientes que têm MITM (ferramentas de software e hardware que suportam 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, podem ocorrer erros relacionados com a utilização de Self-Signed Certificate. Esses erros podem ocorrer porque uma ferramenta de inspeção HTTPS do seu ambiente não reconhece a Kaspersky PKI. Para corrigir esses problemas, deve configurar as exclusões para interagir com serviços externos.

Interface da aplicação



Janela principal da aplicação

Monitorização	• **Relatórios**. Visualize eventos que ocorreram durante a operação da aplicação, componentes e tarefas individuais. • **Cópia de segurança**. Visualize uma lista de cópias guardadas de ficheiros infetados que a aplicação eliminou. • **Tecnologias de deteção de ameaças**. Visualize informações sobre tecnologias de deteção de ameaças e o número de ameaças detetadas por essas tecnologias. • **Kaspersky Security Network**. Estado da ligação entre o Kaspersky Endpoint Security e a Kaspersky Security Network, e estatísticas da KSN global. *A Kaspersky Security Network (KSN)* é uma infraestrutura de serviços na nuvem que fornece o acesso à Base de Conhecimento online da Kaspersky, que contém informações sobre a reputação de ficheiros, recursos da Internet e software. A utilização de dados da Kaspersky Security Network permite uma resposta mais rápida do Kaspersky Endpoint Security a novas ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos diagnósticos positivos. Se participar na Kaspersky Security Network, os serviços da KSN irão fornecer ao Kaspersky Endpoint Security informações sobre a reputação dos endereços Web verificados, bem como informações sobre a categoria e a reputação dos ficheiros verificados. • **Monitor de Atividade das Aplicações**. Visualize informações sobre a operação das aplicações instaladas. A Monitorização das Atividades da Aplicação mantém um registo dos ficheiros, registo e eventos do sistema operativo associados à aplicação. • **Monitor de Rede**. Visualize informações sobre a atividade de rede do computador em tempo real. • **Monitor de encriptação**. Monitoriza o processo de encriptação ou desencriptação de disco em tempo real. O Monitor de Encriptação está disponível se o componente Encriptação de disco Kaspersky ou Encriptação de Unidade BitLocker estiver instalado.
Segurança	Estado operacional dos componentes instalados. Também pode proceder à configuração de componentes ou visualização de relatórios.
Atualizar	Gerir tarefas de atualização do Kaspersky Endpoint Security. Pode atualizar bases de dados de antivírus e módulos de aplicação e reverter a última atualização. Um administrador pode ocultar a secção do utilizador ou restringir a gestão de tarefas.
Tarefas	Gerir as tarefas de verificação do Kaspersky Endpoint Security. Pode executar uma verificação de software malicioso e a verificação de integridade da aplicação. Um administrador pode ocultar tarefas de um utilizador ou restringir a gestão de tarefas.
Licença	Licenciamento da aplicação. Pode comprar uma licença, ativar a aplicação ou renovar uma subscrição. Também pode ver informações sobre a licença atual.

	Configurar as definições da aplicação. Um administrador pode proibir alterações às definições do Kaspersky Security Center.
	Informações sobre a aplicação: versão atual do Kaspersky Endpoint Security, data de lançamento da base de dados, chave e outras informações. Também pode seguir para os recursos de informação da Kaspersky que fornecem informações úteis, recomendações e respostas a perguntas frequentes sobre como adquirir, instalar e utilizar a aplicação.
	Mensagens que contém informações sobre atualizações disponíveis e pedidos de acesso a ficheiros encriptados e dispositivos.

Ícone da aplicação na área de notificação da barra de tarefas

Imediatamente após a instalação do Kaspersky Endpoint Security, o ícone da aplicação é apresentado na área de notificação da barra de tarefas do Microsoft Windows.

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

O ícone tem os seguintes objetivos:

- Indicar a atividade da aplicação.
- Funcionar como atalho para o menu de contexto e janela principal da aplicação.

Os seguintes estados do ícone da aplicação são fornecidos para apresentar informações operacionais da aplicação:

- O ícone significa que todos os componentes de proteção crítica da aplicação estão ativados. O Kaspersky Endpoint Security apresenta um aviso se o utilizador tiver de executar uma ação, por exemplo, reiniciar o computador depois de atualizar a aplicação.
- O ícone significa que os componentes de proteção crítica da aplicação estão desativados ou com um funcionamento incorreto. Os componentes de proteção podem funcionar incorretamente, por exemplo, se a licença expirou ou como resultado de um erro na aplicação. O Kaspersky Endpoint Security apresenta um aviso com uma descrição do problema na proteção do computador.

O menu de contexto do ícone da aplicação contém os seguintes itens:

- **Kaspersky Endpoint Security for Windows**. Abre a janela principal da aplicação. Nesta janela, pode ajustar o funcionamento dos componentes e tarefas da aplicação e ver as estatísticas dos ficheiros processados e das ameaças detetadas.
- **Pausar proteção/Retomar proteção**. Pausa a operação de todos os componentes de proteção e controlo que não estejam assinalados por um cadeado () na política. Antes de executar esta operação, recomenda-se a desativação da política do Kaspersky Security Center.

  Antes de colocar em pausa a operação dos componentes de proteção e controlo, a aplicação solicita a password para aceder ao Kaspersky Endpoint Security (password da conta ou password temporária). Pode então selecionar o período de pausa: durante um período de tempo específico, até uma reinicialização ou mediante pedido do utilizador.

  Este item do menu contextual está disponível se a proteção por password estiver ativada. Para retomar a operação dos componentes de proteção e controlo, clique em **Retomar proteção** no menu contextual da aplicação.

Colocar em pausa a operação dos componentes de proteção e controlo não afeta o desempenho das tarefas de atualização e verificação de software malicioso. A aplicação continua também a utilizar o Kaspersky Security Network.

- **Desativar política/Ativar política**. Desativar uma política do Kaspersky Security Center no computador. Todas as definições do Kaspersky Endpoint Security estão disponíveis para configuração, incluindo definições que têm um cadeado fechado na política (). Se a política estiver desativada, a aplicação solicita a password de acesso ao Kaspersky Endpoint Security (password da conta ou password temporária). Este item do menu contextual está disponível se a proteção por password estiver ativada. Para ativar a política, selecione **Ativar política** no menu contextual da aplicação.

- **Definições**. Abre a janela de configurações da aplicação.

- **Suporte**. Isto abre uma janela que contém a informação necessária para entrar em contacto com o Suporte técnico da Kaspersky.

- **Sobre**. Este item abre uma janela de informação com os detalhes da aplicação.

- **Sair**. Este item permite sair do Kaspersky Endpoint Security. Clicar neste item de menu contextual retira a aplicação da memória RAM do computador.



Menu de contexto do ícone da aplicação

Interface simplificada da aplicação

Se uma política do Kaspersky Security Center configurada para apresentar a interface simplificada da aplicação for aplicada a um computador cliente em que o Kaspersky Endpoint Security esteja instalado, a janela principal da aplicação não fica disponível neste computador cliente. Clique com o botão direito do rato para abrir o menu de contexto do ícone do Kaspersky Endpoint Security (veja a imagem abaixo) com os seguintes itens:

- **Desativar política/Ativar política**. Desativar uma política do Kaspersky Security Center no computador. Todas as definições do Kaspersky Endpoint Security estão disponíveis para configuração, incluindo definições que têm um cadeado fechado na política (). Se a política estiver desativada, a aplicação solicita a password de acesso ao Kaspersky Endpoint Security (password da conta ou password temporária). Este item do menu contextual está disponível se a proteção por password estiver ativada. Para ativar a política, selecione **Ativar política** no menu contextual da aplicação.

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

  - **Verificação de integridade da aplicação**.

  - **Reversão das bases de dados para a sua versão anterior**.

  - **Verificação completa**.

  - **Verificação Personalizada**.

- **Verificação de Áreas Críticas**.
- **Atualização**.

- **Suporte**. Isto abre uma janela que contém a informação necessária para entrar em contacto com o Suporte técnico da Kaspersky.
- **Sair**. Este item permite sair do Kaspersky Endpoint Security. Clicar neste item de menu contextual retira a aplicação da memória RAM do computador.



Menu de contexto do ícone da aplicação aquando da apresentação da interface simplificada

Configurar a apresentação da interface da aplicação

Pode configurar o modo de apresentação da interface da aplicação de um utilizador. O utilizador pode interagir com a aplicação da seguinte forma:

- **Simplified**. Num computador do cliente, a janela principal da aplicação está inacessível e apenas o ícone na área de notificação do Windows está disponível. No menu contextual do ícone, o utilizador pode realizar um número limitado de operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security também apresenta apenas as notificações que requerem uma ação do utilizador acima do ícone da aplicação.
- **Full**. Num computador do cliente, a janela principal do Kaspersky Endpoint Security e o ícone na área de notificação do Windows estão disponíveis. No menu contextual do ícone, o utilizador pode realizar operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security apresenta também notificações acima do ícone da aplicação.
- **Do not display user interface**. Num computador do cliente, não são apresentados quaisquer sinais da operação do Kaspersky Endpoint Security. O ícone na área de notificação do Windows e as notificações não estão disponíveis.

Como configurar o modo de apresentação da interface da aplicação na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais** → **Interface**.

4. No bloco **Interação com o utilizador**, configure como a interface da aplicação será apresentada:

   - **Apresentar interface de utilizador**. Num computador do cliente, a janela principal do Kaspersky Endpoint Security e o ícone na área de notificação do Windows estão disponíveis. No menu contextual do ícone, o utilizador pode realizar operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security apresenta também notificações acima do ícone da aplicação. Se necessário, pode ativar a funcionalidade **Secção Ocultar Monitor de Atividade das Aplicações** para ocultar dados sobre a atividade das aplicações no computador, restringindo assim o acesso do utilizador à ferramenta Monitor de atividade das aplicações.

   - **Apresentar interface simplificada**. Num computador do cliente, a janela principal da aplicação está inacessível e apenas o ícone na área de notificação do Windows está disponível. No menu contextual do ícone, o utilizador pode realizar um número limitado de operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security também apresenta apenas as notificações que requerem uma ação do utilizador acima do ícone da aplicação.

   - **Não apresentar interface do utilizador**. Num computador do cliente, não são apresentados quaisquer sinais da operação do Kaspersky Endpoint Security. O ícone na área de notificação do Windows e as notificações não estão disponíveis.

5. Guarde as suas alterações.

Como configurar o modo de apresentação da interface da aplicação na Web Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **General Settings** → **User Interaction**.

5. No bloco **Visibility for users**, configure como a interface da aplicação será apresentada:

   - **Display user interface**. Se esta funcionalidade estiver desativada, não serão apresentados sinais da atividade do Kaspersky Endpoint Security num computador cliente. O ícone na área de notificação do Windows e as notificações não estão disponíveis.

   - **Simplified**. Num computador do cliente, a janela principal da aplicação está inacessível e apenas o ícone na área de notificação do Windows está disponível. No menu contextual do ícone, o utilizador pode realizar um número limitado de operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security também apresenta apenas as notificações que requerem uma ação do utilizador acima do ícone da aplicação.

   - **Full**. Num computador do cliente, a janela principal do Kaspersky Endpoint Security e o ícone na área de notificação do Windows estão disponíveis. No menu contextual do ícone, o utilizador pode realizar operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security apresenta também notificações acima do ícone da aplicação.

   - **Hide Application Activity Monitor section**. Se deseja ocultar as informações de atividade da aplicação no computador do utilizador, pode restringir o acesso do utilizador à ferramenta Monitor de atividade das aplicações.

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

Preparar a aplicação para utilização

Depois de implementar a aplicação nos computadores cliente, para trabalhar com o Kaspersky Endpoint Security a partir do Kaspersky Security Center Web Console, precisa de realizar as seguintes ações:

- Criar e configurar uma política.

  Pode utilizar políticas para aplicar definições idênticas do Kaspersky Endpoint Security em todos os computadores cliente de um grupo de administração. O Quick Start Wizard do Kaspersky Security Center cria automaticamente uma política para o Kaspersky Endpoint Security.

- Crie as tarefas *Atualização das bases de dados e módulos da aplicação* e *Verificação de software malicioso*.

  A tarefa *Atualização das bases de dados e módulos da aplicação* é necessária para manter a segurança do computador atualizada. Quando a tarefa é executada, o Kaspersky Endpoint Security atualiza as bases de dados antivírus e os módulos da aplicação. A tarefa *Atualização das bases de dados e módulos da aplicação* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização das bases de dados e módulos da aplicação*, instale o Kaspersky Endpoint Security for Windows Management Plug-in enquanto executa o Assistente.

  A tarefa *Verificação de software malicioso* é necessária para a deteção vírus e outro software malicioso. Precisa de criar manualmente a tarefa *Verificação de software malicioso*.

  Como criar uma tarefa de Verificação de software malicioso na Consola de Administração (MMC)

  1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Tasks**.

     A lista de tarefas é aberta.

  2. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Verificação de software malicioso**.

Passo 2. Âmbito de verificação

Crie a lista de objetos que o Kaspersky Endpoint Security verifica durante a execução de uma tarefa de verificação.

Passo 3. Ação do Kaspersky Endpoint Security

Escolha a ação após a deteção de ameaças:

- **Desinfetar, eliminar se a desinfeção falhar**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação elimina o ficheiro.

- **Desinfetar, informar se a desinfeção falhar**. Se esta opção estiver selecionada, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção falhar, o Kaspersky Endpoint Security adiciona a informação sobre os ficheiros infetados que são detetados à lista de ameaças ativas.

- **Informar**. Se esta opção for selecionada, o Kaspersky Endpoint Security adiciona a informação sobre ficheiros infetados à lista de ameaças ativas na deteção destes ficheiros.

- **Executar a Desinfeção Avançada imediatamente**. Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security utiliza a tecnologia Desinfeção Avançada para processar ameaças ativas durante a verificação.

  A Tecnologia de Desinfeção Avançada visa apagar do sistema operativo as aplicações maliciosas, cujos processos já tenham iniciado na memória RAM e que impedem que o Kaspersky Endpoint Security os remova utilizando outros métodos. Deste modo, a ameaça é neutralizada. Enquanto a Desinfeção Avançada decorre, é recomendado não iniciar novos processos nem editar o registo do sistema operativo. A tecnologia de desinfeção avançada utiliza recursos consideráveis do sistema operativo, o que poderá tornar outras aplicações mais lentas. Quando a Desinfeção Avançada terminar, o Kaspersky Endpoint Security reinicia o computador sem solicitar confirmação ao utilizador.

- **Run only when the computer is idle**. 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 ecrã estiver ativada. Se interrompeu a execução da tarefa (por exemplo, ao desbloquear o computador), o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que foi interrompido. Esta opção de agendamento permite-lhe conservar os recursos do computador quando o computador está a ser utilizado.

Passo 4. Selecionar os dispositivos aos quais a tarefa será atribuída

Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.

- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.

- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 5. Selecionar a conta para executar a tarefa

Selecione uma conta para executar a tarefa *Verificação de software malicioso*. Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de utilizador local. Se o âmbito de verificação incluir unidades de rede ou outros objetos com acesso restrito, selecione uma conta de utilizador com os direitos de acesso suficientes.

Passo 6. Configurar um agendamento de início de uma tarefa

Configure um agendamento para iniciar uma tarefa, por exemplo, manualmente ou depois da transferência das bases de dados de antivírus para o repositório.

Passo 7. Definir o nome da tarefa

Introduza um nome para a tarefa, por exemplo, *Verificação diária completa*.

Passo 8. Completar a criação da tarefa

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa. Na sequência disto, a tarefa Verificação de software malicioso será executada nos computadores do utilizador de acordo com o calendário especificado.

Como criar uma tarefa de Verificação de software malicioso na Consola Web

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **Malware Scan**.

   c. No campo **Task name**, introduza uma breve descrição, por exemplo, *Verificação semanal*.

   d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Avance para o passo seguinte.

5. Selecione uma conta para executar a tarefa. Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de utilizador local.

6. Conclua o assistente.

   Será apresentada uma nova tarefa na lista de tarefas.

7. Para configurar a programação da tarefa, aceda às propriedades da tarefa.

   Recomenda-se que a tarefa seja agendada para ser executada, pelo menos, uma vez por semana.

8. Selecione a caixa de verificação junto à tarefa.

9. Clique em **Start**.

   Pode controlar o estado da tarefa e o número de dispositivos nos quais a tarefa foi concluída com êxito ou concluída com um erro.

Na sequência disto, a tarefa Verificação de software malicioso será executada nos computadores do utilizador de acordo com o calendário especificado.

- Otimize o desempenho do Kaspersky Endpoint Security.

Gerir políticas

Uma *política* é uma conjunto de definições da aplicação que são definidas para um grupo de administração. Pode configurar várias políticas com diferentes valores para uma aplicação. Uma aplicação pode ser executada sob diferentes definições para diferentes grupos de administração. Cada grupo de administração pode ter a sua própria política para uma aplicação.

Cada definição de política tem o atributo ("cadeado"). O estado deste atributo determina se a definição será transmitida para os dispositivos geridos no grupo de administração:

- Se o "cadeado" estiver aberto (), o valor desta definição não será passado para os dispositivos geridos. A definição estará disponível para modificação na interface local da aplicação. Estas definições são chamadas de *desbloqueadas*.

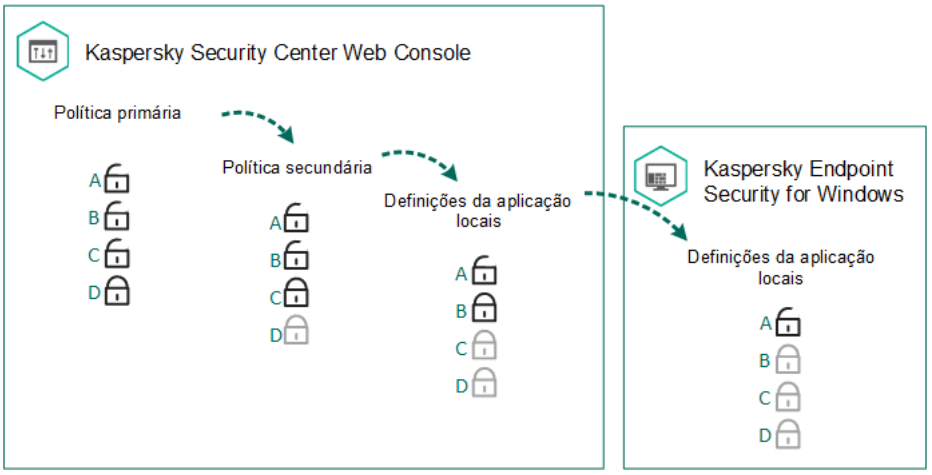
- Se o "cadeado" estiver fechado (), o valor desta definição será passado e aplicado aos dispositivos geridos. Estas definições são chamadas de *bloqueadas*. As definições bloqueadas não estão disponíveis para modificação na interface local da aplicação.

As definições da política são enviadas para os computadores cliente pelo Agente de Rede durante a *sincronização*. Por predefinição, o Servidor de administração executa a sincronização imediatamente após a modificação das definições de política. A porta UDP 15000 no computador do cliente é utilizada para sincronização. Por predefinição, o Servidor de Administração executa a sincronização a cada 15 minutos. Se a sincronização falhar após a alteração das definições de política, a próxima tentativa de sincronização será executada segundo o programa definido.

Herança de definições

Políticas, como grupos de administração, são organizadas em hierarquia. *Política secundária* é uma política para níveis de hierarquia imbricados, ou seja, uma política para grupos de administração aninhados e servidores de administração secundários.

Por predefinição, a política secundária herda as definições da política principal. Se a definição na política principal tiver o atributo ("cadeado" fechado), então nas políticas secundárias e nas definições de aplicações locais, o valor dessa definição será substituído de acordo com a política principal e a definição será bloqueada. Se for necessário, pode desativar a herança das definições da política principal. As políticas relativas a um estado fora do escritório não afetam outras políticas na hierarquia de grupos de administração.



Herança de definições

Os direitos de acesso às definições de política (ler, gravar, executar) são especificadas para cada utilizador que tenha acesso ao Servidor de Administração do Kaspersky Security Center e separadamente para cada âmbito funcional do Kaspersky Endpoint Security. Para configurar os direitos de acesso às definições de política, aceda à secção **Security** da janela de propriedades do Kaspersky Security Center Administration Server (por predefinição, esta secção está oculta na interface da consola).

Revisões de políticas

O Kaspersky Security Center monitoriza as alterações às políticas e cria revisões. Uma *revisão* é um conjunto de parâmetros modificados guardados pelo utilizador. As revisões permitem comparar e reverter alterações nos parâmetros da política. Para além do conjunto de parâmetros alterados, a revisão inclui informações sobre o utilizador que efetuou as alterações, bem como a hora, o endereço IP, o comentário do utilizador e outros dados relevantes.

Para visualizar o registo de revisões, abra as propriedades da política e aceda à secção **Revision history**. Para obter mais informação detalhada sobre como trabalhar com revisões, consulte a Ajuda do Kaspersky Security Center.

Criar uma política

Ao criar uma política, o assistente sugere definições que são relevantes para o modo selecionado. Por exemplo, para o modo Light Agent, tem de adicionar um Servidor de Proteção (SVM). Ao utilizar a aplicação para proteger um servidor SQL, tem de adicionar exclusões de verificação predefinidas para garantir que o funcionamento do servidor não sofre interferências. O assistente sugere definições de política relevantes depois de selecionar um modo. Pode então editar estas definições nas propriedades da política.

Como criar uma política na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Managed devices** da árvore na Consola de Administração, selecione a pasta com o nome do grupo de administração ao qual os computadores cliente em questão pertencem.
3. Na área de trabalho, selecione o separador **Policies**.
4. Clique em **New policy**.

   O Assistente de Política é iniciado.
5. Siga as instruções do Assistente de Política.

Passo 1. Selecionar a aplicação para criar política de grupo

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

Passo 2. Nomear a política de grupo

Insira um nome para a política de grupo, por exemplo, *Política para o escritório*.

Também pode criar novas políticas com base nas políticas existentes usando o Assistente de Políticas. Para o fazer, ao especificar o nome da política de grupo, selecione a caixa de verificação **Use policy settings for an earlier version of the application**. O assistente também permite criar uma política do Kaspersky Endpoint Security (KES) com base numa política de uma solução diferente, por exemplo, o Kaspersky Security for Windows Server (KSWS) ou o Kaspersky Security for Virtualization Light Agent for Windows

Passo 3. Participar na Kaspersky Security Network

Leia e aceite os termos da Declaração da Kaspersky Security Network (KSN).

Passo 4. Selecionar o modo de utilização da aplicação em computadores

Dependendo da utilização pretendida do Kaspersky Endpoint Security, pode configurar uma política para os seguintes modos de aplicação:

- Modo padrão para proteger anfitriões

Neste modo, pode selecionar como deseja configurar a política:

- **Criar uma política com definições predefinidas**. As definições predefinidas são consideradas as ideais. Estas definições são recomendadas pelos peritos da Kaspersky. As definições predefinidas fornecem o nível de proteção recomendado e o uso ideal dos recursos.

- **Alterar definições da política no Assistente**. Este método permite gerir as definições de política passo a passo, através de um assistente. Também pode gerir as definições de política através de um ficheiro de configuração da aplicação (consulte o passo seguinte).

- Endpoint Detection and Response Agent para proteger contra ameaças avançadas e ataques direcionados.

  O *Endpoint Detection and Response Agent* é uma aplicação instalada em estações de trabalho e servidores individuais na infraestrutura de TI da organização para dar suporte as soluções de Detection and Response da Kaspersky. No passo seguinte, terá de selecionar uma solução para a integração do EDR Agent.

- Light Agent para proteger ambientes virtuais.

  Para utilizar a aplicação no modo Light Agent, tem de configurar uma ligação com uma máquina virtual SVM. Estas definições são necessárias para que a aplicação funcione no modo Light Agent.

O Kaspersky Endpoint Security oferece uma política comum para todos os modos de aplicação e tipos de SO. Isto significa que a política abrange todas as definições. No entanto, a aplicação pode ignorar algumas das definições da política porque o Kaspersky Endpoint Security é implementado num modo no qual algumas funcionalidades não estão disponíveis. Por exemplo, ao usar a aplicação no modo Endpoint Detection and Response Agent, apenas as definições relevantes para a integração com as soluções Kaspersky Detection and Response e para a integração com o KUMA estarão disponíveis.

Recomendamos a utilização de diferentes políticas para diferentes modos e tipos de sistemas operativos.

Passo 5. Importar definições

Este passo está disponível se selecionar a configuração manual da política no passo 4.

Pode criar uma política com base nas definições do Kaspersky Endpoint Security a partir de um ficheiro de configuração CFG. O Assistente de Nova Política não suporta ficheiros de configuração encriptados. Ao exportar o ficheiro de configuração, ignore o passo de encriptação do ficheiro.

Ao importar um ficheiro de configuração CFG da aplicação, nem todas as definições de política estão disponíveis no assistente. Por exemplo, faltam perfis de política nas definições da aplicação. Se pretender transferir todas as definições e perfis para a política, pode importar outra política a partir de um ficheiro KLP.

Ao importar um ficheiro de configuração, o Kaspersky Endpoint Security não transfere as passwords dos cripto-contentores. Se utilizar a autenticação de dois fatores ao ligar-se aos servidores, terá de definir as passwords do cripto-contentor a partir do zero.

Passo 6 – 10. Configurar as definições de política

Este passo está disponível se selecionar a configuração manual da política no passo 4.

Siga os passos para gerir as definições da política.

Passo 11. Configurar a zona fiável

Configurar a zona fiável. Pode adicionar exclusões de verificação predefinidas e aplicações fiáveis. Exclusões de verificação predefinidas e aplicações fiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e System Center Configuration Manager. Isto significa que não é necessário configurar manualmente uma zona fiável para a aplicação nos servidores. As exclusões de verificação predefinidas e as aplicações fiáveis também podem ajudá-lo a configurar rapidamente o Kaspersky Endpoint Security no modo Light Agent em ambientes virtuais Citrix e VMware.

Passo 12. Selecionar o estado da política

- **Active**. Depois seguinte sincronização, a política será utilizada como a política ativa do computador.

  As definições de uma política ativa são guardadas nos computadores cliente durante a sincronização. Não é possível aplicar simultaneamente várias políticas a um computador, por isso apenas é possível ter uma política ativa em cada grupo.

- **Inactive**. Política de reserva. Se necessário, uma política inativa pode mudar para o estado ativo.

  Pode criar um número ilimitado de políticas inativas. Uma política inativa não afeta as definições da aplicação em computadores na rede. As políticas inativas destinam-se a preparações para situações de emergência, como um ataque de vírus. Se ocorrer um ataque através das unidades amovíveis, pode ativar uma política que bloqueia o acesso às unidades USB. Neste caso, a política ativa torna-se automaticamente inativa.

- **Out-of-office**. A política é ativada quando um computador abandona a rede da organização.

Conclua o assistente.

Como criar uma política na Consola Web e na Consola de Nuvem

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique em **Add**.

   O Assistente de Política é iniciado.
3. Selecione o Kaspersky Endpoint Security e clique em **Next**.
4. Leia e aceite os termos da Declaração da Kaspersky Security Network (KSN) e clique em **Next**.

5. Selecione o modo da aplicação:

   - Standard mode to protect workstations and servers
   - Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks.

     Se selecionar este modo, poderá criar uma política para integrar o computador com as soluções Kaspersky Detection and Response. O assistente pede-lhe para configurar a integração para o Kaspersky Managed Detection and Response e, em seguida, para o Kaspersky Anti Targeted Attack Platform (EDR).
   - Light Agent to protect virtual environments.

     Se selecionar este modo, na próxima etapa, tem de configurar a ligação ao Servidor de Proteção (SVM). Estas definições são necessárias para que a aplicação funcione no modo Light Agent.

   O Kaspersky Endpoint Security oferece uma política comum para todos os modos de aplicação e tipos de SO. Isto significa que a política abrange todas as definições. No entanto, a aplicação pode ignorar algumas das definições da política porque o Kaspersky Endpoint Security é implementado num modo no qual algumas funcionalidades não estão disponíveis. Por exemplo, ao usar a aplicação no modo Endpoint Detection and Response Agent, apenas as definições relevantes para a integração com as soluções Kaspersky Detection and Response e para a integração com o KUMA estarão disponíveis.

   Recomendamos a utilização de diferentes políticas para diferentes modos e tipos de sistemas operativos.

6. Configurar a zona fiável. Pode adicionar exclusões de verificação predefinidas e aplicações fiáveis. Exclusões de verificação predefinidas e aplicações fiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e System Center Configuration Manager. Isto significa que não é necessário configurar manualmente uma zona fiável para a aplicação nos servidores. As exclusões de verificação predefinidas e as aplicações fiáveis também podem ajudá-lo a configurar rapidamente o Kaspersky Endpoint Security no modo Light Agent em ambientes virtuais Citrix e VMware.

7. No separador **General**, pode executar as seguintes ações:

   - Mudar o nome de política.
   - Selecione o estado da política:

     - **Active**. Depois seguinte sincronização, a política será utilizada como a política ativa do computador.

       As definições de uma política ativa são guardadas nos computadores cliente durante a sincronização. Não é possível aplicar simultaneamente várias políticas a um computador, por isso apenas é possível ter uma política ativa em cada grupo.
     - **Inactive**. Política de reserva. Se necessário, uma política inativa pode mudar para o estado ativo.

       Pode criar um número ilimitado de políticas inativas. Uma política inativa não afeta as definições da aplicação em computadores na rede. As políticas inativas destinam-se a preparações para situações de emergência, como um ataque de vírus. Se ocorrer um ataque através das unidades amovíveis, pode ativar uma política que bloqueia o acesso às unidades USB. Neste caso, a política ativa torna-se automaticamente inativa.
     - **Out-of-office**. A política é ativada quando um computador abandona a rede da organização.

- Configurar a herança de definições:

  - **Inherit settings from parent policy**. Se este botão estiver ativado, os valores de definição da política são herdados da política superior. Não é possível editar as definições da política se estiver definido para a política principal.

  - **Force inheritance of settings in child policies**. Se o botão estiver ativado, os valores das definições da política são propagados para as políticas secundárias. Nas propriedades da política secundária, o botão de comutação **Inherit settings from parent policy** será automaticamente ativado e não pode ser desativado. As definições da política são herdadas da política principal, exceto as definições assinaladas com . Não é possível editar as definições da política secundária se estiver definido para a política principal.

8. No separador **Application settings**, pode configurar as definições da política do Kaspersky Endpoint Security.

9. Conclua o assistente.

Deste modo, as definições do Kaspersky Endpoint Security serão configuradas nos computadores cliente durante a seguinte sincronização. Pode consultar informações sobre a política que está a ser aplicada no computador na interface do Kaspersky Endpoint Security clicando no botão no ecrã principal (por exemplo, o nome da política). Para tal, nas definições da política do Agente de Rede, precisa de ativar a receção de dados da política alargada. Para obter mais informações sobre uma política do Agente de Rede, consulte a Ajuda do Kaspersky Security Center.

Exportar e importar uma política

O Kaspersky Endpoint Security permite exportar uma política com as suas definições e perfis para um ficheiro KLP. Pode então utilizar a funcionalidade de exportação/importação de políticas para criar cópias de segurança das políticas, migrar políticas para outro servidor ou, por exemplo, migrar políticas do Kaspersky Security Center Windows para o Kaspersky Security Center Linux. Para obter informações sobre a gestão de políticas, consulte a Ajuda do Kaspersky Security Center.

Como exportar e importar uma política na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.

2. Na pasta **Managed devices** da árvore na Consola de Administração, abra a pasta com o nome do grupo de administração ao qual os computadores cliente em questão pertencem.

3. Na área de trabalho, selecione o separador **Policies**.

4. Para exportar uma política:

   a. Clique na política que deseja exportar.

   b. Clique na ligação **Export policy to file** à direita na janela.

   c. Na janela que se abre, especifique o nome do ficheiro KLP para o qual pretende exportar a política e selecione a pasta para guardar o ficheiro.

   d. Guardar o ficheiro.

5. Para importar uma política:

    a. Clique em **Import policy from file**.

    b. Na janela que se abre, selecione o ficheiro de política KLP que pretende importar.

    c. Abrir o ficheiro.

    Isto adiciona uma nova política com o estado *Inactive policy*.

Como exportar e importar a política na Web Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Para exportar uma política:

    a. Selecione a caixa de verificação junto à política que pretende exportar.

    b. Selecione o botão **Export**.

    c. Na janela que se abre, especifique o nome do ficheiro KLP para o qual pretende exportar a política e selecione a pasta para guardar o ficheiro.

    d. Guardar o ficheiro.
3. Para importar uma política:

    a. Clique em **Import**.

    b. Selecione o ficheiro de política KLP que deseja importar.

    c. Após a política ser processada com sucesso, selecione o grupo de administração ao qual deseja aplicá-la.

    d. Clique no botão **Complete** para finalizar a importação da política.

    Isto adiciona uma nova política com o estado *Inactive*.

Indicador de nível de segurança

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

- **Nível de proteção alto**. O indicador assume este valor e fica verde se todos os componentes das seguintes categorias forem ativados:
    - **Crítica**. Esta categoria inclui os seguintes componentes:
        - Proteção contra ameaças de ficheiros.
        - Deteção de comportamento.
        - Prevenção de explorações.

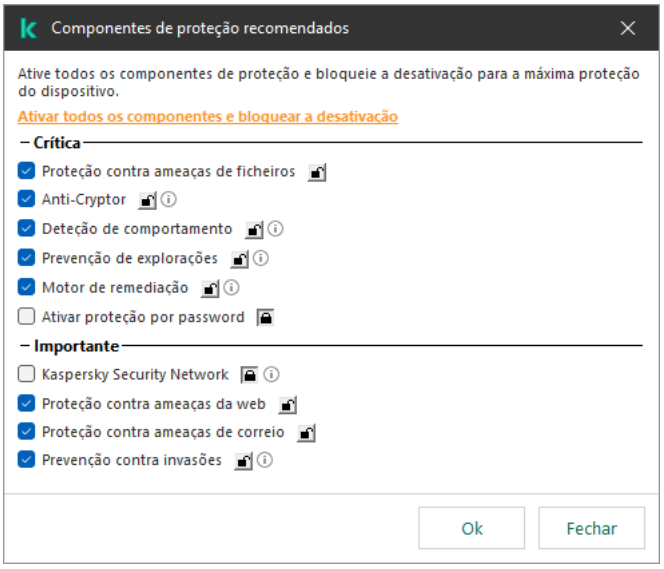
- Motor de remediação.
- Proteção dos serviços da aplicação contra gestão externa.

- **Importante**. Esta categoria inclui os seguintes componentes:
  - Kaspersky Security Network.
  - Proteção contra ameaças da Web.
  - Proteção contra ameaças de correio.
  - Prevenção contra invasões.
  - Proteção por password.

- **Nível de proteção médio**. O indicador assume este valor e fica amarelo se um dos componentes importantes for desativado.
- **Nível de proteção baixo**. O indicador assume este valor e fica vermelho num dos seguintes casos:
  - Um ou vários componentes críticos são desativados.
  - Dois ou mais componentes importantes são desativados.

Se o indicador tiver o valor **Nível de proteção médio** ou **Nível de proteção baixo**, aparece uma ligação que abre a janela **Componentes de proteção recomendados** à direita do indicador. Nesta janela, pode ativar qualquer um dos componentes de proteção recomendados.

Depois de atualizar a aplicação, o indicador de nível de proteção poderá indicar um nível de proteção inferior ao que existia antes da atualização. Isto acontece porque a versão mais recente da aplicação introduz novos componentes ou funcionalidades que são importantes para a segurança do computador. Depois de atualizar a aplicação, tem de gerir as novas definições para garantir que o nível de proteção permanece elevado.



Indicador do nível de segurança da política

Gestão de tarefas

Para administrar o Kaspersky Endpoint Security através do Kaspersky Security Center, pode criar os seguintes tipos de tarefas:

- Tarefas locais, configuradas para um computador cliente individual.
- Tarefas de grupo, configuradas para computadores cliente dentro de grupos de administração.
- Tarefas para a seleção de computadores.

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 suporta as seguintes tarefas:

- **Verificação de software malicioso**. O Kaspersky Endpoint Security verifica a existência de vírus e outras ameaças nas áreas do computador especificadas nas definições da tarefa. A tarefa *Verificação de software malicioso* é necessária para o funcionamento do Kaspersky Endpoint Security e é criada durante o Quick Start Wizard. Recomenda-se que a tarefa seja agendada para ser executada, pelo menos, uma vez por semana.
- **Adicionar chave**. O Kaspersky Endpoint Security adiciona uma chave para ativar aplicações, incluindo uma chave adicional. Antes de executar a tarefa, certifique-se de que o número de computadores nos quais a tarefa deverá ser executada não excede o número de computadores permitidos pela licença.
- **Alterar componentes da aplicação**. O Kaspersky Endpoint Security instala ou remove componentes em computadores cliente de acordo com a lista de componentes especificados nas definições de tarefas. O componente Proteção contra ameaças de ficheiros não pode ser removido. O número ideal de componentes do Kaspersky Endpoint Security ajuda a preservar os recursos de computador.
- **Inventário**. O Kaspersky Endpoint Security recebe informações sobre todos os ficheiros executáveis da aplicação armazenados no computador. A tarefa *Inventário* é executada pelo componente Controlo das Aplicações. Se o componente Controlo das Aplicações não estiver instalado, a tarefa será terminada com um erro.
- **Atualização das bases de dados e módulos da aplicação**. O Kaspersky Endpoint Security atualiza as bases de dados e módulos da aplicação. A tarefa *Atualização das bases de dados e módulos da aplicação* é necessária para o funcionamento do Kaspersky Endpoint Security e é criada durante o Quick Start Wizard. Recomenda-se configurar um programa que execute a tarefa pelo menos uma vez por dia.
- **Eliminar dados**. O Kaspersky Endpoint Security elimina ficheiros e pastas dos computadores dos utilizadores imediatamente ou se não houver ligação ao Kaspersky Security Center durante um período prolongado de tempo.
- **Reverter atualização**. O Kaspersky Endpoint Security reverte a última atualização das bases de dados e módulos da aplicação. Isto pode ser necessário se, por exemplo, as novas bases de dados contiverem dados incorretos que podem causar o bloqueio de uma aplicação segura pelo Kaspersky Endpoint Security.

- **Verificação de integridade da aplicação**. O Kaspersky Endpoint Security analisa os ficheiros da aplicação, verifica os ficheiros para detetar sinais de corrupção ou modificações e verifica as assinaturas digitais dos ficheiros da aplicação.

- **Gestão das contas de Agente de Autenticação**. O Kaspersky Endpoint Security configura as definições da conta do Agente de Autenticação. Um Agente de Autenticação é necessário para trabalhar com unidades encriptadas. Antes de o sistema operativo ser carregado, o utilizador tem de concluir a autenticação com o Agente.

Se a aplicação estiver a funcionar como parte do Endpoint Detection and Response solution pela Kaspersky, pode executar tarefas adicionais como ações de resposta à deteção (responses). Por exemplo, pode terminar processos remotamente utilizando a tarefa *Terminar processo*.

> As tarefas apenas são executadas num computador se o Kaspersky Endpoint Security estiver em execução.

Criar uma tarefa

Como criar uma tarefa na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Selecione a pasta **Tasks** na árvore da Consola de Administração.
3. Clique em **New task**.
   O Assistente de Tarefas é iniciado.
4. Siga as instruções do Assistente de Tarefas.

Como criar uma tarefa na Web Console

1. Na janela principal da Consola Web, selecione **Tasks**.
   A lista de tarefas é aberta.
2. Clique em **Add**.
   O Assistente de Tarefas é iniciado.
3. Configurar as definições de tarefa:
   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.
   b. Na lista pendente **Task type**, selecione a tarefa que pretende executar nos computadores dos utilizadores.
   c. No campo **Task name**, introduza uma breve descrição.
   d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.
4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Avance para o passo seguinte.

5. Selecione uma conta para executar a tarefa. Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de utilizador local.

6. Conclua o assistente.

Será apresentada uma nova tarefa na lista de tarefas. A tarefa terá as predefinições. Aceda às propriedades da tarefa para configurar as definições da tarefa. Para executar uma tarefa, deve selecionar a caixa de verificação oposta à tarefa e clicar no botão **Start**. Após o início da tarefa, pode pausar e retomar a tarefa mais tarde.

Na lista de tarefas, pode monitorizar os resultados da tarefa, que incluem o estado da tarefa e as estatísticas do desempenho da tarefa nos computadores. Também pode criar uma seleção de eventos para monitorizar a execução das tarefas (**Monitoring → Event selections**). Para obter mais informações sobre a seleção de eventos, consulte a Ajuda do Kaspersky Security Center. Os resultados da execução da tarefa são também guardados localmente no registo (log) de eventos do Windows e nos relatórios do Kaspersky Endpoint Security.

Gerir o acesso às tarefas

Os direitos de acesso às tarefas do Kaspersky Endpoint Security (ler, gravar, executar) são definidas para cada utilizador que tenha acesso ao Servidor de Administração do Kaspersky Security Center, através das definições de acesso às áreas funcionais do Kaspersky Endpoint Security. Para configurar o acesso às áreas funcionais do Kaspersky Endpoint Security, aceda à secção **Security** da janela de propriedades do Servidor de Administração do Kaspersky Security Center. Para obter mais informações sobre a gestão de tarefas no Kaspersky Security Center, consulte a Ajuda do Kaspersky Security Center.

Pode configurar os direitos dos utilizadores para acederem às tarefas utilizando uma política (*modo de gestão de tarefas*). Por exemplo, pode ocultar tarefas de grupo na interface do Kaspersky Endpoint Security.

Como configurar o modo de gestão de tarefas na interface do Kaspersky Endpoint Security através da Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Tarefas locais → Gestão de tarefas**.

4. Configure o modo de gestão de tarefas (consulte a tabela abaixo).

5. Guarde as suas alterações.

Como configurar o modo de gestão de tarefas na interface do Kaspersky Endpoint Security através da Consola Web

1. Na janela principal da Consola Web, selecione o separador **Asset management → Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **General Settings → User Interaction**.

5. Em **Permitted actions**, configure o modo de gestão de tarefas (consulte a tabela abaixo).

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

Definições de gestão de tarefas

Parâmetro	Descrição
Access to local tasks	Se a caixa de verificação estiver selecionada, as tarefas locais são apresentadas na interface local do Kaspersky Endpoint Security. Se não existirem restrições de política adicionais, o utilizador pode configurar e executar tarefas. Contudo, a configuração do agendamento de execução da tarefa permanece indisponível para o utilizador. O utilizador apenas pode executar tarefas manualmente. Se esta caixa de seleção estiver desmarcada, as tarefas locais ficam ocultas na interface da aplicação. Neste modo, as tarefas locais não são executadas executam conforme planeado. As Tarefas não podem ser iniciadas ou configuradas na interface local do Kaspersky Endpoint Security ou ao trabalhar com a command line. Um utilizador pode iniciar um verificação de um ficheiro ou pasta selecionando a opção **Verificar vírus** no menu de contexto do ficheiro ou pasta. A tarefa de verificação é iniciada com os valores predefinidos para a tarefa de verificação personalizada.
View group tasks	Se a caixa de verificação estiver selecionada, as tarefas do grupo são apresentadas na interface local do Kaspersky Endpoint Security. O utilizador pode visualizar a lista de todas as tarefas na interface da aplicação. Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security apresenta uma lista de tarefas vazia.
Manage group tasks	Se a caixa de seleção estiver marcada, os utilizadores podem iniciar e parar as tarefas de grupo especificadas na consola do Kaspersky Security Center. Os utilizadores podem iniciar e parar tarefas na interface da aplicação ou na interface simplificada da aplicação. Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security inicia tarefas agendadas automaticamente ou o administrador inicia as tarefas manualmente na consola do Kaspersky Security Center.

Configurar definições da aplicação locais

No Kaspersky Security Center, pode configurar as definições do Kaspersky Endpoint Security num computador específico. São as *definições da aplicação local*. Algumas definições podem não estar acessíveis para edição. Estas definições são bloqueadas pelo atributo nas propriedades da política.

Como configurar as definições da aplicação local na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.

2. Na pasta **Managed devices** da árvore na Consola de Administração, abra a pasta com o nome do grupo de administração ao qual os computadores cliente em questão pertencem.

3. Na área de trabalho, selecione o separador **Devices**.

4. Clique duas vezes para abrir a janela de propriedades do computador.

5. Na janela de propriedades do computador, selecione a secção **Applications**.

6. Na lista de aplicações da Kaspersky instaladas no computador, selecione **Kaspersky Endpoint Security for Windows (14.2)** e clique duas vezes para abrir as propriedades da aplicação.

7. Na secção **Definições gerais**, configure o Kaspersky Endpoint Security, bem como os Relatórios e Armazenamento.

   As restantes secções na janela de propriedades da aplicação são padrão para o Kaspersky Security Center. É fornecida uma descrição destas secções na Ajuda do Kaspersky Security Center.

Se uma aplicação estiver sujeita a uma política que proíbe alterações em definições específicas, não poderá editá-las ao configurar as definições da aplicação na secção **Definições gerais**.

8. Guarde as suas alterações.

Como configurar as definições da aplicação local na Consola Web e Consola de Nuvem

1. Na janela principal da Consola Web, selecione **Asset management** → **Assets (Devices)**.
2. Selecione um computador para o qual quer configurar definições da aplicação locais.

   As propriedades do computador são apresentadas.
3. Selecione o separador **Applications**.
4. Clique em **Kaspersky Endpoint Security for Windows 14.2**.

   As definições da aplicação locais são apresentadas.
5. Selecione o separador **Application settings**.
6. Configure as definições da aplicação locais.
7. Guarde as suas alterações.

As definições da aplicação local são iguais às definições da política, exceto no que diz respeito às definições de encriptação.

Iniciar e parar o Kaspersky Endpoint Security

Após instalar o Kaspersky Endpoint Security no computador de um utilizador, a aplicação é iniciada automaticamente. Por predefinição, o Kaspersky Endpoint Security é iniciado após o arranque do sistema operativo. Não é possível configurar a inicialização automática da aplicação nas definições do sistema operativo.

A transferência das bases de dados de antivírus do Kaspersky Endpoint Security após o arranque do sistema operativo pode demorar até dois minutos, dependendo das capacidades do computador. Durante este período, o nível de proteção do computador é reduzido. A transferência das bases de dados de antivírus quando o Kaspersky Endpoint Security é iniciado num sistema operativo já iniciado não causa uma redução do nível de proteção do computador.

Como configurar o arranque do Kaspersky Endpoint Security na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais** → **Definições da aplicação**.
4. Utilize a caixa de seleção **Iniciar a aplicação no arranque do computador (recomendado)** para configurar o arranque da aplicação.
5. Guarde as suas alterações.

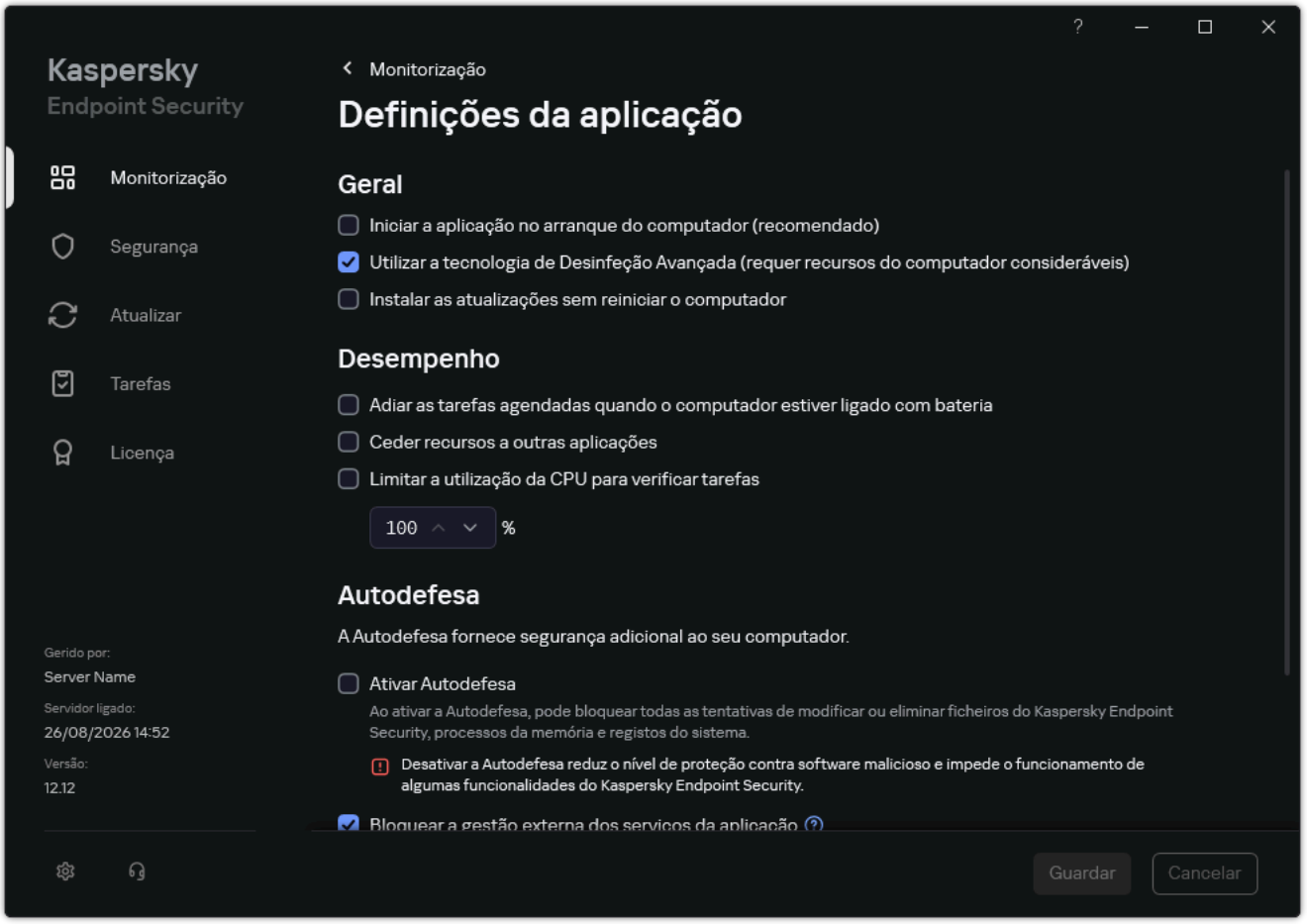
Como configurar o arranque do Kaspersky Endpoint Security na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **User Interaction**.
5. Utilize a caixa de seleção **Start Kaspersky Endpoint Security on computer startup (recommended)** para configurar o arranque da aplicação.
6. Guarde as suas alterações.

Como configurar o arranque do Kaspersky Endpoint Security na interface de aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Definições da aplicação**.



Definições do Kaspersky Endpoint Security for Windows

3. Utilize a caixa de seleção **Iniciar a aplicação no arranque do computador (recomendado)** para configurar o arranque da aplicação.

4. Guarde as suas alterações.

Os especialistas da Kaspersky não recomendam a paragem manual do Kaspersky Endpoint Security, uma vez que tal expõe o computador e os dados pessoais do utilizador a ameaças. Se necessário, pode pausar a proteção do computador o tempo que for preciso, sem parar a aplicação.

Pode monitorizar o estado da aplicação utilizando o widget do **Protection status**.

Como iniciar ou parar o Kaspersky Endpoint Security na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.

2. Na pasta **Managed devices** da árvore na Consola de Administração, abra a pasta com o nome do grupo de administração ao qual os computadores cliente em questão pertencem.

3. Na área de trabalho, selecione o separador **Devices**.

4. Clique duas vezes para abrir a janela de propriedades do computador.

5. Na janela de propriedades do computador, selecione a secção **Applications**.

6. Na lista de aplicações da Kaspersky instaladas no computador, selecione **Kaspersky Endpoint Security for Windows (14.2)** e clique duas vezes para abrir as propriedades da aplicação.

7. Execute uma das ações seguintes:

   - Para iniciar a aplicação, clique no botão  à direita da lista de aplicações da Kaspersky.
   - Para parar a aplicação, clique no botão  à direita da lista de aplicações da Kaspersky.

Como iniciar ou parar o Kaspersky Endpoint Security na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Assets (Devices)**.

2. Clique no nome do computador onde pretende iniciar ou parar o Kaspersky Endpoint Security.

   É aberta a janela de propriedades do computador.

3. Selecione o separador **Applications**.

4. Selecione a caixa de verificação oposta **Kaspersky Endpoint Security for Windows**.

5. Clique no botão **Iniciar** ou **Parar**.

Como iniciar ou parar o Kaspersky Endpoint Security a partir da command line

1. Execute o interpretador de linha de comando (cmd.exe) como administrador.

2. Aceda à pasta onde se encontra o ficheiro executável klpsm.exe.

3. Para iniciar a aplicação a partir da command line, introduza `klpsm.exe start_avp_service`.

4. Para parar a aplicação a partir da command line, introduza `klpsm.exe stop_avp_service`.

Para parar a aplicação a partir da command line, ative a gestão externa dos serviços do sistema.



Iniciar e parar a aplicação a partir da linha de comandos

Pausar e retomar a proteção e controlo do computador

Pausar a proteção e controlo do computador significa desativar todos os componentes de proteção e controlo do Kaspersky Endpoint Security durante algum tempo.

O estado da aplicação é apresentado utilizando o ícone de aplicação na área de notificação da barra de tarefas.

- O ícone significa que a proteção e controlo do computador estão pausadas.
- O ícone significa que a proteção e controlo do computador estão ativadas.

Pausar ou retomar a proteção e controlo do computador não afeta as tarefas de verificação ou atualização.

Se já estiverem estabelecidas ligações de rede no momento em que a proteção e controlo do computador são colocadas em pausa ou retomadas, é apresentada uma notificação relativa à interrupção destas ligações de rede.

Para pausar a proteção e controlo do computador:

1. Clique com o botão direito do rato para visualizar o menu de contexto do ícone da aplicação na área de notificação da barra de tarefas.
2. No menu de contexto, selecione **Pausar proteção** (consulte a figura abaixo).

   Este item do menu contextual está disponível se a proteção por password estiver ativada.

3. Selecione uma das opções seguintes:

   - **Pausar durante <período de tempo>** – a proteção e o controlo do computador serão retomados após o período de tempo especificado na lista pendente abaixo.
   - **Pausar até a aplicação reiniciar** — a proteção e o controlo do computador serão retomados depois de reiniciar a aplicação ou reiniciar o sistema operativo. O início automático da aplicação tem de estar ativado para utilizar esta opção.
   - **Pausar** – a proteção e controlo do computador serão retomados quando decidir reativá-los.

4. Clique em **Pausar proteção**.

O Kaspersky Endpoint Security irá colocar em pausa o funcionamento de todos os componentes de proteção e controlo que não estejam identificados com uma fechadura (🔒) na política. Antes de executar esta operação, recomenda-se a desativação da política do Kaspersky Security Center.



Menu de contexto do ícone da aplicação

Para retomar a proteção e controlo do computador:

1. Clique com o botão direito do rato para visualizar o menu de contexto do ícone da aplicação na área de notificação da barra de tarefas.
2. No menu de contexto, selecione **Retomar proteção**.

Pode retomar a proteção e o controlo do computador em qualquer altura, independentemente da proteção do computador e da opção de pausa de controlo selecionada anteriormente.

Criar e utilizar um ficheiro de configuração

Um ficheiro de configuração com as definições do Kaspersky Endpoint Security permite-lhe realizar as seguintes tarefas:

- Executar a instalação local do Kaspersky Endpoint Security através da command line com as configurações predefinidas.
- Executar a instalação remota do Kaspersky Endpoint Security através das configurações predefinidas do Kaspersky Security Center.
- Transferir as definições da aplicação para uma política.
- Migrar as definições do Kaspersky Endpoint Security de um computador para o outro (veja as instruções abaixo).

Exportar um ficheiro de configuração

A partir da versão 14.2 do Kaspersky Endpoint Security, o ficheiro de configuração exportado pode ser encriptado. Uma vez que o ficheiro de configuração pode conter credenciais, recomendamos que encripte o ficheiro de configuração. Não é possível editar um ficheiro encriptado. Qualquer tentativa de modificar um ficheiro de configuração irá corrompê-lo.

A encriptação do ficheiro de configuração tem as seguintes características especiais:

- O Kaspersky Endpoint Security permite importar ficheiros encriptados apenas na interface de utilizador da aplicação ou através da linha de comandos. Não é possível utilizar um ficheiro deste tipo numa consola do Kaspersky Security Center para configurar uma política ou instalar remotamente a aplicação. Se pretender adicionar o ficheiro a uma política ou a um pacote de instalação, ignore o passo de encriptação do ficheiro.
- Não é possível recuperar a palavra-passe de um ficheiro encriptado.
- As versões do Kaspersky Endpoint Security anteriores à 14.1 não suportam a importação de ficheiros de configuração encriptados. Se pretender importar o ficheiro para uma versão anterior da aplicação, ignore o passo de encriptação do ficheiro.

Para criar um ficheiro de configuração:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Gerir definições**.
3. Clique em **Exportar**.
4. Para guardar o ficheiro de configuração, a Proteção por password tem de estar ativada. O utilizador deve ter a permissão para **Exportar definições**.
5. Na janela que se abre, especifique o caminho no qual pretende guardar o ficheiro de configuração e introduza o nome do mesmo.

   Para utilizar o ficheiro de configuração para a instalação local ou remota do Kaspersky Endpoint Security, deve denominá-lo install.cfg.

6. Se necessário, ative o botão de alternância **Encriptar o ficheiro exportado** e introduza a palavra-passe de encriptação do ficheiro de configuração.

   Guarde a palavra-passe num local seguro. Não é possível recuperar esta palavra-passe.

7. Guardar o ficheiro.

Como resultado, a aplicação cria um ficheiro de configuração.

Importar um ficheiro de configuração

Ao importar um ficheiro de configuração, o Kaspersky Endpoint Security não transfere as passwords dos cripto-contentores. Se utilizar a autenticação de dois fatores ao ligar-se aos servidores, terá de definir as passwords do cripto-contentor a partir do zero.

Para importar as definições do Kaspersky Endpoint Security de um ficheiro de configuração:

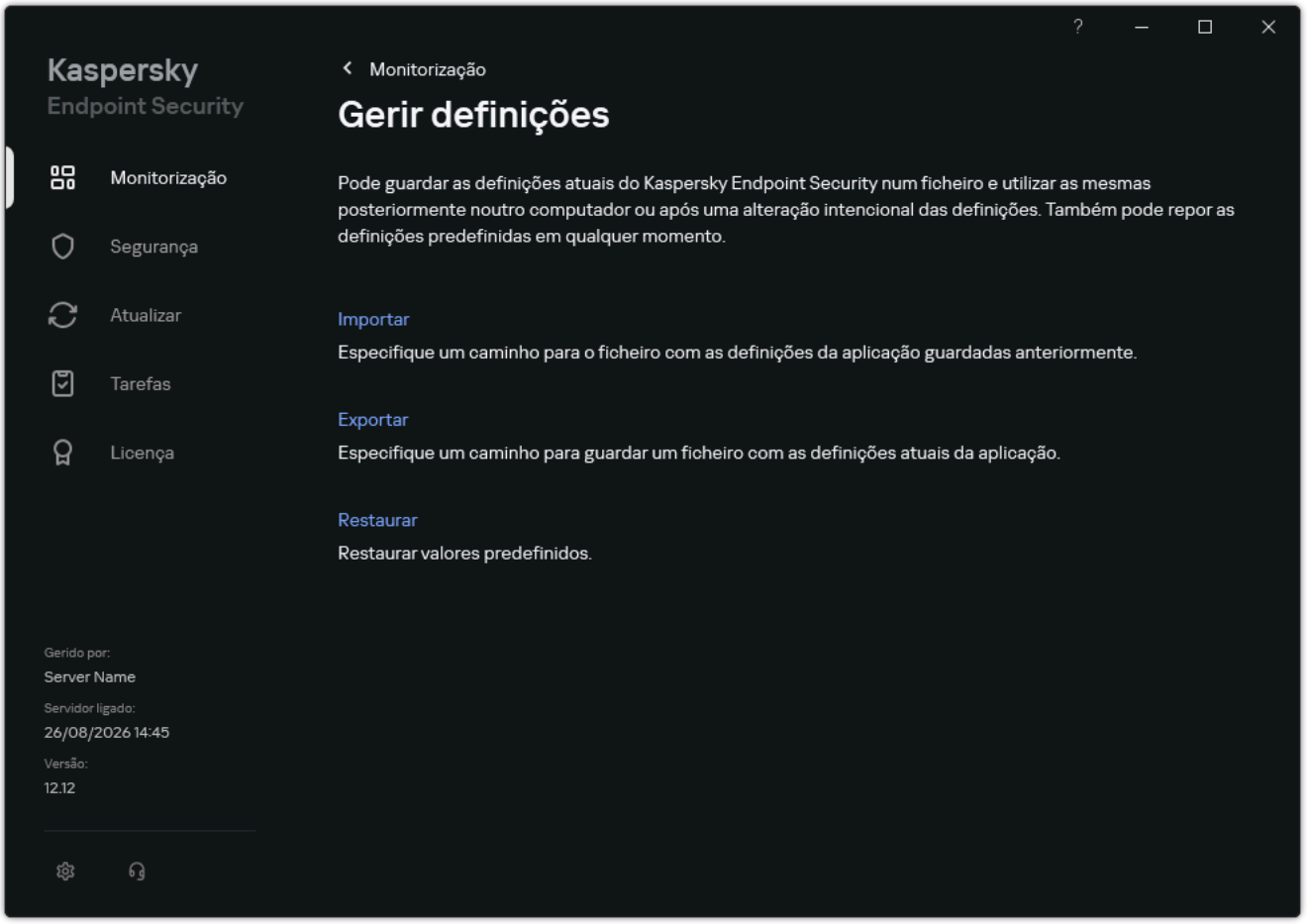
1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Gerir definições**.
3. Clique em **Importar**.
4. Na janela que se abre, introduza o caminho para o ficheiro de configuração.

5. Se o ficheiro de configuração estiver encriptado, introduza a palavra-passe que especificou durante a exportação.

   Se se tiver esquecido da palavra-passe de encriptação do ficheiro de configuração, não poderá recuperá-la. Neste caso, terá de repetir os passos de exportação do ficheiro de configuração.

6. Abrir o ficheiro.

Todos os valores de definições do Kaspersky Endpoint Security serão estabelecidos de acordo com o ficheiro de configuração selecionado.



Gerir as definições da aplicação

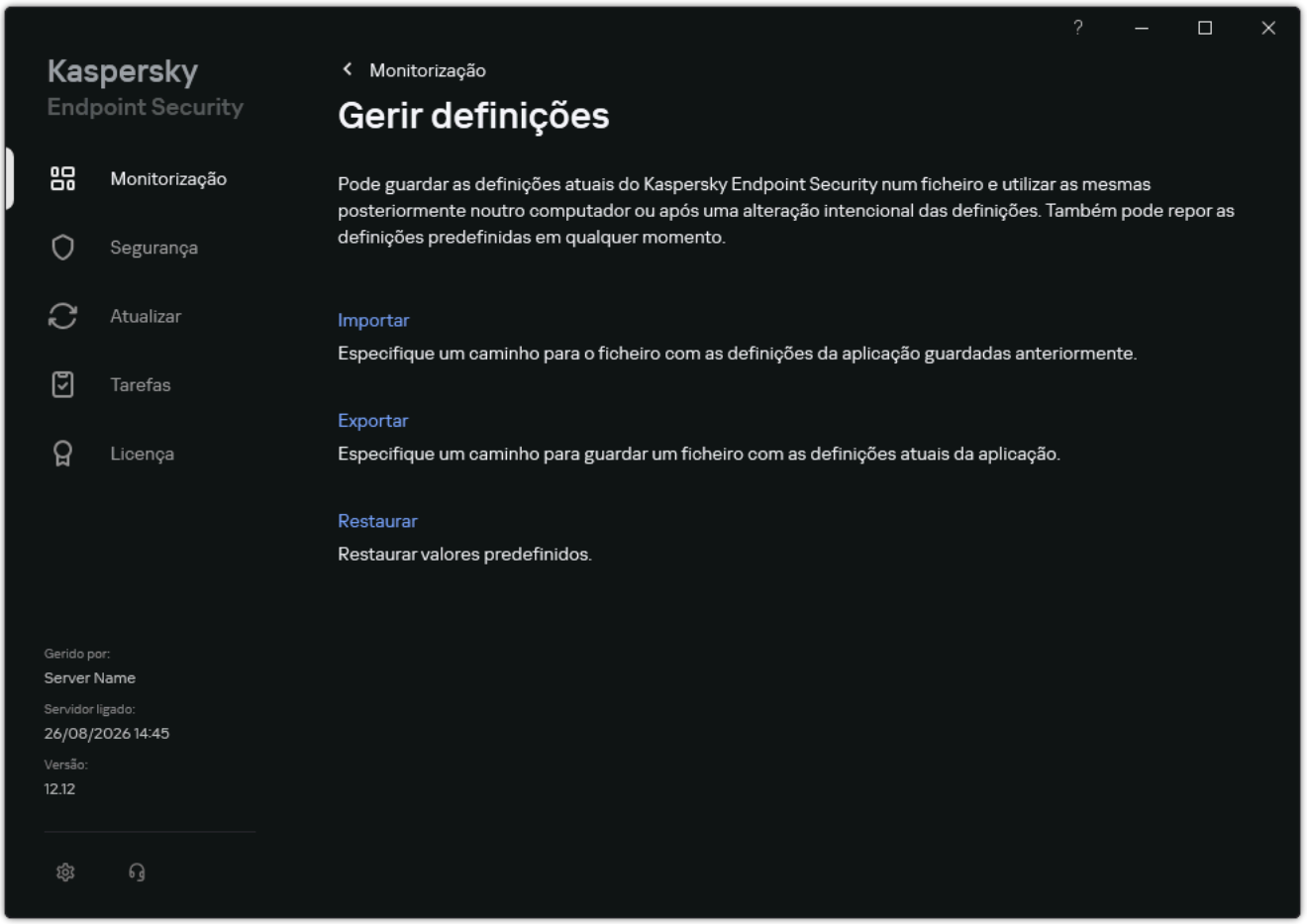
Restaurar as predefinições da aplicação

Pode restaurar as definições da aplicação recomendadas pela Kaspersky a qualquer momento. Quando as definições são restauradas, o nível de segurança **Recomendado** é definido para todos os componentes de proteção.

Para restaurar as predefinições da aplicação:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Gerir definições**.
3. Clique em **Restaurar**.

4. Guarde as suas alterações.



Gerir as definições da aplicação

Desempenho do Kaspersky Endpoint Security e compatibilidade com outras aplicações

O desempenho do Kaspersky Endpoint Security refere-se ao número de tipos de objetos que podem danificar o computador e que são detetáveis, bem como ao consumo de energia e à utilização de recursos do computador.

Selecionar tipos de objetos detetáveis

O Kaspersky Endpoint Security permite-lhe ajustar a proteção do seu computador e selecionar os tipos de objetos que a aplicação deteta em funcionamento. O Kaspersky Endpoint Security verifica sempre o sistema operativo quanto à presença de vírus, worms e programas Trojan. Não é possível desativar a verificação destes tipos de objetos. Tal software malicioso pode causar danos significativos no computador. Para uma maior segurança do computador, pode expandir o intervalo de tipos de objetos detetáveis, ativando a monitorização de software legal que pode ser utilizado por criminosos para danificar o seu computador ou dados pessoais.

Utilizar o modo de poupança de energia

O consume de energia das aplicações é um aspeto chave nos computadores portáteis. As tarefas agendadas do Kaspersky Endpoint Security normalmente consomem recursos consideráveis. Quando o computador está a funcionar com bateria, pode utilizar o modo de poupança de energia para otimizar a carga da bateria.

No modo de poupança 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;

Se o modo de poupança de energia estiver ou não ativado, o Kaspersky Endpoint Security interrompe as tarefas de encriptação quando um computador portátil muda para alimentação combateria. A aplicação retoma as tarefas de encriptação quando o computador portátil muda de bateria para ligação à eletricidade.

Conceder recursos do computador a outras aplicações

O consumo de recursos do computador durante a verificação do computador pode aumentar a carga nos subsistemas da CPU e do disco rígido. Para resolver o problema do funcionamento em simultâneo durante períodos de carga acrescida sobre o CPU e os subsistemas das unidades de disco rígido, o Kaspersky Endpoint Security pode conceder recursos para outras aplicações.

Utilização da tecnologia de desinfeção avançada

Atualmente, as aplicações maliciosas conseguem penetrar nos níveis mais baixos de um sistema operativo, o que os torna, praticamente, impossíveis de eliminar. Após detetar atividade maliciosa no sistema operativo, o Kaspersky Endpoint Security realiza uma desinfeção minuciosa que utiliza tecnologia de desinfeção avançada especial. *A Tecnologia de Desinfeção Avançada* visa apagar do sistema operativo as aplicações maliciosas, cujos processos já tenham iniciado na memória RAM e que impedem que o Kaspersky Endpoint Security os remova utilizando outros métodos. Deste modo, a ameaça é neutralizada. Enquanto a Desinfeção Avançada decorre, é recomendado não iniciar novos processos nem editar o registo do sistema operativo. A tecnologia de desinfeção avançada utiliza recursos consideráveis do sistema operativo, o que poderá tornar outras aplicações mais lentas.

Após o processo de Desinfeção Avançada concluir num computador com o Microsoft Windows para estações de trabalho, o Kaspersky Endpoint Security solicita ao utilizador permissão para reiniciar o computador. Após o reinicio do sistema, o Kaspersky Endpoint Security elimina os ficheiros de software malicioso e inicia uma verificação completa mais rápida do computador.

Não é possível apresentar um pedido de reinício num computador com o Microsoft Windows para servidores de ficheiros, devido às especificidades do Kaspersky Endpoint Security. Um reinício não previsto de um servidor de ficheiros pode originar problemas relacionados com a indisponibilidade temporária dos dados do servidor de ficheiros ou perda de dados não guardados. É recomendado reiniciar um servidor apenas conforme planeado. Por este motivo, a tecnologia de Desinfeção Avançada está desativada para servidores de ficheiros por predefinição.

Se for detetada uma infeção ativa num servidor de ficheiros, é enviado um evento ao Kaspersky Security Center com informações a indicar a necessidade de uma Desinfeção Avançada. Para desinfetar uma infeção ativa de um servidor de ficheiros, ative a tecnologia de Desinfeção Avançada para servidores e inicie uma tarefa de grupo de *Verificação de software malicioso* numa altura conveniente para os utilizadores do servidor.

Ativar ou desativar o modo de poupança de energia

O *modo de poupança de energia* é uma funcionalidade que reduz a carga sobre os recursos do portátil e prolonga a autonomia da bateria sem comprometer significativamente o nível de segurança. No modo de poupança de energia, a aplicação limita a execução de tarefas agendadas. Desta forma, o modo de poupança de energia garante um equilíbrio entre o nível de segurança e a autonomia da bateria do portátil.

Quando o modo de poupança de energia está ativado e o computador está ligado com bateria, as seguintes tarefas não são executadas, mesmo que estejam agendadas:

- *Verificação completa*.
- *Verificação de Áreas Críticas*.
- *Verificação Personalizada*.
- *Verificação de integridade da aplicação*.
- *Verificação IOC*.
- *Atualização das bases de dados e módulos da aplicação* (apenas correções)

A aplicação ignora as atualizações programadas da base de dados apenas quando o portátil está a funcionar com a bateria e o nível de carga da bateria é inferior a 30% (valor predefinido). Pode alterar o nível mínimo de carga da bateria a partir do qual a aplicação começa a ignorar as atualizações programadas da base de dados de antivírus ao editar o registo (consulte as instruções abaixo). Em todos os outros casos, o Kaspersky Endpoint Security atualiza as bases de dados de acordo com a programação, independentemente de o portátil estar ligado à corrente ou a funcionar com a bateria, ou de a aplicação se encontrar no modo de poupança de energia.

Como ativar ou desativar o modo de poupança de energia na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Definições gerais** → **Definições da aplicação**.
5. No bloco **Desempenho**, use a caixa de verificação **Adiar as tarefas agendadas quando o computador estiver ligado com bateria** para ativar ou desativar o modo de economia de energia.
6. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

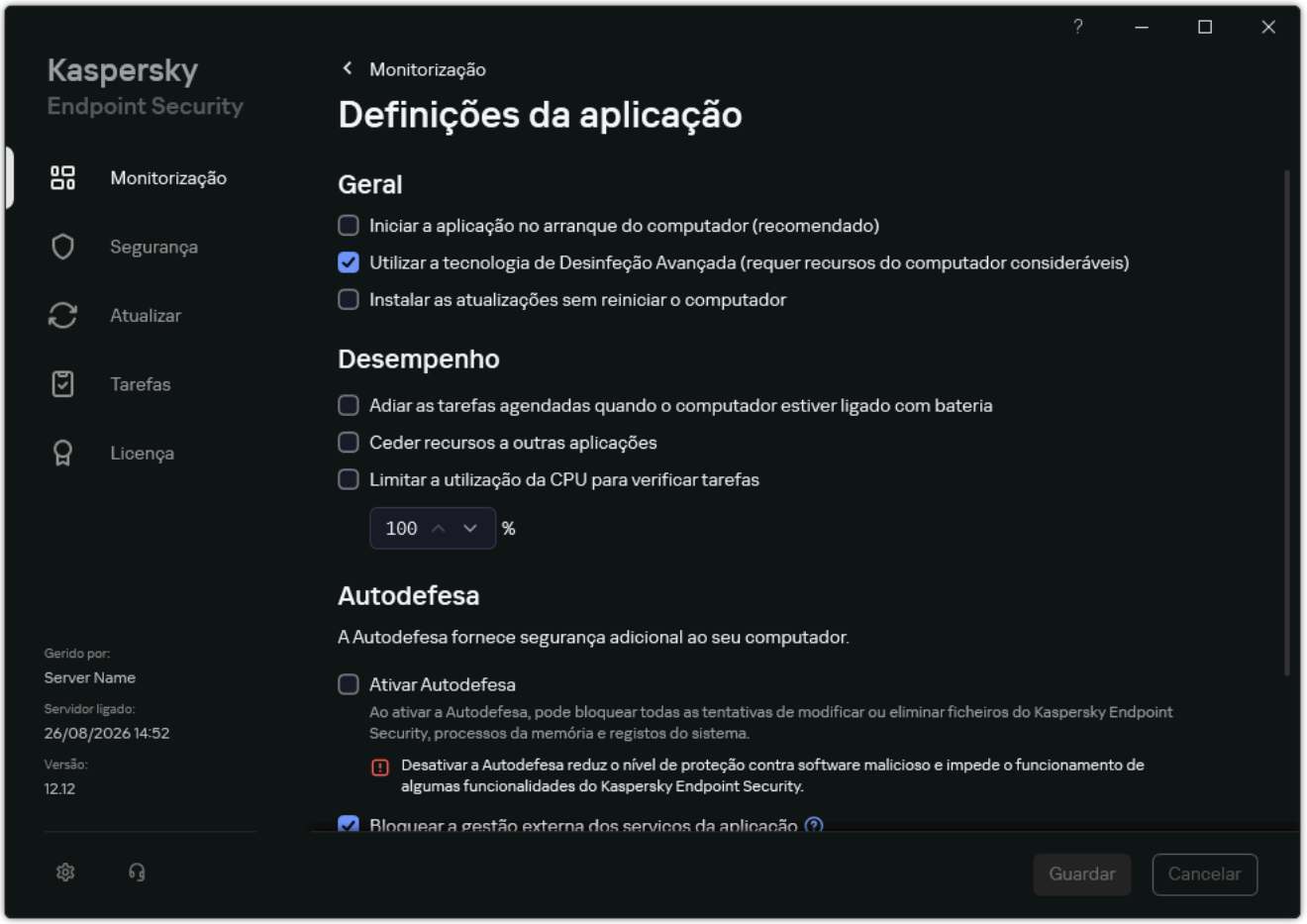
Como ativar ou desativar o modo de poupança de energia na Consola Web

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **Performance**.
5. No bloco **Postpone or skip scheduled tasks while running on battery power**, use a caixa de verificação **Postpone or skip scheduled tasks while running on battery power (depends on OS)** para ativar ou desativar o modo de economia de energia.
6. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar ou desativar o modo de poupança de energia na interface da aplicação

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Definições gerais** → **Definições da aplicação**.



Definições do Kaspersky Endpoint Security for Windows

3. No bloco **Desempenho**, use a caixa de verificação **Adiar as tarefas agendadas quando o computador estiver ligado com bateria** para ativar ou desativar o modo de economia de energia.
4. Guarde as suas alterações.

Como alterar o nível mínimo de carga a partir do qual a aplicação começa a ignorar as atualizações programadas da base de dados de antivírus

1. Abra o editor de registo no computador.
2. No editor de registo, vá para a seguinte secção:
   - Para sistemas operativos de 64 bits: `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES.14.2\environment]`
   - Para sistemas operativos 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 a aplicação começa a ignorar as atualizações programadas da base de dados de antivírus.

Ativar ou desativar a concessão de recursos para outras aplicações

O consumo de recursos do computador pelo Kaspersky Endpoint Security durante a verificação do computador pode aumentar a carga nos subsistemas da CPU e do disco rígido. Isto pode tornar as outras aplicações mais lentas. Para otimizar o desempenho, o Kaspersky Endpoint Security possui um *modo de transferência de recursos para outras aplicações*. Neste modo, o sistema operativo pode diminuir a prioridade das linhas de execução de tarefas de verificação do Kaspersky Endpoint Security quando a carga da CPU é elevada. Isto permite redistribuir os recursos do sistema operativo para outras aplicações. Desta forma, as tarefas de verificação irão receber menos tempo de CPU. Como resultado, o Kaspersky Endpoint Security irá demorar mais tempo a verificar o computador. Por predefinição, a aplicação está configurada para ceder recursos a outras aplicações.

Como ativar ou desativar a concessão de recursos a outras aplicações na Administration Console (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais → Definições da aplicação**.
4. No bloco **Desempenho**, use a caixa de verificação **Ceder recursos a outras aplicações** para ativar ou desativar a concessão de recursos para outras aplicações.
5. Guarde as suas alterações.

Como ativar ou desativar a concessão de recursos a outras aplicações na Web Console e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings → Performance**.

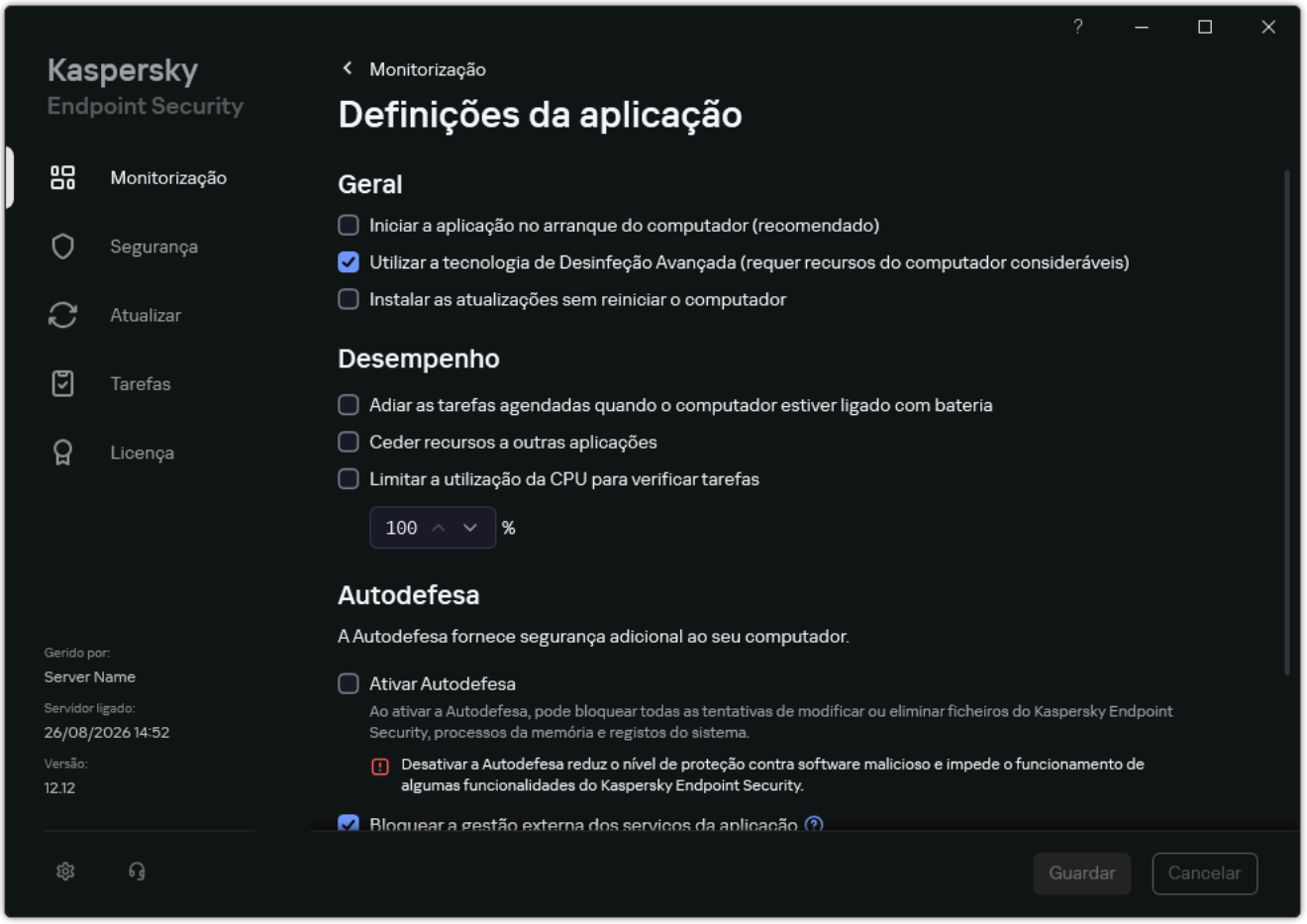
5. No bloco **Yield resources to other applications**, utilize o botão **Yield resources to other applications** para ativar ou desativar a concessão de recursos para outras aplicações.

6. Guarde as suas alterações.

Como ativar ou desativar a concessão de recursos a outras aplicações na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Definições gerais → Definições da aplicação**.



Definições do Kaspersky Endpoint Security for Windows

3. No bloco **Desempenho**, use a caixa de verificação **Ceder recursos a outras aplicações** para ativar ou desativar a concessão de recursos para outras aplicações.

4. Guarde as suas alterações.

Melhores práticas para otimizar o desempenho do Kaspersky Endpoint Security

Ao implantar o Kaspersky Endpoint Security for Windows, pode usar 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 conhecimento de Suporte Técnico.

Geral

Configure as definições gerais da aplicação de acordo com as seguintes recomendações:

1. Atualize o Kaspersky Endpoint Security para a versão mais recente.

   As versões mais recentes da aplicação têm erros corrigidos, estabilidade melhorada e desempenho otimizado.

2. Ative os componentes de proteção com definições predefinidas.

   As definições predefinidas são consideradas as ideais. Estas definições são recomendadas pelos peritos da Kaspersky. As definições predefinidas fornecem o nível de proteção recomendado e o uso ideal dos recursos. Se necessário, pode restaurar definições predefinidas da aplicação.

3. Ative as funcionalidades de otimização do desempenho da aplicação.

   A aplicação possui funcionalidades de otimização do desempenho: modo de conservação de energia e conceder recursos para outras aplicações. Certifique-se de que estas opções estão ativadas.

Verificação de software malicioso nas estações de trabalho

Ativar Verificação em segundo plano é recomendado para Verificação de software malicioso em estações de trabalho. *Verificação em segundo plano* é um modo de verificação do Kaspersky Endpoint Security que não exibe notificações para o utilizador. A Verificação de fundo requer menos recursos informáticos que outros tipos de verificação (tal como uma verificação total). Neste modo, o Kaspersky Endpoint Security verifica objetos de arranque, o sector de arranque, a memória do sistema e a partição do sistema. As definições de verificação em segundo plano são consideradas as ideais. Estas definições são recomendadas pelos peritos da Kaspersky. Assim, para realizar uma Verificação de software malicioso no computador, pode usar apenas o modo de verificação em segundo plano, sem usar outras tarefas de verificação.

Se a verificação em segundo plano não se adequar às suas necessidades, configure a tarefa de *Verificação de software malicioso* de acordo com as seguintes recomendações:

1. Defina um limite para o consumo de recursos da CPU durante a verificação do computador.

   Pode limitar a utilização da CPU ao executar a tarefa *Verificação de software malicioso*. Para o fazer, nas definições da aplicação, especifique a percentagem máxima de carga da CPU para todos os núcleos que podem ser utilizados durante a verificação do computador. Isto pode aumentar o tempo que demora a verificar o computador.

2. Configure o agendamento de verificações do computador ideal.

   Pode configurar a tarefa para ser executada quando o computador estiver a funcionar com carga mínima. Por exemplo, pode configurar a tarefa para ser executada à noite ou aos fins de semana.

   Se os utilizadores desligarem o computador fora do horário de expediente, pode ativar a função Wake-on-LAN. A funcionalidade Wake-on-LAN permite ligar o computador remotamente mediante o envio de um sinal especial pela rede local. Para utilizar esta funcionalidade, deve ativar a Wake-on-LAN nas definições do BIOS. Pode também desligar o computador automaticamente após a conclusão da verificação.

   Se não conseguiu configurar um agendamento de verificações ideal, defina as tarefas para serem executadas apenas quando o computador estiver inativo. O Kaspersky Endpoint Security inicia a tarefa de verificação se o computador estiver bloqueado ou se a proteção de ecrã estiver ativada. Se interrompeu a execução da tarefa (por exemplo, ao desbloquear o computador), o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que foi interrompido.

3. Definir um âmbito de verificação.

   Selecione os seguintes objetos para verificação (conjunto mínimo de âmbitos de verificação):

   - Memória Kernel
   - Executar processos e objetos de arranque
   - Setores de arranque
   - %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 da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. A tecnologia iSwift é um avanço da tecnologia iChecker para o sistema de ficheiros NTFS.

   - Tecnologia iChecker.

     Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. Existem limites para a tecnologia iChecker: não funciona com ficheiros grandes e aplica-se apenas a ficheiros com uma estrutura que o Kaspersky Internet Security reconheça (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

   Só pode ativar as tecnologias iSwift e iChecker na Consola de administração (MMC) e na interface do Kaspersky Endpoint Security. Não pode ativar estas tecnologias na Consola Web do Kaspersky Security Center.

5. Desative a verificação de ficheiros protegidos por password.

   Se a verificação de ficheiros protegidos por password estiver ativada, um pedido de password é apresentado antes de o ficheiro ser verificado. Como a tarefa é recomendada para ser agendada durante o horário fora do escritório, o utilizador não pode inserir a password. Pode verificar ficheiros protegidos por password manualmente.

6. Desativar o lançamento simultâneo de várias tarefas de verificação.

   O Kaspersky Endpoint Security vai colocar em fila novas tarefas de verificação se a verificação atual continuar. Isto ajuda a otimizar a carga no computador.

Verificação de software malicioso nos servidores

Configure a tarefa de *Verificação de software malicioso* de acordo com as seguintes recomendações:

1. Defina um limite para o consumo de recursos da CPU durante a verificação do computador.

   Pode limitar a utilização da CPU ao executar a tarefa *Verificação de software malicioso*. Para o fazer, nas definições da aplicação, especifique a percentagem máxima de carga da CPU para todos os núcleos que podem ser utilizados durante a verificação do computador. Isto pode aumentar o tempo que demora a verificar o computador.

2. Configure o agendamento de verificações do computador ideal.

   Pode configurar a tarefa para ser executada quando o computador estiver a funcionar com carga mínima. Por exemplo, pode configurar a tarefa para ser executada à noite ou aos fins de semana.

3. Ativar as tecnologias iSwift e iChecker.

   - Tecnologia iSwift.

     Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. A tecnologia iSwift é um avanço da tecnologia iChecker para o sistema de ficheiros NTFS.

   - Tecnologia iChecker.

     Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. Existem limites para a tecnologia iChecker: não funciona com ficheiros grandes e aplica-se apenas a ficheiros com uma estrutura que o Kaspersky Internet Security reconheça (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

   Só pode ativar as tecnologias iSwift e iChecker na Consola de administração (MMC) e na interface do Kaspersky Endpoint Security. Não pode ativar estas tecnologias na Consola Web do Kaspersky Security Center.

4. Desative a verificação de ficheiros protegidos por password.

   Se a verificação de ficheiros protegidos por password estiver ativada, um pedido de password é apresentado antes de o ficheiro ser verificado. Como a tarefa é recomendada para ser agendada durante o horário fora do escritório, o utilizador não pode inserir a password. Pode verificar ficheiros protegidos por password manualmente.

5. Desativar o lançamento simultâneo de várias tarefas de verificação.

   O Kaspersky Endpoint Security vai colocar em fila novas tarefas de verificação se a verificação atual continuar. Isto ajuda a otimizar a carga no computador.

Kaspersky Security Network

Para proteger o seu computador de forma mais eficaz, o Kaspersky Endpoint Security utiliza dados recebidos de utilizadores em todo o mundo. A Kaspersky Security Network foi concebida para obter esses dados.

A Kaspersky Security Network (KSN) é uma infraestrutura de serviços na nuvem que fornece o acesso à Base de Conhecimento online da Kaspersky, que contém informações sobre a reputação de ficheiros, recursos da Internet e software. A utilização de dados da Kaspersky Security Network permite uma resposta mais rápida do Kaspersky Endpoint Security a novas ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos diagnósticos positivos. Se participar na Kaspersky Security Network, os serviços da KSN irão fornecer ao Kaspersky Endpoint Security informações sobre a reputação dos endereços Web verificados, bem como informações sobre a categoria e a reputação dos ficheiros verificados.

Edite as definições do Kaspersky Security Network de acordo com as seguintes recomendações:

1. Desativar o modo KSN alargado.

   O modo KSN avançado é um modo no qual o Kaspersky Endpoint Security envia dados adicionais à Kaspersky.

2. Configurar a Kaspersky Private Security Network.

   Kaspersky Private Security Network (KPSN) é uma solução que permite que utilizadores de computadores que alojam o Kaspersky Endpoint Security ou outras aplicações da Kaspersky tenham acesso às bases de dados de reputação do Kaspersky Security Network e a outros dados estatísticos sem enviar dados para o KSN a partir de seus próprios computadores.

3. Ativar o modo de nuvem.

   O Modo de nuvem refere-se ao modo operacional da aplicação no qual o Kaspersky Endpoint Security utiliza uma versão simplificada das bases de dados antivírus. A Kaspersky Security Network suporta a operação da aplicação quando estão a ser usadas bases de dados antivírus simplificadas. A versão simplificada das bases de dados antivírus permite-lhe utilizar cerca de metade da RAM do computador que de outra forma seria utilizada com as bases de dados habituais. Se não participar na Kaspersky Security Network ou se o Modo de nuvem estiver desativado, o Kaspersky Endpoint Security transfere a versão completa das bases de dados antivírus dos servidores da Kaspersky.

Verificação de software malicioso

Uma verificação de software malicioso é essencial para a segurança do computador. Executar verificações de software malicioso regularmente pode excluir a possibilidade de proliferação de software malicioso que não é detetado pelos componentes de proteção devido a uma definição de nível de segurança baixo ou por outras razões.

O Kaspersky Endpoint Security não verifica ficheiros cujo conteúdo está localizado no armazenamento na nuvem do OneDrive e cria entradas de registo informando que estes ficheiros não foram verificados.

Verificação completa

Uma verificação minuciosa de todo o computador. O Kaspersky Endpoint Security verifica os seguintes objetos:

- Memória Kernel
- Objetos carregados ao iniciar o sistema operativo
- Setores de arranque
- Cópia de segurança do sistema operativo
- Todas as unidades de disco rígido e amovíveis

Os especialistas da Kaspersky recomendam que não altere o âmbito de verificação da tarefa *Verificação completa*.

Para conservar os recursos do computador, é recomendado para executar uma tarefa de verificação de fundo em vez de uma verificação completa. Isto não irá afetar o nível de segurança do computador.

Verificação de Áreas Críticas

Por predefinição, o Kaspersky Endpoint Security verifica a memória Kernel, os processos em execução e os setores de inicialização do disco.

Os especialistas da Kaspersky recomendam que não altere o âmbito de verificação da tarefa *Verificação de Áreas Críticas*.

Verificação Personalizada

O Kaspersky Endpoint Security verifica os objetos selecionados pelo utilizador. Pode verificar qualquer objeto da seguinte lista:

- Memória do sistema
- Objetos carregados ao iniciar o sistema operativo
- Cópia de segurança do sistema operativo
- Unidades de disco rígido, amovíveis e de rede
- Qualquer ficheiro selecionado

Verificação em segundo plano

Verificação em segundo plano é um modo de verificação do Kaspersky Endpoint Security que não exibe notificações para o utilizador. A Verificação de fundo requer menos recursos informáticos que outros tipos de verificação (tal como uma verificação total). Neste modo, o Kaspersky Endpoint Security verifica objetos de arranque, o sector de arranque, a memória do sistema e a partição do sistema.

Verificação de integridade da aplicação

O Kaspersky Endpoint Security verifica se os módulos de aplicação foram corrompidos ou modificados.

Verificar o computador

Uma verificação é essencial para a segurança do computador. Executar verificações de software malicioso regularmente pode excluir a possibilidade de proliferação de software malicioso que não é detetado pelos componentes de proteção devido a uma definição de nível de segurança baixo ou por outras razões. O componente fornece proteção ao computador com a ajuda das bases de dados antivírus, o serviço de nuvem da Kaspersky Security Network e análise heurística.

O Kaspersky Endpoint Security tem as seguintes tarefas padrão predefinidas: *Verificação completa*, *Verificação de Áreas Críticas* e *Verificação Personalizada*. Se a sua organização tiver o sistema de administração do Kaspersky Security Center implementado, pode criar uma tarefa *Verificação de software malicioso* e configurar a verificação.

Como executar uma tarefa de verificação na Administration Console (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Tasks**.

3. Selecione a tarefa de verificação e clique duas vezes para abrir as propriedades da tarefa.

   Se necessário, crie a tarefa *Verificação de software malicioso*.

4. Na janela de propriedades da tarefa, selecione a secção **Definições**.

5. Configure a tarefa de verificação (consulte a tabela abaixo).

   Se necessário, configure o agendamento da tarefa de verificação.

6. Guarde as suas alterações.

7. Execute a tarefa de verificação.

O Kaspersky Endpoint Security começará a verificar o computador. Se o utilizador interrompeu a execução da tarefa (por exemplo, ao desligar 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 Web Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Tasks**.

   A lista de tarefas é aberta.

2. Clique na tarefa de verificação.

   É apresentada a janela de propriedades da tarefa.

3. Selecione o separador **Application settings**.

4. Configure a tarefa de verificação (consulte a tabela abaixo).

   Se necessário, configure o agendamento da tarefa de verificação.

5. Guarde as suas alterações.

6. Execute a tarefa de verificação.

O Kaspersky Endpoint Security começará a verificar o computador. Se o utilizador interrompeu a execução da tarefa (por exemplo, ao desligar 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 da aplicação

1. Na janela principal da aplicação, aceda à secção **Tarefas**.

2. Na lista de tarefas, selecione a tarefa de verificação e clique em ⚙.

> Se a tarefa de verificação não for apresentada, tal significa que o administrador proibiu a utilização de tarefas locais na política.

> Na interface da aplicação, pode configurar apenas tarefas de verificação locais: *Verificação completa*, *Verificação de Áreas Críticas*, *Verificação Personalizada*. Não é possível configurar, na interface da aplicação, tarefas de grupo adicionadas através da Consola do Kaspersky Security Center. O botão ⚙ não é apresentado para tarefas de grupo.

3. Configure a tarefa de verificação (consulte a tabela abaixo).

   Se necessário, configure o agendamento da tarefa de verificação.

4. Guarde as suas alterações.

5. Execute a tarefa de verificação.

   O Kaspersky Endpoint Security começará a verificar o computador. A aplicação mostrará o progresso da verificação, o número de ficheiros verificados e o tempo restante da verificação. Pode parar a tarefa a qualquer momento clicando no botão **Parar**.

Para otimizar o desempenho do Kaspersky Endpoint Security durante a verificação do computador, pode gerir as definições avançadas da tarefa *Verificação completa* e limitar a utilização de recursos da CPU.

No Kaspersky Security Center, também pode usar a tarefa *Verificação em segundo plano*, em vez da tarefa *Verificação completa* para otimizar o desempenho da aplicação. Isto não irá afetar o nível de segurança do computador. Não é possível configurar a verificação em segundo plano.

Como resultado, o Kaspersky Endpoint Security verifica o computador e, se for detetada uma ameaça, executa a ação configurada nas definições da aplicação. Normalmente, a aplicação tenta desinfetar os ficheiros infetados. Como resultado, os ficheiros infetados podem receber os estados seguintes:

- **Adiado**. O ficheiro infetado não pôde ser desinfetado. A aplicação elimina o ficheiro infetado após a reinicialização do computador.
- **Registado**. O ficheiro infetado não pôde ser desinfetado. A aplicação adiciona informações sobre ficheiros infetados detetados para a lista de ameaças ativas.
- **Não suporta escrita** ou **Erro de escrita**. O ficheiro infetado não pôde ser desinfetado. A aplicação não tem acesso de escrita.
- **Já processado**. A aplicação detetou um ficheiro infetado anteriormente. A aplicação desinfeta ou elimina o ficheiro infetado após a reinicialização do computador.

Definições de verificação

Parâmetro	Descrição
Nível de segurança	O Kaspersky Endpoint Security pode utilizar diferentes grupos de definições para executar uma verificação. Estes grupos de definições armazenados na aplicação chamam-se *níveis de segurança*: • **Alto**. O Kaspersky Endpoint Security verifica todos os tipos de ficheiros. Ao verificar ficheiros, a aplicação verifica arquivos, pacotes de distribuição, ficheiros de formato do office, mas não verifica arquivos protegidos por password. Quando este nível de segurança é definido, a aplicação utiliza a análise heurística com o nível de detalhe **Nível avançado**. • **Recomendado**. O Kaspersky Endpoint Security verifica todos os tipos de ficheiros. Ao verificar ficheiros, a aplicação verifica arquivos, pacotes de distribuição, ficheiros de formato do office, mas não verifica arquivos protegidos por password. Quando este nível de segurança é definido, a aplicação utiliza a análise heurística com o nível de detalhe **Nível médio**. • **Baixo**. O Kaspersky Endpoint Security verifica apenas os formatos de ficheiro especificados. Ao verificar ficheiros, a aplicação verifica arquivos, pacotes de distribuição, ficheiros de formato do office, mas não verifica arquivos protegidos por password. Quando este nível de segurança é definido, a aplicação utiliza a análise heurística com o nível de detalhe **Nível superficial**. Pode selecionar um dos níveis de segurança predefinidos ou configurar manualmente as definições do nível de segurança. Se alterar as definições de nível de segurança, pode sempre repor as definições de nível de segurança recomendadas.

Parâmetro	Descrição
Ação após deteção de ameaças	**Desinfetar, eliminar se a desinfeção falhar**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação elimina o ficheiro. **Desinfetar, informar se a desinfeção falhar**. Se esta opção estiver selecionada, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção falhar, o Kaspersky Endpoint Security adiciona a informação sobre os ficheiros infetados que são detetados à lista de ameaças ativas. **Informar**. Se esta opção for selecionada, o Kaspersky Endpoint Security adiciona a informação sobre ficheiros infetados à lista de ameaças ativas na deteção destes ficheiros. Antes de tentar desinfetar ou eliminar um ficheiro infetado, a aplicação cria uma cópia de segurança do ficheiro para o caso de vir a precisar de o restaurar ou de o mesmo poder ser desinfetado no futuro. Ao detetar ficheiros infetados que fazem parte da aplicação Loja Windows, o Kaspersky Endpoint Security tenta eliminar esses ficheiros.
Executar a Desinfeção Avançada imediatamente *(disponível apenas na Consola do Kaspersky Security Center)*	A Desinfeção Avançada durante uma tarefa de verificação de vírus num computador só é executada se a funcionalidade Desinfeção Avançada for ativada nas propriedades da política aplicada a este computador. Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security desinfeta a infeção ativa imediatamente após ser detetada durante a execução da tarefa de verificação de vírus. Depois de a infeção ativa ser desinfetada, o Kaspersky Endpoint Security reinicia o computador sem solicitar confirmação ao utilizador. Se a caixa de verificação não estiver selecionada, o Kaspersky Endpoint Security não desinfeta a infeção ativa imediatamente após ser detetada durante a execução da tarefa de verificação de vírus. O Kaspersky Endpoint Security gera eventos de infeção ativa em relatórios de aplicações locais e no Kaspersky Security Center. A infeção ativa pode ser desinfetada quando a tarefa de verificação de vírus é executada novamente com a funcionalidade Desinfeção Avançada ativada. Deste modo, o administrador do sistema pode escolher o momento adequado para realizar a Desinfeção Avançada e, posteriormente, reiniciar os computadores automaticamente.
Âmbito de verificação	Lista de objetos que o Kaspersky Endpoint Security verifica durante a execução de uma tarefa de verificação. Os objetos no âmbito de verificação podem incluir a memória kernel, os processos em execução, setores de arranque, armazenamento da cópia de segurança do sistema, discos rígidos, unidades amovíveis ou unidades de rede, uma pasta ou um ficheiro. No Kaspersky Endpoint Security for Windows 12.12, o e-mail está excluído do âmbito da verificação da aplicação. A verificação dos e-mails recebidos e enviados é realizada pelo componente Proteção contra ameaças de correio. Se estiver a utilizar uma versão anterior do plug-in de gestão, a aplicação exclui o e-mail do âmbito da verificação, mesmo que a política o inclua.
Agendamento da verificação	**Manually**. Modo de execução, no qual pode iniciar a verificação manualmente quando for conveniente para si. **By schedule**. Neste modo de execução da tarefa, a aplicação inicia a tarefa de verificação em conformidade com o agendamento criado pelo utilizador. Se este modo de execução da tarefa de verificação estiver selecionado, pode também iniciar manualmente a tarefa de verificação.
Adiar execução, após o início da aplicação, durante N minutos	Início adiado da tarefa de verificação até após o início da aplicação. No arranque do sistema operativo, há muitos processos em execução. Por conseguinte, é vantajoso adiar a execução da tarefa de verificação em vez de a executar imediatamente após o início do Kaspersky Endpoint Security.
Executar tarefas ignoradas	Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security inicia a tarefa ignorada logo que possível. A tarefa pode ser ignorada, por exemplo, se o computador estiver desligado no momento de início da tarefa agendada. Quando a aplicação tem a oportunidade de executar tarefas ignoradas, inicia as tarefas aleatoriamente num determinado intervalo de tempo para distribuir a carga no computador. Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security não executa tarefas ignoradas. Em alternativa, executa a tarefa seguinte, em conformidade com o agendamento atual.

Parâmetro	Descrição
Executar apenas quando o computador está inativo	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 ecrã estiver ativada. Se interrompeu a execução da tarefa (por exemplo, ao desbloquear o computador), o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que foi interrompido. Esta opção de agendamento permite-lhe conservar os recursos do computador quando o computador está a ser utilizado.
Executar verificação como	Por predefinição, a tarefa de verificação é executada no nome do utilizador com cujos direitos está registado no sistema operativo. O âmbito de proteção pode incluir unidades de rede ou outros objetos que exigem direitos especiais de acesso. Pode especificar um utilizador que possua os direitos adequados nas definições da tarefa de verificação da aplicação e executar a tarefa de verificação com a conta deste utilizador.
Tipos de ficheiros	O Kaspersky Endpoint Security considera os ficheiros sem extensão como sendo ficheiros executáveis. A aplicação verifica sempre ficheiros executáveis, independentemente dos tipos de ficheiros selecionados para verificação. **Todos os ficheiros**. Se esta definição estiver ativada, o Kaspersky Endpoint Security verifica todos os ficheiros sem exceção (todos os formatos e extensões). **Ficheiros verificados por formato**. Se esta configuração estiver ativada, a aplicação verifica apenas ficheiros infetáveis. Antes de verificar um ficheiro para código malicioso, o cabeçalho interno do ficheiro é analisado para determinar o formato do ficheiro (por exemplo, .txt, .doc ou .exe). A verificação também procura ficheiros com extensões de ficheiro específicas. **Ficheiros verificados por extensão**. Se esta configuração estiver ativada, a aplicação verifica apenas ficheiros infetáveis. O formato do ficheiro é então determinado com base na extensão do ficheiro. Por predefinição, o Kaspersky Endpoint Security verifica os ficheiros pelo seu formato. A verificação dos ficheiros por extensão é menos segura porque um ficheiro malicioso pode ter uma extensão que não está na lista de ficheiros potencialmente infetáveis (por exemplo, `.123`)
Verificar apenas os ficheiros novos e modificados	Verifica apenas os ficheiros novos e os que foram modificados desde a última vez em que foram verificados. Isto ajuda a reduzir a duração de uma verificação. Este modo aplica-se a ficheiros simples e compostos.
Ignorar ficheiros verificados durante mais de N segundo(s)	Limitar o tempo de execução da tarefa. Após o período especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está assinalada como concluída. Quando o Kaspersky Endpoint Security voltar a executar a tarefa, esta será executada desde o início e de acordo com o agendamento.
Não execute duas tarefas de verificação ao mesmo tempo	Adiar as tarefas de verificação agendadas se uma verificação agendada iniciada anteriormente ainda estiver em execução. O Kaspersky Endpoint Security colocará em fila as tarefas de verificação agendadas se a verificação atual continuar em execução. Isto ajuda a otimizar a carga no computador. Por exemplo, existem tarefas de verificação agendadas para serem executadas às 18:00 e às 20:00. O Kaspersky Endpoint Security adiará a tarefa de verificação das 20:00 se a tarefa de verificação agendada para as 18:00 ainda estiver em execução. A aplicação executará uma verificação após a conclusão da tarefa iniciada às 18:00. 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 amovíveis em ligação. • Verificar no menu de contexto. • Verificação de Áreas Críticas que foi iniciada mediante a deteção de um Indicador de Compromisso (IoC). Se esta caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security permite-lhe executar várias tarefas de verificação ao mesmo tempo. A execução de várias tarefas de verificação requer mais recursos do computador.
Verificar arquivos	A verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros arquivos. A aplicação verifica arquivos não só pela extensão, mas também pelo formato. Ao verificar os arquivos, a aplicação efetua uma descompactação recursiva. Isto permite a deteção de ameaças dentro de arquivos multinível (um arquivo dentro de um arquivo).
Verificar pacotes de distribuição	Verificar pacotes de distribuição de aplicações de terceiros.
Verificar ficheiros em formatos do Microsoft Office	Verifica ficheiros do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Ficheiros de formato do Office incluem objetos OLE também. A aplicação verifica ficheiros em formato de escritório menores que 1 MB, independentemente de a caixa de seleção estar marcada ou não.

Parâmetro	Descrição
Verificar ficheiros de formatos de e-mail	Verificação de ficheiros de formato de e-mail e base de dados de e-mail. A aplicação verifica ficheiros PST e OST utilizados por clientes de correio MS Outlook e Windows Mail, bem como ficheiros EML. O Kaspersky Endpoint Security não oferece suporte à versão de 64 bits do cliente de e-email Microsoft Outlook. Isto significa que o Kaspersky Endpoint Security não verifica ficheiros do Microsoft Outlook (ficheiros PST e OST), se uma versão de 64 bits do Microsoft Outlook estiver instalada no computador, mesmo se o correio estiver incluído no âmbito de verificação. Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security divide o ficheiro de formato de e-mail nos respetivos componentes (cabeçalho, corpo, anexos) e verifica a existência de ameaças nos mesmos. Se esta caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security verifica o ficheiro de formato de e-mail como um ficheiro único. Quando um objeto malicioso é descoberto em ficheiros PST ou OST, o Kaspersky Endpoint Security torna-o inofensivo de acordo com a ação selecionada (por exemplo, desinfeção ou eliminação do ficheiro). Se forem detetados objetos maliciosos em ficheiros de outros clientes de e-mail (por exemplo, o Mozilla Thunderbird), o Kaspersky Endpoint Security não desinfeta nem elimina esses ficheiros, para evitar a eliminação indesejada das suas mensagens de e-mail. O Kaspersky Endpoint Security apenas adiciona informações sobre objetos detetados na lista de ameaças ativas. Tem de tomar medidas para eliminar mensagens de e-mail com ficheiros maliciosos em anexo na interface de utilizador do seu cliente de e-mail. Se, por qualquer motivo, não for possível eliminar de imediato as mensagens com objetos maliciosos, pode processar essas ameaças na interface de utilizador do Kaspersky Endpoint Security ao adicionar os objetos detetados à lista de exclusões da verificação.
Verificar arquivos protegidos por password	Se a caixa de verificação estiver selecionada, a aplicação verifica os arquivos protegidos por password. Para que seja possível verificar os ficheiros num arquivo ser-lhe-á pedido que introduza a password. Se a caixa de verificação estive desmarcada, a aplicação ignora a verificação dos arquivos protegidos por password.
Não descompactar ficheiros compostos extensos	Se esta caixa de verificação estiver selecionada, a aplicação não verifica ficheiros compostos se o tamanho destes exceder o valor especificado. Se esta caixa de verificação for desmarcada, a aplicação verifica ficheiros compostos de todos os tamanhos. A aplicação verifica ficheiros grandes extraídos de arquivos, independentemente de a caixa de seleção estar selecionada ou não.
Aprendizagem automática e análise de assinaturas	O método de análise de assinaturas e aprendizagem automática utiliza a base de dados do Kaspersky Endpoint Security que contém descrições de ameaças conhecidas e formas de as neutralizar. A proteção que utiliza este método fornece o nível de segurança mínimo aceitável. Com base nas recomendações dos especialistas da Kaspersky, a aprendizagem automática e a análise de assinaturas estão sempre ativadas.
Análise heurística	A tecnologia foi desenvolvida para detetar ameaças que não é possível detetar utilizando a versão atual das bases de dados da aplicação da Kaspersky. Permite detetar ficheiros que podem estar infetados com um vírus desconhecido ou com uma variante de um vírus conhecido. Ao verificar ficheiros de códigos maliciosos, o analisador heurístico executa instruções nos ficheiros executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível da análise heurística garante um equilíbrio entre o detalhe das procuras de novas ameaças, a carga nos recursos do sistema operativo e a duração da análise heurística.
Tecnologia iSwift *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. A tecnologia iSwift é um avanço da tecnologia iChecker para o sistema de ficheiros NTFS.
Tecnologia iChecker *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. Existem limites para a tecnologia iChecker: não funciona com ficheiros grandes e aplica-se apenas a ficheiros com uma estrutura que o Kaspersky Internet Security reconheça (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

Verificar unidades amovíveis quando forem ligadas ao computador

O Kaspersky Endpoint Security verifica todos os ficheiros que executa ou copia, mesmo que o ficheiro esteja localizado numa unidade removível (o componente de Proteção contra ameaças de ficheiros). Para impedir a propagação de vírus e outro malware, pode configurar verificações automáticas de unidades removíveis quando estas são ligadas ao computador. O Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção falhar, o Kaspersky Endpoint Security apaga os ficheiros. O componente mantém um computador seguro executando verificações que implementam aprendizagem automática, análise heurística (nível elevado) e análise de assinatura. O Kaspersky Endpoint Security também utiliza tecnologias de otimização de verificação iSwift e iChecker. As tecnologias estão sempre ativas e não podem ser desativadas.

Como configurar as verificações das unidades amovíveis na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Tarefas locais** → **Verificação das unidades amovíveis**.
4. Na lista pendente **Ação ao ligar uma unidade amovível**, selecione **Verificação detalhada** ou **Verificação Rápida**.
5. Configure opções avançadas para a verificação de unidades amovíveis (consulte a tabela abaixo).
6. Guarde as suas alterações.

Como configurar as verificações das unidades amovíveis na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **Removable Drives Scan**.
5. Use o botão de alternar da **Removable Drives Scan ENABLED** para ativar ou desativar o componente.
6. No bloco **Scan type**, selecione **Detailed Scan** ou **Quick Scan**.
7. Configure opções avançadas para a verificação de unidades amovíveis (consulte a tabela abaixo).
8. Guarde as suas alterações.

Como configurar as verificações das unidades amovíveis na interface da aplicação

1. Na janela principal da aplicação, aceda à secção **Tarefas**.
2. Na lista de tarefas, selecione a tarefa de verificação e clique em ⚙.

3. Use o botão de alternar **Verificação das unidades amovíveis** para ativar ou desativar verificações de unidades amovíveis durante a ligação ao computador.

4. Configure opções avançadas para a verificação de unidades amovíveis (consulte a tabela abaixo).

5. Guarde as suas alterações.

Como resultado, o Kaspersky Endpoint Security executa uma verificação de unidades amovíveis em unidades amovíveis com um tamanho inferior ao tamanho máximo especificado. Se a tarefa *Verificação das unidades amovíveis* não for apresentada, tal significa que o administrador proibiu a utilização de tarefas locais na política.

Definições da tarefa de Verificação das unidades amovíveis

Parâmetro	Descrição
Scan type	**Detailed Scan**. Se esta opção estiver selecionada, o Kaspersky Endpoint Security verifica todos os ficheiros quando uma unidade amovível é conectada, incluindo ficheiros incorporados em objetos compostos, arquivos, pacotes de distribuição e ficheiros em formato Office. O Kaspersky Endpoint Security não verifica ficheiros em formatos de correio ou arquivos protegidos por password. **Quick Scan**. Se esta opção estiver selecionada, quando liga uma unidade amovível, o Kaspersky Endpoint Security verifica apenas os ficheiros de formatos específicos que são mais vulneráveis a infeções e não descompacta os objetos compostos.
Maximum drive size (MB)	Se esta caixa de verificação estiver selecionada, o Kaspersky Endpoint Security executa a ação selecionada nas unidades amovíveis com um tamanho inferior ao tamanho máximo da unidade especificado. Se o tamanho da unidade amovível exceder o valor configurado, o Kaspersky Endpoint Security irá ignorar a verificação. Se a caixa de verificação não estiver selecionada, o Kaspersky Endpoint Security irá executar a ação selecionada em unidades amovíveis de qualquer tamanho.
Hide scan progress bar	Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security apresenta o progresso das verificações de unidades amovíveis numa janela separada e na seção **Tarefas**. Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security executa uma verificação em 2.º plano das unidades amovíveis.
Prevent users from stopping the scan	Se esta caixa de verificação for selecionada, então para a tarefa de verificação das unidades removíveis na interface local do Kaspersky Endpoint Security, o botão **Parar** na secção **Tarefas** e o botão **Parar** na janela de verificação das unidades amovíveis não está disponível.

Verificação de fundo

Verificação em segundo plano é um modo de verificação do Kaspersky Endpoint Security que não exibe notificações para o utilizador. A Verificação de fundo requer menos recursos informáticos que outros tipos de verificação (tal como uma verificação total). Neste modo, o Kaspersky Endpoint Security verifica objetos de arranque, o sector de arranque, a memória do sistema e a partição do sistema.

Para conservar os recursos do computador, é recomendado para executar uma tarefa de verificação de fundo em vez de uma verificação completa. Isto não irá afetar o nível de segurança do computador. Estas tarefas têm o mesmo âmbito de verificação. Para otimizar a carga no computador, a aplicação não executa uma tarefa de Verificação Completa e uma tarefa de Verificação em Segundo Plano ao mesmo tempo. Se já tiver executado uma tarefa de Verificação Completa, o Kaspersky Endpoint Security não irá iniciar uma tarefa de Verificação em Segundo Plano durante sete dias após a conclusão da tarefa de Verificação Completa.

Uma verificação de fundo é iniciada nos casos seguintes:

- Após uma atualização da base de dados de antivírus.
- 30 minutos após o Kaspersky Endpoint Security ter iniciado.
- A cada seis horas.
- Quando o computador está inativo por cinco minutos ou mais (o computador está bloqueado ou a proteção de ecrã está ligada).

A verificação de fundo quando o computador está inativo é interrompida quando qualquer uma das seguintes condições for verdadeira:

- O computador entrou no modo ativo.

  Se a verificação de fundo não tiver sido executada durante mais de dez dias, a verificação não é interrompida.

- O computador (portátil) passou para o modo de bateria.

Quando executa a Verificação de fundo, o Kaspersky Endpoint Security não verifica os ficheiros com conteúdos localizados no armazenamento da nuvem do OneDrive.

Como ativar verificações em segundo plano na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Tarefas locais** → **Verificação em segundo plano**.
4. Use a caixa de verificação **Ativar Verificação em segundo plano** para ativar ou desativar as verificações em segundo plano.
5. Guarde as suas alterações.

Como ativar verificações em segundo plano na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **File Threat Protection**.
5. Sob **Background Scan**, use o botão de alternar da **Background Scan ENABLED** para ativar ou desativar a verificação de fundo.
6. Guarde as suas alterações.

Como ativar verificações em segundo plano na interface da aplicação

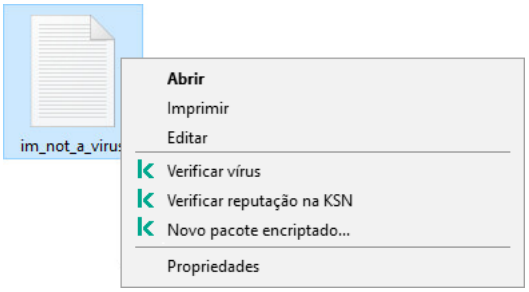
1. Na janela principal da aplicação, aceda à secção **Tarefas**.
2. Na lista de tarefas, selecione a tarefa de verificação e clique em ⚙.
3. Use o botão de alternar **Verificação em segundo plano** para ativar ou desativar as verificações em segundo plano.
4. Guarde as suas alterações.

Se a tarefa *Verificação em segundo plano* não for apresentada, tal significa que o administrador proibiu a utilização de tarefas locais na política.

Verificar a partir do menu de contexto

O Kaspersky Endpoint Security permite-lhe realizar uma verificação de ficheiros individuais em busca de vírus e outro software malicioso no menu contextual.

Quando executa uma verificação a partir do menu contextual, o Kaspersky Endpoint Security não verifica os ficheiros com conteúdos localizados no armazenamento da nuvem do OneDrive.



Verificar a partir do menu de contexto

Como configurar as verificações a partir do menu de contexto na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Tarefas locais** → **Verificação a partir do menu de contexto**.
4. Configurar as verificações a partir do menu de contexto (consulte a tabela abaixo).
5. Guarde as suas alterações.

Como configurar as verificações a partir do menu de contexto na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **File Threat Protection**.
5. Sob **Scan from Context Menu**, configure a Verificação a partir do menu de contexto (consulte a tabela abaixo).
6. Guarde as suas alterações.

Como configurar as verificações a partir do menu de contexto na interface da aplicação

1. Na janela principal da aplicação, aceda à secção **Tarefas**.
2. Na lista de tarefas, selecione a tarefa de verificação e clique em ⚙.
3. Configurar as verificações a partir do menu de contexto (consulte a tabela abaixo).
4. Guarde as suas alterações.

Se a tarefa *Verificação a partir do menu de contexto* não for apresentada, tal significa que o administrador proibiu a utilização de tarefas locais na política.

Definições da tarefa da Verificação do menu de contexto

Parâmetro	Descrição
Nível de segurança	O Kaspersky Endpoint Security pode utilizar diferentes grupos de definições para executar uma verificação. Estes grupos de definições armazenados na aplicação chamam-se *níveis de segurança*: • **Alto**. O Kaspersky Endpoint Security verifica todos os tipos de ficheiros. Ao verificar ficheiros, a aplicação verifica arquivos, pacotes de distribuição, ficheiros de formato do office, mas não verifica arquivos protegidos por password. Quando este nível de segurança é definido, a aplicação utiliza a análise heurística com o nível de detalhe **Nível avançado**. • **Recomendado**. O Kaspersky Endpoint Security verifica todos os tipos de ficheiros. Ao verificar ficheiros, a aplicação verifica arquivos, pacotes de distribuição, ficheiros de formato do office, mas não verifica arquivos protegidos por password. Quando este nível de segurança é definido, a aplicação utiliza a análise heurística com o nível de detalhe **Nível médio**. • **Baixo**. O Kaspersky Endpoint Security verifica apenas os formatos de ficheiro especificados. Ao verificar ficheiros, a aplicação verifica arquivos, pacotes de distribuição, ficheiros de formato do office, mas não verifica arquivos protegidos por password. Quando este nível de segurança é definido, a aplicação utiliza a análise heurística com o nível de detalhe **Nível superficial**.
Ação após deteção de ameaças	**Desinfetar, eliminar se a desinfeção falhar**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação elimina o ficheiro. **Desinfetar, informar se a desinfeção falhar**. Se esta opção estiver selecionada, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção falhar, o Kaspersky Endpoint Security adiciona a informação sobre os ficheiros infetados que são detetados à lista de ameaças ativas. **Informar**. Se esta opção for selecionada, o Kaspersky Endpoint Security adiciona a informação sobre ficheiros infetados à lista de ameaças ativas na deteção destes ficheiros.
Tipos de ficheiros	O Kaspersky Endpoint Security considera os ficheiros sem extensão como sendo ficheiros executáveis. A aplicação verifica sempre ficheiros executáveis, independentemente dos tipos de ficheiros selecionados para verificação. **Todos os ficheiros**. Se esta definição estiver ativada, o Kaspersky Endpoint Security verifica todos os ficheiros sem exceção (todos os formatos e extensões). **Ficheiros verificados por formato**. Se esta configuração estiver ativada, a aplicação verifica apenas ficheiros infetáveis. Antes de verificar um ficheiro para código malicioso, o cabeçalho interno do ficheiro é analisado para determinar o formato do ficheiro (por exemplo, .txt, .doc ou .exe). A verificação também procura ficheiros com extensões de ficheiro específicas. **Ficheiros verificados por extensão**. Se esta configuração estiver ativada, a aplicação verifica apenas ficheiros infetáveis. O formato do ficheiro é então determinado com base na extensão do ficheiro. Por predefinição, o Kaspersky Endpoint Security verifica os ficheiros pelo seu formato. A verificação dos ficheiros por extensão é menos segura porque um ficheiro malicioso pode ter uma extensão que não está na lista de ficheiros potencialmente infetáveis (por exemplo, `.123`)
Verificar apenas os ficheiros novos e modificados	Verifica apenas os ficheiros novos e os que foram modificados desde a última vez em que foram verificados. Isto ajuda a reduzir a duração de uma verificação. Este modo aplica-se a ficheiros simples e compostos.
Ignorar ficheiros verificados durante mais de N segundo(s)	Limitar o tempo de execução da tarefa. Após o período especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está assinalada como concluída. Quando o Kaspersky Endpoint Security voltar a executar a tarefa, esta será executada desde o início e de acordo com o agendamento.
Verificar arquivos	A verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros arquivos. A aplicação verifica arquivos não só pela extensão, mas também pelo formato. Ao verificar os arquivos, a aplicação efetua uma descompactação recursiva. Isto permite a deteção de ameaças dentro de arquivos multinível (um arquivo dentro de um arquivo).

Parâmetro	Descrição
Verificar pacotes de distribuição	A caixa de verificação ativa ou desativa a verificação de pacotes de distribuição.
Verificar ficheiros em formatos do Microsoft Office	Verifica ficheiros do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Ficheiros de formato do Office incluem objetos OLE também. A aplicação verifica ficheiros em formato de escritório menores que 1 MB, independentemente de a caixa de seleção estar marcada ou não.
Verificar ficheiros de formatos de e-mail	Verificação de ficheiros de formato de e-mail e base de dados de e-mail. A aplicação verifica ficheiros PST e OST utilizados por clientes de correio MS Outlook e Windows Mail, bem como ficheiros EML. O Kaspersky Endpoint Security não oferece suporte à versão de 64 bits do cliente de e-email Microsoft Outlook. Isto significa que o Kaspersky Endpoint Security não verifica ficheiros do Microsoft Outlook (ficheiros PST e OST), se uma versão de 64 bits do Microsoft Outlook estiver instalada no computador, mesmo se o correio estiver incluído no âmbito de verificação. Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security divide o ficheiro de formato de e-mail nos respetivos componentes (cabeçalho, corpo, anexos) e verifica a existência de ameaças nos mesmos. Se esta caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security verifica o ficheiro de formato de e-mail como um ficheiro único. Quando um objeto malicioso é descoberto em ficheiros PST ou OST, o Kaspersky Endpoint Security torna-o inofensivo de acordo com a ação selecionada (por exemplo, desinfeção ou eliminação do ficheiro). Se forem detetados objetos maliciosos em ficheiros de outros clientes de e-mail (por exemplo, o Mozilla Thunderbird), o Kaspersky Endpoint Security não desinfeta nem elimina esses ficheiros, para evitar a eliminação indesejada das suas mensagens de e-mail. O Kaspersky Endpoint Security apenas adiciona informações sobre objetos detetados na lista de ameaças ativas. Tem de tomar medidas para eliminar mensagens de e-mail com ficheiros maliciosos em anexo na interface de utilizador do seu cliente de e-mail. Se, por qualquer motivo, não for possível eliminar de imediato as mensagens com objetos maliciosos, pode processar essas ameaças na interface de utilizador do Kaspersky Endpoint Security ao adicionar os objetos detetados à lista de exclusões da verificação.
Verificar arquivos protegidos por password	Se a caixa de verificação estiver selecionada, a aplicação verifica os arquivos protegidos por password. Para que seja possível verificar os ficheiros num arquivo ser-lhe-á pedido que introduza a password. Se a caixa de verificação estive desmarcada, a aplicação ignora a verificação dos arquivos protegidos por password.
Não descompactar ficheiros compostos extensos	Se esta caixa de verificação estiver selecionada, a aplicação não verifica ficheiros compostos se o tamanho destes exceder o valor especificado. Se esta caixa de verificação for desmarcada, a aplicação verifica ficheiros compostos de todos os tamanhos. A aplicação verifica ficheiros grandes extraídos de arquivos, independentemente de a caixa de seleção estar selecionada ou não.
Aprendizagem automática e análise de assinaturas	O método de análise de assinaturas e aprendizagem automática utiliza a base de dados do Kaspersky Endpoint Security que contém descrições de ameaças conhecidas e formas de as neutralizar. A proteção que utiliza este método fornece o nível de segurança mínimo aceitável. Com base nas recomendações dos especialistas da Kaspersky, a aprendizagem automática e a análise de assinaturas estão sempre ativadas.
Análise heurística	A tecnologia foi desenvolvida para detetar ameaças que não é possível detetar utilizando a versão atual das bases de dados da aplicação da Kaspersky. Permite detetar ficheiros que podem estar infetados com um vírus desconhecido ou com uma variante de um vírus conhecido. Ao verificar ficheiros de códigos maliciosos, o analisador heurístico executa instruções nos ficheiros executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível da análise heurística garante um equilíbrio entre o detalhe das procuras de novas ameaças, a carga nos recursos do sistema operativo e a duração da análise heurística.
Tecnologia iSwift	Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. A tecnologia iSwift é um avanço da tecnologia iChecker para o sistema de ficheiros NTFS.
Tecnologia iChecker	Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. Existem limites para a tecnologia iChecker: não funciona com ficheiros grandes e aplica-se apenas a ficheiros com uma estrutura que o Kaspersky Internet Security reconheça (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

Verificação de integridade das aplicações

O Kaspersky Endpoint Security verifica se os módulos de aplicação foram corrompidos ou modificados. Por exemplo, se uma biblioteca da aplicação tiver uma assinatura digital incorreta, a biblioteca é considerada corrupta. A tarefa *Verificação de integridade da aplicação* destina-se a verificar ficheiros da aplicação. Execute a tarefa *Verificação de integridade da aplicação* se o Kaspersky Endpoint Security detetar um objeto malicioso, mas não o neutralizou.

Pode criar a tarefa *Verificação de integridade da aplicação* na Consola Web do Kaspersky Security Center e na Consola de Administração. Não é possível criar uma tarefa na Consola de Nuvem do Kaspersky Security Center.

Podem ocorrer violações da integridade da aplicação nos seguintes casos:

- Um objeto malicioso modificou os ficheiros do Kaspersky Endpoint Security. Neste caso, execute o procedimento para restaurar o Kaspersky Endpoint Security usando as ferramentas do sistema operativo. Após o restauro, execute uma verificação completa do computador e repita a verificação de integridade.
- A assinatura digital expirou. Neste caso, atualize o Kaspersky Endpoint Security.

Como executar uma verificação de integridade da aplicação através da Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Verificação de integridade da aplicação**.

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

Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 3. Configurar um agendamento de início de uma tarefa

Configure um agendamento para iniciar uma tarefa, por exemplo, manualmente ou quando um surto de vírus for detetado.

Passo 4. Definir o nome da tarefa

Introduza um nome para a tarefa, por exemplo, *Verificação de integridade depois do computador estar infetado*.

Passo 5. Completar a criação da tarefa

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa. Como resultado, o Kaspersky Endpoint Security verificará a integridade da aplicação. Pode também configurar um agendamento de verificação de integridade da aplicação nas propriedades da tarefa (consulte a tabela abaixo).

Como executar uma verificação de integridade da aplicação através da Consola Web

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **Application Integrity Check**.

c. No campo **Task name**, introduza uma breve descrição, por exemplo, *Verificar a integridade da aplicação após infeção do computador*.

d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Avance para o passo seguinte.

5. Selecione uma conta para executar a tarefa. Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de utilizador local.

6. Conclua o assistente.

   Será apresentada uma nova tarefa na lista de tarefas.

7. Selecione a caixa de verificação junto à tarefa.

Como resultado, o Kaspersky Endpoint Security verificará a integridade da aplicação. Pode também configurar um agendamento de verificação de integridade da aplicação nas propriedades da tarefa (consulte a tabela abaixo).

Como executar uma verificação de integridade na interface da aplicação

1. Na janela principal da aplicação, aceda à secção **Tarefas**.

2. Tal abre a lista de tarefas; selecione a tarefa *Verificação de integridade da aplicação* e clique em **Executar**.

Como resultado, o Kaspersky Endpoint Security verificará a integridade da aplicação. Pode também configurar um agendamento de verificação de integridade da aplicação nas propriedades da tarefa (consulte a tabela abaixo). Se a tarefa *Verificação de integridade da aplicação* não for apresentada, tal significa que o administrador proibiu a utilização de tarefas locais na política.

Definições da tarefa de verificação de integridade

Parâmetro	Descrição
Agendamento da verificação	**Manualmente**. Modo de execução, no qual pode iniciar a verificação manualmente quando for conveniente para si. **Por agendamento**. Neste modo de execução da tarefa, a aplicação inicia a tarefa de verificação em conformidade com o agendamento criado pelo utilizador. Se este modo de execução da tarefa de verificação estiver selecionado, pode também iniciar manualmente a tarefa de verificação.
Executar tarefas ignoradas	Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security inicia a tarefa ignorada logo que possível. A tarefa pode ser ignorada, por exemplo, se o computador estiver desligado no momento de início da tarefa agendada. Quando a aplicação tem a oportunidade de executar tarefas ignoradas, inicia as tarefas aleatoriamente num determinado intervalo de tempo para distribuir a carga no computador. Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security não executa tarefas ignoradas. Em alternativa, executa a tarefa seguinte, em conformidade com o agendamento atual.
Executar apenas quando o computador está inativo	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 ecrã estiver ativada. Se interrompeu a execução da tarefa (por exemplo, ao desbloquear o computador), o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que foi interrompido. Esta opção de agendamento permite-lhe conservar os recursos do computador quando o computador está a ser utilizado.

Editar o âmbito de verificação

O *Âmbito de verificação* é uma lista de caminhos das pastas e de caminhos verificados pelo Kaspersky Endpoint Security ao executar a tarefa. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.

Para editar o âmbito de verificação, recomendamos a utilização da tarefa *Verificação Personalizada*. Os especialistas da Kaspersky recomendam que não altere o âmbito da tarefas *Verificação completa* e *Verificação de Áreas Críticas*.

O Kaspersky Endpoint Security tem os seguintes objetos predefinidos como parte do âmbito de verificação:

- **Memória do Sistema**.
- **A executar processos e objetos de arranque**.

  Memória ocupada por processos e ficheiros executáveis da aplicação que são executados no arranque do sistema.
- **Setores de inicialização do disco**.

  Setores de inicialização do disco rígido e disco removível.
- **Cópia de segurança do sistema**.

  Conteúdo da pasta de informação de volume de 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 âmbito da verificação da aplicação. A verificação dos e-mails recebidos e enviados é realizada pelo componente Proteção contra ameaças de correio. Se estiver a utilizar uma versão anterior do plug-in de gestão, a aplicação exclui o e-mail do âmbito da verificação, mesmo que a política o inclua.

  Recomendamos que crie uma tarefa de verificação separada para verificar unidades de rede ou pastas partilhadas. Nas definições da tarefa de *Verificação de software malicioso*, especifique um utilizador que tenha acesso de gravação a esta unidade; é necessário para mitigar as ameaças detetadas. Se o servidor onde a unidade de rede está localizada tiver as suas próprias ferramentas de segurança, não execute a tarefa de verificação dessa unidade. Dessa forma, pode evitar verificar o objeto duas vezes e melhorar o desempenho do servidor.

Para excluir pastas ou ficheiros do âmbito de verificação, adicione a pasta ou ficheiros à zona fiável.

Como editar o âmbito de verificação na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Tasks**.
3. Selecione a tarefa de verificação e clique duas vezes para abrir as propriedades da tarefa.

   Se necessário, crie a tarefa *Verificação de software malicioso*.
4. Na janela de propriedades da tarefa, selecione a secção **Definições**.
5. Na secção **Âmbito de verificação**, clique **Definições**.
6. Na janela que abre, selecione os objetos que deseja adicionar ao âmbito de verificação ou excluir do mesmo.
7. Se pretender adicionar um novo objeto ao âmbito de verificação:

   a. Clique em **Adicionar**.

   b. No campo **Objeto**, introduza o caminho para a pasta ou ficheiro.

   Usar máscaras:

   - O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.
   - Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.
   - O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.

   Pode usar máscaras em qualquer lugar no caminho de um ficheiro ou pasta. Por exemplo, se quiser que o âmbito de verificação inclua a pasta Downloads para todas as contas de utilizador no computador, introduza a máscara `C:\Users\*\Downloads\`.

   O objeto **Este PC** na lista de recursos do ficheiro do computador inclui os seguintes objetos: **Todos os discos rígidos**, **Todos os discos de rede** e **Todas as unidades amovíveis**.

   Pode excluir um objeto das verificações sem o eliminar da lista de objetos no âmbito de verificação. Para o fazer, desmarque a caixa de verificação ao lado do objeto.
8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como editar o âmbito de verificação na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Tasks**.

   A lista de tarefas é aberta.

2. Clique na tarefa de verificação.

   É apresentada a janela de propriedades da tarefa. Se necessário, crie a tarefa *Malware Scan*.

3. Selecione o separador **Application settings**.

4. Na secção **Scan scope**, selecione os objetos que deseja adicionar ao âmbito de verificação ou excluir do mesmo.

5. Se pretender adicionar um novo objeto ao âmbito de verificação:

   a. Clique em **Add**.

   b. Introduza o caminho para a pasta ou ficheiro.

      Usar máscaras:

      - O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.

      - Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

      - O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.

      Pode usar máscaras em qualquer lugar no caminho de um ficheiro ou pasta. Por exemplo, se quiser que o âmbito de verificação inclua a pasta Downloads para todas as contas de utilizador no computador, introduza a máscara `C:\Users\*\Downloads\`.

   Pode excluir um objeto das verificações sem o eliminar da lista de objetos no âmbito de verificação. Para tal, desative o botão ao lado do mesmo.

6. Guarde as suas alterações.

Como editar o âmbito de verificação na interface da aplicação

1. Na janela principal da aplicação, aceda à secção **Tarefas**.

2. Tal abre a lista de tarefas; selecione a tarefa *Verificação Personalizada* e clique em **Selecionar**.

   Também pode editar o âmbito de verificação de outras tarefas. Os especialistas da Kaspersky recomendam que não altere o âmbito da tarefas *Verificação completa* e *Verificação de Áreas Críticas*.

3. Na janela que abre, selecione os objetos que deseja adicionar ao âmbito de verificação.

4. Guarde as suas alterações.

Se a tarefa de verificação não for apresentada, tal significa que o administrador proibiu a utilização de tarefas locais na política.

Execução de uma verificação agendada

A verificação de malware através da tarefa *Verificação de software malicioso* pode ser demorada e pode aumentar o consumo de recursos do computador pelo Kaspersky Endpoint Security. Por conseguinte, recomenda-se que se escolha o momento ideal para executar a tarefa, de modo a minimizar o impacto no desempenho de outras aplicações.

Por exemplo, se os funcionários da sua organização trabalham em horários fixos, pode configurar uma verificação do computador para ser executada à noite ou aos fins de semana. Se, por algum motivo, não for possível executar a tarefa (por exemplo, o computador estava desligado naquela altura), pode configurar a tarefa ignorada para ser automaticamente executada assim que for possível. Esta função deve ser utilizada com precaução, uma vez que pode tornar as aplicações no computador do utilizador mais lentas quando o computador é ligado pela manhã.

Se não conseguir definir um horário de verificação ideal que se adapte às suas necessidades, pode configurar a verificação para ser executada quando uma das seguintes condições especiais for cumprida:

- Após uma atualização da base de dados.

  O Kaspersky Endpoint Security executa a verificação do computador com as bases de dados de assinaturas atualizadas.

- Após o início da aplicação.

  O Kaspersky Endpoint Security executa uma verificação do computador após um período de tempo especificado a partir do início da aplicação. No arranque do sistema operativo, há muitos processos em execução. Por conseguinte, é vantajoso adiar a execução da tarefa de verificação em vez de a executar imediatamente após o início do Kaspersky Endpoint Security.

- Funcionalidade Wake-on-LAN.

  O Kaspersky Endpoint Security executa a verificação do computador de acordo com o agendamento, mesmo se o computador estiver desligado. Para tal, a aplicação utiliza a funcionalidade Wake-on-LAN do sistema operativo. A funcionalidade Wake-on-LAN permite ligar o computador remotamente mediante o envio de um sinal especial pela rede local. Para utilizar esta funcionalidade, deve ativar a Wake-on-LAN nas definições do BIOS.

  Apenas pode configurar a execução da verificação através da funcionalidade Wake-on-LAN para a tarefa *Verificação de software malicioso* no Kaspersky Security Center. Não é possível ativar a Wake-on-LAN para executar verificações do computador na interface da aplicação.

- Quando o computador está inativo.

  O Kaspersky Endpoint Security executa uma verificação do computador de acordo com o agendamento quando a proteção de ecrã está ligada ou o ecrã está bloqueado. Se o utilizador desbloquear o computador, o Kaspersky Endpoint Security pausa a verificação. Neste caso, a Verificação Completa poderá demorar vários dias a concluir.

- 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 no momento de início da tarefa agendada. Quando a aplicação tem a oportunidade de executar tarefas ignoradas, inicia as tarefas aleatoriamente num determinado intervalo de tempo para distribuir a carga no computador.

Como configurar o agendamento de verificações na Consola Web e na Cloud Console.

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique na tarefa de verificação.

   É apresentada a janela de propriedades da tarefa.

3. Na janela de propriedades da tarefa, selecione o separador **Schedule**.

4. Configure o agendamento da tarefa de verificação.

5. Dependendo da frequência selecionada, configure as definições avançadas que especificam o agendamento de execução da tarefa (consulte a tabela abaixo).

6. Guarde as suas alterações.

Como configurar o agendamento de verificações na interface da aplicação

Apenas pode configurar o agendamento da verificação se não estiver a ser aplicada uma política no computador. Para computadores sob a influência de uma política, pode configurar o agendamento da tarefa *Verificação de software malicioso* no Kaspersky Security Center.

1. Na janela principal da aplicação, aceda à secção **Tarefas**.

2. Na lista de tarefas, selecione a tarefa de verificação e clique em ⚙.

   Pode configurar um agendamento para executar uma verificação completa, uma verificação de áreas críticas ou uma verificação de integridade. Só pode executar uma verificação personalizada manualmente.

3. Clique em **Agendamento da verificação**.

4. Na janela que abre, configure o agendamento de execução da tarefa de verificação.

5. Dependendo da frequência selecionada, configure as definições avançadas que especificam o agendamento de execução da tarefa (consulte a tabela abaixo).

6. Guarde as suas alterações.

Definições do agendamento de verificações

Parâmetro	Descrição
Agendamento da verificação	**Manualmente**. Modo de execução, no qual pode iniciar a verificação manualmente quando for conveniente para si. **Por agendamento**. Neste modo de execução da tarefa, a aplicação inicia a tarefa de verificação em conformidade com o agendamento criado pelo utilizador. Se este modo de execução da tarefa de verificação estiver selecionado, pode também iniciar manualmente a tarefa de verificação.
Adiar execução, após o início da aplicação, durante N minutos	Início adiado da tarefa de verificação até após o início da aplicação. No arranque do sistema operativo, há muitos processos em execução. Por conseguinte, é vantajoso adiar a execução da tarefa de verificação em vez de a executar imediatamente após o início do Kaspersky Endpoint Security.
Executar tarefas ignoradas	Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security inicia a tarefa ignorada logo que possível. A tarefa pode ser ignorada, por exemplo, se o computador estiver desligado no momento de início da tarefa agendada. Quando a aplicação tem a oportunidade de executar tarefas ignoradas, inicia as tarefas aleatoriamente num determinado intervalo de tempo para distribuir a carga no computador. Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security não executa tarefas ignoradas. Em alternativa, executa a tarefa seguinte, em conformidade com o agendamento atual.

Parâmetro	Descrição
Executar apenas quando o computador está inativo	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 ecrã estiver ativada. Se interrompeu a execução da tarefa (por exemplo, ao desbloquear o computador), o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que foi interrompido. Esta opção de agendamento permite-lhe conservar os recursos do computador quando o computador está a ser utilizado.
Use automatically randomized delay for task starts *(disponível apenas na Consola do Kaspersky Security Center)*	Se a caixa de verificação estiver selecionada, a tarefa não é executada estritamente de acordo com o agendamento, mas de forma aleatória dentro de um determinado intervalo, ou seja, as horas de início da tarefa são distribuídas. As horas de início aleatórias ajudam a evitar que um grande número de computadores acedam simultaneamente ao Servidor de administração quando a tarefa é executada de acordo com o agendamento. O intervalo de horas de início aleatórias é calculado automaticamente quando a tarefa é criada, consoante o número de computadores que têm a tarefa atribuída. Posteriormente, a tarefa é sempre executada na hora de início calculada. No entanto, sempre que as definições da tarefa são alteradas ou a tarefa é executada manualmente, a hora de início calculada muda. Se a caixa de verificação não estiver selecionada, a tarefa será executada exatamente na hora agendada.
Use randomized delay for task starts within an interval of (min)	Se esta caixa de verificação estiver selecionada, a tarefa é executada em computadores numa altura aleatória dentro de um determinado período. As horas de início aleatórias ajudam a evitar que um grande número de computadores acedam simultaneamente ao Servidor de administração quando a tarefa é executada de acordo com o agendamento. Se a caixa de verificação não estiver selecionada, a tarefa será executada exatamente na hora agendada.
Stop the task if it runs longer than (min) *(disponível apenas na Consola do Kaspersky Security Center)*	Limitar o tempo de execução da tarefa. Após o período especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está assinalada como concluída. Quando o Kaspersky Endpoint Security voltar a executar a tarefa, esta será executada desde o início e de acordo com o agendamento. Para reduzir o tempo de execução da tarefa, pode, por exemplo, configurar o âmbito de verificação ou otimizar a verificação.
Turn on devices by using the Wake-on-LAN function before starting the task (min) *(disponível apenas na Consola do Kaspersky Security Center)*	Se a caixa de verificação estiver selecionada, o sistema operativo do computador terá um determinado período de tempo para concluir o arranque antes de a tarefa ser executada. O período de tempo predefinido é 5 minutos. Selecione a caixa de verificação se desejar executar a tarefa em todos os computadores, incluindo computadores desligados.
Shut down the devices after completing the task *(disponível apenas na Consola do Kaspersky Security Center)*	Se esta caixa de seleção estiver selecionada, o computador será encerrado após a conclusão da tarefa. Por exemplo, pode ativar esta funcionalidade para analisar o computador às sextas-feiras após o horário de trabalho. Quando a tarefa termina, a aplicação desliga o computador para o fim de semana.
Pausar a tarefa	Pode especificar um período durante o qual a execução de uma tarefa agendada anteriormente será suspensa. Assim que o período especificado terminar, a tarefa será retomada. Isto pode ser necessário, por exemplo, para minimizar o impacto do Kaspersky Endpoint Security no desempenho do seu computador durante os períodos de maior utilização.
Desativar agendamento a partir de	Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security deixará de executar a tarefa agendada a partir da data especificada. A tarefa será definida para o modo **Manualmente**.

Executar uma verificação com outra conta de utilizador

Por predefinição, a tarefa de verificação é executada no nome do utilizador com cujos direitos está registado no sistema operativo. O âmbito de proteção pode incluir unidades de rede ou outros objetos que exigem direitos especiais de acesso. Pode especificar um utilizador que possua os direitos adequados nas definições da tarefa de verificação da aplicação e executar a tarefa de verificação com a conta deste utilizador.

Pode executar as seguintes verificações com outra conta de utilizador:

- Verificação de áreas críticas.
- Verificação completa.

- Verificação personalizada.
- Verificar no menu de contexto.

Não é possível configurar os direitos do utilizador para executar uma Verificação das unidades amovíveis, Verificação em segundo plano ou Verificação de integridade.

Como executar uma verificação com outra conta de utilizador na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Managed devices** da árvore na Consola de Administração, abra a pasta com o nome do grupo de administração ao qual os computadores cliente em questão pertencem.
3. Na área de trabalho, selecione o separador **Tasks**.
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 secção **Account**.
6. Introduza as credenciais da conta do utilizador cujos direitos deseja usar para executar uma tarefa de verificação.
7. Guarde as suas alterações.

Como executar uma verificação com outra conta de utilizador na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Tasks**.

   A lista de tarefas é aberta.
2. Clique na tarefa de verificação.

   É apresentada a janela de propriedades da tarefa.
3. Selecione o separador **Settings**.
4. No bloco **Account**, clique no botão **Settings**.
5. Introduza as credenciais da conta do utilizador cujos direitos deseja usar para executar uma tarefa de verificação.
6. Guarde as suas alterações.

Como executar uma verificação com outra conta de utilizador na interface da aplicação

1. Na janela principal da aplicação, aceda à secção **Tarefas**.
2. Na lista de tarefas, selecione a tarefa de verificação e clique em ⚙.
3. Nas propriedades da tarefa, selecione **Definições avançadas** → **Executar verificação como**.
4. Na janela que abre, introduza as credenciais da conta do utilizador cujos direitos deseja usar para executar uma tarefa de verificação.
5. Guarde as suas alterações.

Se a tarefa de verificação não for apresentada, tal significa que o administrador proibiu a utilização de tarefas locais na política.

Optimização da verificação

Limitar a utilização da CPU durante a verificação do computador

Pode limitar a utilização da CPU ao executar a tarefa *Verificação de software malicioso*. Isto pode aumentar o tempo que demora a verificar o computador.

Como limitar a utilização da CPU ao verificar o computador na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais** → **Definições da aplicação**.
4. Em **Desempenho**, selecione a caixa de verificação **Limitar a utilização da CPU para verificar tarefas** e introduza o valor médio do consumo de recursos da CPU em percentagem.
5. Guarde as suas alterações.

Como limitar a utilização da CPU ao verificar o computador na Web Console

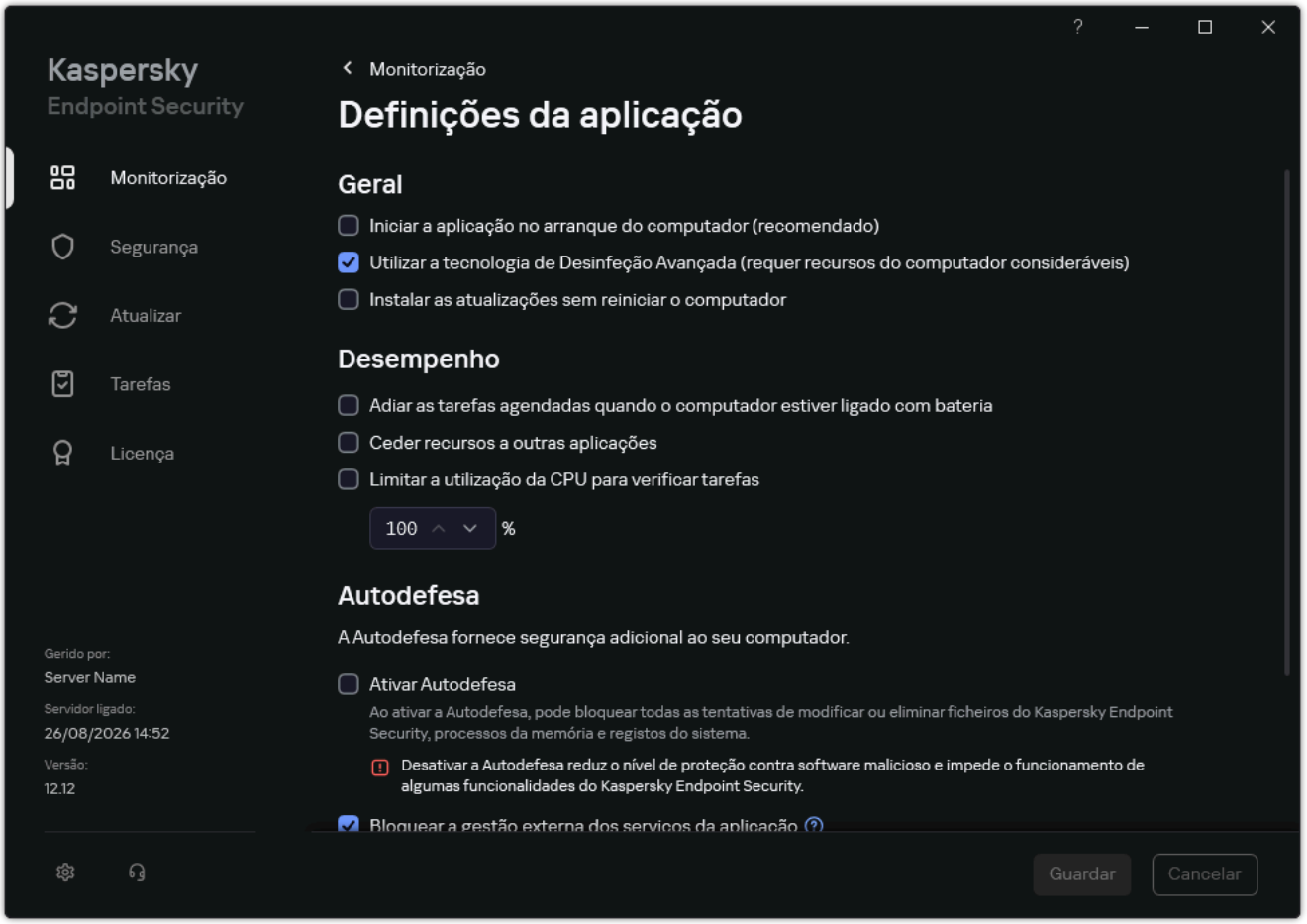
1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **Performance**.
5. Em **Limit CPU usage for scan tasks**, defina o botão **Limit CPU usage for scan tasks** e introduza o valor médio do consumo de recursos da CPU em percentagem.
6. Guarde as suas alterações.

Como limitar a utilização da CPU ao verificar o computador na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Definições gerais** → **Definições da aplicação**.



Definições do Kaspersky Endpoint Security for Windows

3. Em **Desempenho**, selecione a caixa de verificação **Limitar a utilização da CPU para verificar tarefas** e introduza o valor médio do consumo de recursos da CPU em percentagem.

4. Guarde as suas alterações.

Configurar definições de tarefa avançadas para Verificação de software malicioso.

Pode otimizar a verificação de ficheiros: reduzir a duração da verificação e aumentar a velocidade de funcionamento do Kaspersky Endpoint Security. Isto pode ser conseguido, verificando apenas os ficheiros novos e os ficheiros que foram modificados desde a verificação anterior. Este modo aplica-se a ficheiros simples e compostos. Também pode definir um limite para verificar um ficheiro individual. Depois de excedido o intervalo de tempo especificado, o Kaspersky Endpoint Security exclui o ficheiro da verificação atual (exceto no caso de arquivos e objetos que incluem vários ficheiros).

Uma técnica comum de ocultar vírus e outro software malicioso consiste em implantá-los em ficheiros compostos, como arquivos ou bases de dados. Para detetar vírus e outro software malicioso que estejam ocultos desta forma, é necessário descompactar o ficheiro composto, o que pode reduzir a velocidade da verificação. Pode limitar o tipo de ficheiros compostos a verificar, acelerando assim a verificação.

Também pode ativar as tecnologias iChecker e iSwift. As tecnologias iChecker e iSwift otimizam a velocidade da verificação de ficheiros, excluindo os ficheiros que não foram modificados desde a verificação mais recente.

Como otimizar a verificação na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Tasks**.
3. Selecione a tarefa de verificação e clique duas vezes para abrir as propriedades da tarefa.

   Se necessário, crie a tarefa *Verificação de software malicioso*.
4. Na janela de propriedades da tarefa, selecione a secção **Definições**.
5. No bloco **Nível de segurança**, clique no botão **Definições**.

   Tal abre a janela de definições da tarefa de verificação.
6. No bloco **Otimização**, configure as definições de verificação:

   - **Verificar apenas os ficheiros novos e modificados**. Verifica apenas os ficheiros novos e os que foram modificados desde a última vez em que foram verificados. Isto ajuda a reduzir a duração de uma verificação. Este modo aplica-se a ficheiros simples e compostos.

     Também pode configurar a verificação de novos ficheiros por tipo. Por exemplo, pode verificar todos os pacotes de distribuição e apenas verificar novos arquivos e ficheiros de formato do Office.

   - **Ignorar ficheiros verificados durante mais de N seg**. Limitar o tempo de execução da tarefa. Após o período especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está assinalada como concluída. Quando o Kaspersky Endpoint Security voltar a executar a tarefa, esta será executada desde o início e de acordo com o agendamento.

   - **Não execute duas tarefas de verificação ao mesmo tempo**. Adiar as tarefas de verificação agendadas se uma verificação agendada iniciada anteriormente ainda estiver em execução. O Kaspersky Endpoint Security colocará em fila as tarefas de verificação agendadas se a verificação atual continuar em execução. Isto ajuda a otimizar a carga no computador. Por exemplo, existem tarefas de verificação agendadas para serem executadas às 18:00 e às 20:00. O Kaspersky Endpoint Security adiará a tarefa de verificação das 20:00 se a tarefa de verificação agendada para as 18:00 ainda estiver em execução. A aplicação executará uma verificação após a conclusão da tarefa iniciada às 18:00.
7. Clique em **Adicional**.

   Tal abre a janela de definições de verificação de ficheiros compostos.
8. No bloco **Limite de tamanho**, selecione a caixa de verificação **Não descompactar ficheiros compostos extensos**. Limitar o tempo de execução da tarefa. Após o período especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está assinalada como concluída. Quando o Kaspersky Endpoint Security voltar a executar a tarefa, esta será executada desde o início e de acordo com o agendamento.

   O Kaspersky Endpoint Security verifica ficheiros extensos extraídos de arquivos, independentemente de a caixa de verificação **Não descompactar ficheiros compostos extensos** estar selecionada.
9. Clique em **Ok**.
10. Aceda ao separador **Adicional**.

11. No bloco **Tecnologias de verificação**, selecione as caixas de verificação junto aos nomes das tecnologias que pretende utilizar durante a verificação:

    - **Tecnologia iSwift**. Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. A tecnologia iSwift é um avanço da tecnologia iChecker para o sistema de ficheiros NTFS.

    - **Tecnologia iChecker**. Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. Existem limites para a tecnologia iChecker: não funciona com ficheiros grandes e aplica-se apenas a ficheiros com uma estrutura que o Kaspersky Internet Security reconheça (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

12. Guarde as suas alterações.

Como otimizar a verificação na Web Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Tasks**.

   A lista de tarefas é aberta.

2. Clique na tarefa de verificação.

   É apresentada a janela de propriedades da tarefa. Se necessário, crie a tarefa *Malware Scan*.

3. Selecione o separador **Application settings**.

4. No bloco **Action on threat detection**, selecione a caixa de verificação **Scan only new and modified files**. Verifica apenas os ficheiros novos e os que foram modificados desde a última vez em que foram verificados. Isto ajuda a reduzir a duração de uma verificação. Este modo aplica-se a ficheiros simples e compostos.

   Também pode configurar a verificação de novos ficheiros por tipo. Por exemplo, pode verificar todos os pacotes de distribuição e apenas verificar novos arquivos e ficheiros de formato do Office.

5. No bloco **Scan optimization**, selecione a caixa de verificação **Do not unpack large compound files**. Limitar o tempo de execução da tarefa. Após o período especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está assinalada como concluída. Quando o Kaspersky Endpoint Security voltar a executar a tarefa, esta será executada desde o início e de acordo com o agendamento.

   > O Kaspersky Endpoint Security verifica ficheiros extensos extraídos de arquivos, independentemente de a caixa de verificação **Do not unpack large compound files** estar selecionada.

6. Selecione a caixa de verificação **Do not run multiple scan tasks at the same time**. Adiar as tarefas de verificação agendadas se uma verificação agendada iniciada anteriormente ainda estiver em execução. O Kaspersky Endpoint Security colocará em fila as tarefas de verificação agendadas se a verificação atual continuar em execução. Isto ajuda a otimizar a carga no computador. Por exemplo, existem tarefas de verificação agendadas para serem executadas às 18:00 e às 20:00. O Kaspersky Endpoint Security adiará a tarefa de verificação das 20:00 se a tarefa de verificação agendada para as 18:00 ainda estiver em execução. A aplicação executará uma verificação após a conclusão da tarefa iniciada às 18:00.

7. No bloco **Advanced settings**, selecione a caixa de verificação **Skip file that is scanned for longer than (sec)**. Limitar o tempo de execução da tarefa. Após o período especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está assinalada como concluída. Quando o Kaspersky Endpoint Security voltar a executar a tarefa, esta será executada desde o início e de acordo com o agendamento.

8. Guarde as suas alterações.

Como otimizar a verificação na interface da aplicação

1. Na janela principal da aplicação, aceda à secção **Tarefas**.

2. Na lista de tarefas, selecione a tarefa de verificação e clique em ⚙.

3. Clique em **Definições avançadas**.

4. No bloco **Otimização**, configure as definições de verificação:

   - **Verificar apenas os ficheiros novos e modificados**. Verifica apenas os ficheiros novos e os que foram modificados desde a última vez em que foram verificados. Isto ajuda a reduzir a duração de uma verificação. Este modo aplica-se a ficheiros simples e compostos.

     Também pode configurar a verificação de novos ficheiros por tipo. Por exemplo, pode verificar todos os pacotes de distribuição e apenas verificar novos arquivos e ficheiros de formato do Office.

   - **Ignorar ficheiros verificados durante mais de N segundo(s)**. Limitar o tempo de execução da tarefa. Após o período especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está assinalada como concluída. Quando o Kaspersky Endpoint Security voltar a executar a tarefa, esta será executada desde o início e de acordo com o agendamento.

   - **Não execute duas tarefas de verificação ao mesmo tempo**. Adiar as tarefas de verificação agendadas se uma verificação agendada iniciada anteriormente ainda estiver em execução. O Kaspersky Endpoint Security colocará em fila as tarefas de verificação agendadas se a verificação atual continuar em execução. Isto ajuda a otimizar a carga no computador. Por exemplo, existem tarefas de verificação agendadas para serem executadas às 18:00 e às 20:00. O Kaspersky Endpoint Security adiará a tarefa de verificação das 20:00 se a tarefa de verificação agendada para as 18:00 ainda estiver em execução. A aplicação executará uma verificação após a conclusão da tarefa iniciada às 18:00.

5. No bloco **Limite de tamanho**, selecione a caixa de verificação **Não descompactar ficheiros compostos extensos**. Limitar o tempo de execução da tarefa. Após o período especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está assinalada como concluída. Quando o Kaspersky Endpoint Security voltar a executar a tarefa, esta será executada desde o início e de acordo com o agendamento.

   O Kaspersky Endpoint Security verifica ficheiros extensos extraídos de arquivos, independentemente de a caixa de verificação **Não descompactar ficheiros compostos extensos** estar selecionada.

6. No bloco **Tecnologias de verificação**, selecione as caixas de verificação junto aos nomes das tecnologias que pretende utilizar durante a verificação:

   - **Tecnologia iSwift**. Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. A tecnologia iSwift é um avanço da tecnologia iChecker para o sistema de ficheiros NTFS.

   - **Tecnologia iChecker**. Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. Existem limites para a tecnologia iChecker: não funciona com ficheiros grandes e aplica-se apenas a ficheiros com uma estrutura que o Kaspersky Internet Security reconheça (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

7. Guarde as suas alterações.

Se a tarefa de verificação não for apresentada, tal significa que o administrador proibiu a utilização de tarefas locais na política.

Atualização de bases de dados e módulos de software de aplicação

A atualização das bases de dados e dos módulos da aplicação do Kaspersky Endpoint Security garante a proteção atualizada do computador. Todos os dias surgem novos vírus e outros tipos de software malicioso a nível mundial. As bases de dados do Kaspersky Endpoint Security contêm informações sobre ameaças e formas de neutralizar as mesmas. Para detetar rapidamente ameaças, recomendamos que atualize regularmente as bases de dados e os módulos da aplicação.

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.

As atualizações regulares requerem uma licença válida. Se não existir uma licença atual, só poderá executar uma atualização uma vez.

O computador tem de estar ligado à Internet para transferir com êxito o pacote de atualização dos servidores de atualização da Kaspersky. Por predefinição, as definições da ligação à Internet são automaticamente determinadas. Se estiver a utilizar um servidor de proxy, terá de configurar as definições do servidor de proxy.

As atualizações são transferidas através do protocolo HTTPS. Também podem ser transferidas através do protocolo HTTP quando for impossível transferir as atualizações através do protocolo HTTPS.

Durante uma atualização, os seguintes objetos são transferidos e instalados no computador:

- Bases de dados do Kaspersky Endpoint Security. A proteção do computador é fornecida utilizando bases de dados com assinaturas de vírus e outras ameaças e informações sobre formas de neutralizar as mesmas. Os componentes de proteção utilizam estas informações durante a pesquisa e neutralização de ficheiros infetados no computador. As bases de dados são constantemente atualizadas com registos de novas ameaças e métodos de combate às mesmas. Por isso, recomendamos que atualize regularmente as bases de dados.

  Além das bases de dados do Kaspersky Endpoint Security, também são atualizados os controladores de rede que permitem que os componentes da aplicação intercetem o tráfego de rede.

- Módulos da aplicação. Além das bases de dados do Kaspersky Endpoint Security, também pode atualizar os módulos da aplicação. A atualização dos módulos da aplicação corrige vulnerabilidades no Kaspersky Endpoint Security, adiciona novas funções ou melhora as funções existentes.

Durante uma atualização, as bases de dados e os módulos da aplicação existentes no computador são comparados com a versão atualizada disponível na origem de atualização. Se as atuais bases de dados e módulos da aplicação diferirem das respetivas versões atualizadas, só será instalada no computador a parte das atualizações em falta.

Se as bases de dados estiverem obsoletas, o pacote de atualização pode ser extenso, o que pode implicar um tráfego adicional de internet (até várias dezenas de MB).

As informações sobre o estado atual das bases de dados do Kaspersky Endpoint Security são apresentadas na janela principal da aplicação ou na descrição que vê ao passar o cursor sobre o ícone da aplicação na área de notificação.

A informação sobre os resultados de atualização que ocorrem durante o desempenho da tarefa de atualização está registada no relatório do Kaspersky Endpoint Security.

Se a aplicação estiver a funcionar no modo Light Agent, são necessárias considerações especiais para atualizar as bases de dados e os módulos da aplicação.

Cenários de atualização do módulo da aplicação e base de dados

A atualização das bases de dados e dos módulos da aplicação do Kaspersky Endpoint Security garante a proteção atualizada do computador. Todos os dias surgem novos vírus e outros tipos de software malicioso a nível mundial. As bases de dados do Kaspersky Endpoint Security contêm informações sobre ameaças e formas de neutralizar as mesmas. Para detetar rapidamente ameaças, recomendamos que atualize regularmente as bases de dados e os módulos da aplicação.

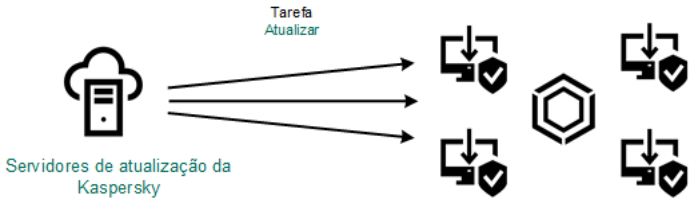
Os seguintes objetos são atualizados nos computadores dos utilizadores:

- Bases de dados de antivírus. As bases de dados de antivírus incluem bases de dados de assinaturas de software malicioso, descrição de ataques à rede, bases de dados de endereços da Web maliciosos e de phishing, bases de dados de faixas, bases de dados de deteção de spam e outros dados.
- Módulos da aplicação. As atualizações dos módulos destinam-se a eliminar vulnerabilidades na aplicação e a melhorar os métodos de proteção do computador. As atualizações dos módulos podem modificar o comportamento dos componentes da aplicação e adicionar novas capacidades.

O Kaspersky Endpoint Security suporta os seguintes cenários para atualizar as bases de dados e módulos da aplicação:

- Atualizar a partir dos servidores da Kaspersky.

  Os servidores de atualização da Kaspersky estão localizados em vários países do mundo. Isto assegura a máxima fiabilidade das atualizações. Se não for possível executar uma atualização num servidor, o Kaspersky Endpoint Security muda para o servidor seguinte.



Atualizar a partir dos servidores da Kaspersky

- Atualização centralizada.

  A atualização centralizada reduz o tráfego de Internet externo e fornece a monitorização conveniente da atualização.

  A atualização centralizada compõe-se dos seguintes passos:

  1. Transfira o pacote de atualização para um armazenamento de rede da organização.

     O pacote de atualização é transferido para o armazenamento pela tarefa do Servidor de Administração designada *Download updates to the Administration Server repository*.

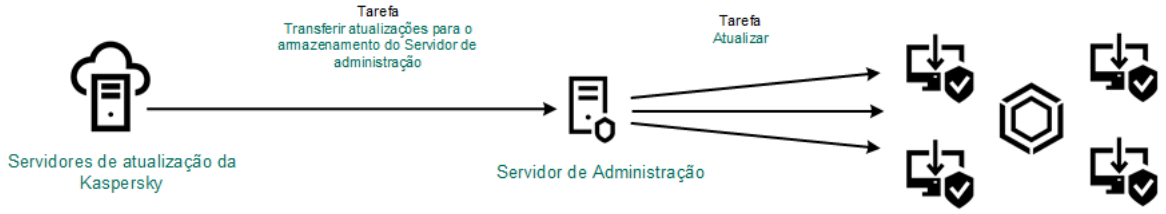
2. Transfira o pacote de atualização para uma pasta partilhada (opcional).

   Pode transferir o pacote de atualização para uma pasta partilhada utilizando os seguintes métodos:

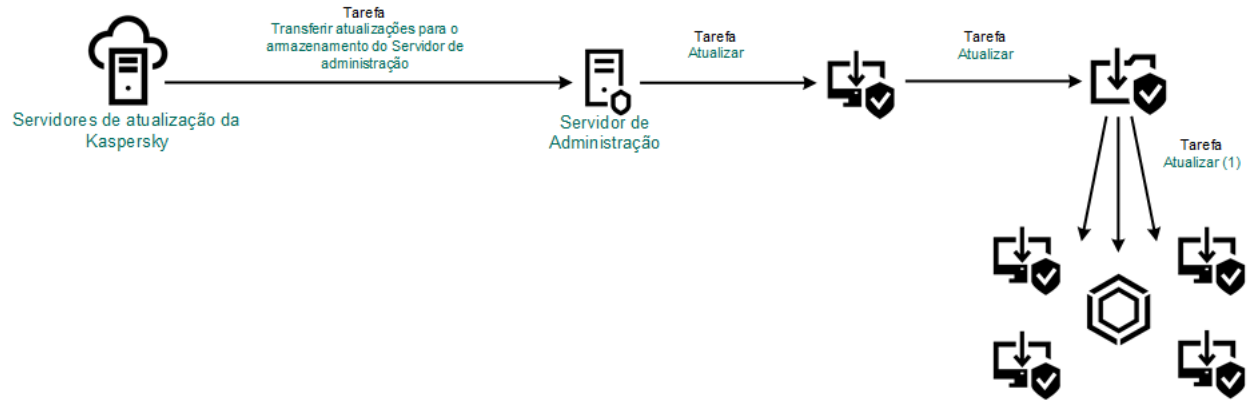
   - Utilizando a tarefa *Atualização das bases de dados e módulos da aplicação* do Kaspersky Endpoint Security. A tarefa destina-se a um dos computadores na rede local da empresa.
   - Utilizar o Utilitário Kaspersky Update. Para obter informações detalhadas sobre a utilização do Utilitário Kaspersky Update, consulte a Base de Conhecimento da Kaspersky.

3. Distribuir o pacote de atualização para computadores cliente.

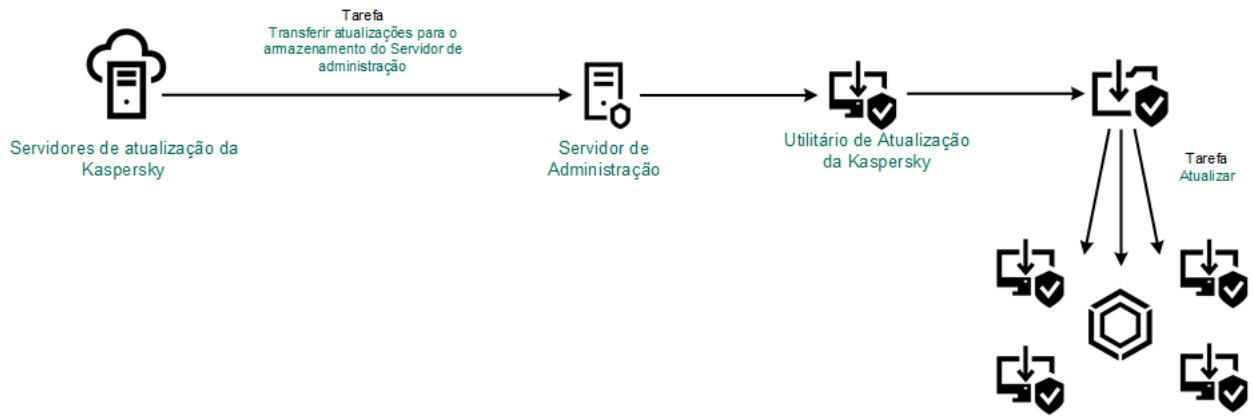
   O pacote de atualização é distribuído aos computadores cliente pela tarefa *Atualização das bases de dados e módulos da aplicação* do Kaspersky Endpoint Security. Pode criar um número ilimitado de tarefas de atualização para cada grupo de administração.



Atualizar a partir do armazenamento de um servidor



Atualizar a partir de uma pasta partilhada



Atualizar utilizando o Utilitário Kaspersky Update

Para o Kaspersky Security Center, a lista predefinida de origens de atualização contém os servidores de atualização do Servidor de Administração do Kaspersky Security Center e da Kaspersky. Para a Consola de Nuvem do Kaspersky Security Center, a lista predefinida de fontes de atualização contém pontos de distribuição e servidores de atualização da Kaspersky. Para obter mais informação detalhadas sobre os pontos de distribuição, consulte a Ajuda da Cloud Console do Kaspersky Security Center. Pode adicionar outras origens de atualização à lista. Pode especificar como origens de atualização servidores HTTP/FTP e pastas partilhadas. Se não for possível executar uma atualização da fonte, o Kaspersky Endpoint Security muda para o seguinte.

As atualizações são transferidas dos servidores de atualização da Kaspersky ou de outros servidores FTP ou HTTP através de protocolos de rede padrão. Se for necessária a ligação a um servidor proxy para aceder à origem da atualização, especifique as definições do servidor proxy nas definições da política do Kaspersky Endpoint Security.

Atualizar a partir do armazenamento de um servidor

Para poupar tráfego de Internet, pode configurar as atualizações das bases de dados e módulos da aplicação em computadores da LAN da organização a partir do armazenamento de um servidor. Para isso, o Kaspersky Security Center deve transferir um pacote de atualização para o armazenamento (servidor FTP ou HTTP, rede ou pasta local) dos Servidores de atualização da Kaspersky. Os outros computadores na LAN da organização podem assim receber o pacote de atualização do armazenamento do servidor.

Configurar as atualizações da base de dados e dos módulo da aplicação a partir do armazenamento de um servidor compõe-se dos seguintes passos:

1. Configure a transferência de um pacote de atualização para o repositório do Servidor de Administração (tarefa *Download updates to the Administration Server repository*).

   A tarefa *Download updates to the Administration Server repository* é criada automaticamente pelo assistente de início rápido do Servidor de Administração e esta 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 a transferência de atualizações para o repositório do Servidor de Administração, consulte a Ajuda do Kaspersky Security Center.

2. Configure as atualizações da base de dados e do módulo da aplicação do armazenamento do servidor especificado para os computadores restantes na LAN da organização (tarefa de *Atualização das bases de dados e módulos da aplicação*).

   Como configurar a atualização do Kaspersky Endpoint Security a partir do armazenamento do servidor especificado na Consola de Administração (MMC)

   1. Abra a Consola de Administração do Kaspersky Security Center.

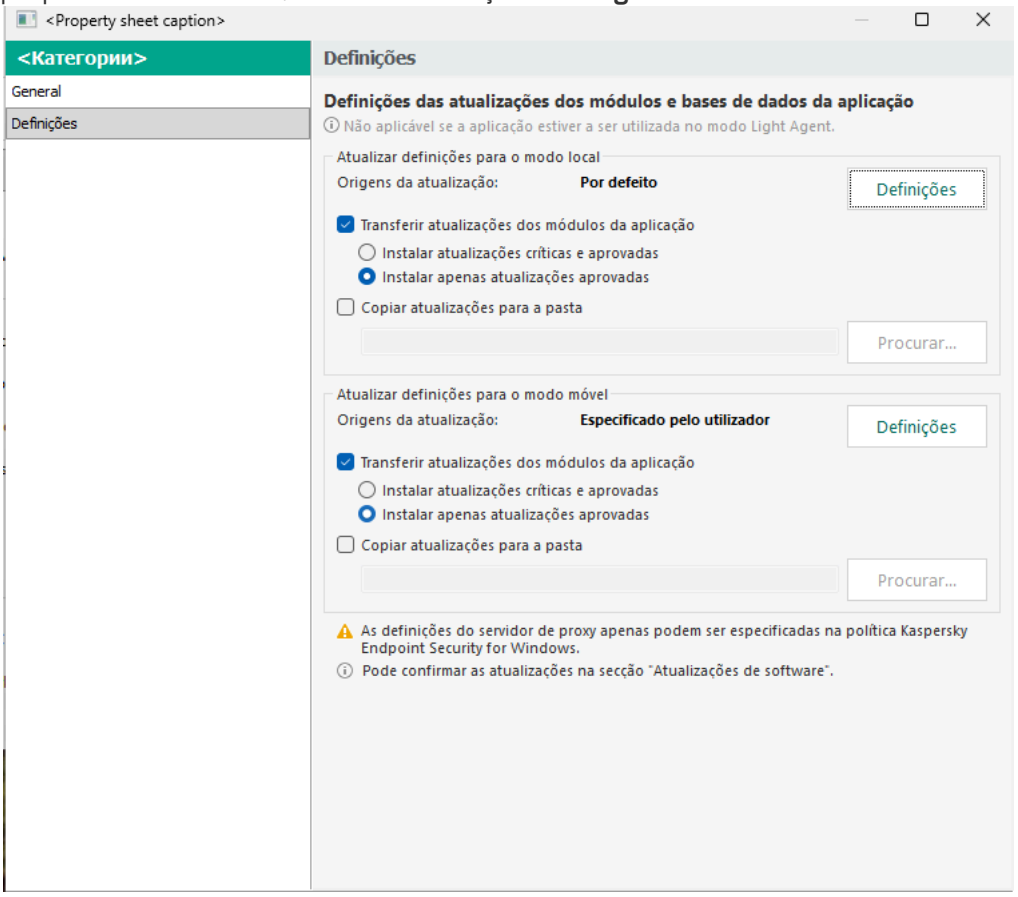
      Na árvore da consola, selecione **Tasks**.

   2. Clique na tarefa **Atualização das bases de dados e módulos da aplicação** do Kaspersky Endpoint Security.

      É apresentada a janela de propriedades da tarefa.

      A tarefa *Atualização das bases de dados e módulos da aplicação* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização das bases de dados e módulos da aplicação*, instale o Kaspersky Endpoint Security for Windows Management Plug-in enquanto executa o Assistente.

3. Na janela de propriedades da tarefa, selecione a secção **Settings**.



Definições de tarefa Atualização das bases de dados e módulos da aplicação

4. No bloco **Atualizar definições para o modo local**, clique no botão **Definições**.

5. Na lista de origens de atualização, certifique-se de que a atualização da origem **Kaspersky Security Center** está ativada. Além disso, a origem **Kaspersky Security Center** tem de ter a prioridade mais alta.

6. Se for necessário, adicione as origens de atualização:

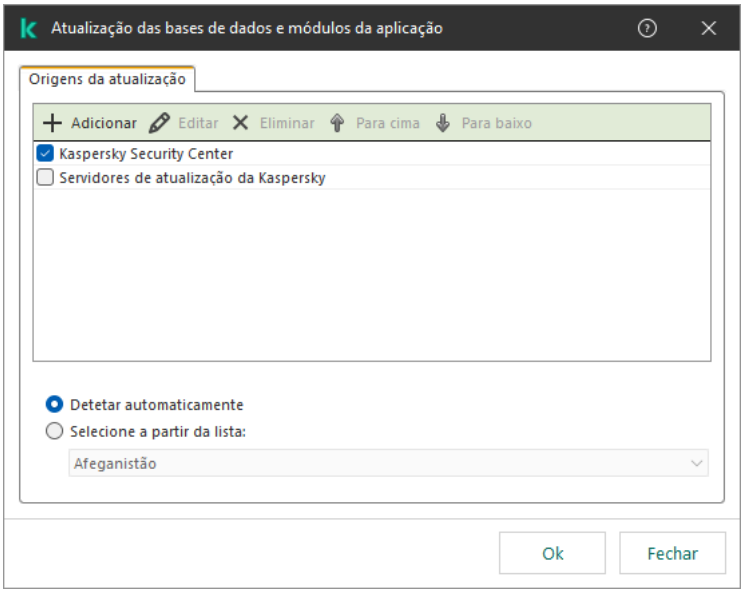
   a. Na lista de origens da atualização, clique no botão **Adicionar**.

   b. No campo **Origens da atualização**, especifique o endereço do servidor FTP ou HTTP, pasta de rede ou pasta local para onde o Kaspersky Security Center copiará o pacote de atualização recebido dos servidores da Kaspersky.

   > O endereço da origem da atualização deve corresponder ao endereço especificado no campo **Folder for storing updates** quando configurou a transferência das atualizações para o armazenamento do servidor (tarefa *Download updates to the Administration Server repository*).

   c. Clique em **OK**.

Pode excluir a origem da atualização sem removê-la da lista de origens de atualização. Para o fazer, desmarque a caixa de verificação ao lado do objeto.



Origens da atualização

7. Configure as prioridades das origens da atualização utilizando os botões **Para cima** e **Para baixo**.

   Se não for possível executar uma atualização através da primeira origem de atualização, o Kaspersky Endpoint Security muda automaticamente para o servidor seguinte.

8. Na janela de propriedades da tarefa, selecione a secção **Schedule** e configure o modo de execução da tarefa.

9. Por padrão, o Kaspersky Endpoint Security executa a tarefa no modo manual.

10. Guarde as suas alterações.

Como configurar a atualização do Kaspersky Endpoint Security do armazenamento do servidor especificado na Consola Web

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Update** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

   A tarefa *Update* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Update*, instale o Kaspersky Endpoint Security for Windows Management Plug-in enquanto executa o Assistente.

3. Selecione o separador **Application settings** → **Local mode**.

4. Na lista de origens de atualização, certifique-se de que a atualização da origem **Kaspersky Security Center** está ativada. Além disso, a origem **Kaspersky Security Center** tem de ter a prioridade mais alta.

5. Se for necessário, adicione as origens de atualização:

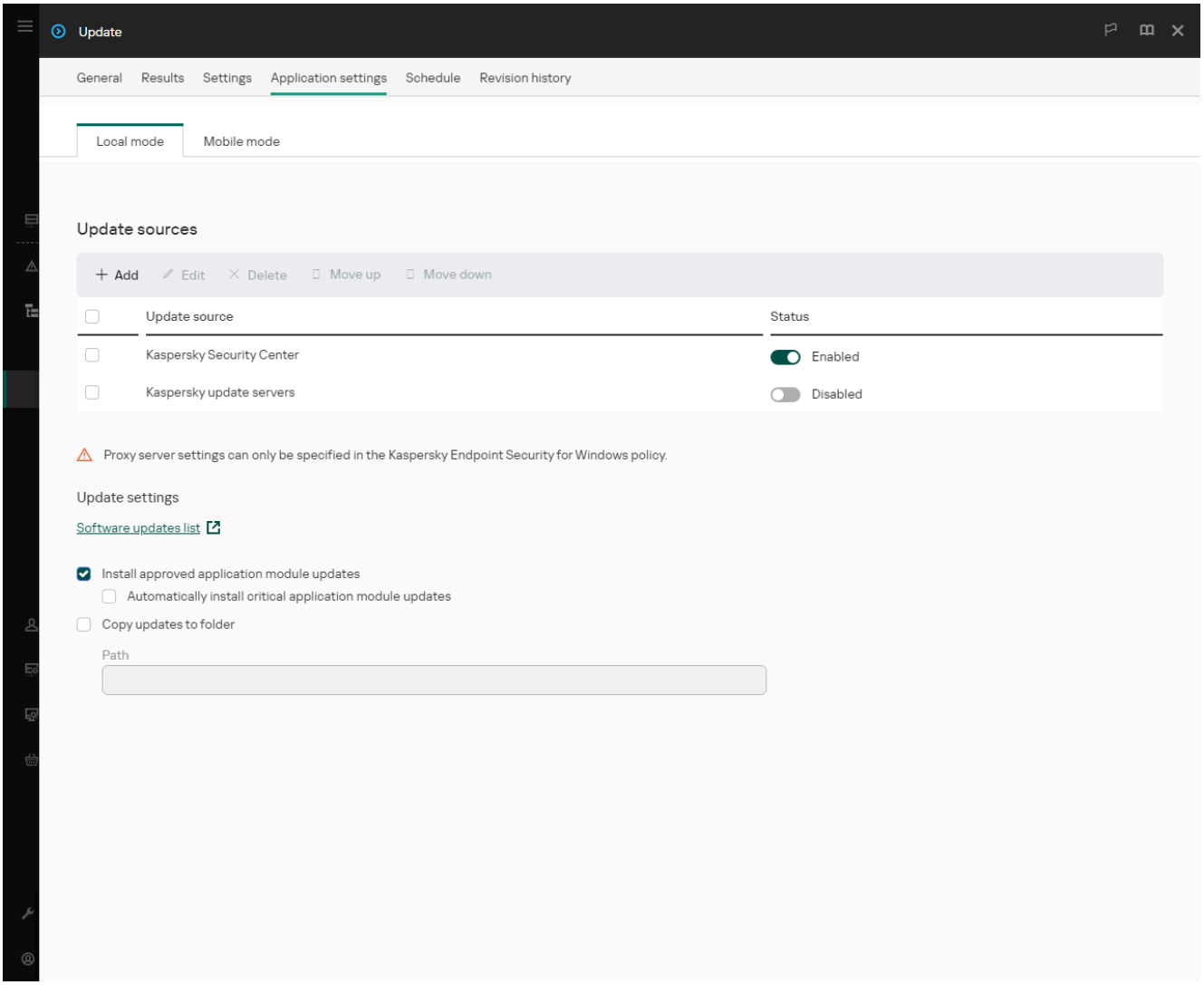
   a. Na lista de origens da atualização, clique no botão **Add**.

   b. No campo **Update sources**, especifique o endereço do servidor FTP ou HTTP, pasta de rede ou pasta local para onde o Kaspersky Security Center copiará o pacote de atualização recebido dos servidores da Kaspersky.

      O endereço da origem da atualização deve corresponder ao endereço especificado no campo **Folder for storing updates** quando configurou a transferência das atualizações para o armazenamento do servidor (tarefa *Download updates to the Administration Server repository*).

   c. Clique em **Save**.

   Pode excluir a origem da atualização sem removê-la da lista de origens de atualização. Para tal, desative o botão ao lado do mesmo.



Origens da atualização

6. Configure as prioridades das origens da atualização utilizando os botões **Move up** e **Move down**.

   Se não for possível executar uma atualização através da primeira origem de atualização, o Kaspersky Endpoint Security muda automaticamente para o servidor seguinte.

7. Na janela de propriedades da tarefa, selecione a secção **Schedule** e configure o modo de execução da tarefa.

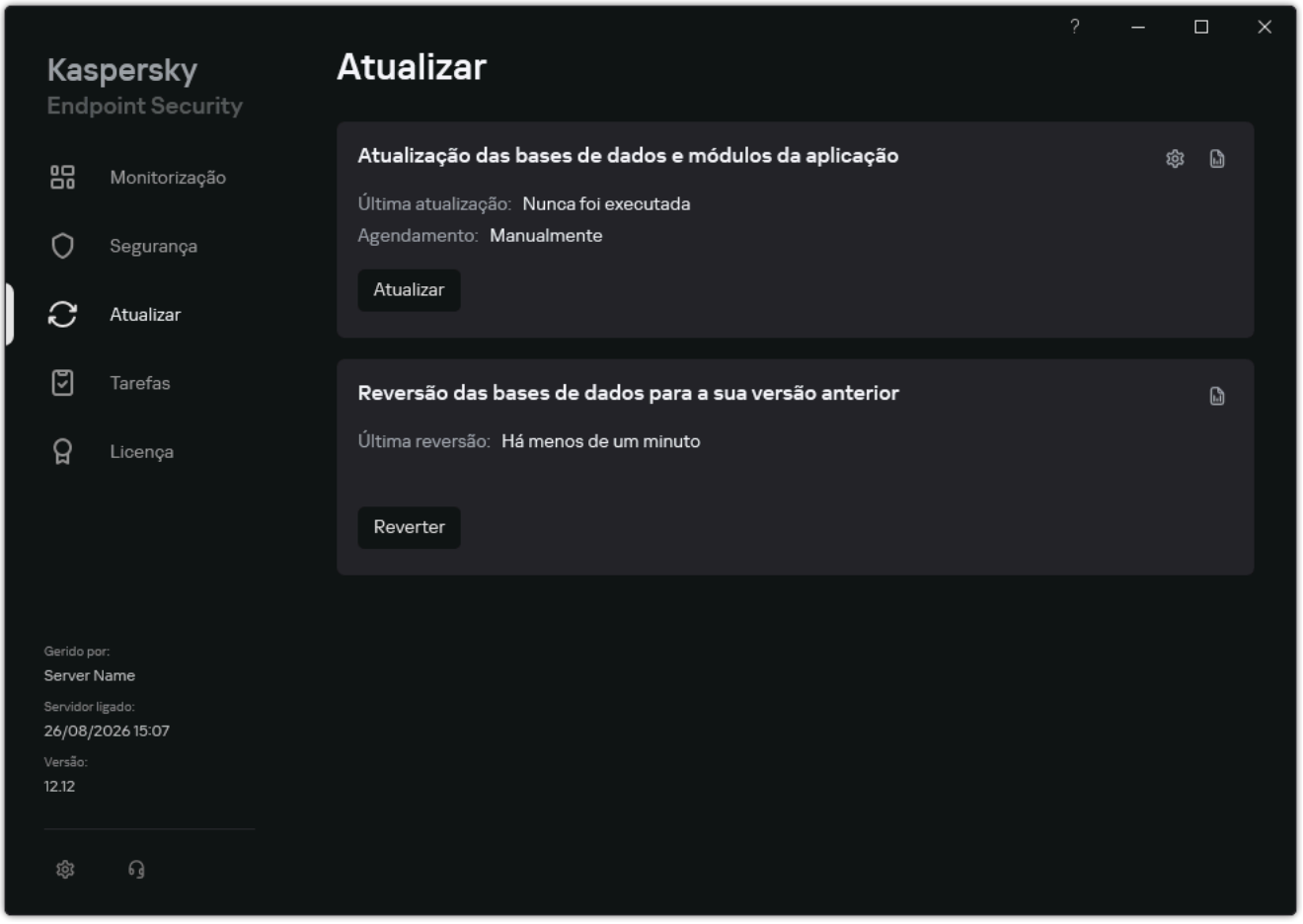
8. Por padrão, o Kaspersky Endpoint Security executa a tarefa no modo manual.

9. Guarde as suas alterações.

Como configurar a atualização do Kaspersky Endpoint Security do armazenamento do servidor especificado na interface da aplicação

Não pode configurar a tarefa de grupo *Atualização das bases de dados e módulos da aplicação* na interface da aplicação. Está disponível apenas uma tarefa de atualização local, *Atualização das bases de dados e módulos da aplicação*, para o utilizador. Se a tarefa *Atualização das bases de dados e módulos da aplicação* não for apresentada, tal significa que o administrador proibiu a utilização de tarefas locais na política.

1. Na janela principal da aplicação, aceda à secção **Atualizar**.



Tarefas de atualização local

2. Tal abre a lista de tarefas; selecione a tarefa *Atualização das bases de dados e módulos da aplicação* e clique em ⚙.

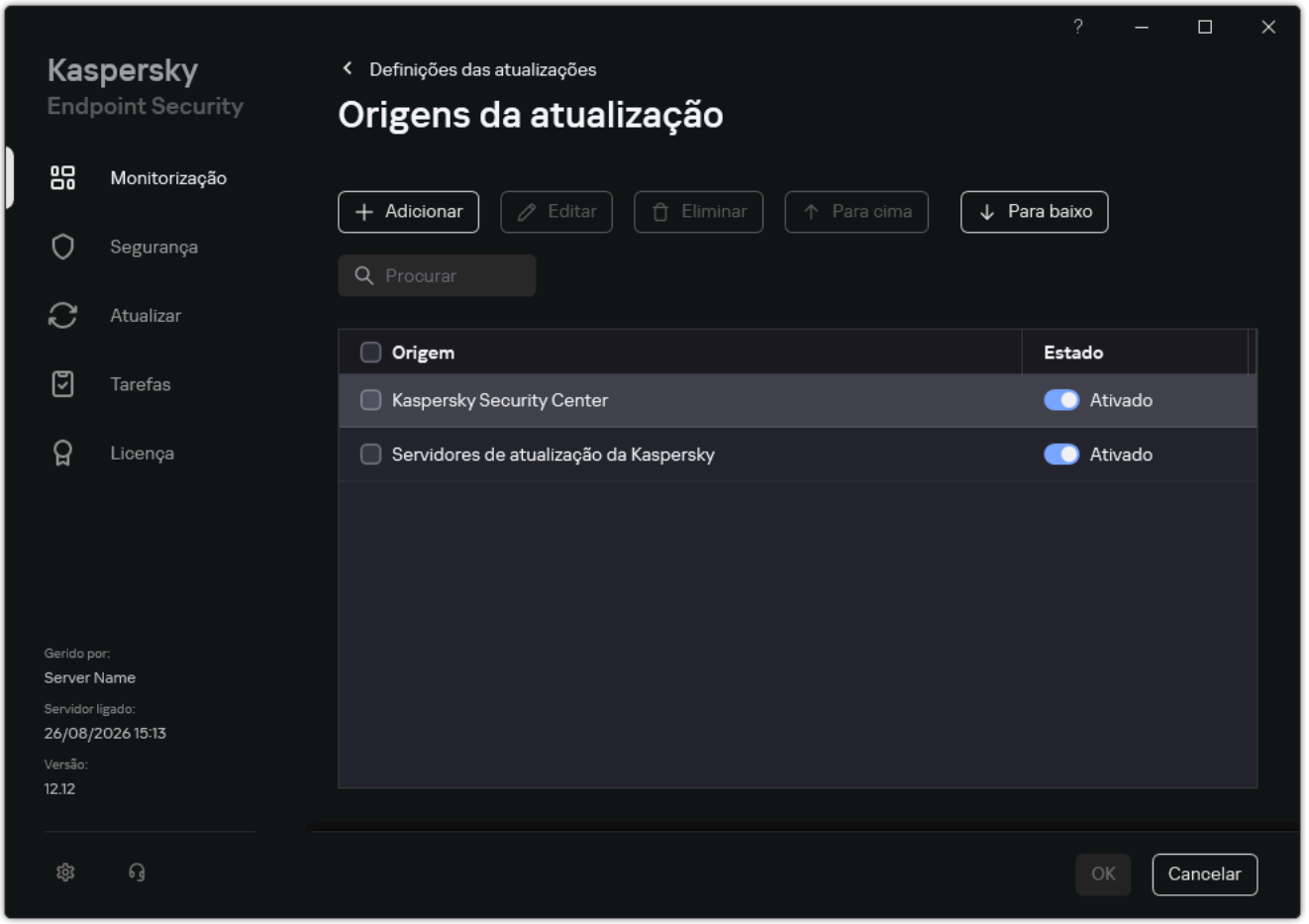
   É apresentada a janela de propriedades da tarefa.

3. Na janela de propriedades da tarefa, clique em **Selecionar origens de atualização**.

4. Na lista de origens de atualização, certifique-se de que a atualização da origem **Kaspersky Security Center** está ativada. Além disso, a origem **Kaspersky Security Center** tem de ter a prioridade mais alta.

5. Se for necessário, adicione as origens de atualização:

   a. Na lista de origens da atualização, clique no botão **Adicionar**.



Origens da atualização

   a. Especifique o endereço do servidor FTP ou HTTP, pasta de rede ou pasta local para onde o Kaspersky Security Center copiará o pacote de atualização recebido dos servidores de atualização da Kaspersky.

      O endereço da origem da atualização deve corresponder ao endereço especificado no campo **Folder for storing updates** quando configurou a transferência das atualizações para o armazenamento do servidor (tarefa *Download updates to the Administration Server repository*).

   b. Clique em **Selecionar**.

   Pode excluir a origem da atualização sem removê-la da lista de origens de atualização. Para tal, desative o botão ao lado do mesmo.

6. Configure as prioridades das origens da atualização utilizando os botões **Para cima** e **Para baixo**.

   Se não for possível executar uma atualização através da primeira origem de atualização, o Kaspersky Endpoint Security muda automaticamente para o servidor seguinte.

   Se um computador for gerido pelo Kaspersky Security Center, não é possível configurar o modo de execução para a tarefa *Atualização das bases de dados e módulos da aplicação*. Só pode executar a tarefa manualmente.

7. Guarde as suas alterações.



Atualizar a partir do armazenamento de um servidor

Atualizar a partir de uma pasta partilhada

Para poupar tráfego de Internet, pode configurar as atualizações das bases de dados e módulos da aplicação em computadores da LAN da organização a partir de uma pasta partilhada. Para isso, um dos computadores na rede local da organização deve receber um pacote de atualização do Servidor de Administração do Kaspersky Security Center ou dos servidores de atualização da Kaspersky e copiar o pacote de atualização recebido para uma pasta partilhada. Os outros computadores na LAN da organização podem assim receber o pacote de atualização desta pasta partilhada.

A versão e localização da aplicação Kaspersky Endpoint Security que copia o pacote de atualização para uma pasta partilhada deve corresponder à versão e localização da aplicação que atualiza as bases de dados da pasta partilhada. Se as versões ou localizações das aplicações não corresponderem, a atualização da base de dados pode terminar com um erro.

Configurar as atualizações da base de dados e dos módulo da aplicação a partir de uma pasta partilhada compõem-se dos seguintes passos:

1. Configurar as atualizações da base de dados e dos módulo da aplicação a partir do armazenamento de um servidor.

2. Ative a cópia de um pacote de atualização para uma pasta partilhada em um dos computadores na rede local.

   Como ativar a cópia do pacote de atualização para a pasta partilhada na Consola de Administração (MMC)

   1. Abra a Consola de Administração do Kaspersky Security Center.

   2. Na árvore da consola, selecione **Tasks**.

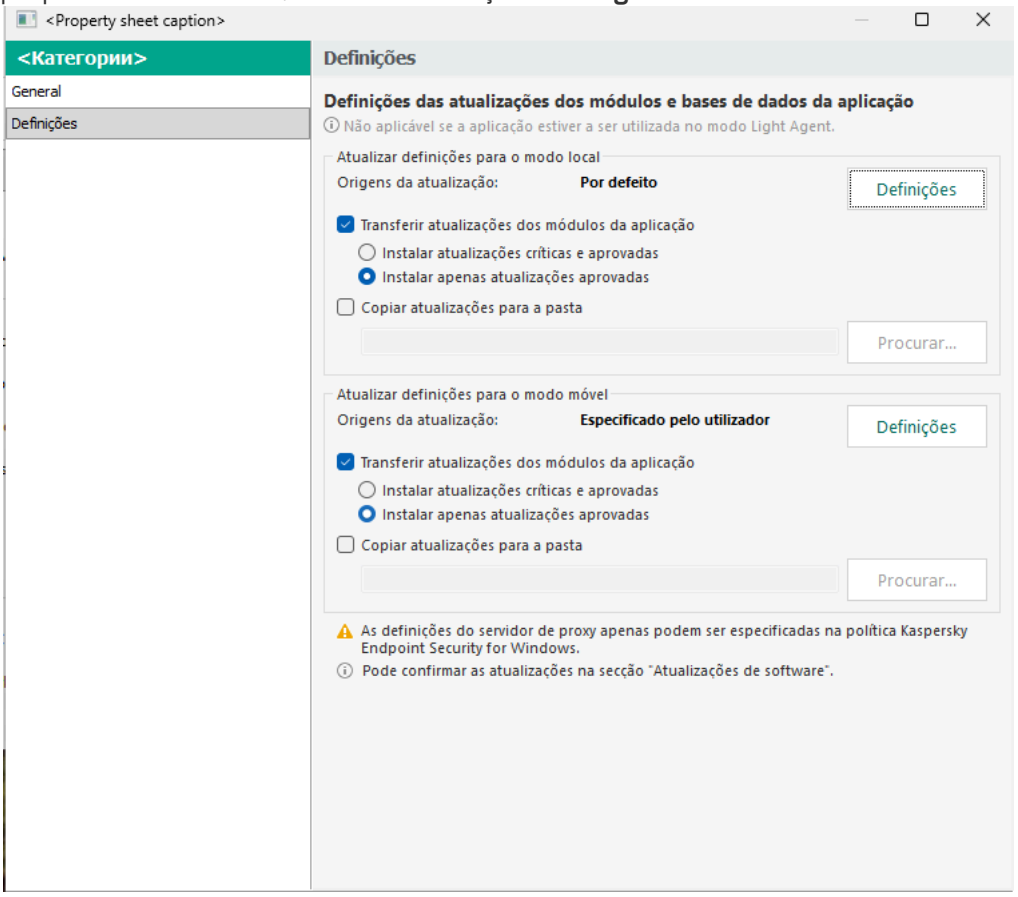
      A tarefa *Atualização das bases de dados e módulos da aplicação* deve ser atribuída a um computador que servirá de origem das atualizações.

   3. Clique na tarefa **Atualização das bases de dados e módulos da aplicação** do Kaspersky Endpoint Security.

      É apresentada a janela de propriedades da tarefa.

      A tarefa *Atualização das bases de dados e módulos da aplicação* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização das bases de dados e módulos da aplicação*, instale o Kaspersky Endpoint Security for Windows Management Plug-in enquanto executa o Assistente.

4. Na janela de propriedades da tarefa, selecione a secção **Settings**.



Definições de tarefa Atualização das bases de dados e módulos da aplicação

5. No bloco **Atualizar definições para o modo local**, clique no botão **Definições**.

6. Configure as origens das atualizações.

   As origens das 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. Selecione a caixa de verificação **Copiar atualizações para a pasta**.

8. No campo **Caminho da pasta**, introduza o caminho UNC para a pasta partilhada (por exemplo, `\\<server name>\KLSHARE\Updates`).

   Se este campo estiver vazio, o Kaspersky Endpoint Security copia o pacote de atualização para a pasta `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

9. Guarde as suas alterações.

Como ativar a cópia do pacote de atualização para a pasta partilhada na Consola Web e Cloud Console

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

   > A tarefa *Update* deve ser atribuída a um computador que servirá de origem das atualizações.

2. Clique na tarefa **Update** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

A tarefa *Update* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Update*, instale o Kaspersky Endpoint Security for Windows Management Plug-in enquanto executa o Assistente.

3. Selecione o separador **Application settings** → **Local mode**.

4. Configure as origens das atualizações.

   As origens das 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. Selecione a caixa de verificação **Copy updates to folder**.

6. No campo **Path**, introduza o caminho UNC para a pasta partilhada (por exemplo, `\\<server name>\KLSHARE\Updates`).

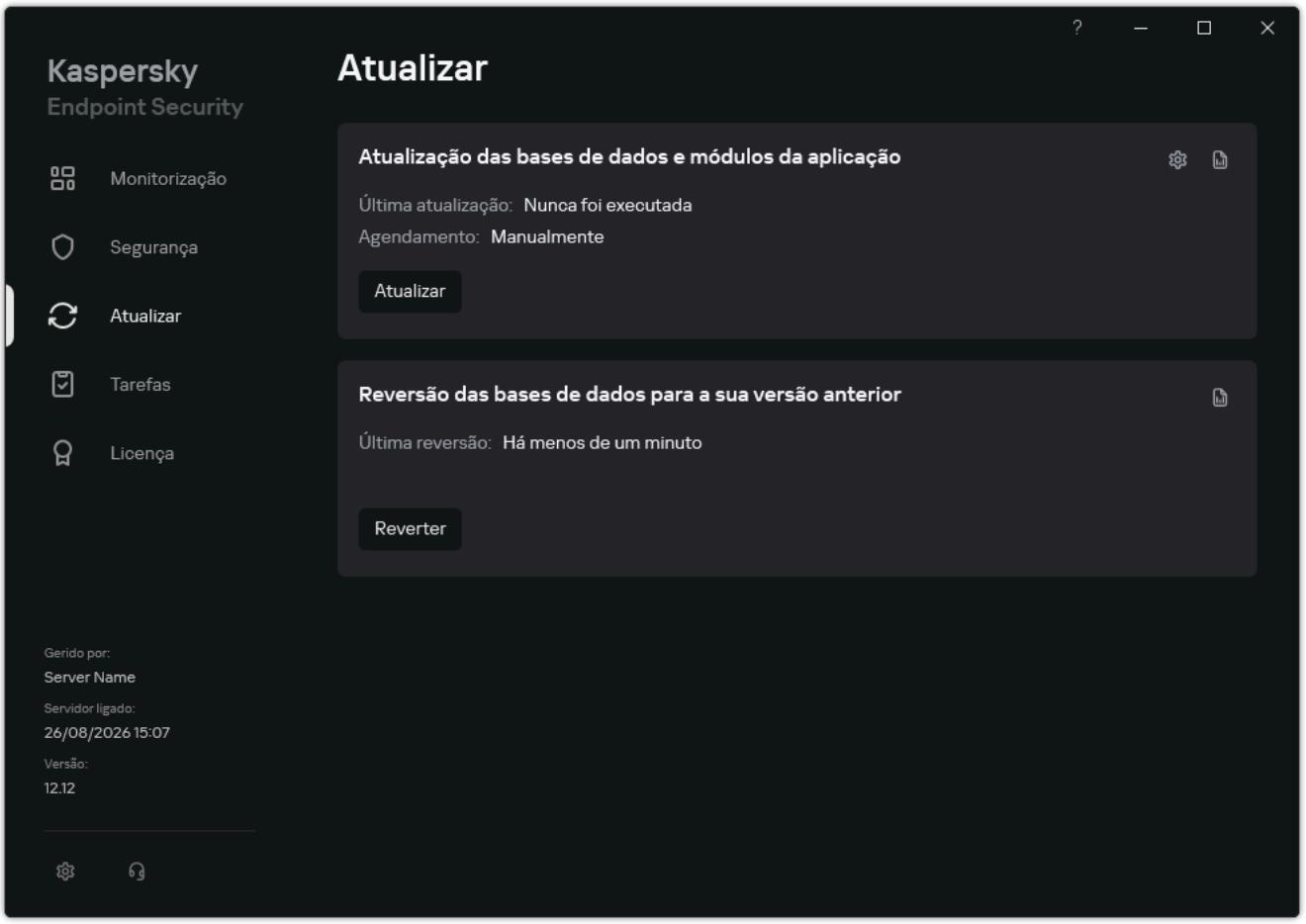
   Se este campo estiver vazio, o Kaspersky Endpoint Security copia o pacote de atualização para a pasta `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

7. Guarde as suas alterações.

Para ativar a cópia do pacote de atualização para a pasta partilhada na interface da aplicação

Não pode configurar a tarefa de grupo *Atualização das bases de dados e módulos da aplicação* na interface da aplicação. Está disponível apenas uma tarefa de atualização local, *Atualização das bases de dados e módulos da aplicação*, para o utilizador. Se a tarefa *Atualização das bases de dados e módulos da aplicação* não for apresentada, tal significa que o administrador proibiu a utilização de tarefas locais na política.

1. Na janela principal da aplicação, aceda à secção **Atualizar**.



Tarefas de atualização local

2. Tal abre a lista de tarefas; selecione a tarefa *Atualização das bases de dados e módulos da aplicação* e clique em ⚙.

   É apresentada a janela de propriedades da tarefa.

3. No bloco **Distribuir atualizações**, selecione a caixa de verificação **Copiar atualizações para a pasta**.

4. Introduza o caminho UNC para a pasta partilhada (por exemplo, `\\<server name>\KLSHARE\Updates`).

5. Guarde as suas alterações.

3. Configure as atualizações da base de dados e do módulo da aplicação da pasta partilhada especificada para os computadores restantes na LAN da organização.

Como configurar atualizações da pasta partilhada na Consola de Administração (MMC)

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **Atualização das bases de dados e módulos da aplicação**.

4. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Tasks**.

   A lista de tarefas é aberta.

5. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

Selecione **Kaspersky Endpoint Security for Windows (14.2) → Atualização das bases de dados e módulos da aplicação**.

Passo 2. Selecionar origens de atualização

Adicione uma nova origem de atualização: uma pasta partilhada. O endereço de origem deve corresponder ao endereço especificado anteriormente no campo **Caminho da pasta** quando configurou a cópia do pacote de atualização para a pasta partilhada (consultar as instruções acima). Configure as prioridades das origens da atualização utilizando os botões **Para cima** e **Para baixo**.

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

Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

A tarefa *Atualização das bases de dados e módulos da aplicação* deve ser atribuída a computadores da LAN da organização, exceto o computador que serve como origem da atualização.

Passo 4. Selecionar a conta para executar a tarefa

Selecione uma conta para executar a tarefa *Atualização das bases de dados e módulos da aplicação*. Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de utilizador local.

Passo 5. Configurar um agendamento de início de uma tarefa

Configure um agendamento para iniciar uma tarefa, por exemplo, manualmente ou depois da transferência das bases de dados de antivírus para o repositório.

Passo 6. Definir o nome da tarefa

Introduza o nome da tarefa, por exemplo *Atualizar a partir de uma pasta partilhada*.

Passo 7. Completar a criação da tarefa

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa. Na sequência disto, a tarefa de atualização será executada nos computadores do utilizador de acordo com o calendário especificado.

Como configurar atualizações a partir da pasta partilhada na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **Update**.

   c. No campo **Task name**, introduza uma breve descrição, por exemplo, *Atualização de uma pasta partilhada*.

   d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

   > A tarefa *Update* deve ser atribuída a computadores da LAN da organização, exceto o computador que serve como origem da atualização.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada e avance para o passo seguinte.

5. Conclua o assistente.

   Será apresentada uma nova tarefa na tabela de tarefas.

6. Clique na tarefa *Update* criada recentemente.

   É apresentada a janela de propriedades da tarefa.

7. Selecione o separador **Application settings** → **Local mode**.

8. No bloco **Update sources**, clique no botão **Add**.

9. Na janela apresentada, introduza o caminho para a pasta partilhada.

   > O endereço de origem deve corresponder ao endereço especificado anteriormente no campo **Path** quando configurou a cópia do pacote de atualização para a pasta partilhada (consultar as instruções acima).

10. Clique em **OK**.

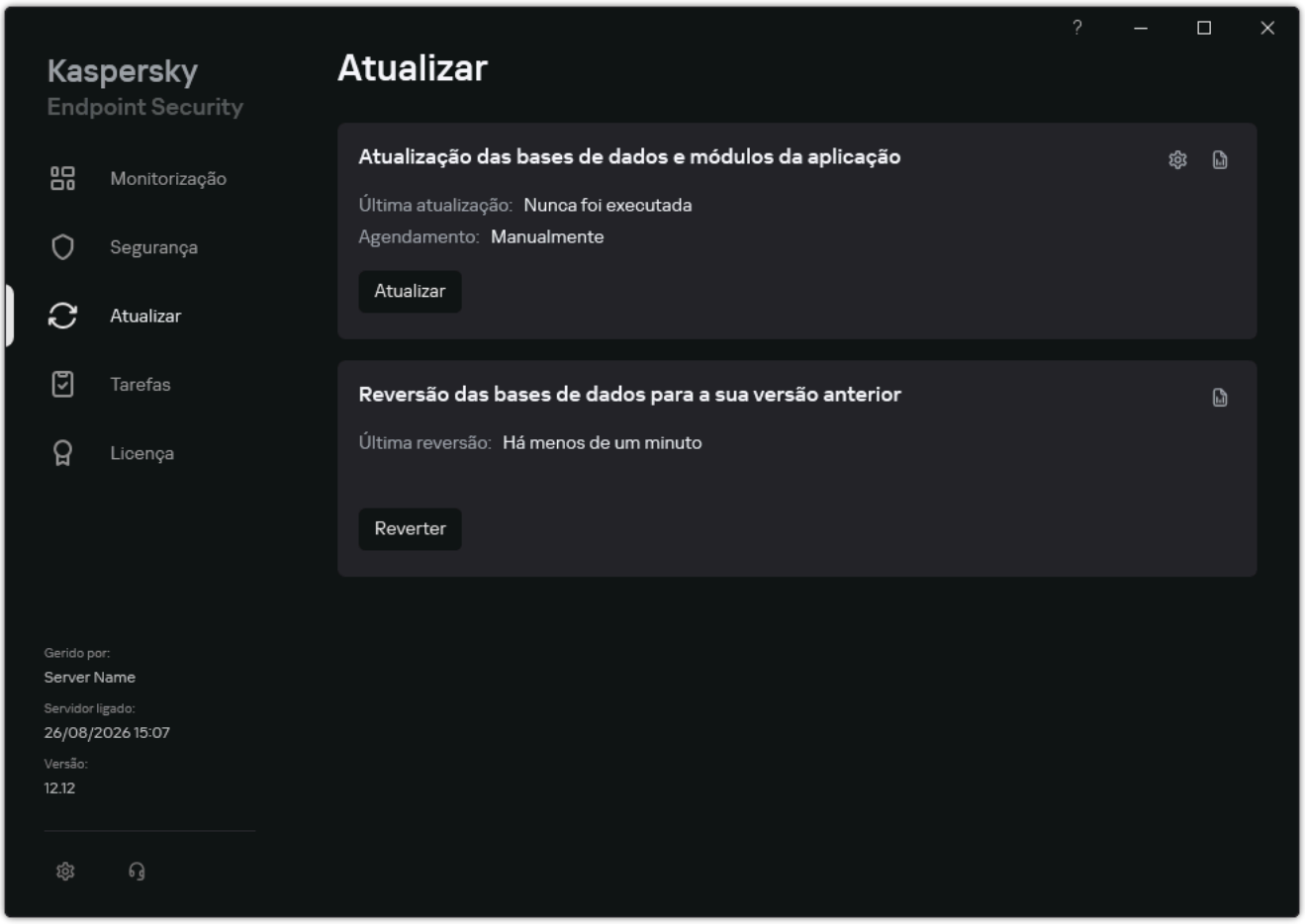
11. Configure as prioridades das origens da atualização utilizando os botões **Move up** e **Move down**.

12. Guarde as suas alterações.

Como configurar atualizações a partir da pasta partilhada na interface da aplicação

Não pode configurar a tarefa de grupo *Atualização das bases de dados e módulos da aplicação* na interface da aplicação. Está disponível apenas uma tarefa de atualização local, *Atualização das bases de dados e módulos da aplicação*, para o utilizador. Se a tarefa *Atualização das bases de dados e módulos da aplicação* não for apresentada, tal significa que o administrador proibiu a utilização de tarefas locais na política.

1. Na janela principal da aplicação, aceda à secção **Atualizar**.



Tarefas de atualização local

2. Tal abre a lista de tarefas; selecione a tarefa *Atualização das bases de dados e módulos da aplicação* e clique em ⚙.

   É apresentada a janela de propriedades da tarefa.

3. Clique em **Selecionar origens de atualização**.

4. Na janela que abre, clique no botão **Adicionar**.

5. Na janela apresentada, introduza o caminho para a pasta partilhada.

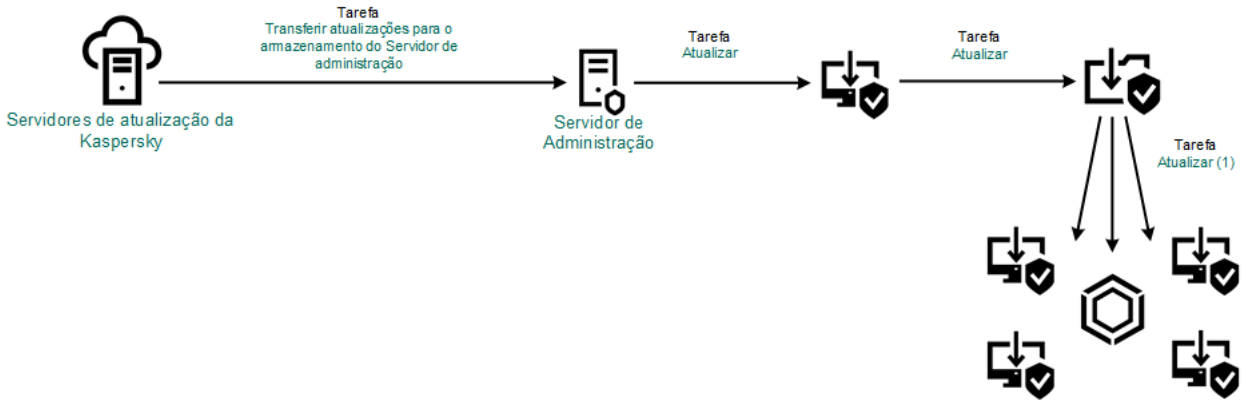
   O endereço de origem deve corresponder ao endereço especificado anteriormente quando configurou a cópia do pacote de atualização para a pasta partilhada (consultar as instruções acima).

6. Clique em **Selecionar**.

7. Configure as prioridades das origens da atualização utilizando os botões **Para cima** e **Para baixo**.

   Se não for possível executar uma atualização através da primeira origem de atualização, o Kaspersky Endpoint Security muda automaticamente para o servidor seguinte.

8. Guarde as suas alterações.



Atualizar a partir de uma pasta partilhada

Atualizar utilizando o Utilitário Kaspersky Update

Para poupar tráfego de Internet, pode configurar as atualizações das bases de dados e módulos da aplicação em computadores da LAN da organização a partir de uma pasta partilhada utilizando o Utilitário Kaspersky Update. Para isso, um dos computadores na rede local da organização deve receber um pacote de atualização do Servidor de Administração do Kaspersky Security Center ou dos servidores de atualização da Kaspersky e copiar depois os pacotes de atualização recebidos para uma pasta partilhada utilizando o utilitário. Os outros computadores na LAN da organização podem assim receber o pacote de atualização desta pasta partilhada.

A versão e localização da aplicação Kaspersky Endpoint Security que copia o pacote de atualização para uma pasta partilhada deve corresponder à versão e localização da aplicação que atualiza as bases de dados da pasta partilhada. Se as versões ou localizações das aplicações não corresponderem, a atualização da base de dados pode terminar com um erro.

Configurar as atualizações da base de dados e dos módulo da aplicação a partir de uma pasta partilhada compõem-se dos seguintes passos:

1. Configurar as atualizações da base de dados e dos módulo da aplicação a partir do armazenamento de um servidor.

2. Instale o Utilitário Kaspersky Update num dos computadores da LAN da organização.

3. Configure a cópia do pacote de atualização para a pasta partilhada nas definições do Utilitário Kaspersky Update.

   Pode transferir o pacote de distribuição do Utilitário Kaspersky Update através do site do Suporte Técnico da Kaspersky. Depois de instalar o utilitário, selecione a fonte de atualização (por exemplo, o armazenamento do Servidor de Administração) e a pasta partilhada para a qual o Utilitário Kaspersky Update irá copiar os pacotes de actualização. Para obter informações detalhadas sobre a utilização do Utilitário Kaspersky Update, consulte a Base de Conhecimento da Kaspersky.

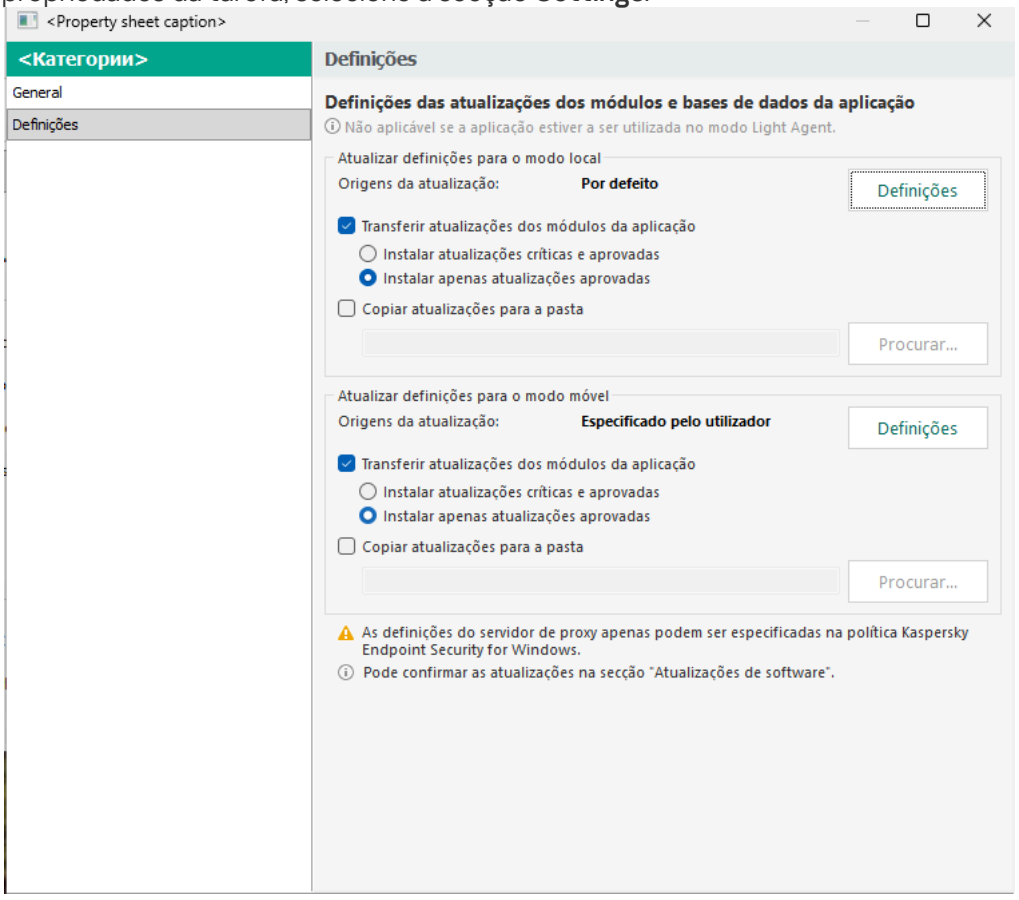
4. Configure as atualizações da base de dados e do módulo da aplicação da pasta partilhada especificada para os computadores restantes na LAN da organização.

Como configurar atualizações da pasta partilhada na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Tasks**.
3. Clique na tarefa **Atualização das bases de dados e módulos da aplicação** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

   A tarefa *Atualização das bases de dados e módulos da aplicação* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização das bases de dados e módulos da aplicação*, instale o Kaspersky Endpoint Security for Windows Management Plug-in enquanto executa o Assistente.
4. Na janela de propriedades da tarefa, selecione a secção **Settings**.



Definições de tarefa Atualização das bases de dados e módulos da aplicação

5. No bloco **Atualizar definições para o modo local**, clique no botão **Definições**.
6. Na lista de origens da atualização, clique no botão **Adicionar**.
7. Na janela que se abre, introduza o caminho UNC para a pasta partilhada (por exemplo, `\\<server name>\KLSHARE\Updates`).

   O endereço de origem deve corresponder ao endereço indicado nas definições do Utilitário Kaspersky Update.
8. Clique em **OK**.

9. Configure as prioridades das origens da atualização utilizando os botões **Para cima** e **Para baixo**.

   Se não for possível executar uma atualização através da primeira origem de atualização, o Kaspersky Endpoint Security muda automaticamente para o servidor seguinte.

10. Guarde as suas alterações.

Como configurar atualizações a partir da pasta partilhada na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Update** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

   A tarefa *Update* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Update*, instale o Kaspersky Endpoint Security for Windows Management Plug-in enquanto executa o Assistente.

3. Selecione o separador **Application settings** → **Local mode**.

4. Na lista de origens da atualização, clique no botão **Add**.

5. Na janela que se abre, introduza o caminho UNC para a pasta partilhada (por exemplo, `\\<server name>\KLSHARE\Updates`).

   O endereço de origem deve corresponder ao endereço indicado nas definições do Utilitário Kaspersky Update.

6. Clique em **OK**.

7. Configure as prioridades das origens da atualização utilizando os botões **Para cima** e **Para baixo**.

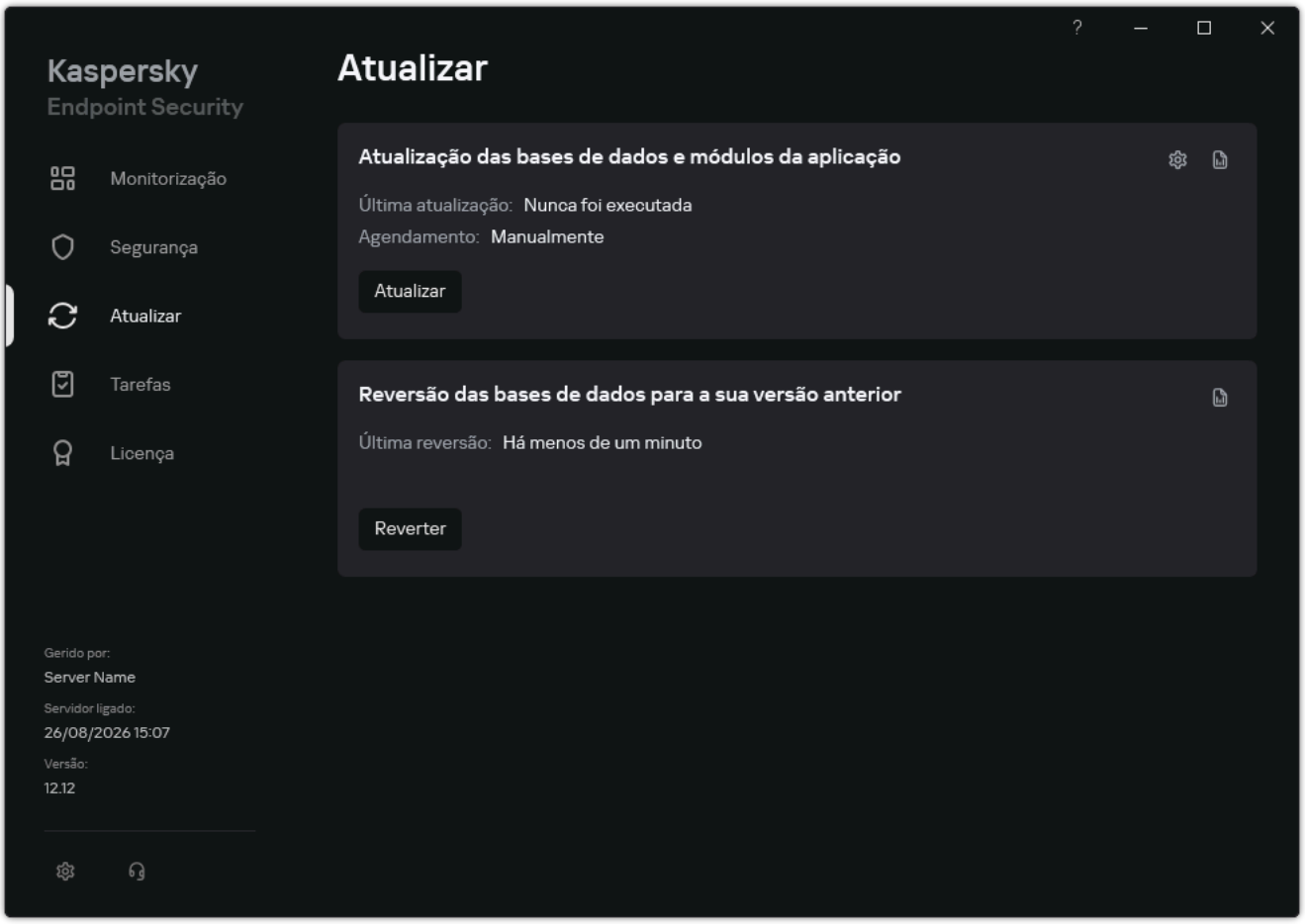
   Se não for possível executar uma atualização através da primeira origem de atualização, o Kaspersky Endpoint Security muda automaticamente para o servidor seguinte.

8. Guarde as suas alterações.

Como configurar atualizações a partir da pasta partilhada na interface da aplicação

Não pode configurar a tarefa de grupo *Atualização das bases de dados e módulos da aplicação* na interface da aplicação. Está disponível apenas uma tarefa de atualização local, *Atualização das bases de dados e módulos da aplicação*, para o utilizador. Se a tarefa *Atualização das bases de dados e módulos da aplicação* não for apresentada, tal significa que o administrador proibiu a utilização de tarefas locais na política.

1. Na janela principal da aplicação, aceda à secção **Atualizar**.



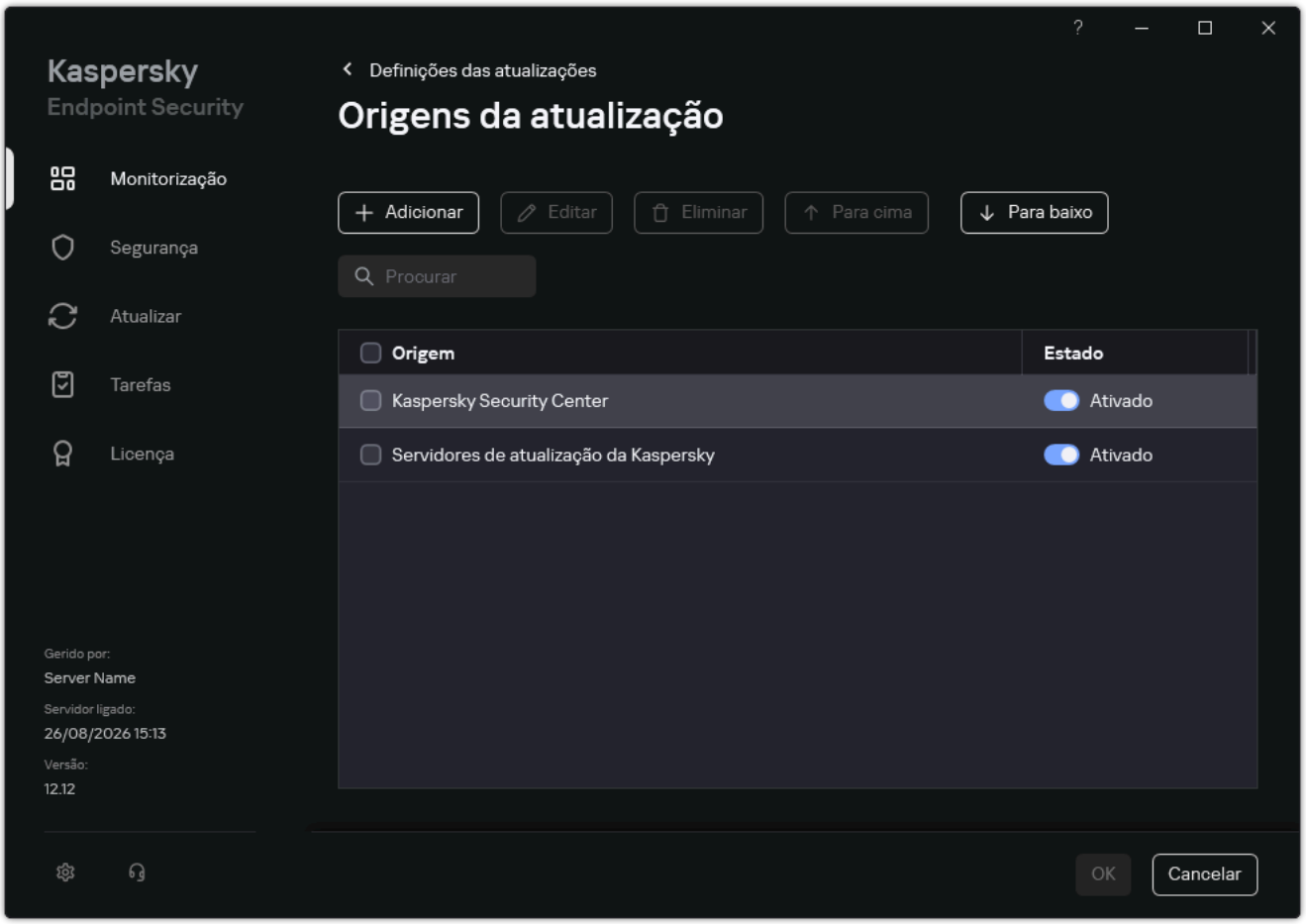
Tarefas de atualização local

2. Tal abre a lista de tarefas; selecione a tarefa *Atualização das bases de dados e módulos da aplicação* e clique em ⚙.

   É apresentada a janela de propriedades da tarefa.

3. Na janela de propriedades da tarefa, clique em **Selecionar origens de atualização**.

4. Na lista de origens da atualização, clique no botão **Adicionar**.



Origens da atualização

5. Introduza o caminho UNC para a pasta partilhada (por exemplo, `\\<server name>\KLSHARE\Updates`).

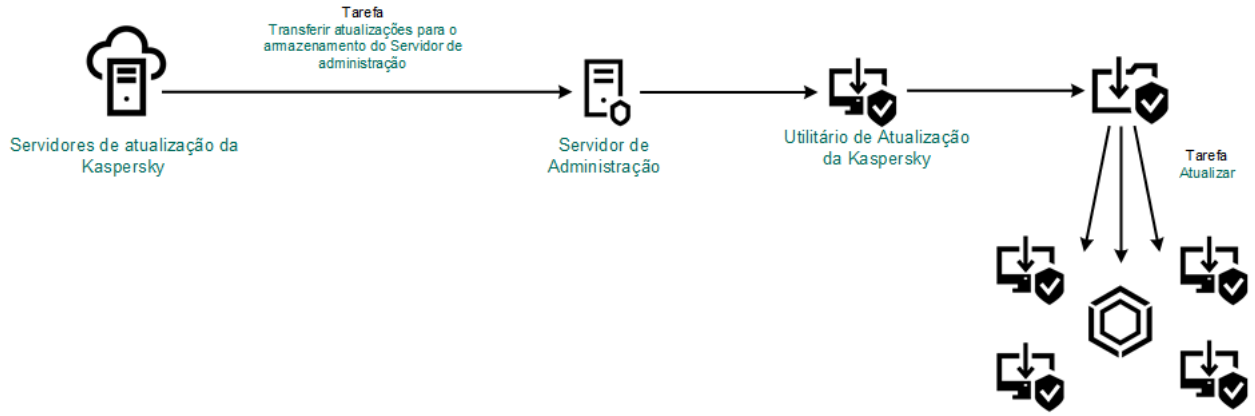
   O endereço de origem deve corresponder ao endereço indicado nas definições do Utilitário Kaspersky Update.

6. Clique em **Selecionar**.

7. Configure as prioridades das origens da atualização utilizando os botões **Para cima** e **Para baixo**.

   Se não for possível executar uma atualização através da primeira origem de atualização, o Kaspersky Endpoint Security muda automaticamente para o servidor seguinte.

8. Guarde as suas alterações.



Atualizar utilizando o Utilitário Kaspersky Update

Atualizar no modo móvel

O *modo móvel* é o modo de funcionamento do Kaspersky Endpoint Security quando um computador sai perímetro de rede da organização (*computador offline*). Para obter mais informações sobre como trabalhar com computadores offline e utilizadores fora do escritório, consulte a Ajuda Online do Kaspersky Security Center.

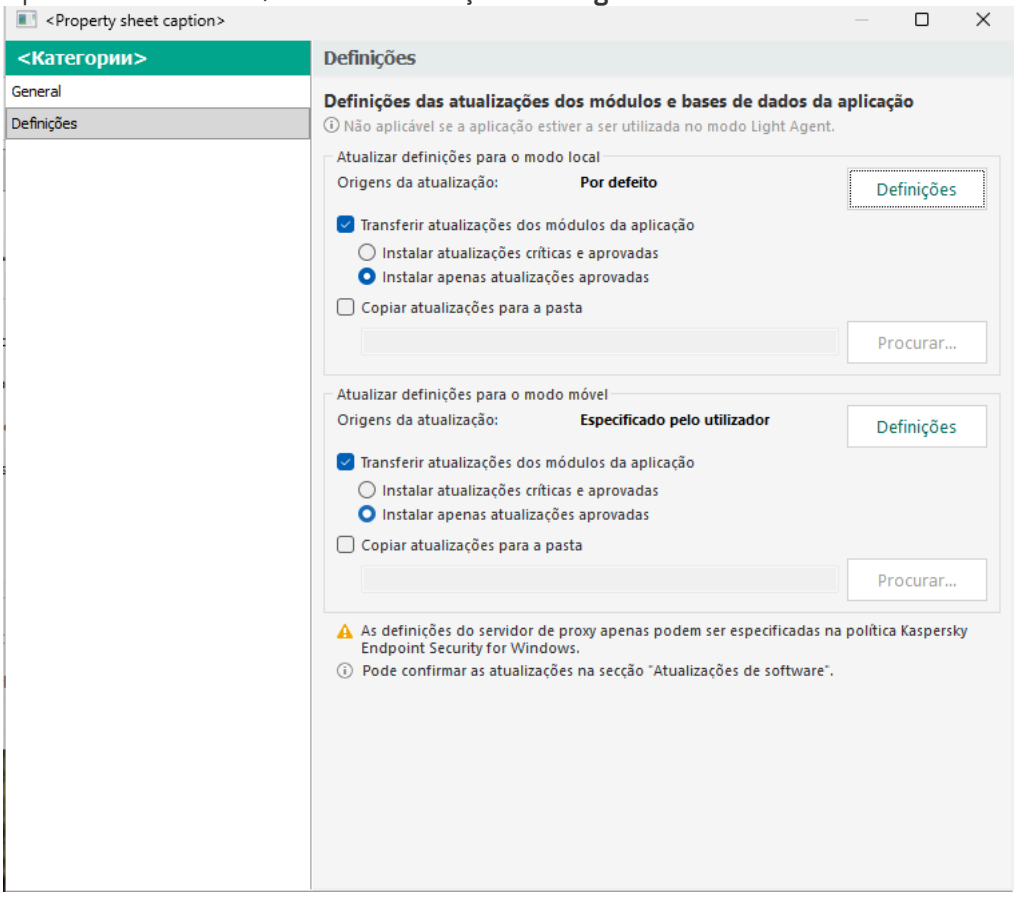
Um computador offline fora da rede da organização não pode ligar-se ao Servidor de administração para atualizar as bases de dados e módulos da aplicação. Por predefinição, apenas os servidores de atualização Kaspersky são utilizados como origem de atualizações para atualizar as bases de dados e módulos da aplicação no modo móvel. A utilização de um servidor de proxy para ligar à Internet é determinada por uma política fora do escritório especial. A política fora do escritório deve ser criada separadamente. Quando muda o Kaspersky Endpoint Security para o modo móvel, a tarefa de atualização é iniciada a cada duas horas.

Como configurar as definições de atualização para o modo móvel na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Tasks**.
3. Clique na tarefa **Atualização das bases de dados e módulos da aplicação** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

   A tarefa *Atualização das bases de dados e módulos da aplicação* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização das bases de dados e módulos da aplicação*, instale o Kaspersky Endpoint Security for Windows Management Plug-in enquanto executa o Assistente.
4. Na janela de propriedades da tarefa, selecione a secção **Settings**.



Definições de tarefa Atualização das bases de dados e módulos da aplicação

5. No bloco **Atualizar definições para o modo móvel**, clique no botão **Definições**.

6. Configure as origens das atualizações. As origens das atualizações podem ser servidores de atualização da Kaspersky, o Servidor de Administração do Kaspersky Security Center, outros servidores FTP e HTTP, pastas locais ou pastas de rede.

7. Guarde as suas alterações.

Como definir as configurações de atualização para o modo móvel na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Update** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

   A tarefa *Update* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Update*, instale o Kaspersky Endpoint Security for Windows Management Plug-in enquanto executa o Assistente.

3. Selecione o separador **Application settings** → **Mobile mode**.

4. Configure as origens das atualizações. As origens das atualizações podem ser servidores de atualização da Kaspersky, o Servidor de Administração do Kaspersky Security Center, outros servidores FTP e HTTP, pastas locais ou pastas de rede.

5. Guarde as suas alterações.

Deste modo, as bases de dados e os módulos da aplicação serão atualizados nos computadores dos utilizadores quando mudarem para o modo móvel.

Iniciar e parar uma tarefa de atualização

Independentemente do modo de execução da tarefa de atualização selecionado, pode iniciar ou parar uma tarefa de atualização do Kaspersky Endpoint Security em qualquer altura.

Para iniciar ou parar uma tarefa de atualização:

1. Na janela principal da aplicação, aceda à secção **Atualizar**.

2. No mosaico **Atualização das bases de dados e módulos da aplicação**, clique no botão **Atualizar** se quiser iniciar a tarefa de atualização.

   O Kaspersky Endpoint Security começará a atualizar os módulos e bases de dados da aplicação. A aplicação apresentará o progresso da tarefa, o tamanho dos ficheiros transferidos e a origem da atualização. Pode parar a tarefa a qualquer momento clicando no botão **Parar atualização**.

Para iniciar ou parar uma tarefa de atualização quando a interface simplificada da aplicação é apresentada:

1. Clique com o botão direito do rato para visualizar o menu de contexto do ícone da aplicação na área de notificação da barra de tarefas.

2. Na lista pendente **Tarefas** do menu de contexto, execute uma das seguintes ações:

   - selecione uma tarefa de atualização que não esteja em execução para iniciá-la
   - selecione uma tarefa de atualização que esteja em execução para pará-la
   - selecione uma tarefa de atualização pausada para retomar ou reiniciá-la

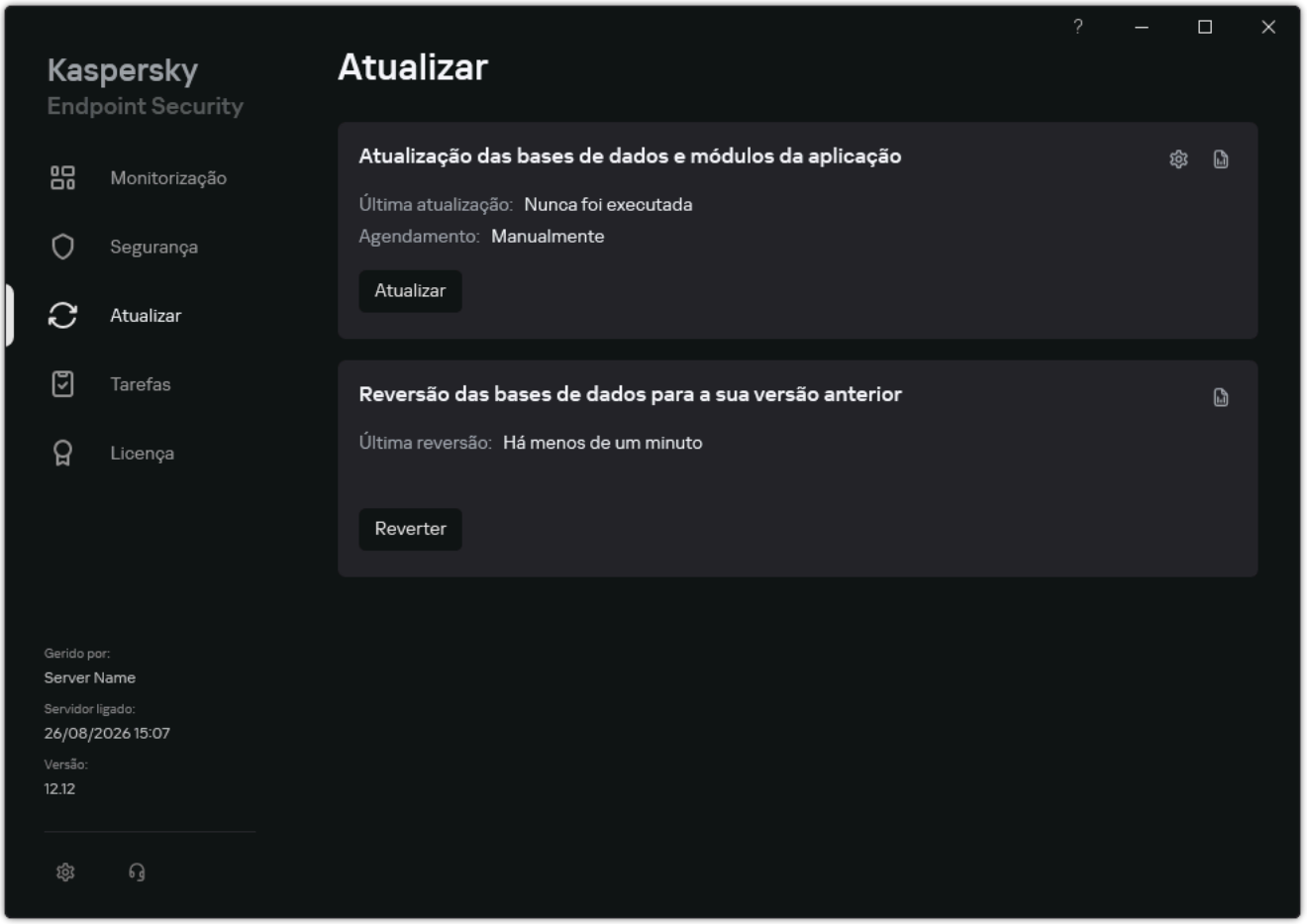
Iniciar uma tarefa de atualização com os direitos de outra conta de utilizador

Por predefinição, a tarefa de atualização do Kaspersky Endpoint Security é iniciada com a conta de utilizador utilizada para iniciar sessão no sistema operativo. Contudo, o Kaspersky Endpoint Security pode ser atualizado a partir de uma origem de atualização a que o utilizador não pode aceder por não ter os direitos necessários (por exemplo, uma pasta partilhada que contém um pacote de atualização) ou de uma origem de atualização para a qual a autenticação do servidor de proxy não está configurada. Nas definições da aplicação, pode especificar um utilizador que tenha esses direitos e iniciar a tarefa de atualização do Kaspersky Endpoint Security com essa conta de utilizador.

Para iniciar uma tarefa de atualização com uma conta de utilizador diferente:

Não pode configurar a tarefa de grupo *Atualização das bases de dados e módulos da aplicação* na interface da aplicação. Está disponível apenas uma tarefa de atualização local, *Atualização das bases de dados e módulos da aplicação*, para o utilizador. Se a tarefa *Atualização das bases de dados e módulos da aplicação* não for apresentada, tal significa que o administrador proibiu a utilização de tarefas locais na política.

1. Na janela principal da aplicação, aceda à secção **Atualizar**.



Tarefas de atualização local

2. Tal abre a lista de tarefas; selecione a tarefa *Atualização das bases de dados e módulos da aplicação* e clique em ⚙.

   É apresentada a janela de propriedades da tarefa.

3. Clique em **Executar atualizações da base de dados com direitos de utilizador**.

4. Na janela que se abre, selecione **Outro utilizador**.

5. Introduza as credenciais da conta de um utilizador com as permissões necessárias para aceder a origem da atualização.

6. Guarde as suas alterações.

Selecionar o modo de execução da tarefa de atualização

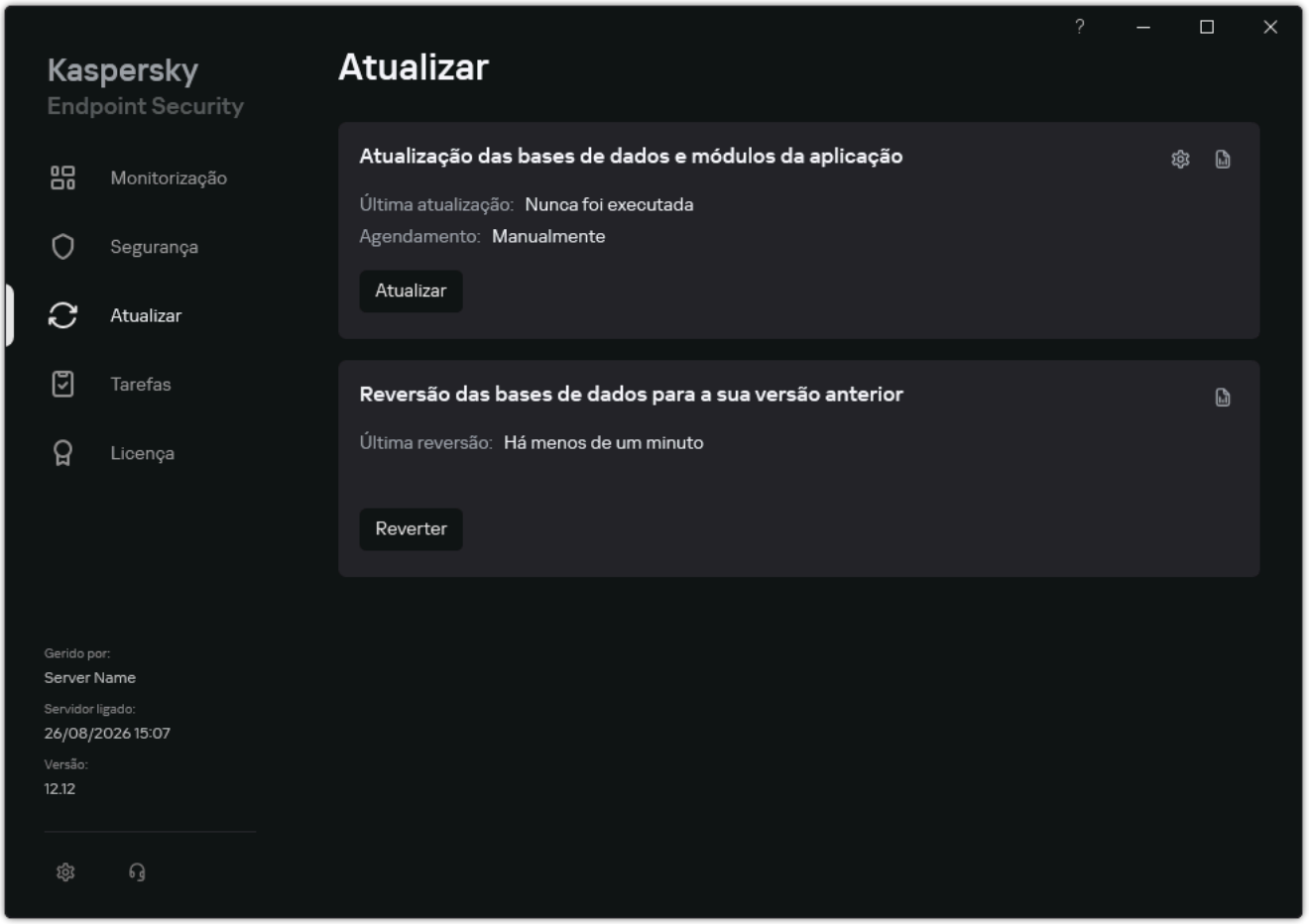
Se não for possível executar a tarefa de atualização por algum motivo (por exemplo, o computador não estava ligado naquela altura), pode configurar a tarefa ignorada para ser automaticamente iniciada assim que possível.

Pode adiar o início da tarefa de atualização após o início da aplicação, caso tenha selecionado o modo de execução da tarefa de atualização **Por agendamento** e a hora de início do Kaspersky Endpoint Security corresponda ao agendamento de inicialização da tarefa de atualização. A tarefa de atualização só pode ser executada depois de decorrido o intervalo de tempo especificado após a inicialização do Kaspersky Endpoint Security.

Para selecionar o modo de execução da tarefa de atualização:

Não pode configurar a tarefa de grupo *Atualização das bases de dados e módulos da aplicação* na interface da aplicação. Está disponível apenas uma tarefa de atualização local, *Atualização das bases de dados e módulos da aplicação*, para o utilizador. Se a tarefa *Atualização das bases de dados e módulos da aplicação* não for apresentada, tal significa que o administrador proibiu a utilização de tarefas locais na política.

1. Na janela principal da aplicação, aceda à secção **Atualizar**.



Tarefas de atualização local

2. Tal abre a lista de tarefas; selecione a tarefa *Atualização das bases de dados e módulos da aplicação* e clique em ⚙.

   É apresentada a janela de propriedades da tarefa.

3. Clique em **Modo de execução**.

4. Na janela que abre, selecione o modo de execução da tarefa de atualização:

   - Se pretender que o Kaspersky Endpoint Security execute a tarefa de atualização em função da disponibilização ou não de um pacote de atualização na origem de atualização, selecione **Automaticamente**. A frequência com que o Kaspersky Endpoint Security verifica a existência de pacotes de atualizações aumenta durante os surtos de vírus e é menos frequente noutras ocasiões.

   - Se pretender iniciar a tarefa de atualização manualmente, selecione **Manualmente**.

   - Se pretender configurar o agendamento de execução para a tarefa de atualização, selecione outras opções. Configure as definições avançadas para iniciar a tarefa de atualização:

     - No campo **Adiar execução, após o início da aplicação, durante N minutos**, especifique o intervalo de tempo durante o qual pretende adiar o início da tarefa de atualização após o início do Kaspersky Endpoint Security.

     - Selecione **Executar verificação agendada no dia seguinte se o computador estiver desligado**, se desejar que o Kaspersky Endpoint Security execute as tarefas de atualização ignoradas assim que possível. Quando a aplicação tem a oportunidade de executar tarefas ignoradas, inicia as tarefas aleatoriamente num determinado intervalo de tempo para distribuir a carga no computador.

5. Guarde as suas alterações.

Adicionar uma origem de atualização

Uma origem de atualização é um recurso que contém atualizações para as bases de dados e os módulos da aplicação do Kaspersky Endpoint Security.

As origens de atualização incluem o servidor do Kaspersky Security Center, os servidores de atualização da Kaspersky e as pastas de rede ou locais.

No caso de os servidores de atualização da Kaspersky estarem indisponíveis, o Kaspersky Endpoint Security pode utilizar domínios alternativos para atualizar as suas bases de dados e módulos de software de aplicações. Para obter informações detalhadas, consulte a Base de Conhecimento de Apoio Técnico da Kaspersky.

A lista predefinida de origens de atualização inclui o Kaspersky Security Center e os servidores de atualização da Kaspersky. Pode adicionar outras origens de atualização à lista. Pode especificar como origens de atualização servidores HTTP/FTP e pastas partilhadas.

O Kaspersky Endpoint Security não suporta atualizações de servidores HTTPS, exceto se forem servidores de atualização da Kaspersky.

Se forem selecionados vários recursos como origens de atualização, o Kaspersky Endpoint Security tentar estabelecer ligação aos mesmos, um após o outro, começando pelo topo da lista, e executa a tarefa de atualização recolhendo o pacote de atualização na primeira origem disponível.

Por predefinição, o Kaspersky Endpoint Security usa o servidor Kaspersky Security Center como a primeira origem de atualização. Isto ajuda a conservar o tráfego durante a atualização. Se uma política não for aplicada ao computador, os servidores Kaspersky serão selecionados como a primeira origem de atualização nas definições da tarefa local *Atualização das bases de dados e módulos da aplicação* porque a aplicação pode não ter acesso ao servidor do Kaspersky Security Center.

Se a aplicação estiver a ser executada no modo Light Agent, é selecionada uma pasta na SVM como origem de atualização.

Como adicionar uma origem de atualização na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.

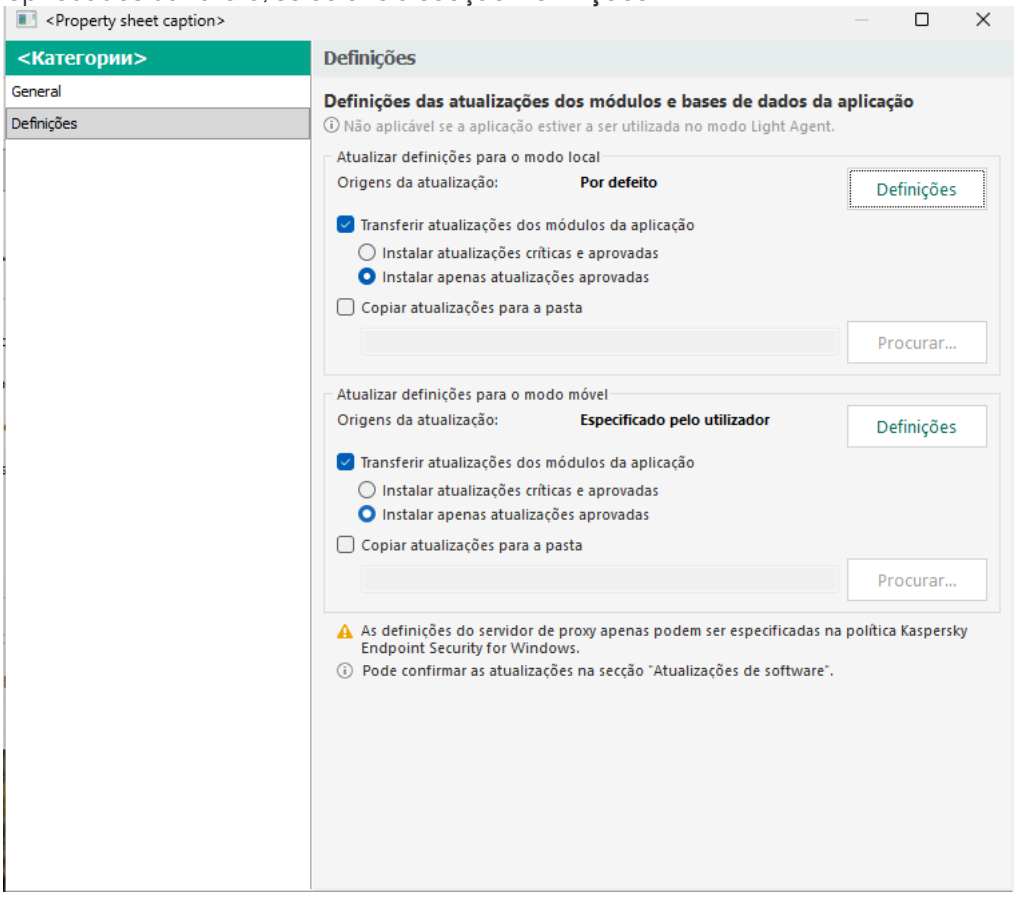
   Na árvore da consola, selecione **Tasks**.

2. Clique na tarefa **Atualização das bases de dados e módulos da aplicação** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

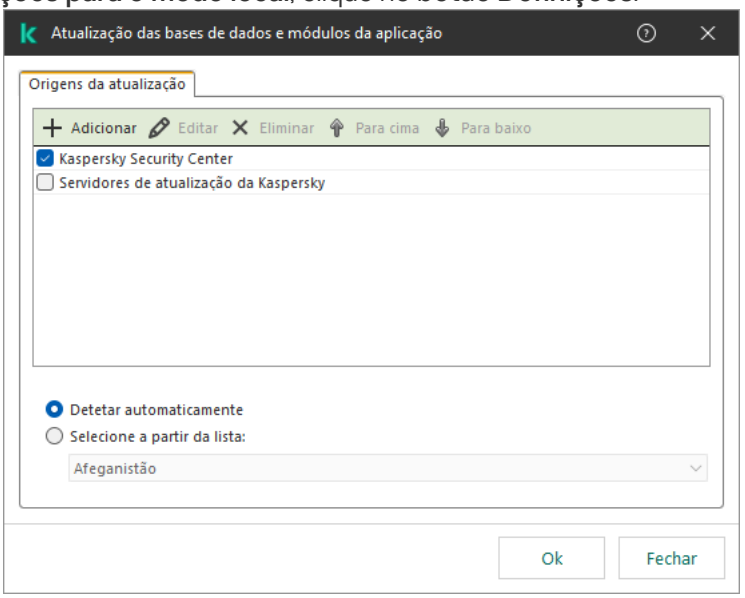
   A tarefa *Atualização das bases de dados e módulos da aplicação* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização das bases de dados e módulos da aplicação*, instale o Kaspersky Endpoint Security for Windows Management Plug-in enquanto executa o Assistente.

3. Na janela de propriedades da tarefa, selecione a secção **Definições**.



Definições de tarefa Atualização das bases de dados e módulos da aplicação

4. No bloco **Atualizar definições para o modo local**, clique no botão **Definições**.



Origens da atualização

5. Na lista de origens da atualização, clique no botão **Adicionar**.

6. No campo **Origens da atualização**, especifique o endereço do servidor FTP ou HTTP, pasta de rede ou pasta local que contém o pacote de atualização.

   É utilizado o seguinte formato de caminho para a origem de atualização:

   - Para um servidor FTP ou HTTP, introduza o respetivo endereço da Web ou endereço IP.

     Por exemplo, `http://dnl-01.geo.kaspersky.com/` ou `93.191.13.103`.

     Para um servidor FTP, pode especificar as definições de autenticação dentro do endereço da Web, no seguinte formato: `ftp://<user name>:<password>@<node>:<port>`.

   - Para uma pasta de rede, introduza o caminho UNC.

     Por exemplo, `\\Server\Share\Update distribution`.

   - No caso de uma pasta local, introduza o caminho completo para essa pasta.

     Por exemplo, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

   Pode excluir a origem da atualização sem removê-la da lista de origens de atualização. Para o fazer, desmarque a caixa de verificação ao lado do objeto.

7. Clique em **OK**.

8. Configure as prioridades das origens da atualização utilizando os botões **Para cima** e **Para baixo**.

   Se não for possível executar uma atualização através da primeira origem de atualização, o Kaspersky Endpoint Security muda automaticamente para o servidor seguinte.

9. Se necessário, adicione uma origem de atualização para o modo móvel. O *modo móvel* é o modo de funcionamento do Kaspersky Endpoint Security quando um computador sai perímetro de rede da organização (*computador offline*).

10. Guarde as suas alterações.

Como adicionar uma origem de atualização na Web Console

1. Na janela principal da Consola Web, selecione **Tasks**.

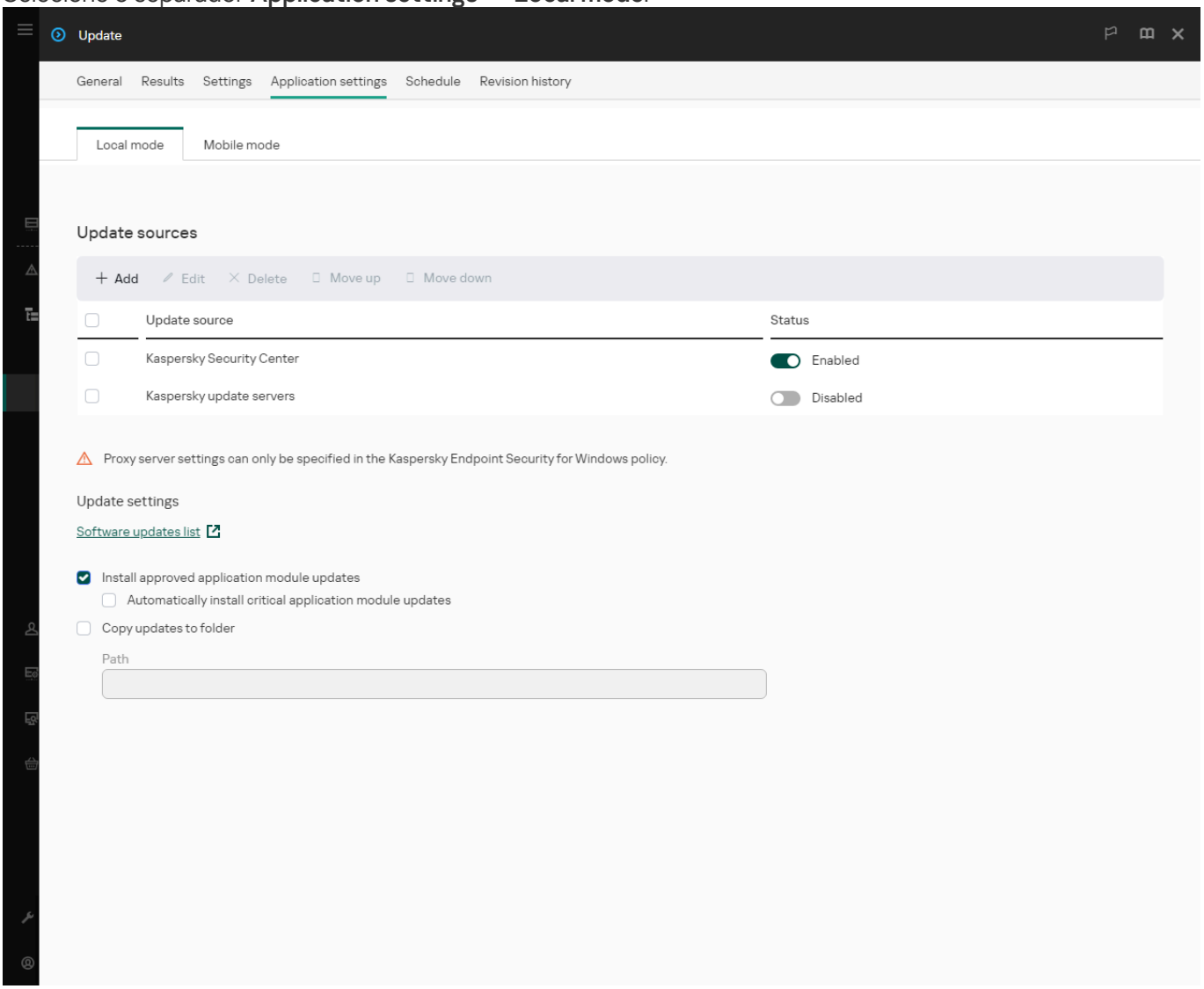
   A lista de tarefas é aberta.

2. Clique na tarefa **Update** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

   A tarefa *Update* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Update*, instale o Kaspersky Endpoint Security for Windows Management Plug-in enquanto executa o Assistente.

3. Selecione o separador **Application settings** → **Local mode**.



Origens da atualização

4. Na lista de origens da atualização, clique no botão **Add**.

5. Na janela apresentada, especifique o endereço do servidor FTP ou HTTP, pasta de rede ou pasta local que contém o pacote de atualização.

   É utilizado o seguinte formato de caminho para a origem de atualização:

   - Para um servidor FTP ou HTTP, introduza o respetivo endereço da Web ou endereço IP.

     Por exemplo, `http://dnl-01.geo.kaspersky.com/` ou `93.191.13.103`.

Para um servidor FTP, pode especificar as definições de autenticação dentro do endereço da Web, no seguinte formato: `ftp://<user name>:<password>@<node>:<port>`.

- Para uma pasta de rede, introduza o caminho UNC.

  Por exemplo, `\\Server\Share\Update distribution`.

- No caso de uma pasta local, introduza o caminho completo para essa pasta.

  Por exemplo, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

Pode excluir a origem da atualização sem removê-la da lista de origens de atualização. Para tal, desative o botão ao lado do mesmo.

6. Clique em **OK**.

7. Configure as prioridades das origens da atualização utilizando os botões **Move up** e **Move down**.

   Se não for possível executar uma atualização através da primeira origem de atualização, o Kaspersky Endpoint Security muda automaticamente para o servidor seguinte.

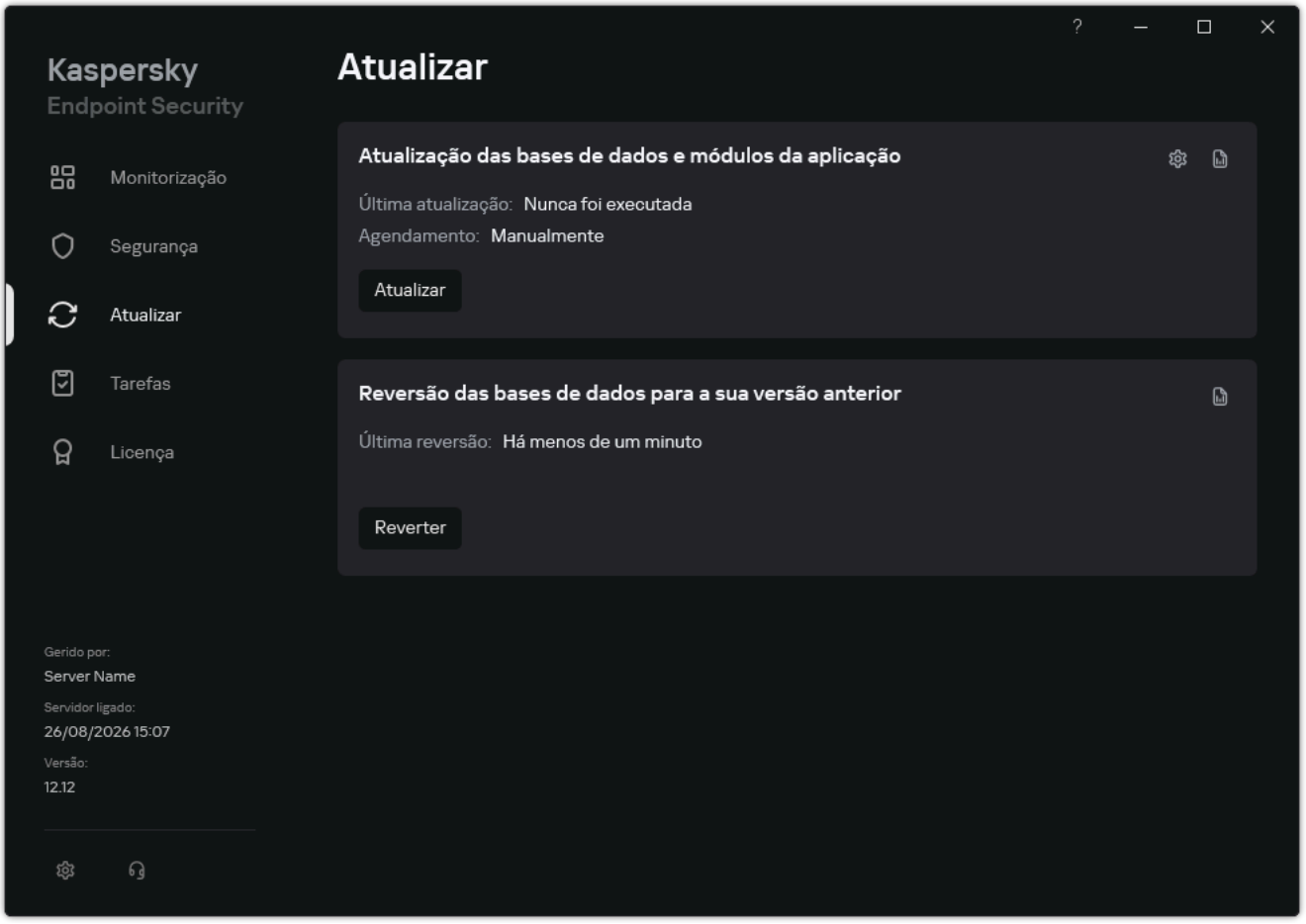
8. Se necessário, adicione uma origem de atualização para o modo móvel. O *modo móvel* é o modo de funcionamento do Kaspersky Endpoint Security quando um computador sai perímetro de rede da organização (*computador offline*).

9. Guarde as suas alterações.

Como adicionar uma origem de atualização na interface da aplicação

Não pode configurar a tarefa de grupo *Atualização das bases de dados e módulos da aplicação* na interface da aplicação. Está disponível apenas uma tarefa de atualização local, *Atualização das bases de dados e módulos da aplicação*, para o utilizador. Se a tarefa *Atualização das bases de dados e módulos da aplicação* não for apresentada, tal significa que o administrador proibiu a utilização de tarefas locais na política.

1. Na janela principal da aplicação, aceda à secção **Atualizar**.



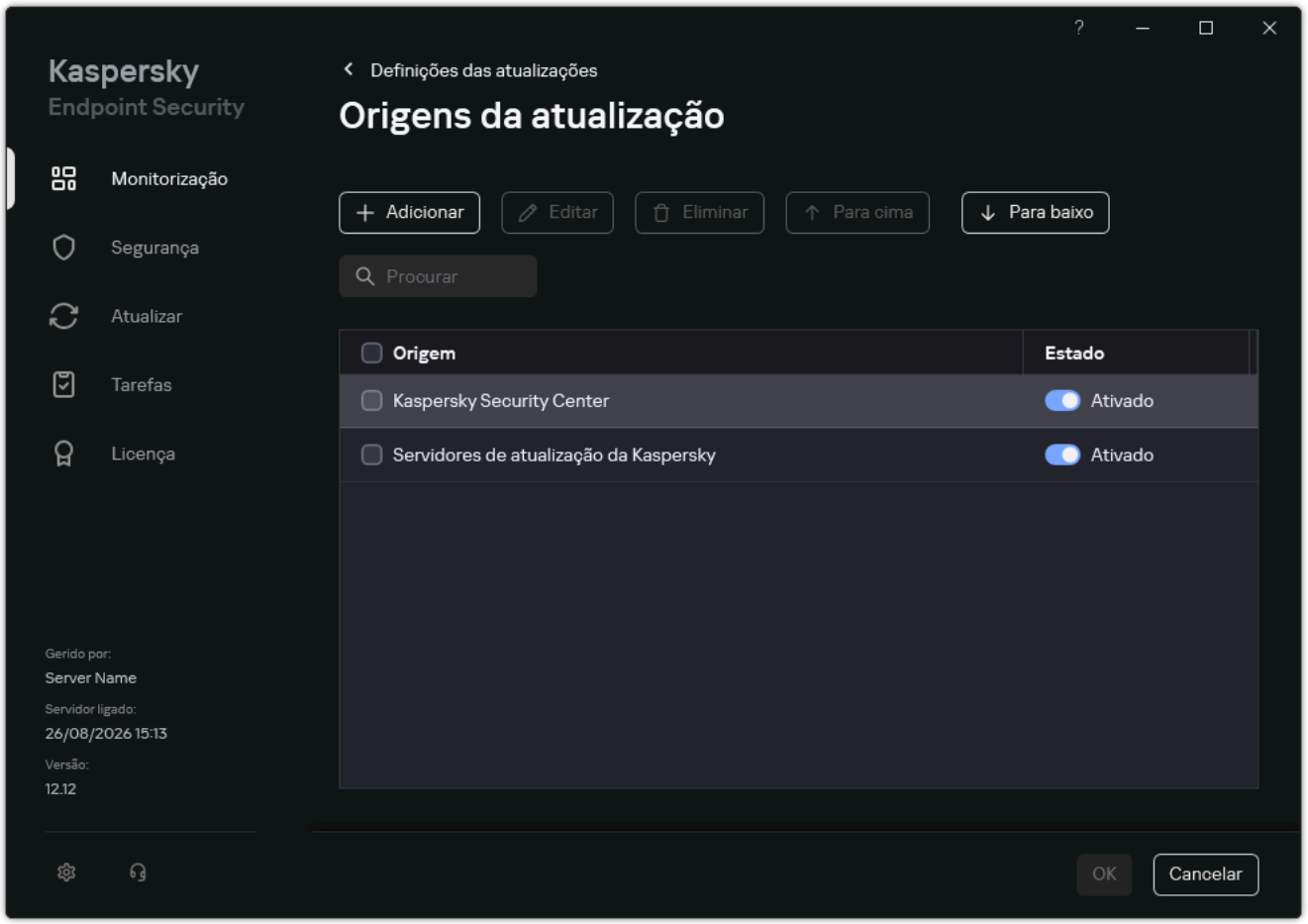
Tarefas de atualização local

2. Tal abre a lista de tarefas; selecione a tarefa *Atualização das bases de dados e módulos da aplicação* e clique em ⚙.

   É apresentada a janela de propriedades da tarefa.

3. Clique em **Selecionar origens de atualização**.

4. Na janela que abre, clique no botão **Adicionar**.



Origens da atualização

5. Na janela apresentada, especifique o endereço do servidor FTP ou HTTP, pasta de rede ou pasta local que contém o pacote de atualização.

   É utilizado o seguinte formato de caminho para a origem de atualização:

   - Para um servidor FTP ou HTTP, introduza o respetivo endereço da Web ou endereço IP.

     Por exemplo, `http://dnl-01.geo.kaspersky.com/` ou `93.191.13.103`.

     Para um servidor FTP, pode especificar as definições de autenticação dentro do endereço da Web, no seguinte formato: `ftp://<user name>:<password>@<node>:<port>`.

   - Para uma pasta de rede, introduza o caminho UNC.

     Por exemplo, `\\Server\Share\Update distribution`.

   - No caso de uma pasta local, introduza o caminho completo para essa pasta.

     Por exemplo, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

6. Clique em **Selecionar**.

7. Configure as prioridades das origens da atualização utilizando os botões **Para cima** e **Para baixo**.

8. Guarde as suas alterações.

Atualizar módulos de aplicação

As atualizações do módulo da aplicação corrigem erros, melhoram o desempenho e adicionam novas funcionalidades. Quando uma nova atualização do módulo da aplicação estiver disponível, precisará de confirmar a instalação da atualização. Pode confirmar a instalação de uma atualização do módulo da aplicação na interface da aplicação ou no Kaspersky Security Center. Sempre que uma atualização está disponível, a aplicação apresenta uma notificação na janela principal do Kaspersky Endpoint Security: . Se as atualizações de módulo da aplicação necessitarem de verificação e aceitação dos termos do Contrato de Licença do Utilizador Final, a aplicação instala as atualizações após a aceitação dos termos do Contrato de Licença do Utilizador Final.

Depois de instalar uma atualização da aplicação, poderá ser necessário reiniciar o computador.

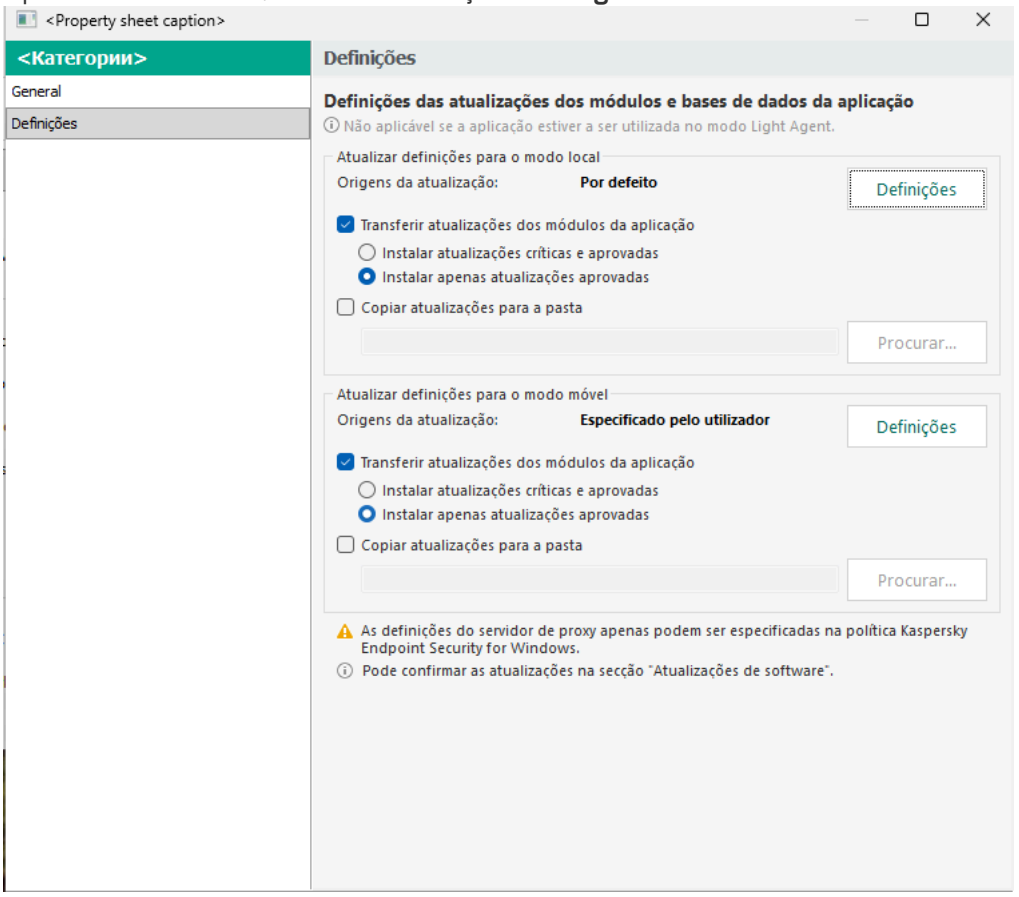
Como configurar as atualizações do módulo da aplicação na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Tasks**.
3. Clique na tarefa **Atualização das bases de dados e módulos da aplicação** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

   A tarefa *Atualização das bases de dados e módulos da aplicação* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização das bases de dados e módulos da aplicação*, instale o Kaspersky Endpoint Security for Windows Management Plug-in enquanto executa o Assistente.

4. Na janela de propriedades da tarefa, selecione a secção **Settings**.



Definições de tarefa Atualização das bases de dados e módulos da aplicação

5. No bloco **Atualizar definições para o modo local**, selecione a caixa de verificação **Transferir atualizações dos módulos da aplicação**.

   Se quiser impedir o descarregamento de atualizações do módulo da aplicação, desmarque a caixa de verificação **Transferir atualizações dos módulos da aplicação** e proíba a utilização das tarefas locais pelo utilizador.

6. Selecione as atualizações do módulo da aplicação que quer instalar.

   - **Instalar atualizações críticas e aprovadas**. Se esta opção estiver selecionada, quando estão disponíveis atualizações de módulo da aplicação o Kaspersky Endpoint Security instala as atualizações críticas automaticamente e todas as outras atualizações de módulo da aplicação apenas após a sua instalação ser aprovada localmente através da interface da aplicação ou no Kaspersky Security Center.

   - **Instalar apenas atualizações aprovadas**. Se esta opção estiver selecionada, quando estão disponíveis atualizações de módulo da aplicação o Kaspersky Endpoint Security instala as mesmas apenas após a sua instalação ser aprovada localmente através da interface da aplicação ou no Kaspersky Security Center. Esta opção está selecionada por predefinição.

7. Se necessário, configure atualizações do módulo da aplicação para o modo móvel. O *modo móvel* é o modo de funcionamento do Kaspersky Endpoint Security quando um computador sai perímetro de rede da organização (*computador offline*).

8. Guarde as suas alterações.

Como configurar atualizações do módulo da aplicação na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Tasks**.

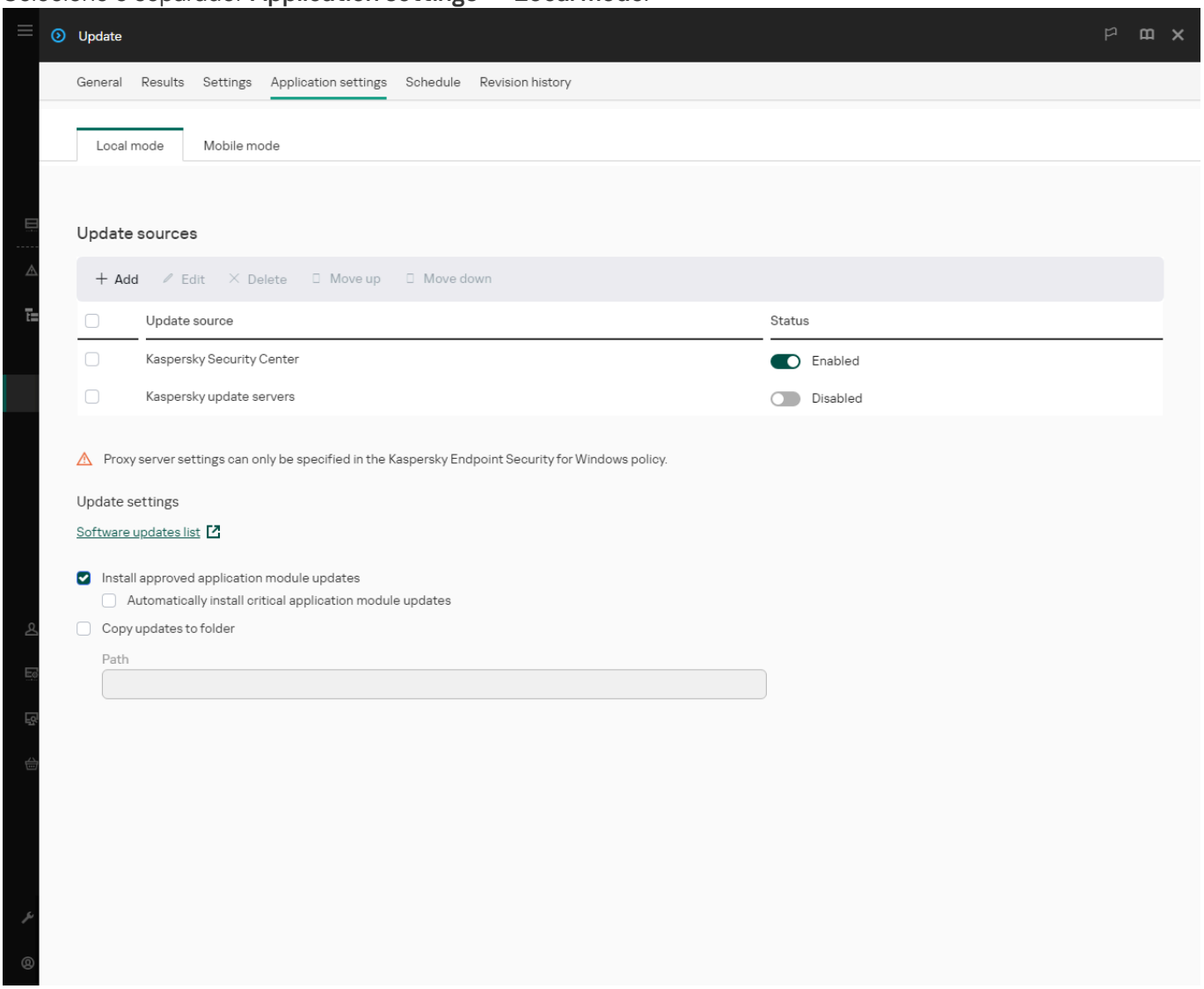
   A lista de tarefas é aberta.

2. Clique na tarefa **Atualização das bases de dados e módulos da aplicação** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

   A tarefa *Atualização das bases de dados e módulos da aplicação* é criada automaticamente pelo assistente de início rápido do Servidor de Administração. Para criar a tarefa *Atualização das bases de dados e módulos da aplicação*, instale o Kaspersky Endpoint Security for Windows Management Plug-in enquanto executa o Assistente.

3. Selecione o separador **Application settings → Local mode**.



Definições de tarefa Update

4. Em **Update settings**, selecione as atualizações do módulo da aplicação que quer instalar:

   - **Install approved application module updates**. Se esta opção estiver selecionada, quando estão disponíveis atualizações de módulo da aplicação o Kaspersky Endpoint Security instala as mesmas apenas após a sua instalação ser aprovada localmente através da interface da aplicação ou no Kaspersky Security Center. Esta opção está selecionada por predefinição.

   - **Automatically install critical application module updates**. Se esta opção estiver selecionada, quando estão disponíveis atualizações de módulo da aplicação o Kaspersky Endpoint Security instala as atualizações críticas automaticamente e todas as outras atualizações de módulo da aplicação apenas após a sua instalação ser aprovada localmente através da interface da aplicação ou no Kaspersky Security Center.

Se quiser impedir o descarregamento de atualizações do módulo da aplicação, desmarque as caixas de verificação **Install approved application module updates** e **Automatically install critical application module updates** e proíba a utilização das tarefas locais pelo utilizador.

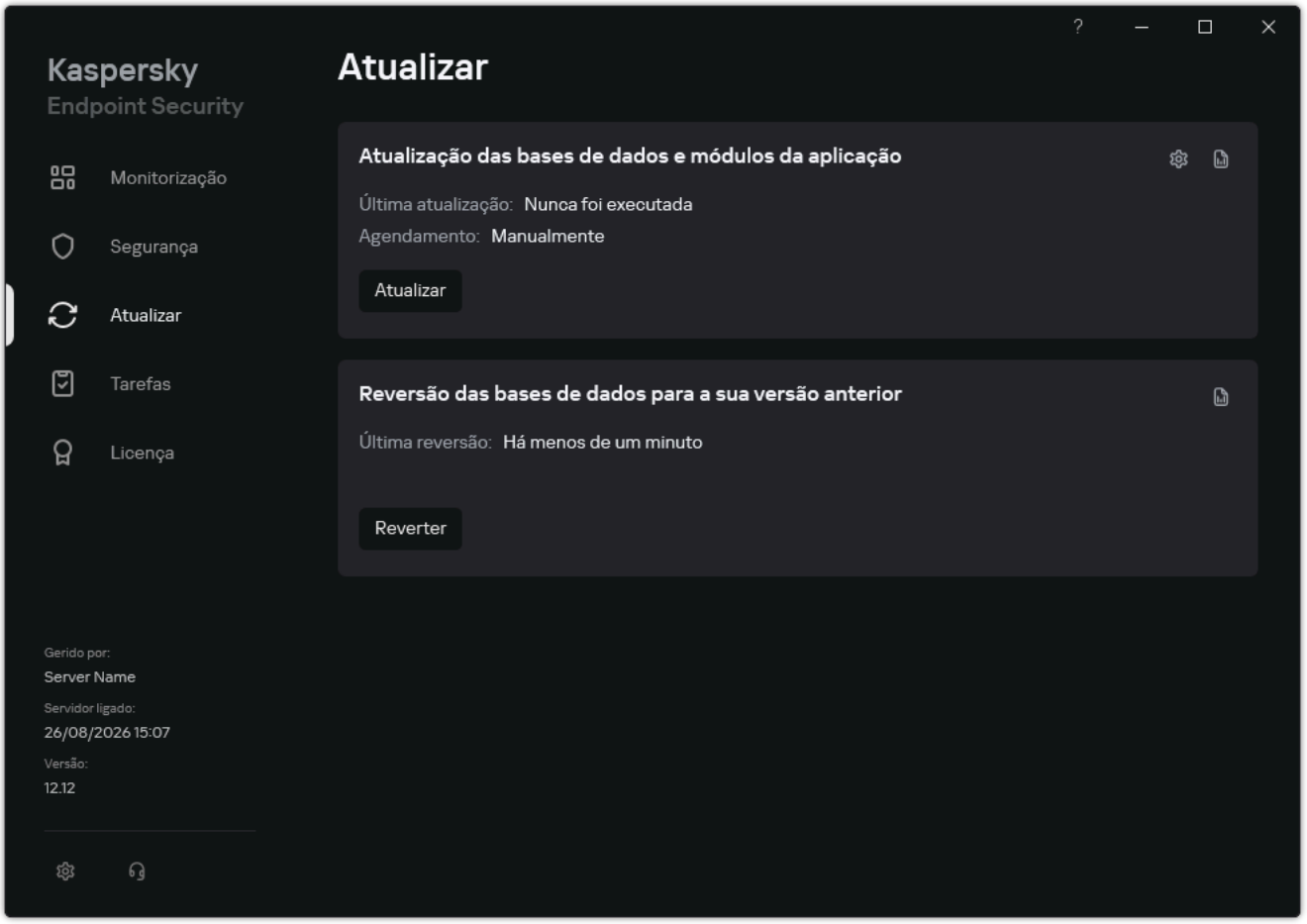
5. Se necessário, configure atualizações do módulo da aplicação para o modo móvel. O *modo móvel* é o modo de funcionamento do Kaspersky Endpoint Security quando um computador sai perímetro de rede da organização (*computador offline*).

6. Guarde as suas alterações.

Como configurar as atualizações do módulo da aplicação na interface da aplicação

Não pode configurar a tarefa de grupo *Atualização das bases de dados e módulos da aplicação* na interface da aplicação. Está disponível apenas uma tarefa de atualização local, *Atualização das bases de dados e módulos da aplicação*, para o utilizador. Se a tarefa *Atualização das bases de dados e módulos da aplicação* não for apresentada, tal significa que o administrador proibiu a utilização de tarefas locais na política.

1. Na janela principal da aplicação, aceda à secção **Atualizar**.



Tarefas de atualização local

2. Tal abre a lista de tarefas; selecione a tarefa *Atualização das bases de dados e módulos da aplicação* e clique em ⚙.

   É apresentada a janela de propriedades da tarefa.

3. No bloco **Transferir e instalar as atualizações dos módulos de aplicação**, selecione a caixa de verificação **Transferir atualizações dos módulos da aplicação**.

4. Selecione as atualizações do módulo da aplicação que quer instalar.

   - **Instalar atualizações críticas e aprovadas**. Se esta opção estiver selecionada, quando estão disponíveis atualizações de módulo da aplicação o Kaspersky Endpoint Security instala as atualizações críticas automaticamente e todas as outras atualizações de módulo da aplicação apenas após a sua instalação ser aprovada localmente através da interface da aplicação ou no Kaspersky Security Center.

   - **Instalar apenas atualizações aprovadas**. Se esta opção estiver selecionada, quando estão disponíveis atualizações de módulo da aplicação o Kaspersky Endpoint Security instala as mesmas apenas após a sua instalação ser aprovada localmente através da interface da aplicação ou no Kaspersky Security Center. Esta opção está selecionada por predefinição.

5. Guarde as suas alterações.

Utilizar um servidor proxy para atualizações

Pode ser necessário para especificar as definições do servidor proxy para transferir as atualizações da base de dados da origem da atualização. Se existirem várias origens da atualização, as definições do servidor proxy são aplicadas a todas as origens. Se não for necessário um servidor proxy para algumas origens da atualização, pode desativar a utilização de um servidor proxy nas propriedades da política. O Kaspersky Endpoint Security também utilizará um servidor de proxy para aceder ao Kaspersky Security Network e aos servidores de ativação.

Para configurar uma ligação às origens da atualização através de um servidor proxy:

1. Na janela principal da Consola Web, clique em ⚙.

   A janela de propriedades do Servidor de administração abre-se.

2. Aceda à secção **Configuring internet access**.

3. Selecione a caixa de verificação **Use proxy server**.

4. Configure as definições de ligações do servidor proxy: definições de endereço do servidor proxy, porta e autenticação (nome de utilizador e password).

5. Guarde as suas alterações.

Para desativar utilização de um servidor de proxy para um grupo de administração específico:

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **General Settings** → **Network Settings**.

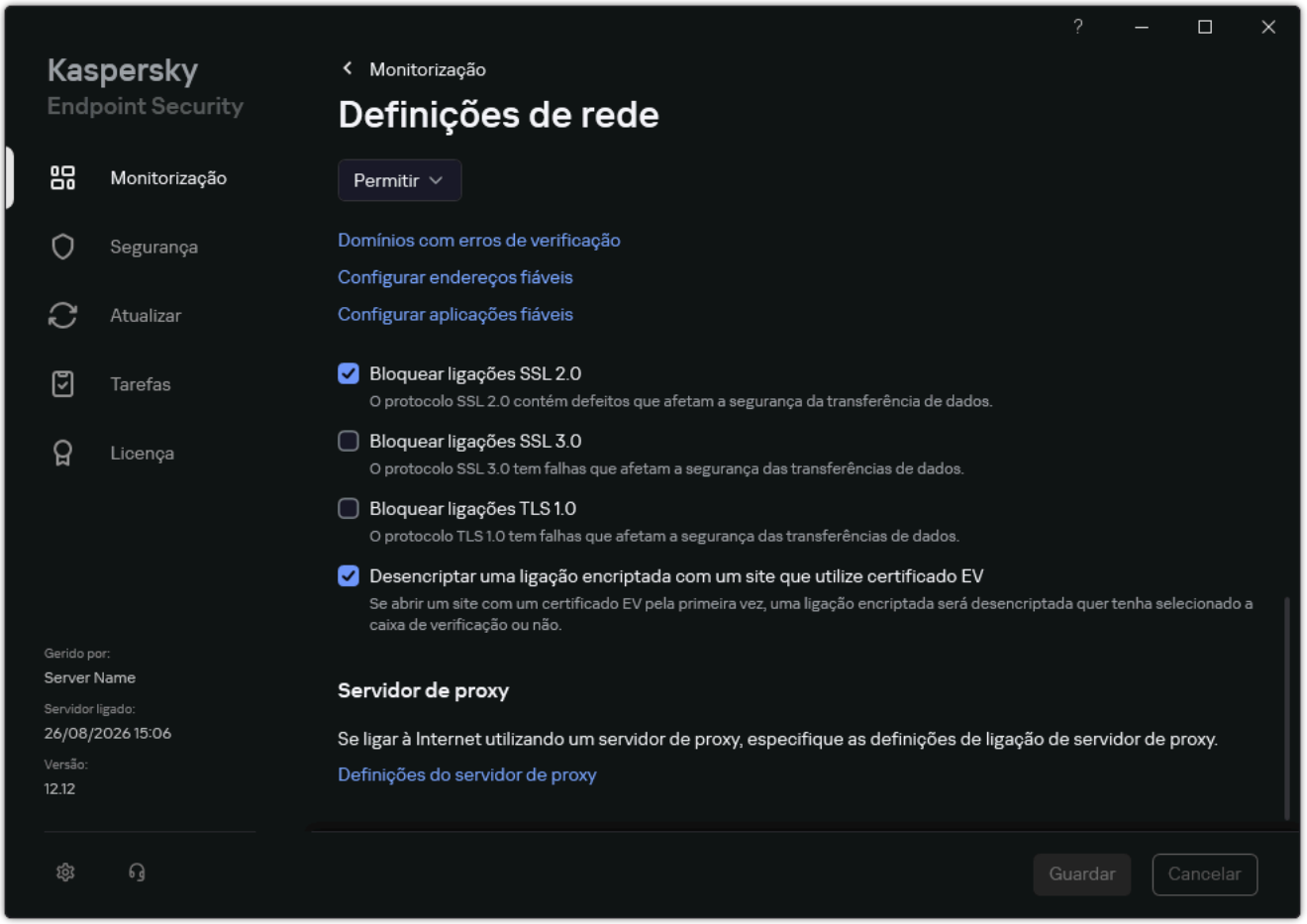
5. No bloco **Proxy server**, clique no botão **Settings**.

6. Na janela que abre, selecione a caixa de verificação **Bypass a proxy server for local addresses**.

7. Guarde as suas alterações.

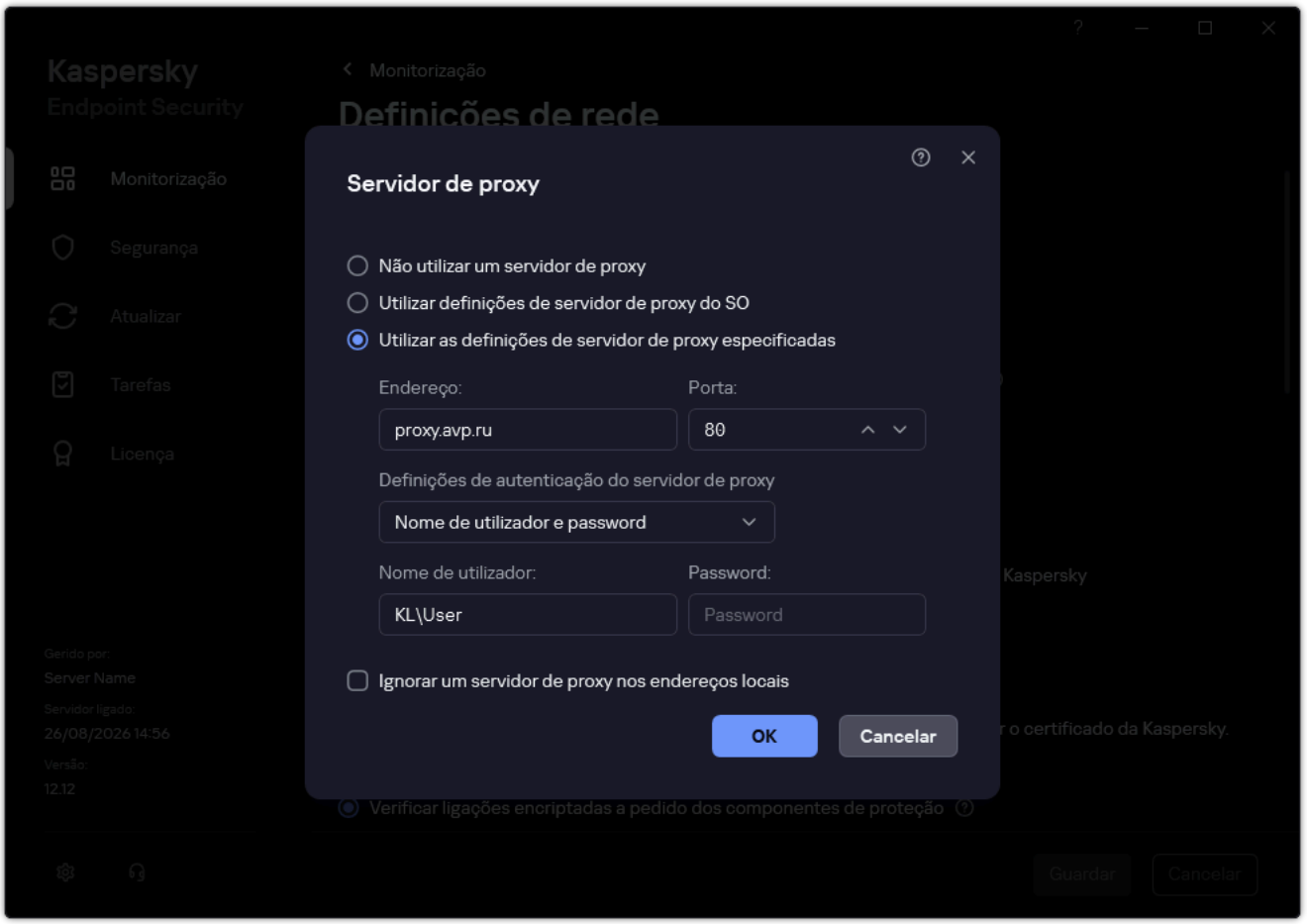
Para configurar as definições do servidor de proxy na interface da aplicação:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Definições de rede**.



Definições da rede de aplicações

3. No bloco **Servidor de proxy**, clique na ligação **Definições do servidor de proxy**.



Definições de ligação do servidor de proxy

4. Na janela que abre, selecione uma das seguintes opções para determinar o endereço do servidor de proxy:

   - **Utilizar definições de servidor de proxy do SO**.

     Esta opção está selecionada por predefinição. O Kaspersky Endpoint Security usa as definições do servidor de proxy que são definidas nas definições do sistema operativo.

   - **Utilizar as definições de servidor de proxy especificadas**.

     Se tiver selecionado esta opção, configure as definições para a ligação ao servidor de proxy: endereço e porta do servidor de proxy.

5. Selecione como pretende que a aplicação seja autenticada no servidor proxy. Por defeito, a aplicação utiliza a autenticação NTLM do domínio do utilizador atual.

6. Se pretender desativar a utilização do servidor de proxy ao atualizar as bases de dados e módulos da aplicação a partir de uma pasta partilhada, selecione a caixa de verificação **Ignorar um servidor de proxy nos endereços locais**.

7. Guarde as suas alterações.

Como resultado, o Kaspersky Endpoint Security utilizará o servidor de proxy para transferir o módulo da aplicação e as atualizações da base de dados. O Kaspersky Endpoint Security também utilizará um servidor de proxy para aceder aos servidores da KSN e aos servidores de ativação Kaspersky. Se a autenticação for necessária no servidor de proxy, mas as credenciais da conta do utilizador não tiverem sido fornecidas ou estiverem incorretas, o Kaspersky Endpoint Security solicitar-lhe-á o nome do utilizador e a password.

Reverter última atualização

Depois de as bases de dados e os módulos da aplicação serem atualizados pela segunda vez, a função de reversão das bases de dados e dos módulos da aplicação para as versões anteriores fica disponível.

Sempre que um utilizador iniciar o processo de atualização, o Kaspersky Endpoint Security cria uma cópia de segurança das bases de dados e módulos da aplicação atuais. Deste modo, pode reverter as bases de dados e os módulos da aplicação para as respetivas versões anteriores, se necessário. Reverter a última atualização é útil, por exemplo, se uma nova versão da base de dados causar um falso positivo que leve o Kaspersky Endpoint Security a bloquear uma aplicação segura.

O Kaspersky Endpoint Security no modo Light Agent não suporta a tarefa *Reverter atualização*.

Como reverter a última atualização na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

1. Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Reverter atualização**.

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

Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 3. Configurar um agendamento de início de uma tarefa

Configure o agendamento de tarefas, por exemplo, manualmente.

Passo 4. Definir o nome da tarefa

Insira um nome para a tarefa.

Passo 7. Completar a criação da tarefa

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa.

Como reverter a última atualização na Consola Web

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **Rollback**.

   c. No campo **Task name**, introduza uma breve descrição, por exemplo, *Reverter atualização*.

   d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Avance para o passo seguinte.

5. Selecione uma conta para executar a tarefa. Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de utilizador local.

6. Conclua o assistente.

7. Será apresentada uma nova tarefa na lista de tarefas.

8. Selecione a caixa de verificação junto à tarefa.

9. Clique em **Start**.

Como reverter a última atualização na interface da aplicação

1. Na janela principal da aplicação, aceda à secção **Atualizar**.



Tarefas de atualização local

2. No mosaico **Reversão das bases de dados para a sua versão anterior**, clique no botão **Reverter**.

O Kaspersky Endpoint Security começará a reverter a última atualização da base de dados. A aplicação apresentará o progresso da reversão, o tamanho dos ficheiros transferidos e a origem da atualização. Pode parar a tarefa a qualquer momento clicando no botão **Parar atualização**.

Tecnologia de desinfeção avançada

Para detetar ameaças ativas, o Kaspersky Endpoint Security usa a tecnologia Desinfeção avançada. A Desinfeção avançada funciona de forma diferente para computadores e servidores. Pode configurar a desinfeção avançada nas definições de tarefa da *Verificação de software malicioso* e nas definições da aplicação.

Se o Kaspersky Endpoint Security não conseguir interromper a execução de malware, pode usar a tecnologia Desinfeção avançada. Para computadores sujeitos à política, a Desinfeção avançada está desativada por defeito por ser uma tecnologia que usa um volume significativo de recursos de computação. Para computadores que não estão sujeitos à política, a Desinfecção Avançada é ativada por defeito.

A Desinfeção avançada funciona de forma diferente para computadores e servidores. Para usar a tecnologia em servidores, tem de ativar a Desinfeção Avançada imediata nas propriedades da tarefa *Verificação de software malicioso*. Este pré-requisito não é necessário para usar a tecnologia em computadores.

Como ativar ou desativar a Tecnologia de Desinfeção Avançada na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais** → **Definições da aplicação**.
4. No bloco **Geral**, use a caixa de verificação **Ativar Tecnologia de Desinfeção Avançada** para ativar ou desativar a Tecnologia de Desinfeção Avançada.
5. Guarde as suas alterações.

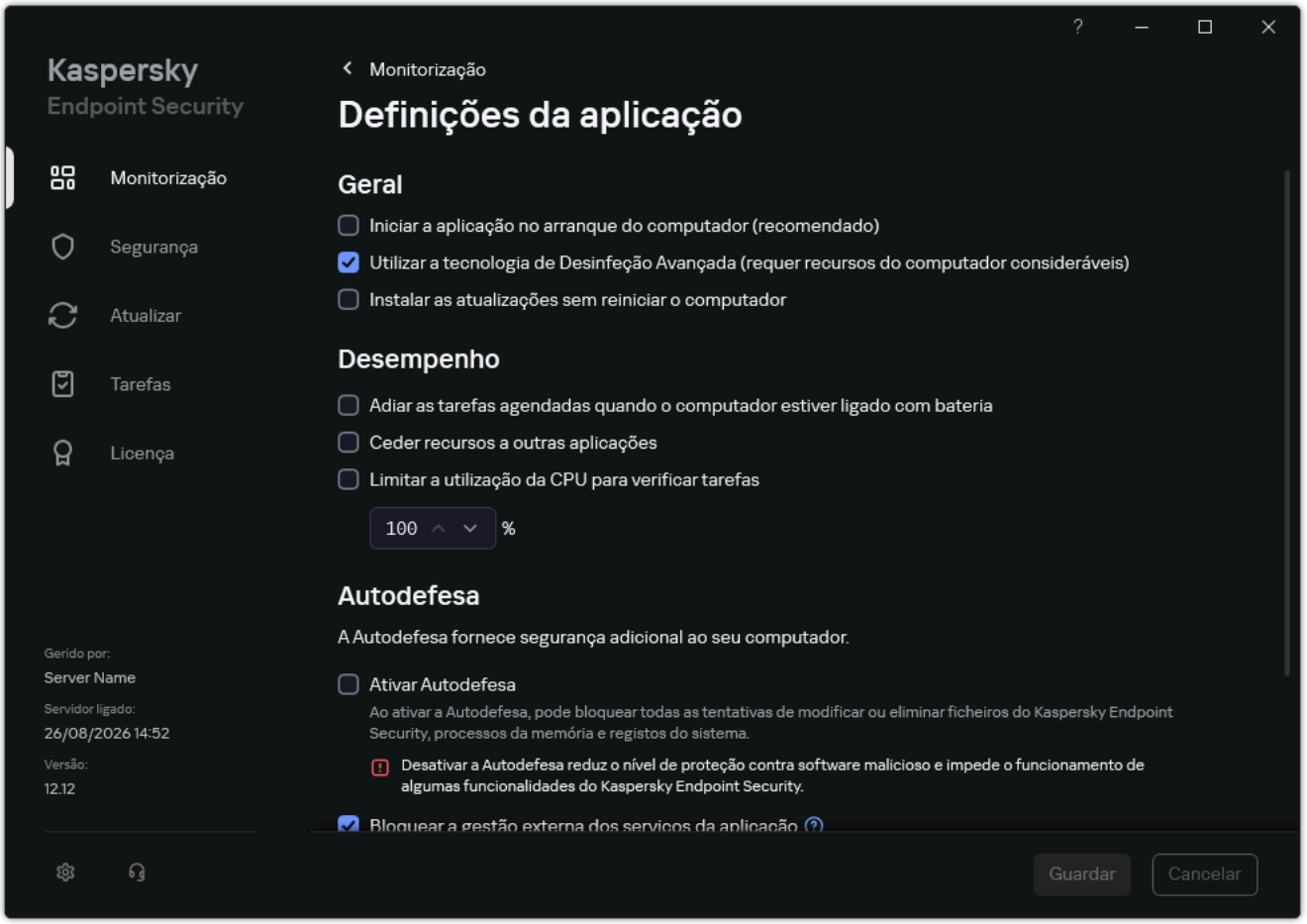
Como ativar ou desativar a Tecnologia de Desinfeção Avançada na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Selecione **General Settings** → **Detection Settings**.
5. No bloco **Advanced Disinfection Technology**, ative ou desative o botão **Advanced Disinfection Technology ENABLED** para ativar ou desativar a Tecnologia de Desinfeção Avançada.
6. Guarde as suas alterações.

Como ativar ou desativar a Tecnologia de Desinfeção Avançada na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Definições da aplicação**.



Definições do Kaspersky Endpoint Security for Windows

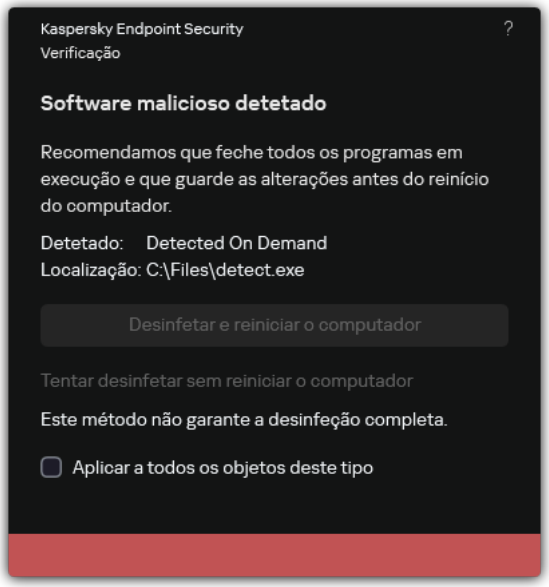
3. No bloco **Geral**, use a caixa de verificação **Utilizar a tecnologia de Desinfeção Avançada (requer recursos do computador consideráveis)** para ativar ou desativar a Tecnologia de Desinfeção Avançada.
4. Guarde as suas alterações.

O utilizador não irá conseguir usar a maioria das funcionalidades do sistema operativo enquanto a Desinfeção Avançada estiver em progresso. Quando a ligação estiver concluída, o computador será reiniciado.

Desinfeção de ameaças ativas em computadores

Para detetar ameaças ativas em computadores, ative a tecnologia Desinfeção avançada nas definições da aplicação. De seguida, configure a experiência do utilizador nas propriedades da tarefa *Verificação de software malicioso*. Existe uma caixa de verificação **Executar a Desinfeção Avançada imediatamente** nas propriedades da tarefa. Se a opção estiver ativa, o Kaspersky Endpoint Security irá realizar a desinfeção sem notificar o utilizador. Quando a ligação estiver concluída, o computador será reiniciado. Se a opção não estiver ativa, o Kaspersky Endpoint Security irá apresentar uma notificação sobre ameaças ativas (ver a figura abaixo). Não pode fechar esta notificação sem processar o ficheiro.

A Desinfeção Avançada durante uma tarefa de verificação de vírus num computador só é executada se a funcionalidade Desinfeção Avançada for ativada nas propriedades da política aplicada a este computador.



Notificação sobre ameaça ativa

Desinfeção de ameaças ativas em servidores

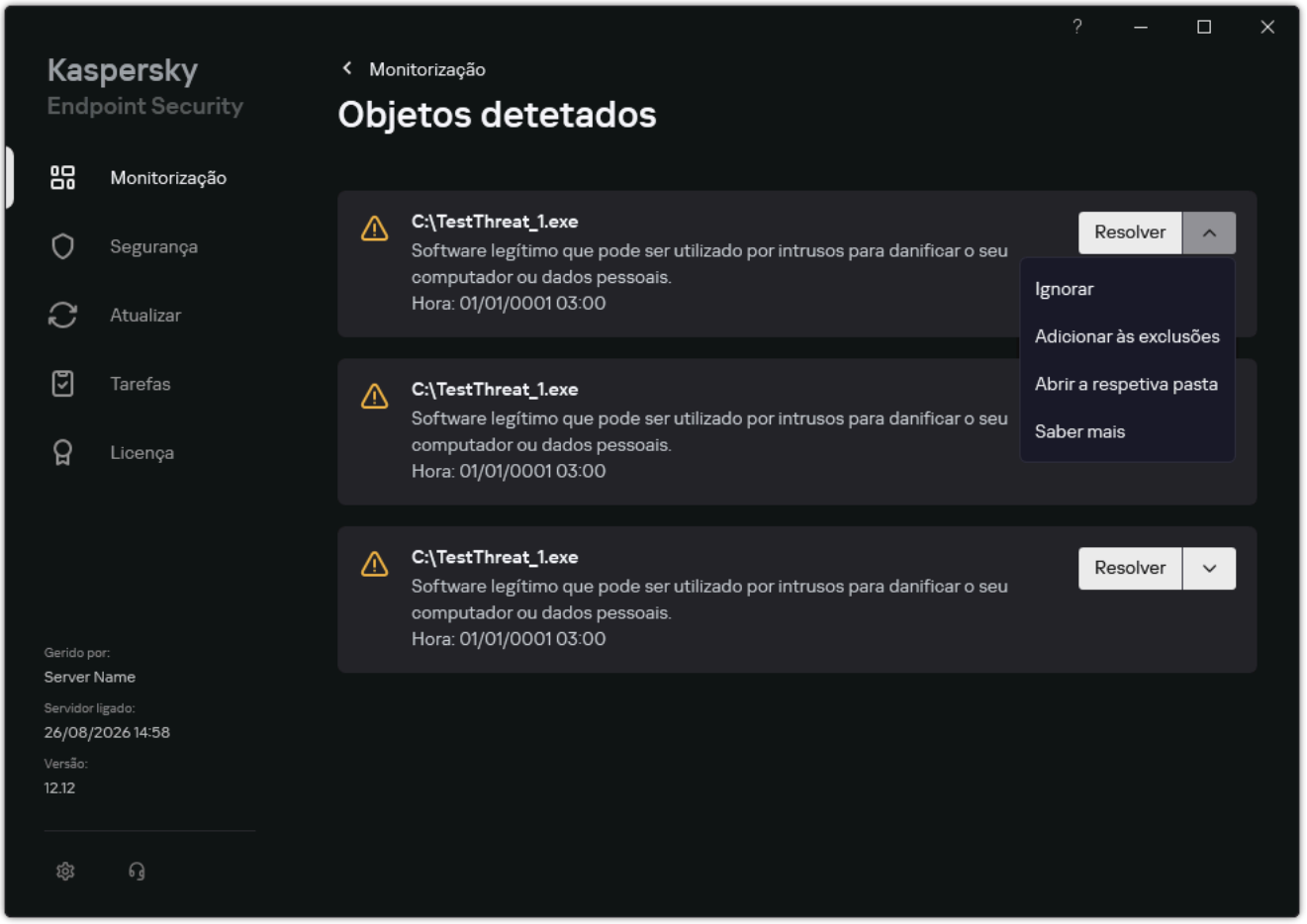
Para detetar ameaças ativas nos servidores, tem de fazer o seguinte:

- ativar a tecnologia Desinfeção avançada nas definições da aplicação;
- ativar a Desinfeção avançada imediata nas propriedades da tarefa *Verificação de software malicioso*.

Se o Kaspersky Endpoint Security for instalado num computador com o Windows para servidores, o Kaspersky Endpoint Security não apresenta a notificação. Como tal, não pode selecionar uma ação para desinfetar uma ameaça ativa. Para desinfetar uma ameaça, tem de Ativar Tecnologia de Desinfeção Avançada nas definições da aplicação e ativar a desinfeção avançada imediata nas definições da *Verificação de software malicioso*. Depois, tem de iniciar uma tarefa *Verificação de software malicioso*.

Eliminar ameaças não processadas

O Kaspersky Endpoint Security regista informações sobre ficheiros que, por algum motivo, não foram processados. Estas informações são registadas sob a forma de eventos na lista de ameaças ativas (ver a figura abaixo).



Uma lista de ameaças ativas

Um ficheiro infectado é considerado *processado* se o Kaspersky Endpoint Security tiver desinfetado o ficheiro ou removido a ameaça como parte da verificação de vírus e outro malware no computador.

O Kaspersky Endpoint Security move o ficheiro para a lista de ameaças ativas se, por alguma razão, não tiver conseguido executar uma ação nesse ficheiro conforme as definições da aplicação especificadas enquanto verificava a existência de vírus e outras ameaças no computador.

Esta situação é possível nos seguintes casos:

- O ficheiro verificado não está disponível (por exemplo, se estiver localizado numa unidade de rede ou unidade amovível sem privilégios de escrita).
- Nas definições da tarefa *Verificação de software malicioso*, a ação após deteção de ameaças é definida como **Informar**. Então, quando a notificação do ficheiro infetado foi apresentada no ecrã, o utilizador selecionou **Ignorar**.

Se houver alguma ameaça não processada, o Kaspersky Endpoint Security altera o ícone para . Na janela principal da aplicação, a notificação de ameaça é apresentada (ver a figura abaixo). No consola do Kaspersky Security Center, o estado do computador é alterado para *Critical* – .

Como processar uma ameaça na Consola de administração (MMC)

1. Na Consola de administração, aceda à pasta **Administration Server** → **Advanced** → **Repositories** → **Active threats**.

   Abre-se a lista de ameaças ativas.

2. Selecione o objeto que pretende processar.

3. Escolha de que forma pretende tratar da ameaça:

   - **Disinfect**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação elimina o ficheiro.

   - **Delete**. Se esta opção for selecionada, a aplicação irá excluir os ficheiros infetados detetados no repositório de ameaças ativas. Neste caso, a aplicação mantém o ficheiro detetado na memória do computador. Para eliminar a ameaça do computador, selecione **Disinfect**.

Como processar uma ameaça na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Operations** → **Repositories** → **Active threats**.

   Abre-se a lista de ameaças ativas.

2. Selecione o objeto que pretende processar.

3. Escolha de que forma pretende tratar da ameaça:

   - **Disinfect**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação elimina o ficheiro.

   - **Delete**. Se esta opção for selecionada, a aplicação irá excluir os ficheiros infetados detetados no repositório de ameaças ativas. Neste caso, a aplicação mantém o ficheiro detetado na memória do computador. Para eliminar a ameaça do computador, selecione **Disinfect**.

Como processar uma ameaça na interface da aplicação

1. Na janela principal da aplicação, na secção **Monitorização**, clique em **A proteção está em risco**.

   Abre-se a lista de ameaças ativas.

2. Selecione o objeto que pretende processar.

3. Escolha de que forma pretende tratar da ameaça:

   - **Resolver**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação elimina o ficheiro.

   - **Adicionar às exclusões**. Se esta ação for selecionada, o Kaspersky Endpoint Security sugere adicionar o ficheiro à lista de exclusões de verificação. As definições de exclusão são configuradas automaticamente. Se a adição de uma exclusão não estiver disponível, isso significa que o administrador desativaou a adição de exclusões nas definições da política.

   - **Ignorar**. Se esta opção for selecionada, o Kaspersky Endpoint Security elimina a entrada da lista de ameaças ativas. Se não restar nenhuma ameaça ativa na lista, o estado do computador altera-se para *OK*. Se o objeto voltar a ser detetado, o Kaspersky Endpoint Security adiciona uma nova entrada à lista de ameaças ativas.

- **Abrir a respetiva pasta**. Se esta opção for selecionada, o Kaspersky Endpoint Security abre a pasta que contém o objeto no gestor de ficheiros. Em seguida, poderá eliminar manualmente o objeto ou movê-lo para uma pasta que não se encontre dento do âmbito de proteção.

- **Saber mais**. Se esta opção for selecionada, o Kaspersky Endpoint Security abre o site da base de dados de vulnerabilidades e ameaças da Kaspersky.

Para processar ameaças ativas na consola do Kaspersky Security Center, deve ativar a transferência de informações sobre ficheiros não processados para o Servidor de Administração. A transferência de dados é ativada por defeito.

Como ativar a transferência de dados de ficheiros não processados na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais** → **Relatórios e armazenamento**.
4. No bloco **Transferência de dados para o Servidor de administração**, clique no botão **Definições**.
5. Selecione a caixa de verificação **Ficheiros não processados**.
6. Guarde as suas alterações.

Como ativar a transferência de dados de ficheiros não processados na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **KSC Integration**.

5. No bloco **Data transfer to Administration Server**, selecione a caixa de verificação **About unprocessed files**.

6. Guarde as suas alterações.



Janela principal da aplicação quando é detetada uma ameaça

Proteção do computador

Estado da Proteção em Tempo Real

O Kaspersky Endpoint Security envia a definição **Real-time protection status** para o Kaspersky Security Center Administration Server; o valor desta definição depende do estado atual dos componentes de proteção da aplicação no computador protegido (consulte a tabela abaixo).

O Kaspersky Endpoint Security determina o estado da proteção em tempo real com base no estado dos seguintes componentes da aplicação:

- Proteção contra ameaças de ficheiros.
- Proteção contra ameaças da Web.
- Proteção contra ameaças de correio.
- Proteção AMSI.
- Prevenção de ataques BadUSB.
- Proteção contra ameaças de Rede.
- Firewall.
- Prevenção de explorações.
- Deteção de comportamento.
- Motor de remediação.
- Prevenção contra invasões.

Pode verificar o estado da proteção em tempo real da aplicação numa consola do Kaspersky Security Center.

Como saber o estado da Proteção em tempo real na Administration Console (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Managed devices**.

O estado atual da Proteção em tempo real é apresentado na lista de dispositivos, na coluna **Real-time protection status**. Se a coluna **Real-time protection status** não estiver disponível, faça a gestão das definições das colunas clicando na ligação **Add/Remove Columns**.

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Managed devices**.

O estado atual da Proteção em tempo real é apresentado na lista de dispositivos, na coluna **Real-time protection status**. Se a coluna **Real-time protection status** não estiver disponível, faça a gestão das definições das colunas clicando na ligação **Add/Remove Columns**.

Como consultar a Proteção do computador em tempo real na Web Console

Na janela principal da Consola Web, selecione **Asset management** → **Assets (Devices)**.

O estado atual da Proteção em tempo real é apresentado na lista de dispositivos, na coluna **Real-time protection status**. Se a coluna **Real-time protection status** não estiver disponível, faça a gestão das definições das colunas (⚙).

Valores possíveis da definição Real-time protection status

Valor	Descrição
Unknown	O Servidor de Administração não dispõe de informações sobre o estado da proteção em tempo real deste computador.
Not installed	Não existem componentes instalados.
Not supported by license	A aplicação não está ativada ou a licença não permite o funcionamento dos componentes instalados.
Failed	Um ou mais componentes apresentam falhas.
Stopped	Um ou mais componentes estão desativados.
Paused	Um ou mais componentes estão em pausa.
Starting	Um ou mais componentes estão a ser ativados.
Running	Os componentes da aplicação estão em funcionamento.

Se o valor da definição **Real-time protection status** no Kaspersky Security Center for diferente de *Running*, verifique se os componentes instalados do Kaspersky Endpoint Security incluídos na lista estão ativados e se a aplicação está ativada.

Proteção contra ameaças de ficheiros

O componente Proteção contra ameaças de ficheiros permite-lhe impedir a infeção do sistema de ficheiros de um computador. Por predefinição, o componente de Proteção contra ameaças de ficheiros reside permanentemente na RAM do computador e verifica todos os ficheiros abertos, guardados ou executados em tempo real. Este componente verifica ficheiros em todas as unidades do computador, incluindo unidades conectadas. O componente fornece proteção ao computador com a ajuda das bases de dados antivírus, o serviço de nuvem da Kaspersky Security Network e análise heurística.

O componente verifica os ficheiros acedidos por um utilizador ou aplicação. Se for detetado um ficheiro malicioso, o Kaspersky Endpoint Security bloqueará a operação do ficheiro. A aplicação desinfeta ou elimina o ficheiro malicioso, dependendo das definições do componente Proteção contra ameaças de ficheiros.

Quando tenta aceder a um ficheiro cujos conteúdos são guardados no armazenamento da nuvem do OneDrive, o Kaspersky Endpoint Security transfere e verifica os conteúdos do ficheiro.

Ativar e desativar a Proteção contra ameaças de ficheiros

Por predefinição, o componente Proteção contra ameaças de ficheiros está ativado e é executado no modo recomendado pelos especialistas da Kaspersky. Para a Proteção contra ameaças de ficheiros, o Kaspersky Endpoint Security pode aplicar diferentes grupos de definições. Estes grupos de definições armazenados na aplicação chamam-se *níveis de segurança*: **Alto**, **Recomendado**, **Baixo**. Considera-se que as definições de nível de segurança **Recomendado** são as definições ideais recomendadas pelos especialistas da Kaspersky (consulte a tabela abaixo). Pode selecionar um dos níveis de segurança predefinidos ou configurar manualmente as definições do nível de segurança. Se alterar as definições de nível de segurança, pode sempre repor as definições de nível de segurança recomendadas.

O componente Proteção contra ameaças de ficheiros utiliza dados recebidos de outros componentes da aplicação. Ativar este componentes é opcional. Os componentes que fornecem dados adicionais incluem:

- Kaspersky Security Network.
- Prevenção contra invasões.
- Deteção de comportamento.

Como ativar ou desativar o componente Proteção contra ameaças de ficheiros na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de ficheiros**.
4. Use a caixa de verificação **Proteção contra ameaças de ficheiros** para ativar ou desativar o componente.
5. Se ativou este componente, execute uma das seguintes ações no bloco **Nível de segurança**:
    - Se quiser aplicar um dos níveis de segurança predefinidos, selecione-o com o controlo de deslize:
        - **Elevado**. Quando este nível de segurança de ficheiros está selecionado, o componente Proteção contra ameaças de ficheiros assume o controlo mais rigoroso de todos os ficheiros abertos, guardados e iniciados. O componente Proteção contra ameaças de ficheiros verifica todos os tipos de ficheiro em todos os discos rígidos, unidades amovíveis e unidades de rede do computador. Também verifica arquivos, pacotes de instalação e objetos OLE incorporados.
        - **Recomendado**. Esse nível de segurança de ficheiro é recomendado pelos especialistas da Kaspersky Lab. O componente Proteção contra ameaças de ficheiros apenas verifica os formatos de ficheiro especificados em todos os discos rígidos, unidades amovíveis, unidades de rede do computador e objetos de OLE incorporados. O componente Proteção contra ameaças de ficheiros não verifica arquivos ou pacotes de instalação.
        - **Baixo**. As definições deste nível de segurança do ficheiro garantem a velocidade máxima da verificação. O componente Proteção contra ameaças de ficheiros verifica apenas ficheiros com as extensões especificadas em todos os discos rígidos, unidades amovíveis e unidades de rede do computador. O componente Proteção contra ameaças de ficheiros não verifica ficheiros compostos.

- Se pretender configurar um nível de segurança personalizado, clique no botão **Definições** e defina as suas próprias definições do componente (consulte a tabela abaixo).

  Pode restaurar os valores dos níveis de segurança predefinidos ao clicar no botão **Por defeito**.

6. No bloco **Ação após deteção de ameaças**, selecione a ação executada pelo Kaspersky Endpoint Security em objetos maliciosos:

   - **Desinfetar, eliminar se a desinfeção falhar**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação elimina o ficheiro.
   - **Desinfetar, bloquear se a desinfeção falhar**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação bloqueia este ficheiro.
   - **Bloquear**. Se esta opção for selecionada, a aplicação bloqueia automaticamente o ficheiro infetado sem tentar desinfetá-lo ou eliminá-lo.
   - **Informar**. Se esta opção for selecionada, o Kaspersky Endpoint Security adiciona a informação sobre ficheiros infetados à lista de ameaças ativas na deteção destes ficheiros.

   Antes de tentar desinfetar ou eliminar um ficheiro infetado, a aplicação cria uma cópia de segurança do ficheiro para o caso de vir a precisar de o restaurar ou de o mesmo poder ser desinfetado no futuro.

7. Guarde as suas alterações.

Como ativar ou desativar o componente Proteção contra ameaças de ficheiros na Web Console e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **File Threat Protection**.
5. Use o botão de alternar da **File Threat Protection ENABLED** para ativar ou desativar o componente.
6. Se pretender adicionar um novo objeto ao âmbito de proteção:

   a. Sob **Advanced settings**, selecione a aba **Protection scope**.

   b. Clique em **Add**.

   c. Isto abre uma janela; nessa janela, selecione os objetos que pretende adicionar ao âmbito de proteção.

Usar máscaras:

- O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.

- Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

- O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.

Pode usar máscaras em qualquer lugar no caminho de um ficheiro ou pasta. Por exemplo, se quiser que o âmbito de verificação inclua a pasta Downloads para todas as contas de utilizador no computador, introduza a máscara `C:\Users\*\Downloads\`.

Pode excluir um objeto da proteção sem o remover da lista de objetos no âmbito de proteção. Para tal, desative o botão ao lado do mesmo.

d. Guarde as suas alterações.

7. No bloco **Action on threat detection**, selecione a ação executada pelo Kaspersky Endpoint Security em objetos maliciosos:

   - **Disinfect, delete if disinfection fails**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação elimina o ficheiro.

   - **Disinfect, block if disinfection fails**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação bloqueia este ficheiro.

   - **Block**. Se esta opção for selecionada, a aplicação bloqueia automaticamente o ficheiro infetado sem tentar desinfetá-lo ou eliminá-lo.

   Antes de tentar desinfetar ou eliminar um ficheiro infetado, a aplicação cria uma cópia de segurança do ficheiro para o caso de vir a precisar de o restaurar ou de o mesmo poder ser desinfetado no futuro.

8. Se necessário, edite as definições avançadas de Proteção contra ameaças de ficheiros.

9. Guarde as suas alterações.

Como ativar ou desativar o componente Proteção contra ameaças de ficheiros na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de ficheiros**.

3. Use o botão de alternar da **Proteção contra ameaças de ficheiros** para ativar ou desativar o componente.

4. Se ativou este componente, execute uma das seguintes ações no bloco **Nível de segurança**:

   - Se quiser aplicar um dos níveis de segurança predefinidos, selecione-o com o controlo de deslize:

     - **Alto**. Quando este nível de segurança de ficheiros está selecionado, o componente Proteção contra ameaças de ficheiros assume o controlo mais rigoroso de todos os ficheiros abertos, guardados e iniciados. O componente Proteção contra ameaças de ficheiros verifica todos os tipos de ficheiro em todos os discos rígidos, unidades amovíveis e unidades de rede do computador. Também verifica arquivos, pacotes de instalação e objetos OLE incorporados.

     - **Recomendado**. Esse nível de segurança de ficheiro é recomendado pelos especialistas da Kaspersky Lab. O componente Proteção contra ameaças de ficheiros apenas verifica os formatos de ficheiro especificados em todos os discos rígidos, unidades amovíveis, unidades de rede do computador e objetos de OLE incorporados. O componente Proteção contra ameaças de ficheiros não verifica arquivos ou pacotes de instalação.

     - **Baixo**. As definições deste nível de segurança do ficheiro garantem a velocidade máxima da verificação. O componente Proteção contra ameaças de ficheiros verifica apenas ficheiros com as extensões especificadas em todos os discos rígidos, unidades amovíveis e unidades de rede do computador. O componente Proteção contra ameaças de ficheiros não verifica ficheiros compostos.

   - Se pretender configurar um nível de segurança personalizado, clique no botão **Definições avançadas** e defina as suas próprias definições do componente (consulte a tabela abaixo).

     Pode restaurar os valores dos níveis de segurança predefinidos ao clicar no botão **Restaurar nível de segurança recomendado**.

5. No bloco **Ação após deteção de ameaças**, selecione a ação executada pelo Kaspersky Endpoint Security em objetos maliciosos:

   - **Desinfetar, eliminar se a desinfeção falhar**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação elimina o ficheiro.

   - **Desinfetar, bloquear se a desinfeção falhar**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação bloqueia este ficheiro.

   - **Bloquear**. Se esta opção for selecionada, a aplicação bloqueia automaticamente o ficheiro infetado sem tentar desinfetá-lo ou eliminá-lo.

   - **Informar**. Se esta opção for selecionada, o Kaspersky Endpoint Security adiciona a informação sobre ficheiros infetados à lista de ameaças ativas na deteção destes ficheiros.

   Antes de tentar desinfetar ou eliminar um ficheiro infetado, a aplicação cria uma cópia de segurança do ficheiro para o caso de vir a precisar de o restaurar ou de o mesmo poder ser desinfetado no futuro.

6. Guarde as suas alterações.

Definições da Proteção contra ameaças de ficheiros recomendadas pelos especialistas da Kaspersky (nível de segurança recomendado)

Parâmetro	Valor	Descrição
Tipos de ficheiros	**Ficheiros verificados por formato**	Se esta configuração estiver ativada, a aplicação verifica apenas ficheiros infetáveis. Antes de verificar um ficheiro para código malicioso, o cabeçalho interno do ficheiro é analisado para determinar o formato do ficheiro (por exemplo, .txt, .doc ou .exe). A verificação também procura ficheiros com extensões de ficheiro específicas.
Análise heurística	**Nível superficial**	A tecnologia foi desenvolvida para detetar ameaças que não é possível detetar utilizando a versão atual das bases de dados da aplicação da Kaspersky. Permite detetar ficheiros que podem estar infetados com um vírus desconhecido ou com uma variante de um vírus conhecido. Ao verificar ficheiros de códigos maliciosos, o analisador heurístico executa instruções nos ficheiros executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível da análise heurística garante um equilíbrio entre o detalhe das procuras de novas ameaças, a carga nos recursos do sistema operativo e a duração da análise heurística.
Verificar apenas os ficheiros novos e modificados	**Ativado**	Verifica apenas os ficheiros novos e os que foram modificados desde a última vez em que foram verificados. Isto ajuda a reduzir a duração de uma verificação. Este modo aplica-se a ficheiros simples e compostos.
Utilizar tecnologia iSwift	**Ativado**	Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. A tecnologia iSwift é um avanço da tecnologia iChecker para o sistema de ficheiros NTFS.
Utilizar tecnologia iChecker	**Ativado**	Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. Existem limites para a tecnologia iChecker: não funciona com ficheiros grandes e aplica-se apenas a ficheiros com uma estrutura que o Kaspersky Internet Security reconheça (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).
Verificar ficheiros em formatos do Microsoft Office	**Ativado**	Verifica ficheiros do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Ficheiros de formato do Office incluem objetos OLE também. A aplicação verifica ficheiros em formato de escritório menores que 1 MB, independentemente de a caixa de seleção estar marcada ou não.
Verificar ficheiros de formatos de e-mail	**Ativado**	Verifica ficheiros em formato de e-mail. A aplicação verifica ficheiros MSG e EML. Ficheiros em formato de e-mail incluem objetos OLE e ficheiros MHT também. O Kaspersky Endpoint Security verifica ficheiros de e-mail com menos de 1 MB, independentemente de a caixa de seleção estar marcada ou não.
Modo de verificação	**Modo inteligente**	Neste modo, a Proteção contra ameaças de ficheiros verifica um objeto com base numa análise das ações tomadas relativamente ao objeto. Por exemplo, ao trabalhar com um documento do Microsoft Office, o Kaspersky Endpoint Security verifica o ficheiro quando é aberto pela primeira vez e fechado pela última vez. As operações intermédias gravadas no ficheiro não fazem com que o mesmo seja verificado.
Ação após deteção de ameaças	**Desinfetar, eliminar se a desinfeção falhar**	Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação elimina o ficheiro.

Pausa automática da Proteção contra ameaças de ficheiros

Pode configurar a Proteção contra ameaças de ficheiros para pausar automaticamente a uma hora especificada ou ao funcionar com aplicações específicas.

A Proteção contra ameaças de ficheiros apenas deve ser colocada em pausa como último recurso se entrar em conflito com algumas aplicações. Se surgir algum conflito durante a execução de um componente, recomendamos que contacte o Suporte Técnico da Kaspersky. Os especialistas do suporte irão ajudá-lo a configurar o componente Proteção contra ameaças de ficheiros para ser executado simultaneamente com outras aplicações no seu computador.

Para configurar a pausa automática da Proteção contra ameaças de ficheiros:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de ficheiros**.
3. Clique em **Definições avançadas**.
4. No bloco **Pausar a proteção contra ameaças de ficheiros**, clique na ligação **Pausar a proteção contra ameaças de ficheiros**.
5. Na janela que abre, configure as definições para pôr em pausa a proteção contra ameaças de ficheiros:
   a. Configure uma agenda para pôr automaticamente em pausa a proteção contra ameaças de ficheiros.
   b. Crie uma lista de aplicações cuja operação deverá provocar a colocação em pausa da proteção contra ameaças de ficheiros para interromper as suas atividades.
6. Guarde as suas alterações.

Alterar a ação a executar em ficheiros infetados pelo componente Proteção contra ameaças de ficheiros

Por predefinição, o componente Proteção contra ameaças de ficheiros tenta automaticamente desinfetar todos os ficheiros infetados que tenham sido detetados. Se a desinfeção falhar, o componente Proteção contra ameaças de ficheiros elimina estes ficheiros.

Para alterar a ação a executar em ficheiros infetados pelo componente Proteção contra ameaças de ficheiros:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de ficheiros**.
3. No bloco **Ação após deteção de ameaças**, selecione a opção relevante:
   - **Desinfetar, eliminar se a desinfeção falhar**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação elimina o ficheiro.
   - **Desinfetar, bloquear se a desinfeção falhar**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação bloqueia este ficheiro.
   - **Bloquear**. Se esta opção for selecionada, a aplicação bloqueia automaticamente o ficheiro infetado sem tentar desinfetá-lo ou eliminá-lo.

Antes de tentar desinfetar ou eliminar um ficheiro infetado, a aplicação cria uma cópia de segurança do ficheiro para o caso de vir a precisar de o restaurar ou de o mesmo poder ser desinfetado no futuro.

4. Guarde as suas alterações.

Formar o âmbito de proteção do componente Proteção contra ameaças de ficheiros

O âmbito de proteção refere-se aos objetos que o componente verifica quando ativado. Os âmbitos de proteção de componentes diferentes têm propriedades diferentes. A localização e o tipo de ficheiros a verificar são propriedades do âmbito de proteção do componente Proteção contra ameaças de ficheiros. Por predefinição, o componente Proteção contra ameaças de ficheiros verifica apenas os ficheiros potencialmente infetáveis que são executados a partir de discos rígidos, unidades amovíveis e unidades de rede.

Ao selecionar o tipo de ficheiros a verificar, tenha em atenção o seguinte:

1. Há uma baixa probabilidade de introduzir código malicioso em ficheiros de determinados formatos e a sua subsequente ativação (por exemplo, formato TXT). Por outro lado, existem formatos de ficheiro que contêm código executável (tais como .exe, .dll). O código executável pode também estar contido em ficheiros de formatos que não se destinam para esta finalidade (por exemplo, o formato DOC). O risco de intrusão e ativação de código malicioso nesses ficheiros é elevado.

2. Um intruso pode enviar um vírus ou outro aplicação maliciosa para o computador num ficheiro executável cujo nome tenha sido mudado para a extensão .txt. Se selecionar a verificação de ficheiros por extensão, a aplicação omite este ficheiro durante a verificação. Se a verificação de ficheiros por formato for selecionada, o Kaspersky Endpoint Security analisa o cabeçalho do ficheiro, independentemente da sua extensão. Se esta análise revelar que o ficheiro tem o formato de um ficheiro executável, a aplicação verifica-o.

Para criar o âmbito de proteção:

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de ficheiros**.

3. Clique em **Definições avançadas**.

4. No bloco **Tipos de ficheiros**, especifique o tipo de ficheiros que pretende que o componente Proteção contra ameaças de ficheiros verifique:

   - **Todos os ficheiros**. Se esta definição estiver ativada, o Kaspersky Endpoint Security verifica todos os ficheiros sem exceção (todos os formatos e extensões).

   - **Ficheiros verificados por formato**. Se esta configuração estiver ativada, a aplicação verifica apenas ficheiros infetáveis. Antes de verificar um ficheiro para código malicioso, o cabeçalho interno do ficheiro é analisado para determinar o formato do ficheiro (por exemplo, .txt, .doc ou .exe). A verificação também procura ficheiros com extensões de ficheiro específicas.

   - **Ficheiros verificados por extensão**. Se esta configuração estiver ativada, a aplicação verifica apenas ficheiros infetáveis. O formato do ficheiro é então determinado com base na extensão do ficheiro.

5. Clique na hiperligação **Editar âmbito de proteção**.

6. Na janela que abre, selecione os objetos que deseja adicionar ao âmbito de proteção ou excluir do mesmo.

   Não é possível remover ou editar objetos que estejam incluídos no âmbito de proteção predefinido.

7. Se pretender adicionar um novo objeto ao âmbito de proteção:

   a. Clique em **Adicionar**.

      Abre-se a árvore de pastas.

   b. No campo **Caminho**, introduza o caminho para a pasta ou ficheiro.

      Usar máscaras:

      - O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.

      - Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

      - O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.

      Pode usar máscaras em qualquer lugar no caminho de um ficheiro ou pasta. Por exemplo, se quiser que o âmbito de verificação inclua a pasta Downloads para todas as contas de utilizador no computador, introduza a máscara `C:\Users\*\Downloads\`.

      O objeto **Este PC** na lista de recursos do ficheiro do computador inclui os seguintes objetos: **Todos os discos rígidos**, **Todos os discos de rede** e **Todas as unidades amovíveis**.

   Pode excluir um objeto das verificações sem o eliminar da lista de objetos no âmbito de verificação. Para o fazer, desmarque a caixa de verificação ao lado do objeto.

8. Guarde as suas alterações.

Utilizar métodos de verificação

O Kaspersky Endpoint Security utiliza uma técnica de verificação chamada Aprendizagem automática e análise de assinaturas. Durante a análise de assinaturas, o Kaspersky Endpoint Security faz corresponder o objeto detetado a registos na respetiva base de dados. Com base nas recomendações dos especialistas da Kaspersky, a aprendizagem automática e a análise de assinaturas estão sempre ativadas.

Para aumentar a eficácia da proteção, pode utilizar a análise heurística. Ao verificar ficheiros de códigos maliciosos, o analisador heurístico executa instruções nos ficheiros executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível da análise heurística garante um equilíbrio entre o detalhe das procuras de novas ameaças, a carga nos recursos do sistema operativo e a duração da análise heurística.

Para configurar a utilização da análise heurística no funcionamento do componente Proteção contra ameaças de ficheiros:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de ficheiros**.
3. Clique em **Definições avançadas**.
4. Se quiser que a aplicação utilize análise heurística para proteção contra ameaças de ficheiros, selecione a caixa de verificação **Análise heurística** no bloco **Métodos de verificação**. Utilize então a barra de deslocamento para definir o nível da análise heurística: **Nível superficial**, **Nível médio** ou **Nível avançado**.
5. Guarde as suas alterações.

Utilizar tecnologias de verificação no funcionamento do componente Proteção contra ameaças de ficheiros

Para configurar a utilização de tecnologias de verificação no funcionamento do componente Proteção contra ameaças de ficheiros:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de ficheiros**.
3. Clique em **Definições avançadas**.
4. Na secção **Tecnologias de verificação**, selecione as caixas de verificação junto aos nomes das tecnologias que pretende utilizar para a proteção contra ameaças de ficheiros:
   - **Utilizar tecnologia iSwift**. Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. A tecnologia iSwift é um avanço da tecnologia iChecker para o sistema de ficheiros NTFS.
   - **Utilizar tecnologia iChecker**. Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. Existem limites para a tecnologia iChecker: não funciona com ficheiros grandes e aplica-se apenas a ficheiros com uma estrutura que o Kaspersky Internet Security reconheça (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).
5. Guarde as suas alterações.

Otimizar a verificação de ficheiros

Pode otimizar a verificação de ficheiros realizada pelo componente Proteção contra ameaças de ficheiros reduzindo o tempo de verificação e aumentando a velocidade de funcionamento do Kaspersky Endpoint Security. Isto pode ser conseguido, verificando apenas os ficheiros novos e os ficheiros que foram modificados desde a verificação anterior. Este modo aplica-se a ficheiros simples e compostos.

Também pode ativar a utilização das tecnologias iChecker e iSwift que otimizam a velocidade da verificação de ficheiros, excluindo os ficheiros que não foram modificados desde a verificação mais recente.

Para otimizar a verificação de ficheiros:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de ficheiros**.
3. Clique em **Definições avançadas**.
4. No bloco **Otimização**, selecione a caixa de verificação **Verificar apenas os ficheiros novos e modificados**.
5. Guarde as suas alterações.

Verificação de ficheiros compostos

Uma técnica comum de ocultar vírus e outro software malicioso consiste em implantá-los em ficheiros compostos, como arquivos ou bases de dados. Para detetar vírus e outro software malicioso que estejam ocultos desta forma, é necessário descompactar o ficheiro composto, o que pode reduzir a velocidade da verificação. Pode limitar o tipo de ficheiros compostos a verificar, acelerando assim a verificação.

O método utilizado para processar um ficheiro composto infetado (desinfeção ou eliminação) depende do tipo do ficheiro.

O componente Proteção contra ameaças de ficheiros desinfeta os ficheiros compostos nos formatos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR e ICE e elimina os ficheiros em todos os outros formatos (exceto bases de dados de correio).

Para configurar a verificação de ficheiros compostos:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de ficheiros**.
3. Clique em **Definições avançadas**.

4. No bloco **Verificação de ficheiros compostos**, especifique os tipos de ficheiros compostos que pretende verificar: arquivos, pacotes de distribuição, ficheiros em formatos de correio ou do office.

5. Se a verificação apenas de ficheiros novos e modificados estiver desativada, configure as definições para verificar cada tipo de ficheiro composto: verificar todos os ficheiros deste tipo ou apenas os novos ficheiros.

   Se a verificação apenas de ficheiros novos e modificados estiver ativada, o Kaspersky Endpoint Security verifica apenas ficheiros novos e modificados de todos os tipos de ficheiros compostos.

6. Configure as definições avançadas para verificar ficheiros compostos.

   - **Não descompactar ficheiros compostos extensos**.

     Se esta caixa de verificação estiver selecionada, o Kaspersky Endpoint Security não verifica ficheiros compostos se o tamanho destes exceder o valor especificado.

     Se esta caixa de verificação for desmarcada, o Kaspersky Endpoint Security verifica ficheiros compostos de todos os tamanhos.

     > O Kaspersky Endpoint Security verifica ficheiros extensos extraídos de arquivos, independentemente de a caixa de verificação **Não descompactar ficheiros compostos extensos** estar selecionada.

   - **Descompactar ficheiros compostos em 2.º plano**.

     Se a caixa de seleção estiver assinalada, o Kaspersky Endpoint Security fornece acesso a ficheiros compostos que são maiores do que o valor especificado antes da verificação desses ficheiros. Neste caso, o Kaspersky Endpoint Security descompacta e verifica os ficheiros compostos em segundo plano.

     Kaspersky Endpoint Security fornece acesso a ficheiros compostos mais pequenos que esse valor somente após descompactar e verificar esses ficheiros.

     Se a caixa de seleção não estiver assinalada, o Kaspersky Endpoint Security apenas fornece acesso a ficheiros compostos após descompactar e verificar os ficheiros de qualquer tamanho.

7. Guarde as suas alterações.

Alterar o modo de verificação

O *Modo de verificação* refere-se à condição que aciona a verificação de ficheiros pelo componente Proteção contra ameaças de ficheiros. Por predefinição, o Kaspersky Endpoint Security verifica os ficheiros no modo inteligente. Neste modo de verificação de ficheiros, o componente Proteção contra ameaças de ficheiros decide se deve ou não verificar os ficheiros após analisar as operações executadas com o ficheiro pelo utilizador, por uma aplicação em nome do utilizador (com a conta utilizada para iniciar sessão ou com uma conta de utilizador diferente) ou pelo sistema operativo. Por exemplo, quando trabalhar com um documento do Microsoft Office Word, o Kaspersky Endpoint Security verifica o ficheiro, primeiro, quando este é aberto e, por último, quando este é fechado. As operações intermédias gravadas no ficheiro não fazem com que o mesmo seja verificado.

Para alterar o modo de verificação de ficheiros:

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de ficheiros**.

3. Clique em **Definições avançadas**.

4. No bloco **Modo de verificação**, selecione o modo pretendido:

   - **Modo inteligente**. Neste modo, a Proteção contra ameaças de ficheiros verifica um objeto com base numa análise das ações tomadas relativamente ao objeto. Por exemplo, ao trabalhar com um documento do Microsoft Office, o Kaspersky Endpoint Security verifica o ficheiro quando é aberto pela primeira vez e fechado pela última vez. As operações intermédias gravadas no ficheiro não fazem com que o mesmo seja verificado.

   - **Ao aceder e modificar**. Neste modo, a Proteção contra ameaças de ficheiros verifica os objetos sem que há uma tentativa para os abrir ou modificar.

   - **Ao aceder**. Neste modo, a Proteção contra ameaças de ficheiros verifica os objetos apenas aquando de uma tentativa para os abrir.

   - **Ao executar**. Neste modo, a Proteção contra ameaças de ficheiros verifica os objetos aquando de uma tentativa para os executar.

5. Guarde as suas alterações.

Verificação de Contentores

Um *contentor* é um ambiente isolado no qual uma aplicação pode ser executada sem interagir diretamente com o sistema operativo. A utilização de contentores envolve os seguintes riscos:

- Os hackers podem explorar vulnerabilidades de contentorização para comprometer aplicações dentro do contentor.

- Os hackers podem explorar uma configuração insegura do ambiente do contentor para obter acesso não autorizado aos dados no computador ou para comprometer a integridade do sistema.

- Um ataque bem-sucedido a um contentor pode permitir que um hacker tenha acesso aos dados no computador.

- Os hackers podem explorar as vulnerabilidades da rede para intercetar o tráfego da rede.

O Kaspersky Endpoint Security analisa ficheiros não apenas em discos, mas também dentro de contentores. Ou seja, o Kaspersky Endpoint Security é uma ferramenta externa para descobrir atividade maliciosa dentro de contentores. Isto permite manter o desempenho dos contentores e evita conflitos com outras aplicações dentro do contentor. A instalação do Kaspersky Endpoint Security dentro do contentor não é suportada.

Para além de fornecer segurança de contentores, o Kaspersky Endpoint Security permite gerir aplicações dentro de contentores através do Controlo das Aplicações. O Controlo das Aplicações é configurado para os contentores da mesma forma que para as aplicações instaladas no computador. A Monitorização da Integridade do Sistema também suporta contentores.

Requisitos dos contentores

- O contentor tem de ser um contentor Docker. Não são suportadas outras ferramentas de contentorização.

- O contentor tem de ser executado no modo de isolamento de processos. O modo de isolamento do Hyper-V não é suportado.

- O contentor tem de ser colocado num servidor Windows Server 2016, 2019 ou 2022 (Docker Host).
- O contentor tem de incluir uma imagem do Windows (Docker Image). O Windows 10 e 11 não são suportados. As imagens Linux não são suportadas.

Ação após deteção de ameaças

Se uma ameaça for detetada dentro de um contentor, a aplicação aplica a ação selecionada para o componente Proteção contra ameaças de ficheiros. A Verificação de Contentores tem definições adicionais (veja as instruções abaixo). Se uma ameaça for detetada, a aplicação bloqueia a atividade maliciosa e executa a ação selecionada (por exemplo, tenta desinfetar o objeto). O Kaspersky Endpoint Security pode parar o contentor se o objeto detetado não puder ser desinfetado. Por padrão, a funcionalidade de paragem do contentor está desativada.

Como configurar a verificação de contentores na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de ficheiros**.
4. Clique em **Definições**.
5. Esta ação abre uma janela; nessa janela, selecione o separador **Adicional**.
6. No bloco **Verificação das operações de ficheiros executadas em contentores do Windows**, configure as definições de verificação dos contentores:
   - **Parar o contentor se a desinfeção falhar**. A aplicação pode não ter direitos de leitura e gravação suficientes para o objeto detetado. Nesse caso, não é possível desinfetar ou eliminar o objeto detetado. Se esta caixa de verificação estiver selecionada, a aplicação bloqueia o objeto detetado e para o contentor. Se esta caixa de verificação estiver desmarcada, a aplicação apenas bloqueia o objeto detetado.
   - **Não verificar operações de ficheiros executadas em contentores do Windows**. Se a caixa de verificação estiver selecionada, a aplicação verifica o contentor apenas no arranque do contentor. Se a caixa de verificação estiver desmarcada, a aplicação analisa o contentor continuamente em tempo real.
7. Guarde as suas alterações.

Como configurar a verificação de contentores na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **File Threat Protection**.
5. Sob **Advanced settings**, selecione a aba **Performance**.

6. No bloco **Scan optimization**, configure as definições de verificação dos contentores:

   - **Stop container if disinfection fails**. A aplicação pode não ter direitos de leitura e gravação suficientes para o objeto detetado. Nesse caso, não é possível desinfetar ou eliminar o objeto detetado. Se esta caixa de verificação estiver selecionada, a aplicação bloqueia o objeto detetado e para o contentor. Se esta caixa de verificação estiver desmarcada, a aplicação apenas bloqueia o objeto detetado.

   - **Do not scan file operations executed in Windows containers**. Se a caixa de verificação estiver selecionada, a aplicação verifica o contentor apenas no arranque do contentor. Se a caixa de verificação estiver desmarcada, a aplicação analisa o contentor continuamente em tempo real.

7. Guarde as suas alterações.

Como configurar a verificação de contentores na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de ficheiros**.

3. No bloco **Verificação das operações de ficheiros executadas em contentores do Windows**, configure as definições de verificação dos contentores:

   - **Parar o contentor se a desinfeção falhar**. A aplicação pode não ter direitos de leitura e gravação suficientes para o objeto detetado. Nesse caso, não é possível desinfetar ou eliminar o objeto detetado. Se esta caixa de verificação estiver selecionada, a aplicação bloqueia o objeto detetado e para o contentor. Se esta caixa de verificação estiver desmarcada, a aplicação apenas bloqueia o objeto detetado.

   - **Não verificar operações de ficheiros executadas em contentores do Windows**. Se a caixa de verificação estiver selecionada, a aplicação verifica o contentor apenas no arranque do contentor. Se a caixa de verificação estiver desmarcada, a aplicação analisa o contentor continuamente em tempo real.

4. Guarde as suas alterações.

Prevenção contra invasões

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para estações de trabalho. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para servidores.

O componente Prevenção contra invasões impede as aplicações de executarem ações que possam ser perigosas para o sistema operativo e garante o controlo do acesso aos recursos do sistema operativo e a dados pessoais. O componente fornece proteção ao computador com a ajuda das bases de dados antivírus e o serviço de nuvem da Kaspersky Security Network.

O componente controla a operação de aplicações utilizando *direitos da aplicação*. Os direitos da aplicação incluem os seguintes parâmetros de acesso:

- Acesso aos recursos do sistema operativo (por exemplo, opções de inicialização automática, chaves de registo)
- Acesso a dados pessoais (por exemplo, ficheiros e aplicações)

A atividade de rede das aplicações é controlada pelo componente da Firewall usando *regras de rede*.

Durante a primeira inicialização da aplicação, o componente Prevenção de Intrusão do Host executa as seguintes ações:

1. Verifica a segurança da aplicação ao usar bases de dados antivírus transferidas.
2. Verifica a segurança da aplicação na Kaspersky Security Network.

   Recomenda-se que participe na Kaspersky Security Network para ajudar o componente Prevenção contra invasões a funcionar de forma mais eficiente.

3. Coloca a aplicação num dos grupos de confiança: *Fiáveis*, *Restrições baixas*, *Restrições altas*, *Não fiáveis*.

   Um grupo fiável define os direitos em que o Kaspersky Endpoint Security se baseia para controlar a atividade da aplicação. O Kaspersky Endpoint Security coloca uma aplicação num grupo fiável, dependendo do nível de perigo que essa aplicação pode representar para o computador.

   O Kaspersky Endpoint Security coloca uma aplicação num grupo fiável para os componentes Firewall e Prevenção de Intrusão do Host. Não pode alterar o grupo fiável apenas para a Firewall ou Prevenção contra invasões.

   Caso se tenha recusado participar na KSN ou não haja rede, o Kaspersky Endpoint Security coloca a aplicação num grupo fiável, dependendo das definições do componente Prevenção de Intrusão do Host. Após receber a reputação da aplicação da KSN, o grupo fiável pode ser alterado automaticamente.

4. Bloqueia as ações da aplicação, dependendo do grupo fiável. Por exemplo, aplicações do grupo fiável *Restrições altas* têm acesso negado aos módulos do sistema operativo.

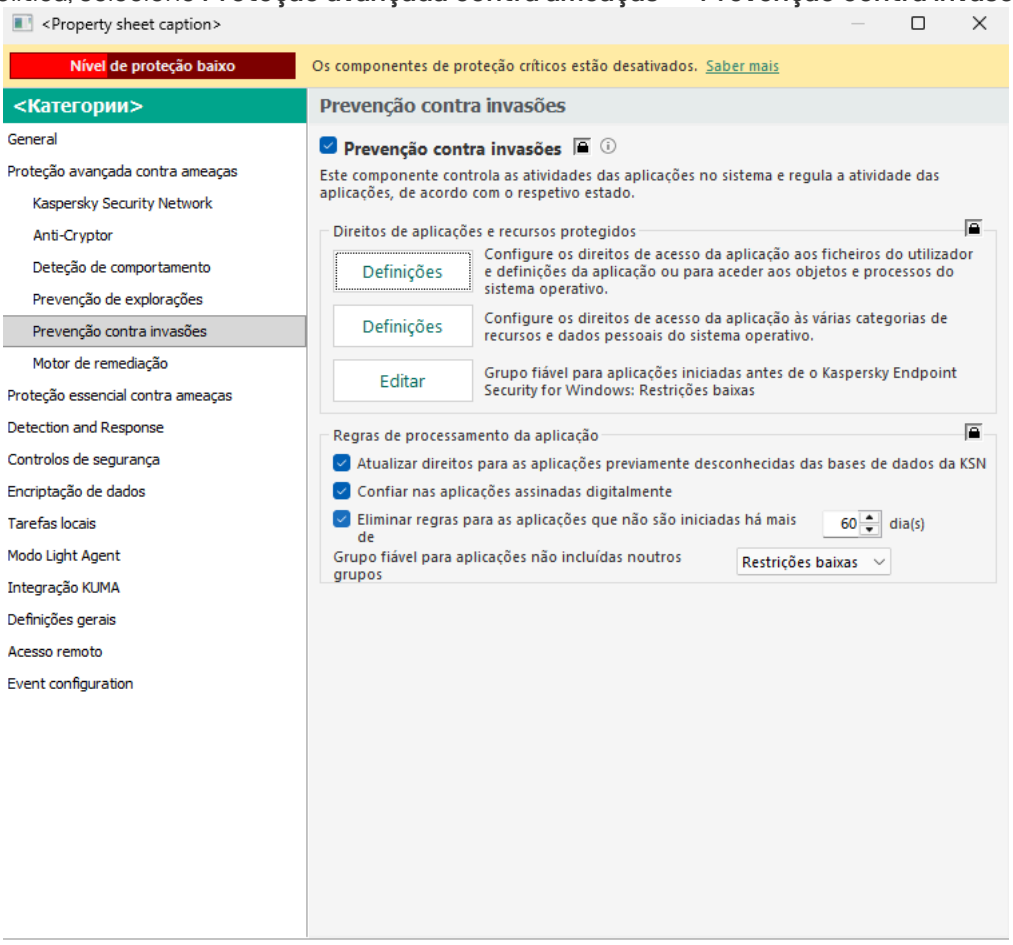
Na próxima vez que a aplicação for iniciada, o Kaspersky Endpoint Security verifica a integridade da aplicação. Se a aplicação não tiver sido modificada, o componente utiliza os direitos atuais da aplicação. Se a aplicação tiver sido modificada, a Kaspersky Endpoint Security analisa a aplicação como se estivesse a ser iniciada pela primeira vez.

Ativar e desativar a Prevenção contra invasões

Por predefinição, a Prevenção contra invasões está ativada e é executada no modo recomendado pelos especialistas da Kaspersky.

Como ativar ou desativar o componente Prevenção contra invasões na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção avançada contra ameaças → Prevenção contra invasões**.



Definições da Prevenção contra intrusões

4. Use a caixa de verificação **Prevenção contra invasões** para ativar ou desativar o componente.
5. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar ou desativar o componente Prevenção contra invasões na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection → Host Intrusion Prevention**.
5. Use o botão de alternar da **Host Intrusion Prevention ENABLED** para ativar ou desativar o componente.
6. Guarde as suas alterações.

Como ativar ou desativar o componente Prevenção contra invasões na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção avançada contra ameaças → Prevenção contra invasões**.
3. Use o botão de alternar da **Prevenção contra invasões** para ativar ou desativar o componente.
4. Guarde as suas alterações.

Se o componente Prevenção contra invasões estiver ativado, o Kaspersky Endpoint Security colocará a aplicação num grupo fiável, dependendo do nível de perigo que esta aplicação pode representar para o computador. O Kaspersky Endpoint Security bloqueará, então, as ações da aplicação em função do grupo fiável.

Gerir grupos fiáveis da aplicação

Quando cada aplicação é iniciada pela primeira vez, o componente Prevenção contra invasões verifica a segurança da aplicação e coloca a aplicação num dos grupos fiáveis.

Na primeira fase da verificação da aplicação, o Kaspersky Endpoint Security procura uma entrada correspondente na base de dados interna de aplicações conhecidas e envia, em simultâneo, um pedido para a base de dados da Kaspersky Security Network (se estiver disponível uma ligação à Internet). Com base nos resultados da procura na base de dados interna e na base de dados do Kaspersky Security Network, a aplicação é colocada num grupo fiável. Sempre que a aplicação é iniciada subsequentemente, o Kaspersky Endpoint Security envia uma nova consulta para a base de dados da KSN e coloca a aplicação num grupo fiável diferente se a reputação da aplicação na base de dados da KSN tiver sido alterada.

Pode selecionar o grupo fiável ao qual pretende que o Kaspersky Endpoint Security coloque automaticamente todas as aplicações desconhecidas. As aplicações que estavam em execução antes do início do Kaspersky Endpoint Security são automaticamente colocadas no grupo fiável definido nas definições de Prevenção contra invasões.

Para aplicações que foram iniciadas antes do Kaspersky Endpoint Security, apenas a atividade de rede é controlada. O controlo é executado de acordo com as regras de rede especificadas nas definições da Firewall.

Alterar o grupo fiável de uma aplicação

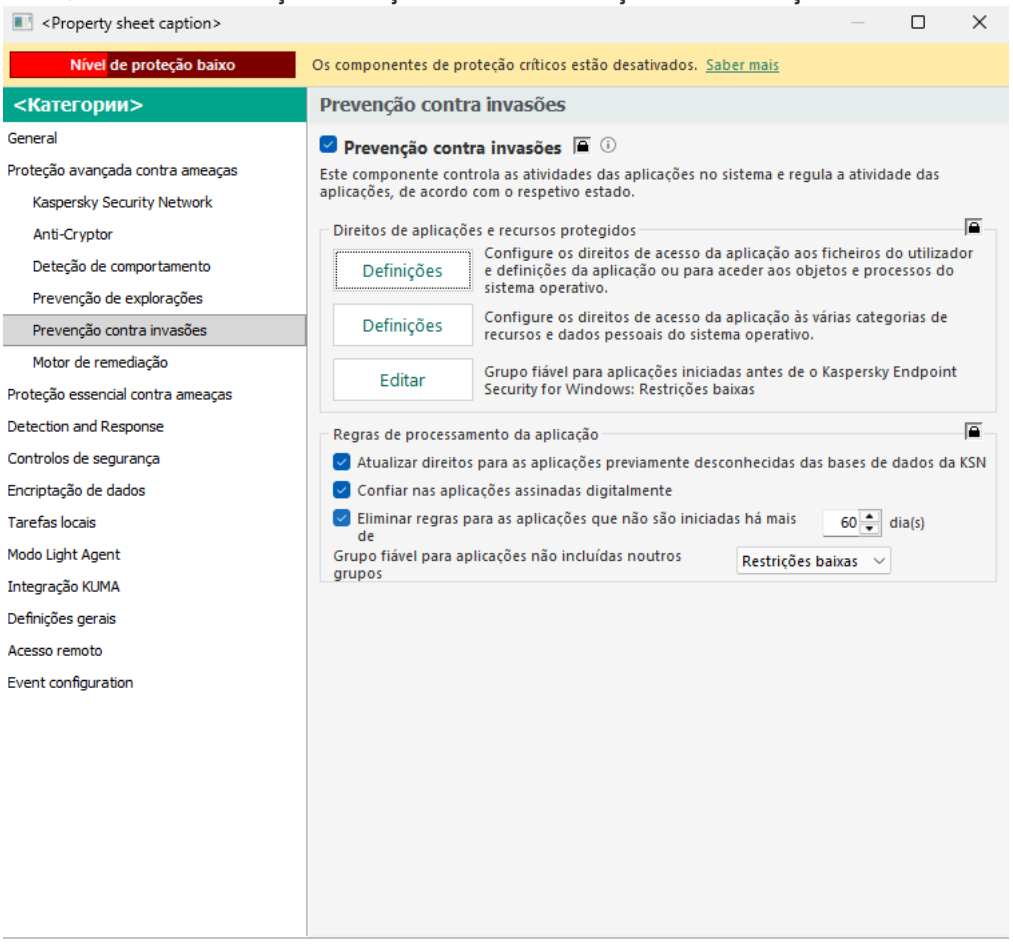
Quando cada aplicação é iniciada pela primeira vez, o componente Prevenção contra invasões verifica a segurança da aplicação e coloca a aplicação num dos grupos fiáveis.

Os especialistas da Kaspersky não recomendam a transferência de aplicações do grupo fiável atribuído automaticamente para outro grupo fiável. Em vez disso, pode modificar os direitos de uma aplicação individual se necessário.

Como alterar o grupo fiável de uma aplicação na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela de política, selecione **Proteção avançada contra ameaças → Prevenção contra invasões**.



Definições da Prevenção contra intrusões

4. No bloco **Direitos de aplicações e recursos protegidos**, clique no botão **Definições**.

   Esta ação abre a janela de configuração dos direitos de aplicações e a lista de recursos protegidos.

5. Selecione o separador **Direitos de aplicações**.

6. Clique em **Adicionar**.

7. Na janela que abre, introduza os critérios de pesquisa da aplicação cujo grupo fiável pretende alterar.

   Pode introduzir o nome da aplicação ou do fornecedor. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.

8. Clique em **Atualizar**.

   O Kaspersky Endpoint Security pesquisa a aplicação na lista consolidada de aplicações instaladas nos computadores geridos. O Kaspersky Endpoint Security apresenta uma lista de aplicações que satisfazem os seus critérios de pesquisa.

9. Selecione a aplicação necessária.

10. Na lista pendente **Adicionar a aplicação selecionada ao grupo fiável**, selecione o grupo fiável necessário para a aplicação.

11. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como alterar o grupo fiável de uma aplicação na Web Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **Host Intrusion Prevention**.
5. No bloco **Application rights and protected resources**, clique na ligação **Application rights and protected resources**.

   Esta ação abre a janela de configuração dos direitos de aplicações e a lista de recursos protegidos.
6. Selecione o separador **Application rights**.

   Uma lista de grupos fiáveis será apresentada no lado esquerdo da janela e as respetivas propriedades serão apresentadas no lado direito.
7. Clique em **Add**.

   É iniciado o Assistente para adicionar uma aplicação a um grupo fiável.
8. Selecione o grupo fiável relevante para a aplicação.
9. Selecione o tipo de **Application**. Avance para o passo seguinte.

   Se pretender alterar o grupo fiável de várias aplicações, selecione o tipo de **Group** e defina um nome para o grupo de aplicações.
10. Na lista de aplicações aberta, selecione as aplicações cujo grupo fiável pretende alterar.

    Utilize um filtro. Pode introduzir o nome da aplicação ou do fornecedor. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.
11. Conclua o assistente.

    A aplicação será adicionada ao grupo fiável.
12. Guarde as suas alterações.

Como alterar o grupo fiável de uma aplicação na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
3. Clique em **Gerir aplicações**.

   Abre-se a lista das aplicações instaladas.
4. Selecione a aplicação necessária.
5. No menu de contexto da aplicação, selecione **Restrições** → **<grupo fiável>**.
6. Guarde as suas alterações.

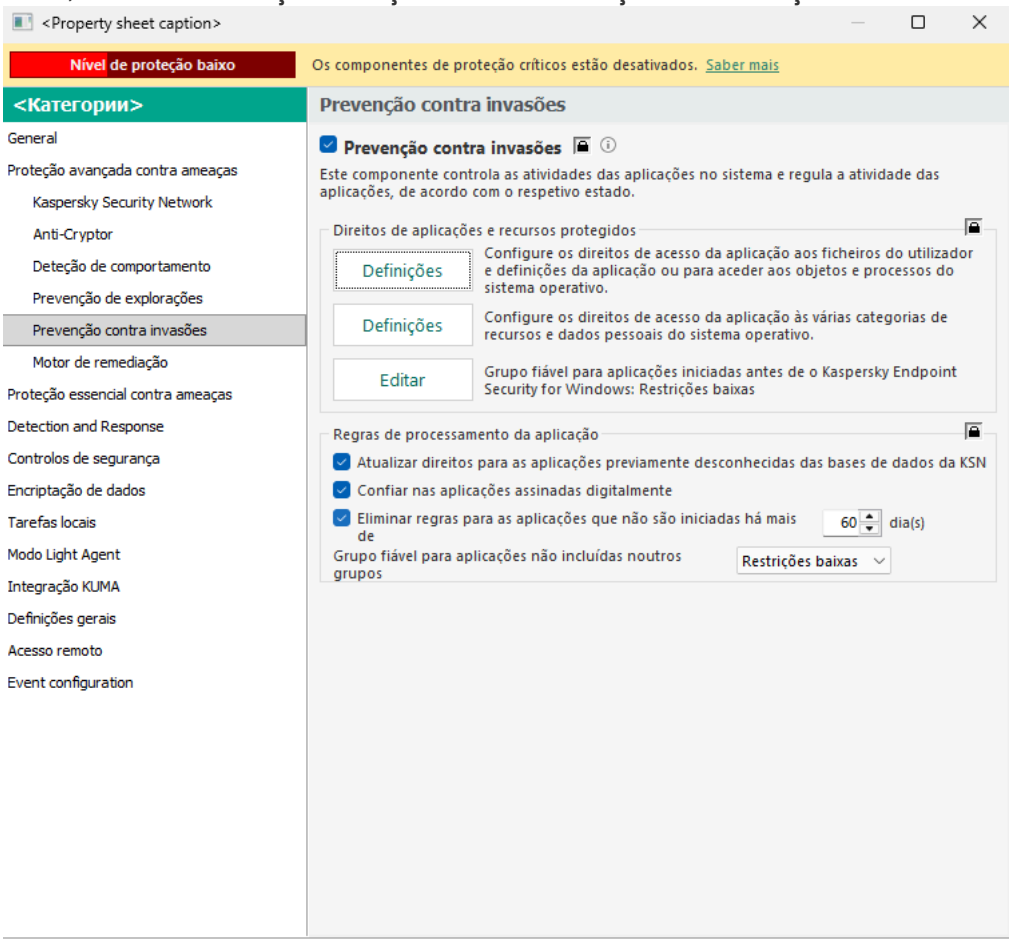
Deste modo, a aplicação será colocada noutro grupo fiável. O Kaspersky Endpoint Security bloqueará, então, as ações da aplicação em função do grupo fiável. O estado *(definido pelo utilizador)* será atribuído à aplicação. Se a reputação da aplicação for alterada na Kaspersky Security Network, o componente Prevenção contra invasões deixará o grupo fiável desta aplicação inalterado.

Configurar os direitos do grupo fiável

Os direitos de aplicações ideais são criados, por predefinição, para diferentes grupos fiáveis. As definições dos direitos de grupos de aplicações que estão num grupo fiável herdam os valores das definições dos direitos de grupo fiável.

Como alterar os direitos do grupo fiável na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção avançada contra ameaças → Prevenção contra invasões**.



Definições da Prevenção contra intrusões

4. No bloco **Direitos de aplicações e recursos protegidos**, clique no botão **Definições**.

   Esta ação abre a janela de configuração dos direitos de aplicações e a lista de recursos protegidos.

5. Aceda ao separador **Direitos de aplicações**.
6. Selecione o grupo fiável necessário.

7. No menu de contexto do grupo fiável, selecione **Direitos de grupos**.

   Esta ação abre as propriedades do grupo fiável.

8. Execute uma das ações seguintes:

   - Se pretender editar os direitos do grupo fiável que regulam as operações com o registo do sistema operativo, ficheiros de utilizador e definições da aplicação, selecione **Ficheiros e registo do sistema**.
   - Se pretender editar os direitos do grupo fiável que regulam o acesso aos processos e objetos do sistema operativo, selecione **Direitos**.

   A atividade de rede das aplicações é controlada pelo componente da Firewall usando *regras de rede*.

9. Para o recurso relevante, na coluna da ação correspondente, clique com o botão direito do rato para abrir o menu de contexto e selecione a opção necessária: **Herdar**, **Permitir** (✓) ou **Bloquear** (⊘).

10. Se pretender monitorizar a utilização de recursos do computador, selecione **Registar eventos** (✓ / ⊘).

    O Kaspersky Endpoint Security registrará informações sobre a operação do componente Prevenção contra invasões. Os relatórios contêm informações sobre as operações com recursos do computador executadas pela aplicação (permitidas ou proibidas). Os relatórios também contêm informações sobre as aplicações que utilizam cada recurso.

11. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como alterar os direitos do grupo fiável na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **Host Intrusion Prevention**.
5. No bloco **Application rights and protected resources**, clique na ligação **Application rights and protected resources**.

   Esta ação abre a janela de configuração dos direitos de aplicações e a lista de recursos protegidos.

6. Aceda ao separador **Application rights**.

   Uma lista de grupos fiáveis será apresentada no lado esquerdo da janela e as respetivas propriedades serão apresentadas no lado direito.

7. Na parte esquerda da janela, selecione o grupo fiável relevante.
8. Na parte direita da janela, na lista suspensa, execute uma das seguintes ações:

   - Se pretender editar os direitos do grupo fiável que regulam as operações com o registo do sistema operativo, ficheiros de utilizador e definições da aplicação, selecione **Files and system registry**.
   - Se pretender editar os direitos do grupo fiável que regulam o acesso aos processos e objetos do sistema operativo, selecione **Rights**.

A atividade de rede das aplicações é controlada pelo componente da Firewall usando *regras de rede*.

9. Para o recurso relevante, na coluna da ação correspondente, selecione a opção necessária: **Inherit**, **Allow** (), **Block** ().

10. Se pretender monitorizar a utilização de recursos do computador, selecione **Log events** (/).

    O Kaspersky Endpoint Security registrará informações sobre a operação do componente Prevenção contra invasões. Os relatórios contêm informações sobre as operações com recursos do computador executadas pela aplicação (permitidas ou proibidas). Os relatórios também contêm informações sobre as aplicações que utilizam cada recurso.

11. Guarde as suas alterações.

Como alterar os direitos do grupo fiável na interface da aplicação

1. Na janela principal da aplicação, clique no botão .

2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.

3. Clique em **Gerir aplicações**.

   Abre-se a lista das aplicações instaladas.

4. Selecione o grupo fiável necessário.

5. No menu de contexto do grupo fiável, selecione **Detalhes e regras**.

   Esta ação abre as propriedades do grupo fiável.

6. Execute uma das ações seguintes:

   - Se pretender editar os direitos do grupo fiável que regulam as operações com o registo do sistema operativo, ficheiros de utilizador e definições da aplicação, selecione **Ficheiros e registo do sistema**.
   - Se pretender editar os direitos do grupo fiável que regulam o acesso aos processos e objetos do sistema operativo, selecione **Direitos**.

A atividade de rede das aplicações é controlada pelo componente da Firewall usando *regras de rede*.

7. Para o recurso relevante, na coluna da ação correspondente, clique com o botão direito do rato para abrir o menu de contexto e selecione a opção necessária: **Herdar**, **Permitir** () ou **Recusar** ().

8. Se pretender monitorizar a utilização de recursos do computador, selecione **Registar eventos** ().

   O Kaspersky Endpoint Security registrará informações sobre a operação do componente Prevenção contra invasões. Os relatórios contêm informações sobre as operações com recursos do computador executadas pela aplicação (permitidas ou proibidas). Os relatórios também contêm informações sobre as aplicações que utilizam cada recurso.

9. Guarde as suas alterações.

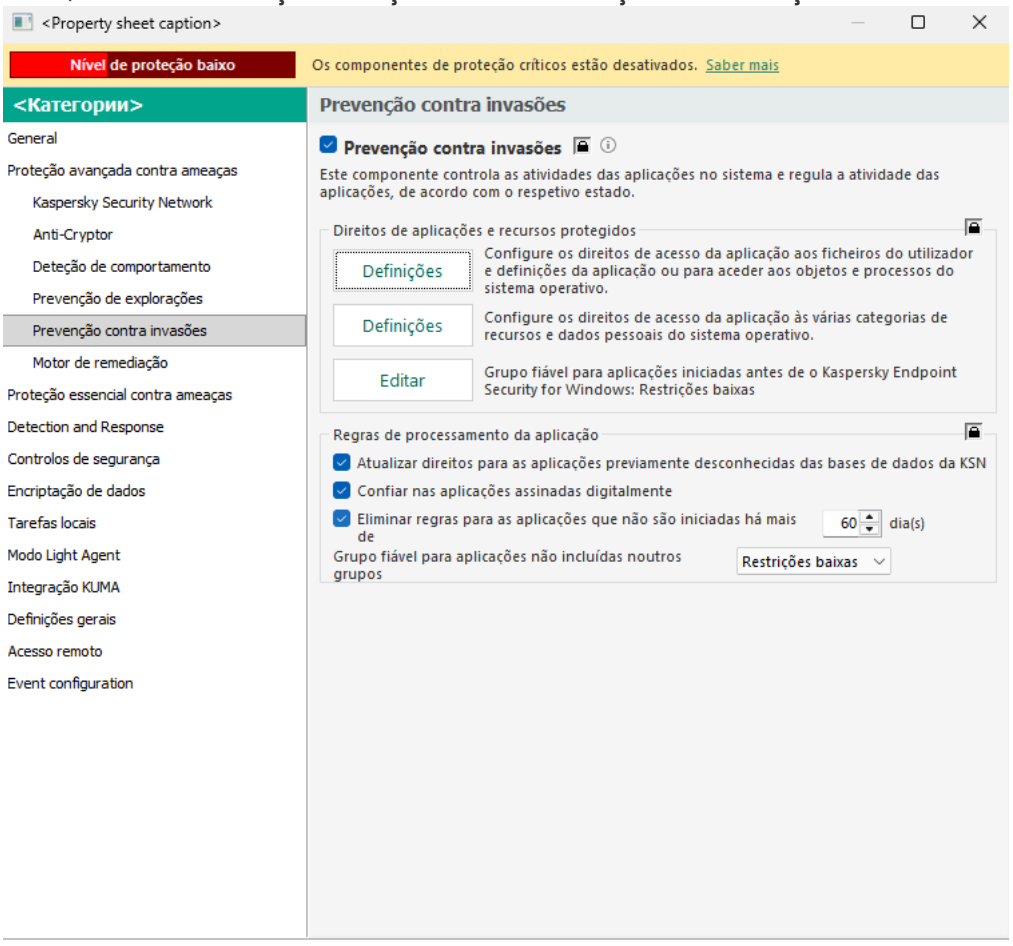
Os direitos do grupo fiável serão alterados. O Kaspersky Endpoint Security bloqueará, então, as ações da aplicação em função do grupo fiável. O estado (*Definições personalizadas*) será atribuído ao grupo fiável.

Selecionar um grupo fiável para aplicações iniciadas antes do Kaspersky Endpoint Security

Para aplicações que foram iniciadas antes do Kaspersky Endpoint Security, apenas a atividade de rede é controlada. O controlo é executado de acordo com as regras de rede especificadas nas definições da Firewall. Para especificar as regras de rede que devem ser aplicadas à monitorização da atividade de rede para essas aplicações, tem de selecionar um grupo fiável.

Como selecionar um grupo fiável para aplicações iniciadas antes do Kaspersky Endpoint Security na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção avançada contra ameaças → Prevenção contra invasões**.



Definições da Prevenção contra intrusões

4. No bloco **Direitos de aplicações e recursos protegidos**, clique no botão **Editar**.
5. Para a definição **Trust group for applications started before Kaspersky Endpoint Security**, selecione o grupo fiável adequado.
6. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como selecionar um grupo fiável para aplicações iniciadas antes do Kaspersky Endpoint Security na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **Host Intrusion Prevention**.
5. Para a definição **Trust group for applications started before Kaspersky Endpoint Security**, selecione o grupo fiável adequado.
6. Guarde as suas alterações.

Como selecionar um grupo fiável para aplicações iniciadas antes do Kaspersky Endpoint Security na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
3. No bloco **Grupo fiável para aplicações iniciadas antes de o Kaspersky Endpoint Security**, selecione o grupo fiável adequado.
4. Guarde as suas alterações.

Deste modo, uma aplicação iniciada antes do Kaspersky Endpoint Security será colocada no outro grupo fiável. O Kaspersky Endpoint Security bloqueará, então, as ações da aplicação em função do grupo fiável.

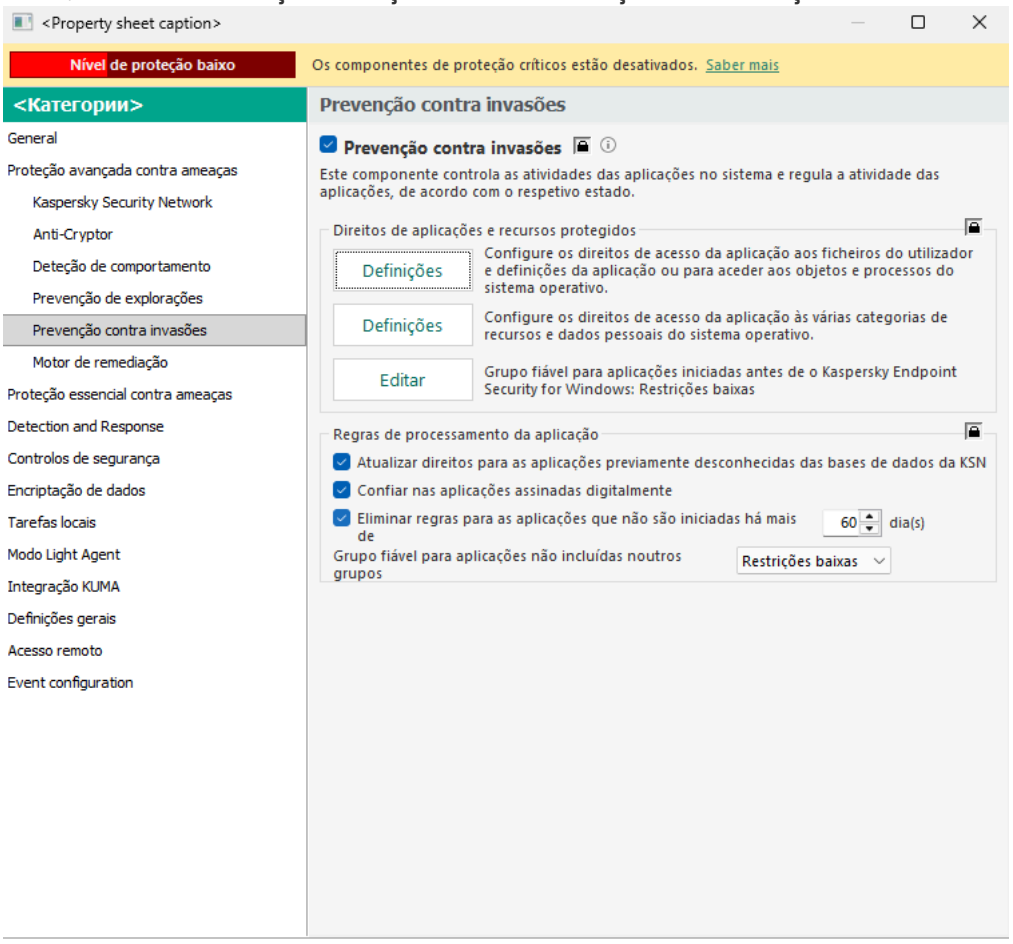
Selecionar um grupo fiável de aplicações desconhecidas

Durante a primeira inicialização da aplicação, o componente Prevenção contra invasões determina o grupo fiável para a aplicação. Se não tiver acesso à Internet ou se o Kaspersky Security Network não tiver informações sobre esta aplicação, o Kaspersky Endpoint Security colocará, por predefinição, a aplicação no grupo *Restrições baixas*. Quando forem detetadas informações sobre uma aplicação previamente desconhecida no KSN, o Kaspersky Endpoint Security atualizará os direitos desta aplicação. Pode editar manualmente os direitos de aplicações.

Como selecionar um grupo fiável para aplicações desconhecidas na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela de política, selecione **Proteção avançada contra ameaças → Prevenção contra invasões**.



Definições da Prevenção contra intrusões

4. No bloco **Application processing rules**, utilize a lista suspensa **Trust group for applications not included in other groups** para selecionar o grupo fiável necessário.

   Se a participação no Kaspersky Security Network estiver ativada, o Kaspersky Endpoint Security envia à KSN um pedido sobre a reputação de uma aplicação sempre que esta for iniciada. Com base na resposta recebida, a aplicação pode ser movida para um grupo fiável diferente do especificado nas definições do componente Prevenção contra invasões.

5. Utilize a caixa de verificação **Update rights for previously unknown applications from KSN database** para configurar a atualização automática dos direitos de aplicações desconhecidas.

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

Como selecionar um grupo fiável para aplicações desconhecidas na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Host Threat Protection → Host Intrusion Prevention**.

5. No bloco **Application processing rules**, utilize a lista suspensa **Trust group for applications not included in other groups** para selecionar o grupo fiável necessário.

   Se a participação no Kaspersky Security Network estiver ativada, o Kaspersky Endpoint Security envia à KSN um pedido sobre a reputação de uma aplicação sempre que esta for iniciada. Com base na resposta recebida, a aplicação pode ser movida para um grupo fiável diferente do especificado nas definições do componente Prevenção contra invasões.

6. Utilize a caixa de verificação **Update rights for previously unknown applications from KSN database** para configurar a atualização automática dos direitos de aplicações desconhecidas.

7. Guarde as suas alterações.

Como selecionar um grupo fiável para aplicações desconhecidas na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Proteção avançada contra ameaças → Prevenção contra invasões**.

3. No bloco **Regras de processamento da aplicação**, selecione o grupo fiável adequado.

   Se a participação no Kaspersky Security Network estiver ativada, o Kaspersky Endpoint Security envia à KSN um pedido sobre a reputação de uma aplicação sempre que esta for iniciada. Com base na resposta recebida, a aplicação pode ser movida para um grupo fiável diferente do especificado nas definições do componente Prevenção contra invasões.

4. Utilize a caixa de verificação **Atualizar regras para aplicações anteriormente desconhecidas do KSN** para configurar a atualização automática dos direitos de aplicações desconhecidas.

5. Guarde as suas alterações.

Selecionar um grupo fiável para aplicações assinadas digitalmente

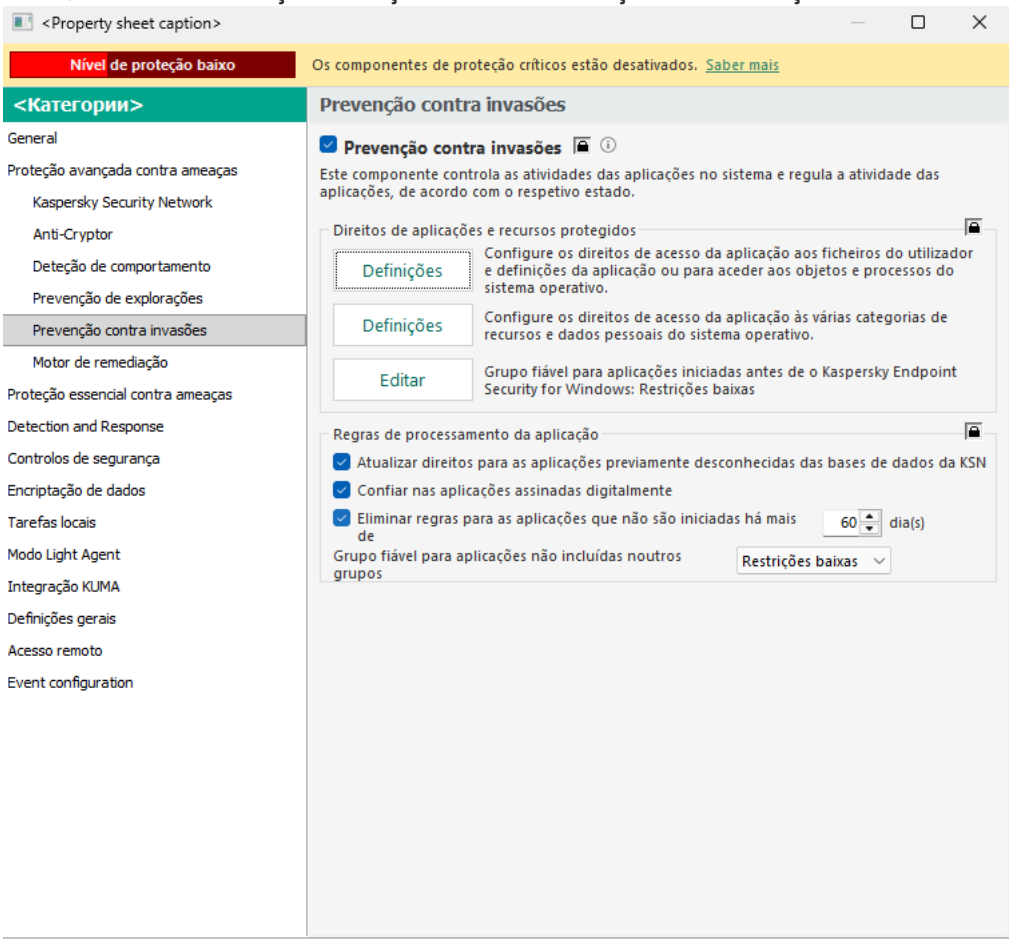
O Kaspersky Endpoint Security coloca sempre as aplicações assinadas por certificados Microsoft ou certificados Kaspersky no grupo de aplicações *Fiáveis*.

Como selecionar um grupo fiável para aplicações assinadas digitalmente na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Proteção avançada contra ameaças → Prevenção contra invasões**.



Definições da Prevenção contra intrusões

4. No bloco **Application processing rules**, utilize a caixa de verificação **Trust digitally signed applications** para ativar ou desativar a atribuição automática ao grupo fiável para aplicações que contêm a assinatura digital de fornecedores fiáveis.

   Fornecedores fiáveis são os fornecedores de software incluídos no grupo fiável pela Kaspersky. Pode também adicionar manualmente um certificado de fornecedor ao arquivo de certificados do sistema fiável.

   Se esta caixa de verificação estiver desmarcada, o componente Prevenção contra invasões não considera as aplicações assinadas digitalmente como fiáveis e utiliza outros parâmetros para determinar o respetivo grupo fiável.

5. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como selecionar um grupo fiável para aplicações assinadas digitalmente na Console Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Host Threat Protection → Host Intrusion Prevention**.

5. No bloco **Application processing rules**, utilize a caixa de verificação **Trust digitally signed applications** para ativar ou desativar a atribuição automática ao grupo fiável para aplicações que contêm a assinatura digital de fornecedores fiáveis.

Fornecedores fiáveis são os fornecedores de software incluídos no grupo fiável pela Kaspersky. Pode também adicionar manualmente um certificado de fornecedor ao arquivo de certificados do sistema fiável.

Se esta caixa de verificação estiver desmarcada, o componente Prevenção contra invasões não considera as aplicações assinadas digitalmente como fiáveis e utiliza outros parâmetros para determinar o respetivo grupo fiável.

6. Guarde as suas alterações.

Como selecionar um grupo fiável para aplicações assinadas digitalmente na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
3. No bloco **Application processing rules**, utilize a caixa de verificação **Trust digitally signed applications** para ativar ou desativar a atribuição automática ao grupo fiável para aplicações que contêm a assinatura digital de fornecedores fiáveis.

   Fornecedores fiáveis são os fornecedores de software incluídos no grupo fiável pela Kaspersky. Pode também adicionar manualmente um certificado de fornecedor ao arquivo de certificados do sistema fiável.

   Se esta caixa de verificação estiver desmarcada, o componente Prevenção contra invasões não considera as aplicações assinadas digitalmente como fiáveis e utiliza outros parâmetros para determinar o respetivo grupo fiável.

4. Guarde as suas alterações.

Gerir direitos da aplicação

Por predefinição, a atividade das aplicações é controlada com base nos direitos de aplicações definidos para o grupo fiável ao qual o Kaspersky Endpoint Security atribuiu a aplicação na primeira vez em que foi iniciada. Se necessário, pode editar os direitos de aplicações para um grupo fiável completo, para uma aplicação individual ou para um grupo de aplicações dentro de um grupo fiável.

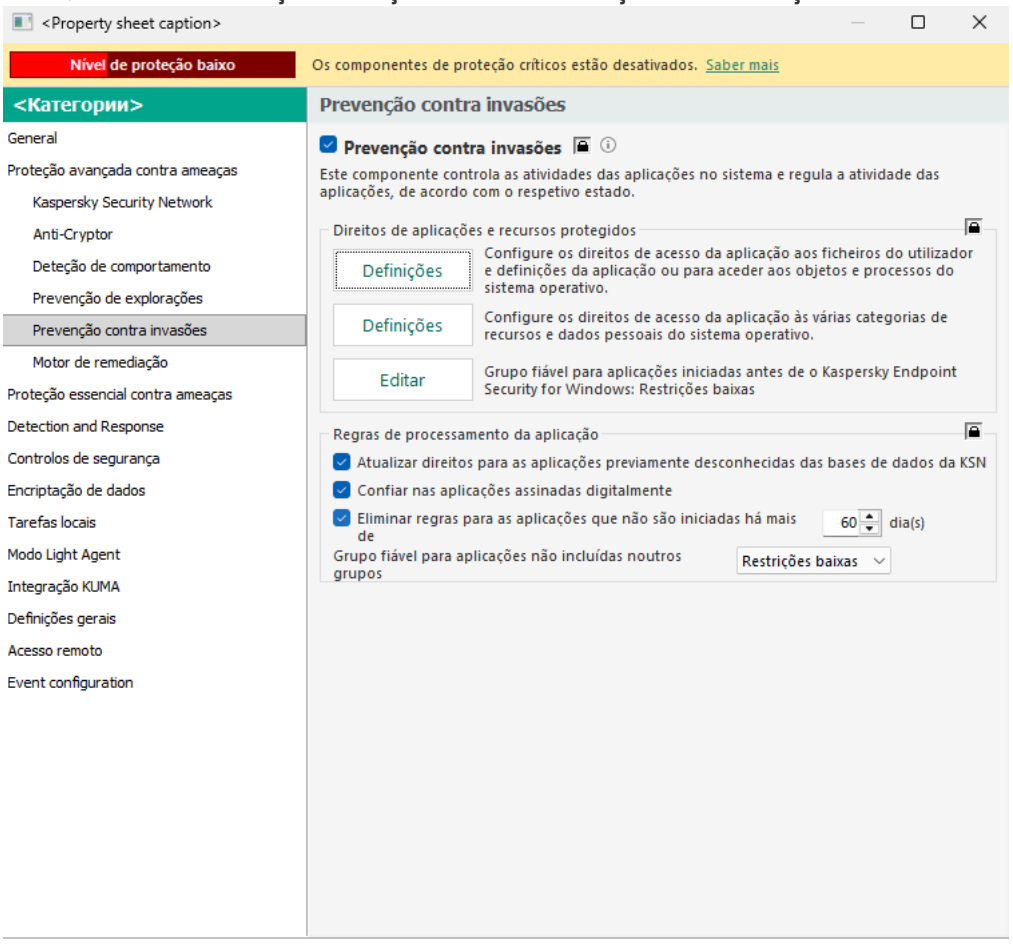
Os direitos de aplicações definidos manualmente têm uma prioridade mais alta do que os direitos de aplicações definidos para um grupo fiável. Ou seja, se os direitos de aplicações definidos manualmente forem diferentes dos direitos de aplicações definidos para um grupo fiável, o componente Prevenção contra invasões controla a atividade das aplicações de acordo com os direitos de aplicações definidos manualmente.

As regras que cria para uma aplicação são herdadas pelas aplicações subordinadas. Por exemplo, se negar toda a atividade de rede a cmd.exe, esta também será negada a notepad.exe se for iniciada através de cmd.exe. Quando uma aplicação não está subordinada à aplicação que executa, as regras não são herdadas.

Como alterar os direitos de aplicações na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela de política, selecione **Proteção avançada contra ameaças → Prevenção contra invasões**.



Definições da Prevenção contra intrusões

4. No bloco **Direitos de aplicações e recursos protegidos**, clique no botão **Definições**.

   Esta ação abre a janela de configuração dos direitos de aplicações e a lista de recursos protegidos.

5. Aceda ao separador **Direitos de aplicações**.

6. Clique em **Adicionar**.

7. Na janela que abre, introduza os critérios para pesquisar a aplicação cujos direitos de aplicações pretende alterar.

   Pode introduzir o nome da aplicação ou do fornecedor. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.

8. Clique em **Atualizar**.

   O Kaspersky Endpoint Security pesquisa a aplicação na lista consolidada de aplicações instaladas nos computadores geridos. O Kaspersky Endpoint Security apresenta uma lista de aplicações que satisfazem os seus critérios de pesquisa.

9. Selecione a aplicação necessária.

10. Na lista suspensa **Adicionar a aplicação selecionada ao grupo fiável**, selecione **Grupos predefinidos** e clique em **Ok**.

    A aplicação será adicionada ao grupo predefinido.

11. Selecione a aplicação relevante e, em seguida, selecione **Direitos de aplicações** no menu de contexto da aplicação.

    Abrem-se as propriedades da aplicação.

12. Execute uma das ações seguintes:

    - Se pretender editar os direitos do grupo fiável que regulam as operações com o registo do sistema operativo, ficheiros de utilizador e definições da aplicação, selecione **Ficheiros e registo do sistema**.
    - Se pretender editar os direitos do grupo fiável que regulam o acesso aos processos e objetos do sistema operativo, selecione **Direitos**.

    A atividade de rede das aplicações é controlada pelo componente da Firewall usando *regras de rede*.

13. Para o recurso relevante, na coluna da ação correspondente, clique com o botão direito do rato para abrir o menu de contexto e selecione a opção necessária: **Herdar**, **Permitir** (✓) ou **Bloquear** (⊘).

14. Se pretender monitorizar a utilização de recursos do computador, selecione **Registar eventos** (✓ / ⊘).

    O Kaspersky Endpoint Security registrará informações sobre a operação do componente Prevenção contra invasões. Os relatórios contêm informações sobre as operações com recursos do computador executadas pela aplicação (permitidas ou proibidas). Os relatórios também contêm informações sobre as aplicações que utilizam cada recurso.

15. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como alterar os direitos de aplicações na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **Host Intrusion Prevention**.
5. No bloco **Application rights and protected resources**, clique na ligação **Application rights and protected resources**.

   Esta ação abre a janela de configuração dos direitos de aplicações e a lista de recursos protegidos.
6. Aceda ao separador **Application rights**.

   Uma lista de grupos fiáveis será apresentada no lado esquerdo da janela e as respetivas propriedades serão apresentadas no lado direito.
7. Clique em **Add**.

   É iniciado o Assistente para adicionar uma aplicação a um grupo fiável.
8. Selecione o grupo fiável relevante para a aplicação.
9. Selecione o tipo de **Application**. Avance para o passo seguinte.

   Se pretender alterar o grupo fiável de várias aplicações, selecione o tipo de **Group** e defina um nome para o grupo de aplicações.
10. Na lista aberta de aplicações, selecione as aplicações cujos direitos de aplicações pretende alterar.

    Utilize um filtro. Pode introduzir o nome da aplicação ou do fornecedor. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.

11. Conclua o assistente.

    A aplicação será adicionada ao grupo fiável.

12. Na parte esquerda da janela, selecione a aplicação relevante.

13. Na parte direita da janela, na lista suspensa, execute uma das seguintes ações:

    - Se pretender editar os direitos do grupo fiável que regulam as operações com o registo do sistema operativo, ficheiros de utilizador e definições da aplicação, selecione **Files and system registry**.
    - Se pretender editar os direitos do grupo fiável que regulam o acesso aos processos e objetos do sistema operativo, selecione **Rights**.

    A atividade de rede das aplicações é controlada pelo componente da Firewall usando *regras de rede*.

14. Para o recurso relevante, na coluna da ação correspondente, selecione a opção necessária: **Inherit**, **Allow** (), **Block** ().

15. Se pretender monitorizar a utilização de recursos do computador, selecione **Log events** (/).

    O Kaspersky Endpoint Security registrará informações sobre a operação do componente Prevenção contra invasões. Os relatórios contêm informações sobre as operações com recursos do computador executadas pela aplicação (permitidas ou proibidas). Os relatórios também contêm informações sobre as aplicações que utilizam cada recurso.

16. Guarde as suas alterações.

Como alterar os direitos de aplicações na interface da aplicação

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
3. Clique em **Gerir aplicações**.

   Abre-se a lista das aplicações instaladas.

4. Selecione a aplicação necessária.
5. No menu de contexto da aplicação, selecione **Detalhes e regras**.

   Abrem-se as propriedades da aplicação.

6. Execute uma das ações seguintes:

   - Se pretender editar os direitos do grupo fiável que regulam as operações com o registo do sistema operativo, ficheiros de utilizador e definições da aplicação, selecione **Ficheiros e registo do sistema**.
   - Se pretender editar os direitos do grupo fiável que regulam o acesso aos processos e objetos do sistema operativo, selecione **Direitos**.

7. Para o recurso relevante, na coluna da ação correspondente, clique com o botão direito do rato para abrir o menu de contexto e selecione a opção necessária: **Herdar**, **Permitir** () ou **Recusar** ().

8. Se pretender monitorizar a utilização de recursos do computador, selecione **Registar eventos** ( ).

   O Kaspersky Endpoint Security registrará informações sobre a operação do componente Prevenção contra invasões. Os relatórios contêm informações sobre as operações com recursos do computador executadas pela aplicação (permitidas ou proibidas). Os relatórios também contêm informações sobre as aplicações que utilizam cada recurso.

9. Selecione o separador **Exclusões** e configure as definições avançadas da aplicação (consulte a tabela abaixo).

10. Guarde as suas alterações.

Definições avançadas da aplicação

Parâmetro	Descrição
Não verificar ficheiros abertos pela aplicação	Todos os ficheiros abertos pela aplicação são excluídos das verificações do Kaspersky Endpoint Security. Por exemplo, se estiver a utilizar aplicações para fazer cópias de segurança de ficheiros, esta funcionalidade ajuda a reduzir o consumo de recursos pelo Kaspersky Endpoint Security.
Não monitorizar a atividade da aplicação	O Kaspersky Endpoint Security não monitoriza a atividade dos ficheiros e da rede da aplicação no sistema operativo. Pode configurar a monitorização da atividade da aplicação para diferentes componentes do Kaspersky Endpoint Security: • **Não monitorizar para os componentes de proteção e controlo**. A atividade da aplicação é monitorizada pelos seguintes componentes: Deteção de comportamento, Prevenção de explorações, Prevenção contra invasões, Motor de remediação e Firewall. • **Não monitorizar o Managed Detection and Response e o Endpoint Detection and Response**. A atividade da aplicação é monitorizada pelo MDR Agent integrado e o EDR (KATA) Agent integrado. • **Não intercetar a entrada interativa da consola para o Endpoint Detection and Response**. O Kaspersky Endpoint Security não envia dados de telemetria sobre a gestão da aplicação na consola. Os dados de telemetria são usados pela Kaspersky Anti Targeted Attack Platform (EDR).
Não herdar restrições do processo parental (aplicação)	As restrições configuradas para o processo principal não serão aplicadas pelo Kaspersky Endpoint Security a um processo subordinado. O processo principal é iniciado por uma aplicação para a qual os direitos de aplicações (Prevenção contra invasões) e as regras de rede de aplicações (Firewall) estão configurados.
Não monitorizar atividade da aplicação secundária	O Kaspersky Endpoint Security não monitorizará a atividade de ficheiros ou de rede de aplicações iniciadas por esta aplicação. Pode aplicar a exclusão de forma recursiva. Para que a aplicação não monitorize a atividade da cadeia completa de aplicações secundárias.
Permitir interação com a interface do Kaspersky Endpoint Security	A Autodefesa do Kaspersky Endpoint Security bloqueia todas as tentativas de gerir serviços de aplicações a partir de um computador remoto. Se a caixa de verificação estiver selecionada, a aplicação de acesso remoto pode efetuar a gestão das definições do Kaspersky Endpoint Security através da interface do Kaspersky Endpoint Security.
Não verificar tráfego encriptado/Não verificar todo o tráfego	O tráfego de rede iniciado pela aplicação será excluído das verificações do Kaspersky Endpoint Security. Pode excluir todo o tráfego ou apenas o tráfego encriptado das verificações. Também pode excluir endereços IP individuais e números de porta das verificações. A aplicação não suporta a exclusão de tráfego de rede se um hash for especificado para uma aplicação fiável, em vez de um caminho.

Proteção dos recursos do sistema operativo e de dados pessoais

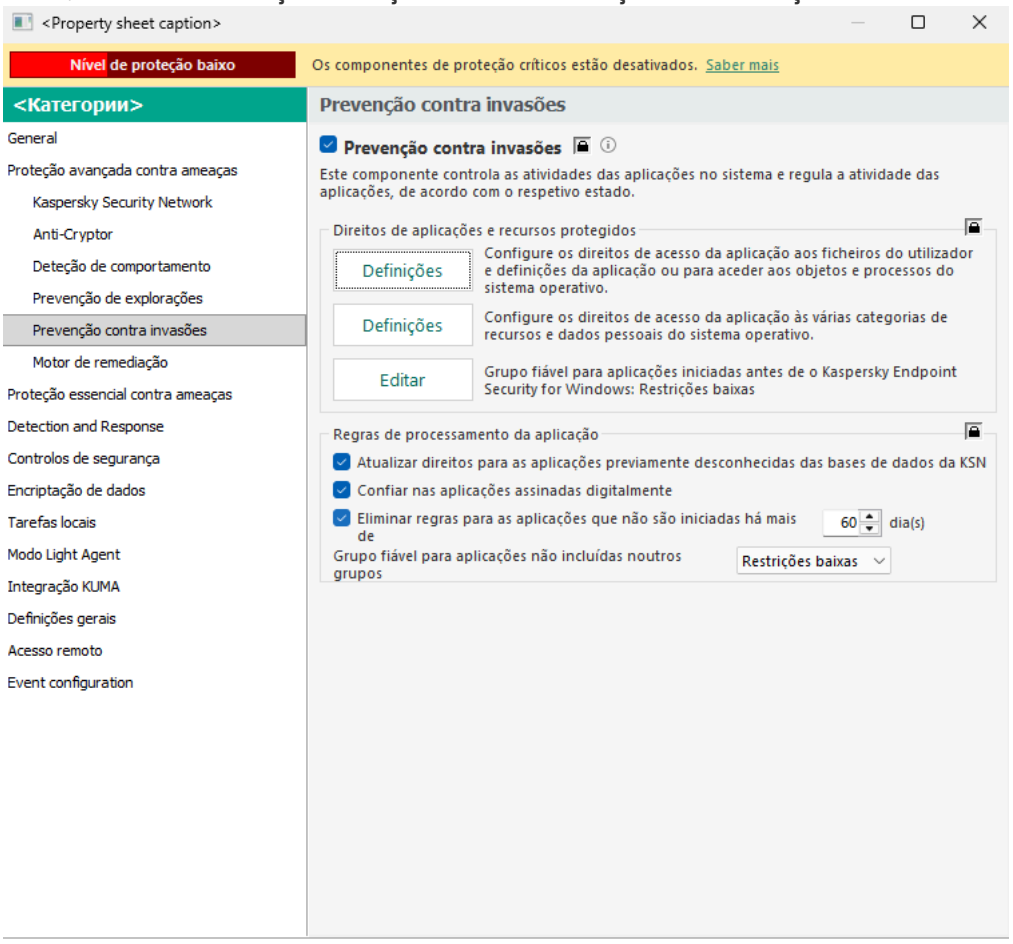
O componente Prevenção contra invasões gere os direitos das aplicações para executarem ações em diversas categorias de recursos do sistema operativo e dados pessoais. Os especialistas da Kaspersky estabeleceram categorias predefinidas de recursos protegidos. Por exemplo, a categoria *Sistema Operativo* possui uma subcategoria *Definições de inicialização* que lista todas as chaves de registo associadas à execução automática de aplicações. Não é possível editar ou apagar as categorias predefinidas de recursos protegidos ou dos recursos protegidos inseridos nestas categorias.

Como adicionar um recurso protegido na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Proteção avançada contra ameaças → Prevenção contra invasões**.



Definições da Prevenção contra intrusões

4. No bloco **Direitos de aplicações e recursos protegidos**, clique no botão **Definições**.

   Esta ação abre a janela de configuração dos direitos de aplicações e a lista de recursos protegidos.

5. Aceda ao separador **Recursos protegidos**.

   Será apresentada uma lista de recursos protegidos na parte esquerda da janela e os direitos correspondentes para aceder a esses recursos, dependendo do grupo fiável específico.

6. Selecione a categoria de recursos protegidos aos quais pretende adicionar um novo recurso protegido.

   Se pretender adicionar uma subcategoria, clique em **Adicionar → Categoria**.

7. Selecione o botão **Adicionar**. Na lista suspensa, selecione o tipo de recurso que pretende adicionar: **Ficheiro ou pasta** ou **Chave de registo**.

8. Na janela que abre, selecione um ficheiro, pasta ou chave de registo.

   Pode ver os direitos das aplicações para aceder aos recursos adicionados. Para tal, selecione um recurso adicionado na parte esquerda da janela e o Kaspersky Endpoint Security mostrará os direitos de acesso para cada grupo fiável. Pode também desativar o controlo da atividade da aplicação com recursos, utilizando a caixa de verificação ao lado de um novo recurso.

9. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como adicionar um recursos protegido na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **Host Intrusion Prevention**.
5. No bloco **Application rights and protected resources**, clique na ligação **Application rights and protected resources**.

   Esta ação abre a janela de configuração dos direitos de aplicações e a lista de recursos protegidos.
6. Aceda ao separador **Protected resources**.

   Será apresentada uma lista de recursos protegidos na parte esquerda da janela e os direitos correspondentes para aceder a esses recursos, dependendo do grupo fiável específico.
7. Clique em **Add**.

   É iniciado o Assistente de Novo Recurso.
8. No bloco **Group name**, selecione a categoria de recursos protegidos aos quais pretende adicionar um novo recurso protegido.

   Se pretender adicionar uma subcategoria, selecione a opção **Category of protected resources**.
9. Selecione o tipo de recurso que pretende adicionar: **File or folder** ou **Registry key**.
10. Selecione um ficheiro, pasta ou chave de registo.
11. Conclua o assistente.

    Pode ver os direitos das aplicações para aceder aos recursos adicionados. Para tal, selecione um recurso adicionado na parte esquerda da janela e o Kaspersky Endpoint Security mostrará os direitos de acesso para cada grupo fiável. Pode também utilizar a caixa de verificação na coluna **Status** para desativar o controlo da atividade da aplicação com recursos.
12. Guarde as suas alterações.

Como adicionar um recurso protegido na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
3. Clique em **Gerir recursos**.

   Abre-se a lista de recursos protegidos.
4. Selecione a categoria de recursos protegidos aos quais pretende adicionar um novo recurso protegido.

   Se pretender adicionar uma subcategoria, clique em **Adicionar** → **Categoria**.
5. Selecione o botão **Adicionar**. Na lista suspensa, selecione o tipo de recurso que pretende adicionar: **Ficheiro ou pasta** ou **Chave de registo**.

6. Na janela que abre, selecione um ficheiro, pasta ou chave de registo.

   Pode ver os direitos das aplicações para aceder aos recursos adicionados. Para tal, selecione um recurso adicionado na parte esquerda da janela e o Kaspersky Endpoint Security mostrará uma lista de aplicações e os direitos de acesso para cada aplicação. Pode também desativar o controlo da atividade da aplicação com recursos, utilizando o botão **Ativar controlo**, na coluna **Estado**.

7. Guarde as suas alterações.

O Kaspersky Endpoint Security controlará o acesso aos recursos adicionados do sistema operativo e aos dados pessoais. O Kaspersky Endpoint Security controla o acesso de uma aplicação aos recursos com base no grupo fiável atribuído à aplicação. Pode também alterar o grupo fiável de uma aplicação.

Eliminar informações acerca de aplicações não utilizadas

O Kaspersky Endpoint Security usa direitos de aplicações para controlar as atividades das aplicações. Os direitos de aplicações são determinados pelo seu grupo fiável. O Kaspersky Endpoint Security coloca uma aplicação num grupo fiável quando a aplicação é iniciada pela primeira vez. Pode alterar manualmente o grupo fiável de uma aplicação. Pode também configurar manualmente os direitos de uma aplicação individual. O Kaspersky Endpoint Security armazena as seguintes informações sobre uma aplicação: grupo fiável da aplicação e direitos da aplicação.

O Kaspersky Endpoint Security elimina automaticamente as informações sobre as aplicações não utilizadas para poupar recursos do computador. O Kaspersky Endpoint Security elimina as informações da aplicação de acordo com as seguintes regras:

- Se o grupo fiável e os direitos de uma aplicação forem determinados automaticamente, o Kaspersky Endpoint Security elimina as informações sobre essa aplicação após 30 dias. Não é possível alterar o período de armazenamento para obter informações sobre a aplicação ou desativar a eliminação automática.

- Se colocar manualmente uma aplicação num grupo fiável ou configurar os seus direitos de acesso, o Kaspersky Endpoint Security eliminará as informações sobre essa aplicação após 60 dias (prazo de armazenamento predefinido). Pode alterar o período de armazenamento para obter informações sobre a aplicação ou desativar a eliminação automática (consulte as instruções abaixo).

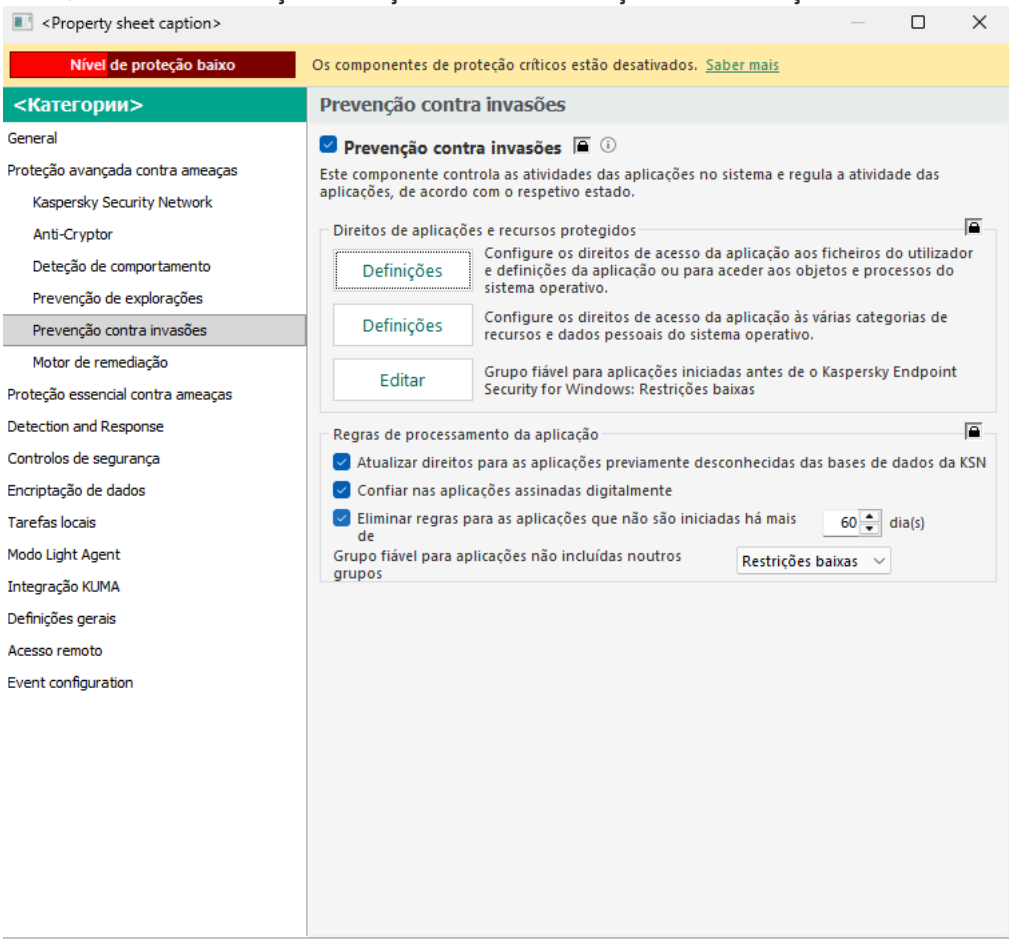
Quando inicia uma aplicação cujas informações foram eliminadas, o Kaspersky Endpoint Security analisa a aplicação como se fosse iniciada pela primeira vez.

Como configurar a eliminação automática de informações sobre aplicações não utilizadas na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Proteção avançada contra ameaças → Prevenção contra invasões**.



Definições da Prevenção contra intrusões

4. No bloco **Regras de processamento da aplicação**, execute uma das seguintes ações:

   - Se deseja configurar a eliminação automática, selecione a caixa de verificação **Eliminar regras para as aplicações que não são iniciadas há mais de N dia(s)** e introduza o número de dias.

     As informações sobre as aplicações que coloca manualmente num grupo fiável ou cujos direitos de acesso configurou manualmente serão eliminadas pelo Kaspersky Endpoint Security após o número de dias definido. As informações acerca de aplicações cujo grupo fiável e direitos da aplicação foram determinados automaticamente serão também eliminados pelo Kaspersky Endpoint Security após 30 dias.

   - Se quiser desativar a eliminação automática, desmarque a caixa de verificação **Eliminar regras para as aplicações que não são iniciadas há mais de N dia(s)**.

     As informações sobre as aplicações que coloca manualmente num grupo fiável ou cujos direitos de acesso configurou manualmente serão armazenadas pelo Kaspersky Endpoint Security indefinidamente, sem nenhum limite de período de armazenamento. O Kaspersky Endpoint Security apenas eliminará informações sobre aplicações cujo grupo fiável e direitos da aplicação foram determinados automaticamente após 30 dias.

5. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como configurar a eliminação automática de informações sobre aplicações não utilizadas na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Host Threat Protection** → **Host Intrusion Prevention**.

5. No bloco **Application processing rules**, execute uma das seguintes ações:

   - Se deseja configurar a eliminação automática, selecione a caixa de verificação **Delete rules for applications that have not been started for longer than (days, 1 to 90)** e introduza o número de dias.

     As informações sobre as aplicações que coloca manualmente num grupo fiável ou cujos direitos de acesso configurou manualmente serão eliminadas pelo Kaspersky Endpoint Security após o número de dias definido. As informações acerca de aplicações cujo grupo fiável e direitos da aplicação foram determinados automaticamente serão também eliminados pelo Kaspersky Endpoint Security após 30 dias.

   - Se quiser desativar a eliminação automática, desmarque a caixa de verificação **Delete rules for applications that have not been started for longer than (days, 1 to 90)**.

     As informações sobre as aplicações que coloca manualmente num grupo fiável ou cujos direitos de acesso configurou manualmente serão armazenadas pelo Kaspersky Endpoint Security indefinidamente, sem nenhum limite de período de armazenamento. O Kaspersky Endpoint Security apenas eliminará informações sobre aplicações cujo grupo fiável e direitos da aplicação foram determinados automaticamente após 30 dias.

6. Guarde as suas alterações.

Como configurar a eliminação automática de informações sobre aplicações não utilizadas na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.

3. No bloco **Regras de processamento da aplicação**, execute uma das seguintes ações:

   - Se deseja configurar a eliminação automática, selecione a caixa de verificação **Eliminar regras para as aplicações que não são iniciadas há mais de N dias (de 1 a 90)** e introduza o número de dias.

     As informações sobre as aplicações que coloca manualmente num grupo fiável ou cujos direitos de acesso configurou manualmente serão eliminadas pelo Kaspersky Endpoint Security após o número de dias definido. As informações acerca de aplicações cujo grupo fiável e direitos da aplicação foram determinados automaticamente serão também eliminados pelo Kaspersky Endpoint Security após 30 dias.

   - Se quiser desativar a eliminação automática, desmarque a caixa de verificação **Eliminar regras para as aplicações que não são iniciadas há mais de N dias (de 1 a 90)**.

     As informações sobre as aplicações que coloca manualmente num grupo fiável ou cujos direitos de acesso configurou manualmente serão armazenadas pelo Kaspersky Endpoint Security indefinidamente, sem nenhum limite de período de armazenamento. O Kaspersky Endpoint Security apenas eliminará informações sobre aplicações cujo grupo fiável e direitos da aplicação foram determinados automaticamente após 30 dias.

4. Guarde as suas alterações.

Monitorizar a Prevenção contra invasões

Pode receber relatórios sobre a operação do componente Prevenção contra invasões. Os relatórios contêm informações sobre as operações com recursos do computador executadas pela aplicação (permitidas ou proibidas). Os relatórios também contêm informações sobre as aplicações que utilizam cada recurso.

Para monitorizar as operações da Prevenção contra invasões, é necessário ativar a gravação de relatórios. Por exemplo, pode ativar o encaminhamento de relatórios para aplicações individuais nas definições do componente Prevenção contra invasões.

Ao configurar a monitorização da Prevenção contra invasões, tenha em consideração a eventual carga de rede ao encaminhar eventos para o Kaspersky Security Center. Pode também ativar a opção de guardar relatórios apenas no registo local do Kaspersky Endpoint Security.

Proteger o acesso a áudio e vídeo

A funcionalidade de proteção do sinal de áudio e a funcionalidade de proteção do acesso à câmara Web não são suportadas em computadores baseados em Arm.

Os cibercriminosos podem utilizar programas especiais para tentar obter acesso a dispositivos que gravam áudio e vídeo (como microfones ou webcams). O Kaspersky Endpoint Security controla quando as aplicações recebem um fluxo de áudio ou de vídeo e protege os dados contra interceções não autorizadas.

Por padrão, o Kaspersky Endpoint Security permite receber fluxos de áudio e vídeo apenas para aplicações do grupo *Fiáveis*. As aplicações dos grupos *Restrições baixas*, *Restrições altas* e *Não fiáveis* não têm permissão para receber fluxos de áudio e vídeo de dispositivos. Pode permitir manualmente que as aplicações recebam o fluxo de áudio e de vídeo.

Funcionalidades especiais da proteção do fluxo de áudio

A proteção do fluxo de áudio tem as seguintes características especiais:

- O componente Prevenção contra invasões tem de estar ativado para esta funcionalidade ser executada.
- Se a aplicação começou a receber o fluxo de áudio antes de o componente Prevenção contra invasões ser iniciado, o Kaspersky Endpoint Security permite que a aplicação receba o fluxo de áudio e não apresenta qualquer notificação.
- Se tiver movido a aplicação para o grupo *Não fiáveis* ou para o grupo *Restrições altas* depois de aplicação ter começado a receber o fluxo de áudio, o Kaspersky Endpoint Security permite à aplicação receber o fluxo de áudio e não apresenta qualquer notificação.
- Após a alteração das definições de acesso da aplicação a dispositivos de gravação de som (por exemplo, se tiver sido bloqueada a receção do fluxo de áudio na aplicação), esta aplicação tem de ser reiniciada para que deixe de receber o fluxo de áudio.

- O controlo do acesso ao fluxo de áudio de dispositivos de gravação de som não depende das definições de acesso da câmara Web de uma aplicação.
- O Kaspersky Endpoint Security apenas protege contra o acesso a microfones integrados e a microfones externos. Não são suportados outros dispositivos de reprodução de áudio.
- O Kaspersky Endpoint Security não pode garantir a proteção de um fluxo de áudio proveniente de dispositivos como, por exemplo, câmaras DSLR, câmaras de vídeo portáteis e câmaras de ação.
- Quando executa aplicações 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 podem ser interrompidas. Esta ação é necessária para ativar a funcionalidade que controla o acesso de aplicações a dispositivos de gravação de som. O serviço de sistema que controla o hardware de áudio será então reiniciado quando Kaspersky Endpoint Security for executado pela primeira vez.

Funcionalidades especiais da proteção do acesso à webcam da aplicação

A funcionalidade de proteção de acesso à webcam tem as seguintes considerações especiais e limitações:

- A aplicação controla vídeos e imagens estáticas resultantes do processamento de dados da webcam.
- A aplicação controla o fluxo de áudio caso este faça parte do fluxo de vídeo recebido da webcam.
- A aplicação controla apenas as webcams ligadas através de USB ou IEEE1394 que são apresentados como Dispositivos de processamento de imagens no Gestor de Dispositivo do Windows.
- O 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 estejam especificadas nesta lista.

Prevenção de ataques BadUSB

Alguns vírus modificam o firmware de dispositivos USB para enganar o sistema operativo e fazer com que ele detete o dispositivo USB como teclado. Como resultado, o vírus pode executar comandos na sua conta de utilizador para transferir malware, por exemplo.

O componente "Prevenção de ataques BadUSB" bloqueia a ligação de dispositivos USB infetados que emulam um teclado ao computador.

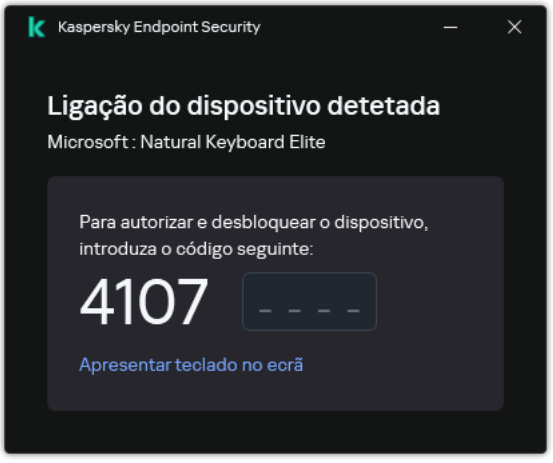
Quando um dispositivo USB é ligado a um computador e identificado pelo sistema operativo como um teclado, a aplicação solicita ao utilizador que introduza um código numérico gerado pela aplicação a partir deste teclado ou utilizando um Teclado no Ecrã, se estiver disponível (consulte a figura abaixo). Este procedimento é conhecido como autorização de teclado.

Se o código tiver sido introduzido corretamente, a aplicação guarda os parâmetros de identificação – VID/PID do teclado e o número da porta à qual foi ligado – na lista de teclados autorizados. A autorização de teclado não precisa de ser repetida quando o teclado voltar a ser ligado ou depois de o sistema operativo ser reiniciado.

Quando o teclado autorizado é ligado ao computador numa porta USB diferente, a aplicação mostra uma solicitação para uma nova autorização deste teclado.

Se o código numérico tiver sido introduzido incorretamente, a aplicação gera um novo código. Pode configurar o número de tentativas de introdução do código numérico. Se o código numérico for introduzido incorretamente várias vezes ou a janela de autorização de teclado estiver fechada (ver figura abaixo), a aplicação bloqueia a ativação deste teclado. Após decorrido o tempo de bloqueio de dispositivo USB ou o sistema operativo ser reiniciado, a aplicação solicita ao utilizador que execute novamente a autorização do teclado.

A aplicação permite a utilização de um teclado autorizado e bloqueia um teclado que não foi autorizado.



Autorização de teclado

Ativar e desativar Prevenção de ataques BadUSB

Os dispositivos USB identificados pelo sistema operativo como teclados e ligados ao computador antes da instalação do componente "Prevenção de ataques BadUSB" são considerados autorizados após a instalação do componente.

Como ativar ou desativar o componente Prevenção de ataques BadUSB na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção essencial contra ameaças** → **Prevenção de ataques BadUSB**.
4. Use a caixa de verificação **Prevenção de ataques BadUSB** para ativar ou desativar o componente.
5. No bloco **Autorização de dispositivo USB na conexão**, ajuste as definições de segurança para a introdução do código de autorização:
   - **Número máximo de tentativas de autorização do dispositivo USB**. Bloquear automaticamente o dispositivo USB se o código de autorização for introduzido incorretamente o número especificado de vezes. Os valores válidos são de 1 a 10. Por exemplo, se permitir cinco tentativas de introdução do código de autorização, a aplicação bloqueia o dispositivo USB após a quinta tentativa sem sucesso. O Kaspersky Endpoint Security apresenta a duração do bloqueio do dispositivo USB. Após decorrido este tempo, tem novamente cinco tentativas para introduzir 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 sem sucesso 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 guarde as suas alterações.

Como ativar ou desativar o componente Prevenção de ataques BadUSB na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **BadUSB Attack Prevention**.
5. Use o botão de alternar da **BadUSB Attack Prevention ENABLED** para ativar ou desativar o componente.

6. No bloco **Authorization of USB devices**, ajuste as definições de segurança para a introdução do código de autorização:

   - **Maximum number of USB device authorization attempts**. Bloquear automaticamente o dispositivo USB se o código de autorização for introduzido incorretamente o número especificado de vezes. Os valores válidos são de 1 a 10. Por exemplo, se permitir cinco tentativas de introdução do código de autorização, a aplicação bloqueia o dispositivo USB após a quinta tentativa sem sucesso. O Kaspersky Endpoint Security apresenta a duração do bloqueio do dispositivo USB. Após decorrido este tempo, tem novamente cinco tentativas para introduzir o código de autorização.

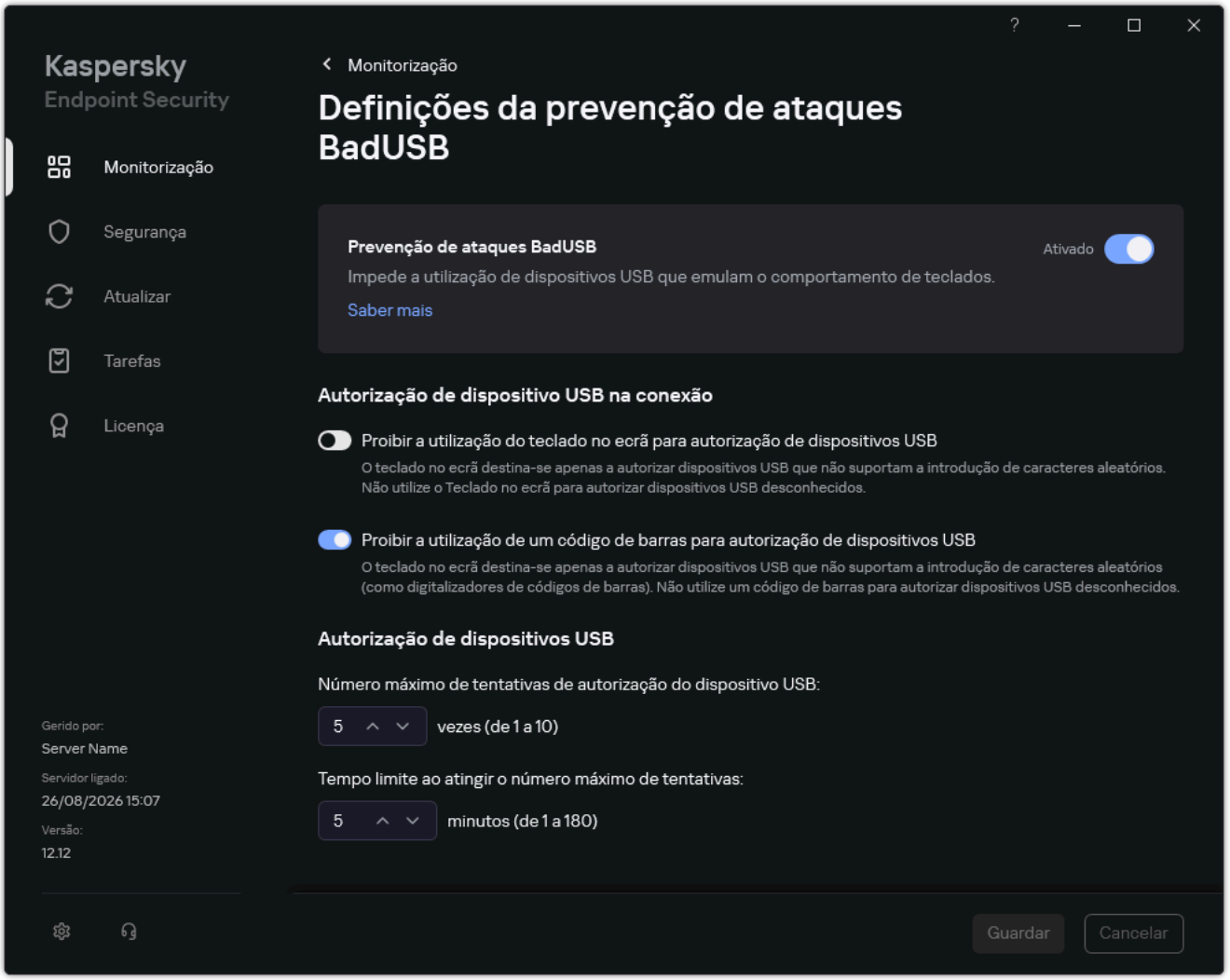
   - **Timeout when reaching the maximum number of attempts (min)**. Duração do bloqueio do dispositivo USB após o número especificado de tentativas sem sucesso de inserir o código de autorização. Os valores válidos são de 1 a 180 (minutos).

7. Guarde as suas alterações.

Como ativar ou desativar o componente Prevenção de ataques BadUSB na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Prevenção de ataques BadUSB**.



Definições do componente de Prevenção de ataques BadUSB

3. Use o botão de alternar da **Prevenção de ataques BadUSB** para ativar ou desativar o componente.

4. No bloco **Autorização de dispositivo USB na conexão**, ajuste as definições de segurança para a introdução do código de autorização:

    - **Número máximo de tentativas de autorização do dispositivo USB**. Bloquear automaticamente o dispositivo USB se o código de autorização for introduzido incorretamente o número especificado de vezes. Os valores válidos são de 1 a 10. Por exemplo, se permitir cinco tentativas de introdução do código de autorização, a aplicação bloqueia o dispositivo USB após a quinta tentativa sem sucesso. O Kaspersky Endpoint Security apresenta a duração do bloqueio do dispositivo USB. Após decorrido este tempo, tem novamente cinco tentativas para introduzir 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 sem sucesso de inserir o código de autorização. Os valores válidos são de 1 a 180 (minutos).

5. Guarde as suas alterações.

Como resultado, se a Prevenção de Ataques BadUSB estiver ativada, o Kaspersky Endpoint Security solicita a autorização de um dispositivo USB ligado identificado como um teclado pelo sistema operativo. O utilizador não pode usar um teclado não autorizado até que este seja autorizado.

Utilizar o teclado no ecrã para autorização de dispositivos USB

O teclado no ecrã apenas deve ser utilizado para a autorização de dispositivos USB que não suportam a introdução de carateres aleatórios (como leitores de códigos de barras). Não recomendamos a utilização do teclado no ecrã para a autorização de dispositivos USB desconhecidos.

Como permitir ou proibir o uso do teclado no ecrã para autorização na Consola de administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Proteção essencial contra ameaças → Prevenção de ataques BadUSB**.

4. Utilize a caixa de verificação **Proibir a utilização do teclado no ecrã para autorização de dispositivos USB** para bloquear ou permitir a utilização do teclado no ecrã para autorização.

5. Guarde as suas alterações.

Como permitir ou proibir o uso do teclado no ecrã para autorização na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

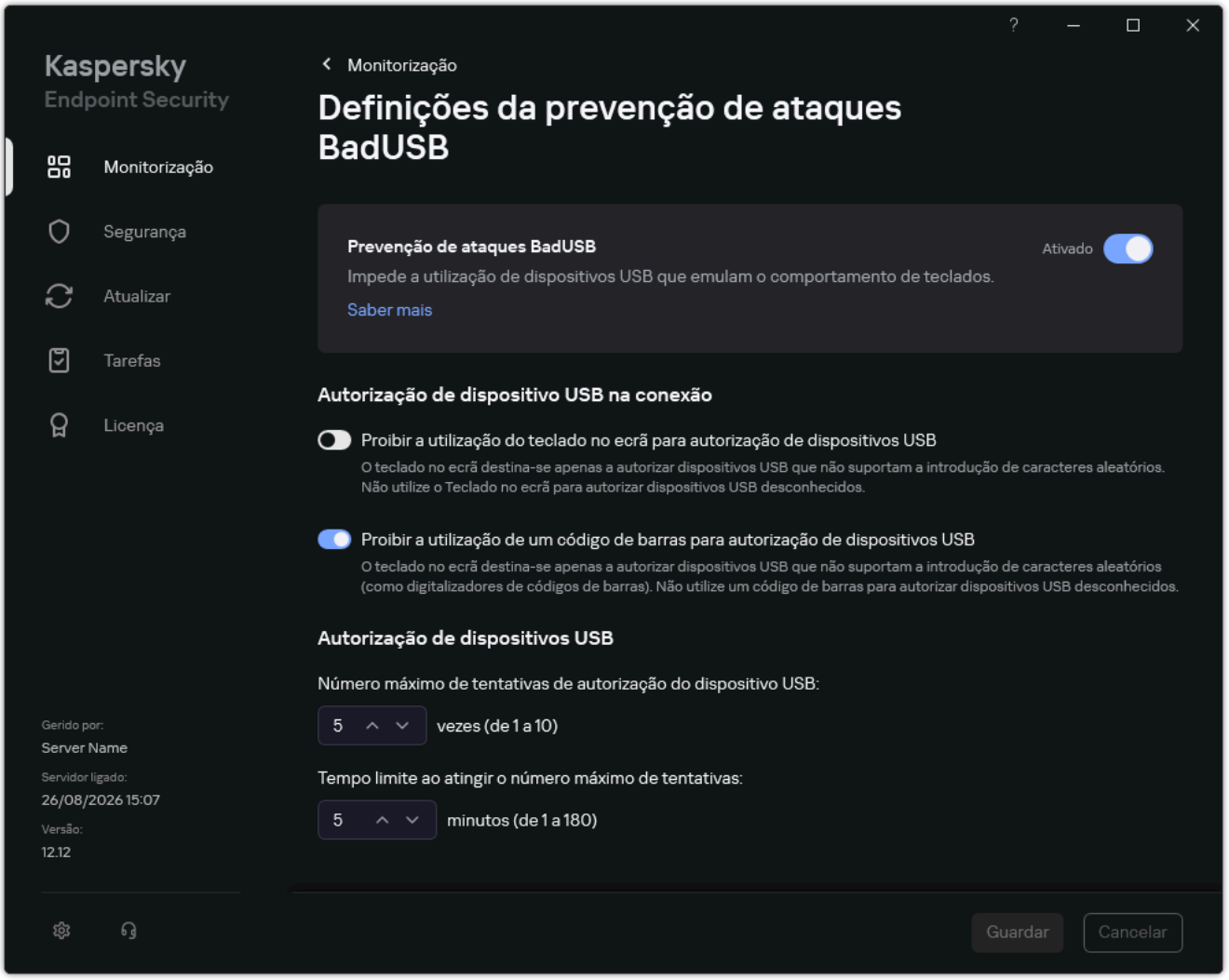
4. Aceda a **Host Threat Protection → BadUSB Attack Prevention**.

5. Utilize a opção **Prohibit use of On-Screen Keyboard for authorization of USB devices** para bloquear ou permitir a utilização do teclado no ecrã para autorização.

6. Guarde as suas alterações.

Como permitir ou proibir o uso do teclado no ecrã para autorização na interface da aplicação

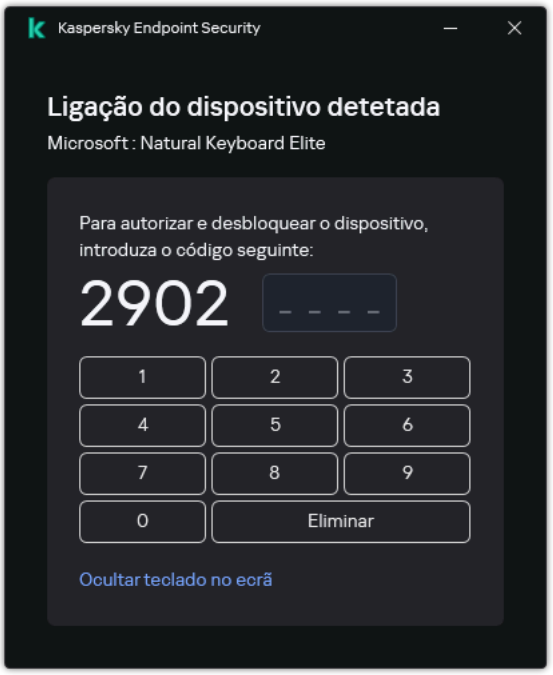
1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Prevenção de ataques BadUSB**.



Definições do componente de Prevenção de ataques BadUSB

3. Utilize a opção **Proibir a utilização do teclado no ecrã para autorização de dispositivos USB** para bloquear ou permitir a utilização do teclado no ecrã para autorização.

4. Guarde as suas alterações.



Autorização de dispositivos USB

Autorização do leitor de código de barras

Ao ligar um leitor de código de barras ao computador, o componente Prevenção de ataques BadUSB identifica este dispositivo como um dispositivo de entrada e pede-lhe que execute a autorização. Para autorizar o leitor de código de barras, deve verificar um código de barras exibido no monitor. A aplicação gera um código de barras no formato Code39 que é suportado pela maioria dos leitores de código de barras e códigos QR.

O Kaspersky Endpoint Security também suporta outro método de autorização do leitor de código de barras. Se estiver a utilizar dispositivos com ecrã tátil, pode utilizar um teclado no ecrã para digitar um código. Para fazer isso, precisa de permitir o teclado no ecrã. Este método é conveniente, por exemplo, no caso de leitores de código de barras fixos incorporados em caixas registadoras. Outros métodos de autorização do leitor de código de barras são proibidos.

Por defeito, a aplicação não utiliza um código de barras para autorização de dispositivos USB.

Como ativar a autorização do dispositivo USB por código de barras na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.

2. Na árvore da consola, selecione **Policies**.

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

4. Na janela de política, selecione **Proteção essencial contra ameaças → Prevenção de ataques BadUSB**.

5. Utilize a caixa de verificação **Proibir a utilização de um código de barras para autorização de dispositivos USB** para bloquear ou permitir a utilização de códigos de barras para autorização.

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

Como ativar a autorização do dispositivo USB por código de barras na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Host Threat Protection** → **BadUSB Attack Prevention**.

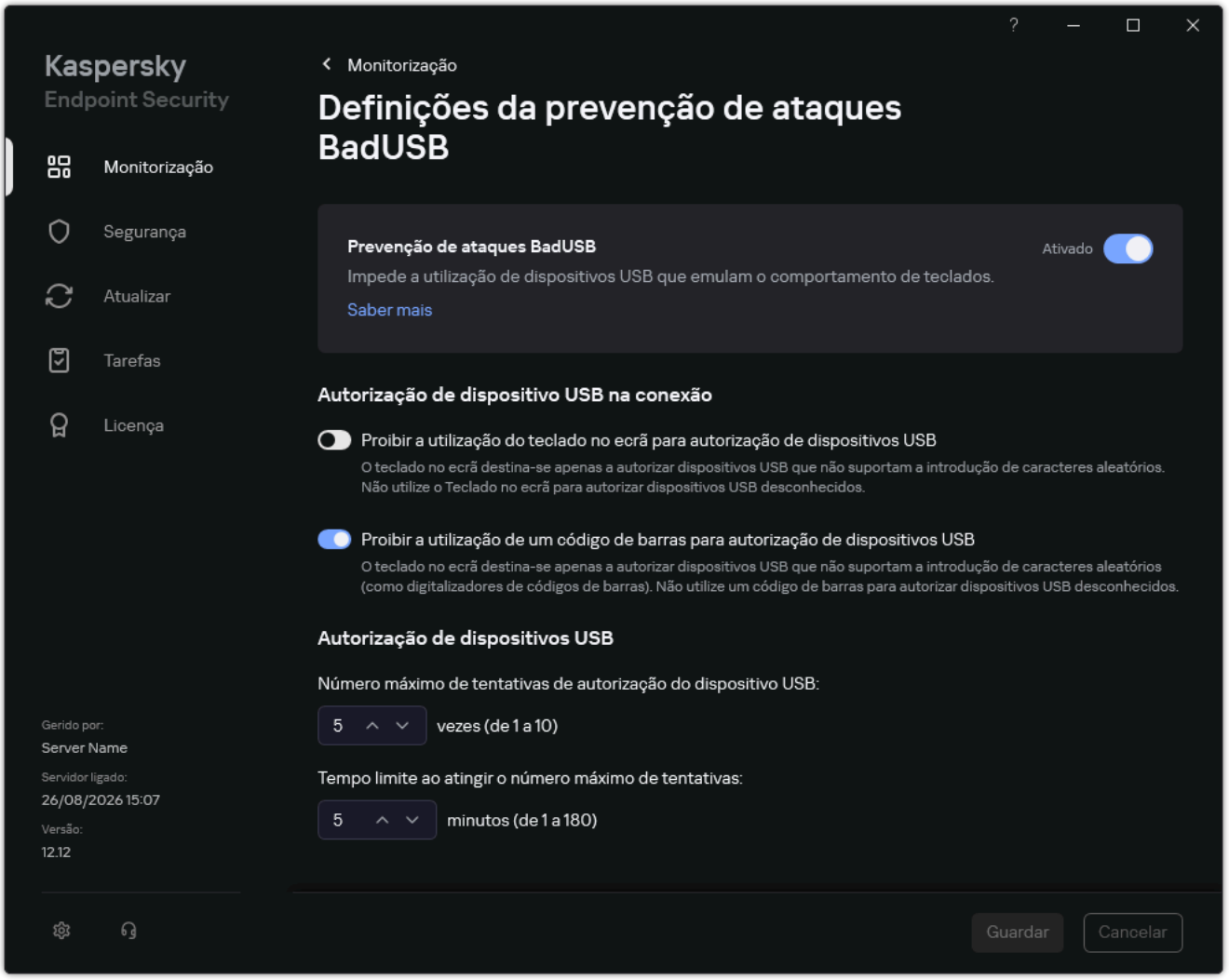
5. Utilize o botão de alternar **Prohibit use of a barcode for authorization of USB devices** para bloquear ou permitir a utilização do teclado no ecrã para autorização.

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

Como ativar a autorização do dispositivo USB por código de barras na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

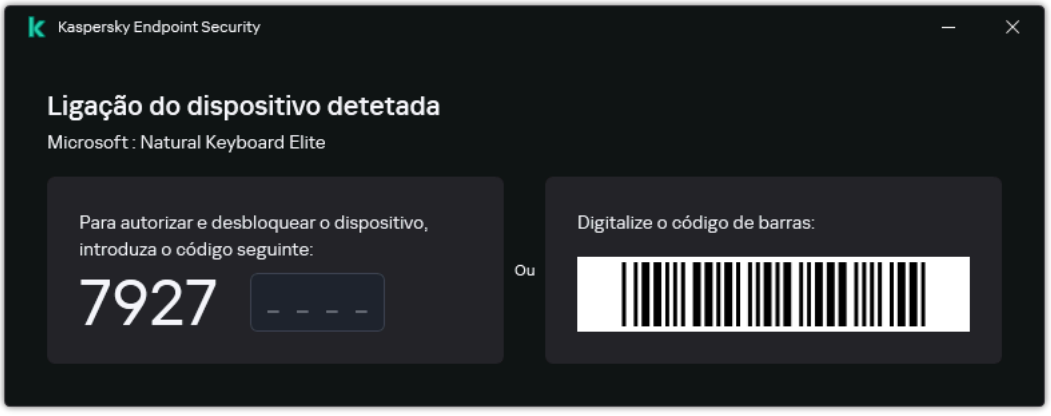
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Prevenção de ataques BadUSB**.



Definições do componente de Prevenção de ataques BadUSB

3. Utilize o botão de alternar **Proibir a utilização de um código de barras para autorização de dispositivos USB** para bloquear ou permitir a utilização do teclado no ecrã para autorização.

4. Guarde as suas alterações.

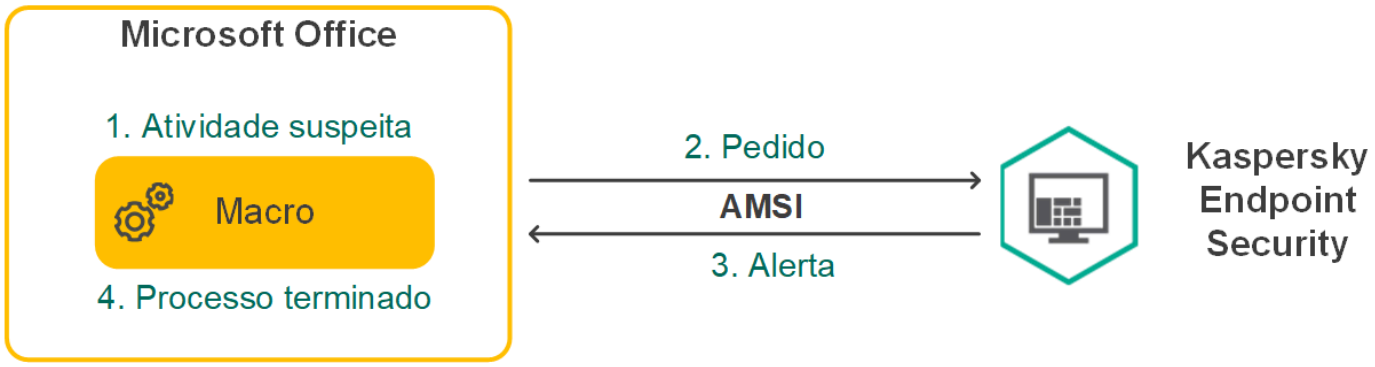


Autorização do leitor de código de barras

Proteção AMSI

O componente de Proteção AMSI destina-se a fins de suporte da Antimalware Scan Interface da Microsoft. A *Antimalware Scan Interface (AMSI)* permite às aplicações de terceiros com suporte AMSI enviar objetos (por exemplo, scripts PowerShell) ao Kaspersky Endpoint Security para uma verificação adicional e receber depois os resultados de verificação destes objetos. As aplicações de terceiros podem incluir, por exemplo, aplicações do Microsoft Office (ver a figura abaixo). Consulte a documentação da Microsoft, para obter informações mais detalhadas sobre AMSI.

A Proteção AMSI só pode detetar uma ameaça e notificar uma aplicação de terceiros sobre a ameaça detetada. Uma aplicação de terceiros depois de receber uma notificação de uma ameaça não permite as ações maliciosas (por exemplo, termina a ação).



Exemplo de operação AMSI

O componente de Proteção AMSI pode recusar um pedido de uma aplicação de terceiros, por exemplo, se esta aplicação exceder o número máximo de pedidos dentro de um intervalo especificado. O Kaspersky Endpoint Security envia informações sobre um pedido rejeitado de uma aplicação de terceiros para o servidor de administração. O componente Proteção AMSI não nega pedidos de aplicações de terceiros para os quais a integração contínua com o componente Proteção AMSI está ativado.

A Proteção AMSI está disponível para os seguintes sistemas operativos para estações de trabalho e servidores:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-sessão
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-sessão
- 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 predefinição, a Proteção AMSI está ativada e a funcionar no modo recomendado pela Kaspersky (consulte a tabela abaixo).

Como ativar ou desativar a Proteção AMSI na Consola de Administração (MMC)

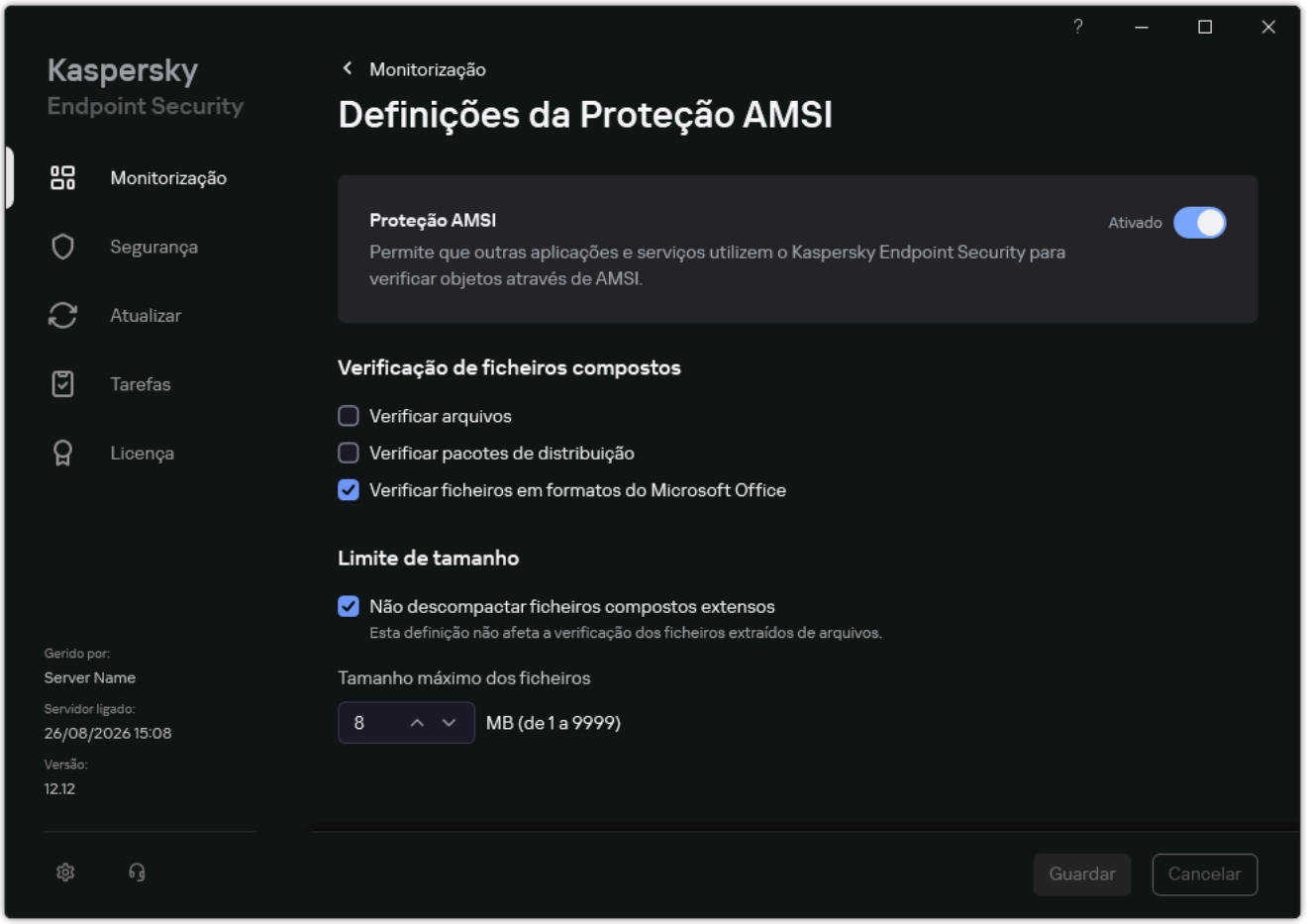
1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção essencial contra ameaças** → **Scanner AMSI**.
4. Use a caixa de verificação **Scanner AMSI** para ativar ou desativar o componente.
5. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar ou desativar a Proteção AMSI na Web Console e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **AMSI Protection**.
5. Use o botão de alternar da **AMSI Protection ENABLED** para ativar ou desativar o componente.
6. Guarde as suas alterações. Para aplicar a política em computadores, feche os cadeados .

Como ativar ou desativar a Proteção AMSI na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção AMSI**.



Definições de Proteção AMSI

3. Use o botão de alternar da **Proteção AMSI** para ativar ou desativar o componente.
4. Guarde as suas alterações.

Definições de Proteção AMSI recomendadas por especialistas da Kaspersky

Parâmetro	Valor	Descrição
Verificar arquivos	**Desativado**	A verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros arquivos. A aplicação verifica arquivos não só pela extensão, mas também pelo formato. Ao verificar os arquivos, a aplicação efetua uma descompactação recursiva. Isto permite a deteção de ameaças dentro de arquivos multinível (um arquivo dentro de um arquivo).
Verificar pacotes de distribuição	**Desativado**	Verificar pacotes de distribuição de aplicações de terceiros.
Verificar ficheiros em formatos do Microsoft Office	**Ativado**	Verifica ficheiros do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Ficheiros de formato do Office incluem objetos OLE também. A aplicação verifica ficheiros em formato de escritório menores que 1 MB, independentemente de a caixa de seleção estar marcada ou não.
Não descompactar ficheiros compostos extensos	**Tamanho máximo dos ficheiros 8 MB**	Se esta caixa de verificação estiver selecionada, a aplicação não verifica ficheiros compostos se o tamanho destes exceder o valor especificado. Se esta caixa de verificação for desmarcada, a aplicação verifica ficheiros compostos de todos os tamanhos. A aplicação verifica ficheiros grandes extraídos de arquivos, independentemente de a caixa de seleção estar selecionada ou não.

Otimizar a verificação de ficheiros pela Proteção AMSI

Pode otimizar a verificação de ficheiros: reduzir a duração da verificação e aumentar a velocidade de funcionamento do Kaspersky Endpoint Security. Pode selecionar os ficheiros compostos que necessitam de ser verificados: arquivos, pacotes de distribuição ou ficheiros em formatos do office. Também pode limitar o tamanho dos ficheiros compostos a serem verificados. O componente de Proteção AMSI não descompacta ficheiros compostos maiores do que o tamanho especificado.

Uma técnica comum para ocultar vírus e outro software malicioso consiste em integrar os mesmos em ficheiros compostos como, por exemplo, arquivos. Para detetar vírus e outro software malicioso que estejam ocultos desta forma, é necessário descompactar o ficheiro composto, o que pode reduzir a velocidade da verificação. Pode limitar o tipo de ficheiros compostos a verificar, acelerando assim a verificação.

Como otimizar a verificação de ficheiros pela Proteção AMSI na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção essencial contra ameaças** → **Scanner AMSI**.
4. No bloco **Verificação de ficheiros compostos**, especifique os tipos de ficheiros compostos que pretende verificar: arquivos, pacotes de distribuição ou ficheiros em formatos do office.
5. No bloco **Limite de tamanho**, execute uma das seguintes ações:
   - Para impedir que o componente de Proteção AMSI descompacte ficheiros compostos de grandes dimensões, selecione a caixa de verificação **Não descompactar ficheiros compostos extensos** e especifique o valor pretendido. O componente de Proteção AMSI não descompacta ficheiros compostos maiores do que o tamanho especificado.
   - Para permitir que o componente de Proteção AMSI descompacte ficheiros compostos de grandes dimensões, desmarque a caixa de verificação **Não descompactar ficheiros compostos extensos**.

   O componente de Proteção AMSI verifica ficheiros extensos extraídos de arquivos, independentemente de a caixa de verificação **Não descompactar ficheiros compostos extensos** estar ou não selecionada.
6. Guarde as suas alterações. Para aplicar a política em computadores, feche os cadeados .

Como otimizar a verificação de ficheiros pela Proteção AMSI na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **AMSI Protection**.

5. No bloco **Scan of compound files**, especifique os tipos de ficheiros compostos que pretende verificar: arquivos, pacotes de distribuição ou ficheiros em formatos do office.

6. No bloco **Scan optimization**, execute uma das seguintes ações:

   - Para impedir que o componente de Proteção AMSI descompacte ficheiros compostos de grandes dimensões, selecione a caixa de verificação **Size limits enabled** e especifique o valor pretendido. O componente de Proteção AMSI não descompacta ficheiros compostos maiores do que o tamanho especificado.

   - Para permitir que o componente de Proteção AMSI descompacte ficheiros compostos de grandes dimensões, desmarque a caixa de verificação **Size limits enabled**.

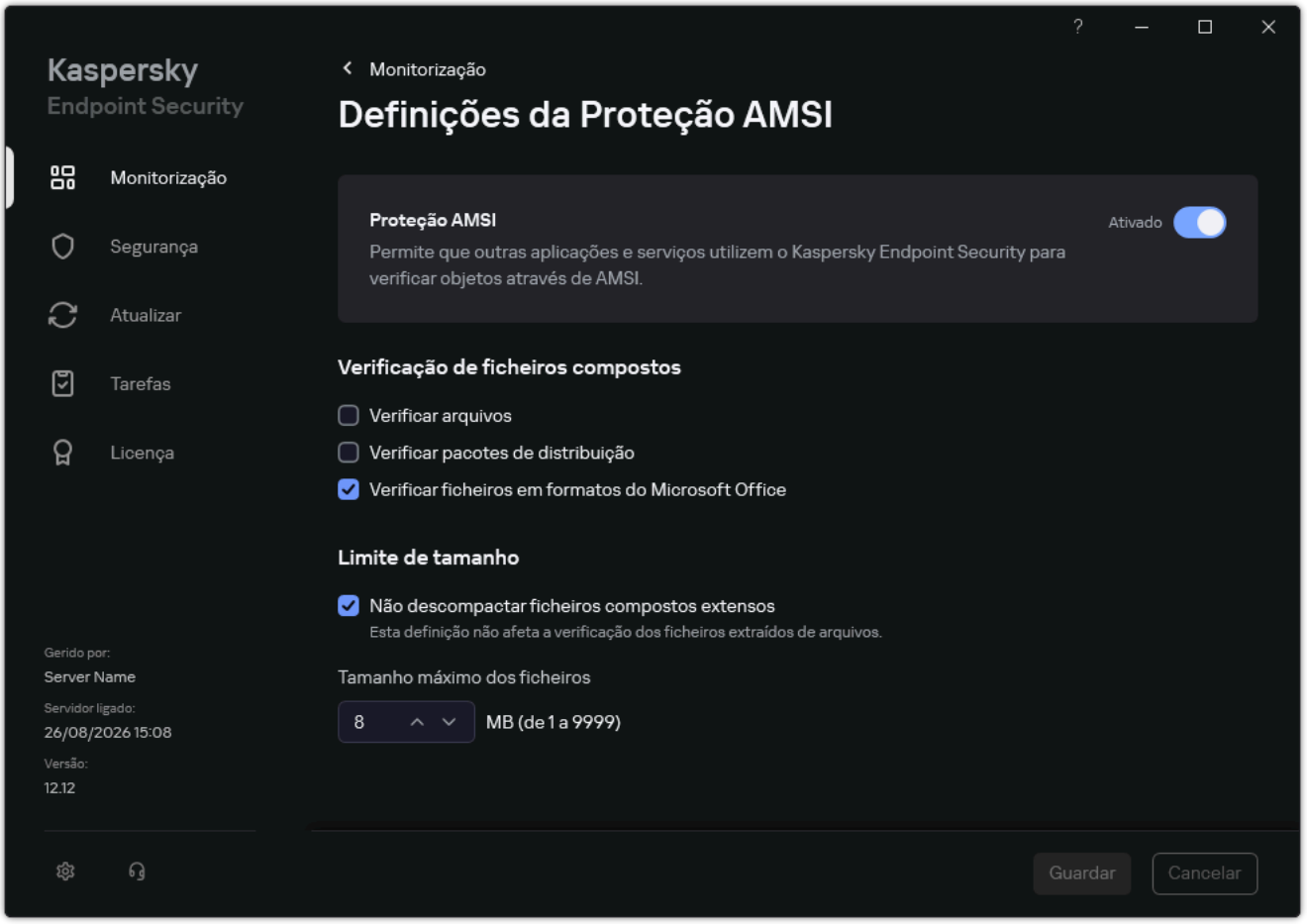
   O componente de Proteção AMSI verifica ficheiros extensos extraídos de arquivos, independentemente de a caixa de verificação **Size limits enabled** estar ou não selecionada.

7. Guarde as suas alterações. Para aplicar a política em computadores, feche os cadeados.

Como otimizar a verificação de ficheiros pela Proteção AMSI na interface da aplicação

1. Na janela principal da aplicação, clique no botão .

2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção AMSI**.



Definições de Proteção AMSI

3. No bloco **Verificação de ficheiros compostos**, especifique os tipos de ficheiros compostos que pretende verificar: arquivos, pacotes de distribuição ou ficheiros em formatos do office.

4. No bloco **Limite de tamanho**, execute uma das seguintes ações:

   - Para impedir que o componente de Proteção AMSI descompacte ficheiros compostos de grandes dimensões, selecione a caixa de verificação **Não descompactar ficheiros compostos extensos** e especifique o valor pretendido. O componente de Proteção AMSI não descompacta ficheiros compostos maiores do que o tamanho especificado.

   - Para permitir que o componente de Proteção AMSI descompacte ficheiros compostos de grandes dimensões, desmarque a caixa de verificação **Não descompactar ficheiros compostos extensos**.

   O componente de Proteção AMSI verifica ficheiros extensos extraídos de arquivos, independentemente de a caixa de verificação **Não descompactar ficheiros compostos extensos** estar ou não selecionada.

5. Guarde as suas alterações.

Proteção contra ameaças da Web

O componente Proteção contra ameaças da Web impede a transferência de ficheiros maliciosos da Internet e também bloqueia a ligação a sites maliciosos e de phishing. O componente fornece proteção ao computador com a ajuda das bases de dados antivírus, o serviço de nuvem da Kaspersky Security Network e análise heurística.

O Kaspersky Endpoint Security monitoriza os tráfegos HTTP, HTTPS e FTP. O Kaspersky Endpoint Security monitoriza URL e endereços IP.

Para utilizar a Proteção contra ameaças da Web, tem de concluir a configuração inicial da aplicação:

- Para monitorização do tráfego HTTPS, ative a verificação de ligações encriptadas (ativado por padrão).
- Selecione as portas que o Kaspersky Endpoint Security deve monitorizar (por defeito, a aplicação monitoriza todas as portas).
- Selecione as aplicações cujo tráfego pretende que o Kaspersky Endpoint Security monitorize. A maioria dos navegadores já está presente na lista de aplicações recomendadas pela Kaspersky. Se o seu navegador não estiver na lista, adicione-o manualmente.
- Recomendamos que injete um script de interação de página de Internet no tráfego de Internet (por padrão, a injeção de script está desativada). Este script permite o registo de eventos de Proteção contra ameaças da Web para o registo de eventos da aplicação, registo de eventos do SO e relatórios.

Quando um utilizador tenta abrir um website de phishing ou malicioso, o Kaspersky Endpoint Security bloqueia o acesso e apresenta um aviso.

Ativar e desativar a Proteção contra ameaças da Web

Por predefinição, o componente Proteção contra ameaças da Web está ativado e é executado no modo recomendado pelos especialistas da Kaspersky. Para Proteção contra ameaças da Web, a aplicação pode aplicar diferentes grupos de definições. Estes grupos de definições armazenados na aplicação chamam-se *níveis de segurança*: **Alto**, **Recomendado**, **Baixo**. Considera-se que as definições de nível de segurança de tráfego de Internet **Recomendado** são as definições ideais recomendadas pelos especialistas da Kaspersky (consulte a tabela abaixo). Pode selecionar um dos níveis de segurança pré-instalados de tráfego de Internet recebido ou transmitido através dos protocolos HTTP e FTP, ou configurar um nível de segurança de tráfego de Internet personalizado. Se alterar as definições do nível de segurança de tráfego de Internet, pode sempre repor as definições de nível de segurança de tráfego de Internet recomendadas.

Pode selecionar ou configurar o nível de segurança apenas na Consola de Administração (MMC) ou na interface local da aplicação. Não pode selecionar ou configurar o nível de segurança na Consola Web ou na Cloud Console.

Como ativar ou desativar o componente Proteção contra ameaças da web na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças da web**.
4. Use a caixa de verificação **Proteção contra ameaças da Web** para ativar ou desativar o componente.
5. Se ativou este componente, execute uma das seguintes ações no bloco **Nível de segurança**:
   - Se quiser aplicar um dos níveis de segurança predefinidos, selecione-o com o controlo de deslize:
     - **Elevado**. O nível de segurança utilizado pelo componente Proteção contra ameaças da Web para efetuar a verificação máxima do tráfego de Internet que um computador recebe via HTTP e FTP. A Proteção contra ameaças da Web verifica detalhadamente todos os objetos de tráfego de Internet, recorrendo à utilização do conjunto completo de bases de dados da aplicação, e executa a análise heurística mais aprofundada possível.
     - **Recomendado**. O nível de segurança que fornece o equilíbrio ideal entre o desempenho da aplicação e a segurança do tráfego de Internet. O componente Proteção contra ameaças da Web executa a análise heurística com o Nível médio de verificação. Este nível de segurança de tráfego de Internet é recomendado pelos especialistas da Kaspersky. Os valores das definições para o nível de segurança recomendado são fornecidos na tabela abaixo.
     - **Baixo**. As definições deste nível de segurança de tráfego de Internet asseguram a verificação mais rápida de tráfego de Internet. O componente Proteção contra ameaças da Web executa a análise heurística com o Nível superficial de verificação.
   - Se pretender configurar um nível de segurança personalizado, clique no botão **Definições** e defina as suas próprias definições do componente (consulte a tabela abaixo).

     Pode restaurar os valores dos níveis de segurança predefinidos ao clicar no botão **Por defeito**.

6. No bloco **Ação após deteção de ameaças**, selecione a ação executada pelo Kaspersky Endpoint Security em objetos maliciosos de tráfego de Internet:

   - **Bloquear**. Se esta opção estiver selecionada e um objeto for detetado do tráfego de Internet, o componente Proteção contra ameaças da Web bloqueia o acesso ao objeto e apresenta uma mensagem no navegador.

   - **Informar**. Se essa opção for selecionada e um objeto infetado for detetado no tráfego de Internet, o Kaspersky Endpoint Security permitirá que esse objeto seja descarregado para o computador, mas adiciona informações sobre o objeto infetado à lista de ameaças ativas.

7. Guarde as suas alterações.

Como ativar ou desativar o componente Proteção contra ameaças da Web na Web Console

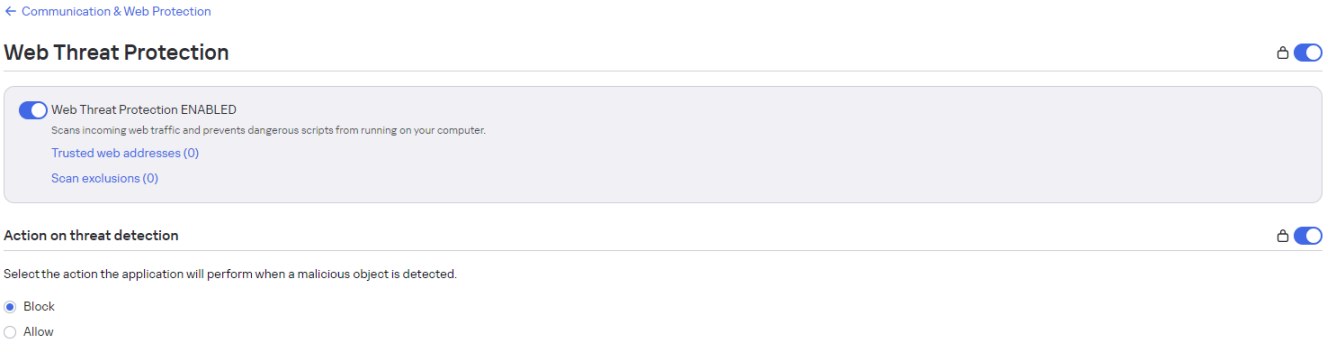
1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Communication & Web Protection** → **Web Threat Protection**.



Definições da Proteção contra ameaças da Web

5. Use o botão de alternar da **Web Threat Protection ENABLED** para ativar ou desativar o componente.

6. No bloco **Action on threat detection**, selecione a ação executada pelo Kaspersky Endpoint Security em objetos maliciosos de tráfego de Internet:

   - **Block**. Se esta opção estiver selecionada e um objeto for detetado do tráfego de Internet, o componente Proteção contra ameaças da Web bloqueia o acesso ao objeto e apresenta uma mensagem no navegador.

   - **Allow, inform, or prompt for action (depends on OS)**. Se essa opção for selecionada e um objeto infetado for detetado no tráfego de Internet, o Kaspersky Endpoint Security permitirá que esse objeto seja descarregado para o computador, mas adiciona informações sobre o objeto infetado à lista de ameaças ativas.

7. Se necessário, faça uma lista de endereços da Internet fiáveis.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar ou desativar o componente Proteção contra ameaças da Web

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças da Web**.
3. Use o botão de alternar da **Proteção contra ameaças da Web** para ativar ou desativar o componente.
4. Se ativou este componente, execute uma das seguintes ações no bloco **Nível de segurança**:
   - Se quiser aplicar um dos níveis de segurança predefinidos, selecione-o com o controlo de deslize:
     - **Alto**. O nível de segurança utilizado pelo componente Proteção contra ameaças da Web para efetuar a verificação máxima do tráfego de Internet que um computador recebe via HTTP e FTP. A Proteção contra ameaças da Web verifica detalhadamente todos os objetos de tráfego de Internet, recorrendo à utilização do conjunto completo de bases de dados da aplicação, e executa a análise heurística mais aprofundada possível.
     - **Recomendado**. O nível de segurança que fornece o equilíbrio ideal entre o desempenho da aplicação e a segurança do tráfego de Internet. O componente Proteção contra ameaças da Web executa a análise heurística com o Nível médio de verificação. Este nível de segurança de tráfego de Internet é recomendado pelos especialistas da Kaspersky. Os valores das definições para o nível de segurança recomendado são fornecidos na tabela abaixo.
     - **Baixo**. As definições deste nível de segurança de tráfego de Internet asseguram a verificação mais rápida de tráfego de Internet. O componente Proteção contra ameaças da Web executa a análise heurística com o Nível superficial de verificação.
   - Se pretender configurar um nível de segurança personalizado, clique no botão **Definições avançadas** e defina as suas próprias definições do componente (consulte a tabela abaixo).

     Pode restaurar os valores dos níveis de segurança predefinidos ao clicar no botão **Restaurar nível de segurança recomendado**.
5. No bloco **Ação após deteção de ameaças**, selecione a ação executada pelo Kaspersky Endpoint Security em objetos maliciosos de tráfego de Internet:
   - **Bloquear**. Se esta opção estiver selecionada e um objeto for detetado do tráfego de Internet, o componente Proteção contra ameaças da Web bloqueia o acesso ao objeto e apresenta uma mensagem no navegador.
   - **Informar**. Se essa opção for selecionada e um objeto infetado for detetado no tráfego de Internet, o Kaspersky Endpoint Security permitirá que esse objeto seja descarregado para o computador, mas adiciona informações sobre o objeto infetado à lista de ameaças ativas.
6. Guarde as suas alterações.

Definições de Proteção contra ameaças da Web recomendadas pelos especialistas da Kaspersky (nível de segurança recomendado)

Parâmetro	Valor	Descrição
Verificar o endereço da Internet contra a base de dados de endereços da internet maliciosos	**Ativado**	A verificação das ligações para determinar se estão incluídas na base de dados de endereços Web maliciosos permite localizar sites que foram adicionados à lista de bloqueio. A base de dados de endereços da Web maliciosos é mantida pela Kaspersky, incluída no pacote de instalação da aplicação e atualizada durante as atualizações da base de dados do Kaspersky Endpoint Security.
Verificar o endereço da Internet contra a base de dados de endereços da Internet de phishing	**Ativado**	A base de dados de endereços da Web de phishing inclui os endereços da Web de sites atualmente conhecidos, que são utilizados para iniciar ataques de phishing. A Kaspersky complementa esta base de dados de ligações de phishing com endereços obtidos da organização internacional Anti-Phishing Working Group. A base de dados de endereços de phishing está incluída no pacote de instalação da aplicação e é complementada com atualizações da base de dados do Kaspersky Endpoint Security.
Usar análise heurística (Proteção contra ameaças da Web)	**Nível médio**	A tecnologia foi desenvolvida para detetar ameaças que não é possível detetar utilizando a versão atual das bases de dados da aplicação da Kaspersky. Permite detetar ficheiros que podem estar infetados com um vírus desconhecido ou com uma variante de um vírus conhecido. Quando o tráfego da Internet é verificado quanto a vírus e outras aplicações que apresentam uma ameaça, o analisador heurístico executa instruções nos ficheiros executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível da análise heurística garante um equilíbrio entre o detalhe das procuras de novas ameaças, a carga nos recursos do sistema operativo e a duração da análise heurística.
Usar análise heurística (Anti-Phishing)	**Ativado**	A tecnologia foi desenvolvida para detetar ameaças que não é possível detetar utilizando a versão atual das bases de dados da aplicação da Kaspersky. Permite detetar ficheiros que podem estar infetados com um vírus desconhecido ou com uma variante de um vírus conhecido.
Ação após deteção de ameaças	**Bloquear**	Se esta opção estiver selecionada e um objeto for detetado do tráfego de Internet, o componente Proteção contra ameaças da Web bloqueia o acesso ao objeto e apresenta uma mensagem no navegador.

Configurar métodos de deteção de endereços da Web maliciosos

A Proteção contra ameaças da web deteta endereços da web maliciosos através de bases de dados de antivírus, o serviço de nuvem da Kaspersky Security Network e a análise heurística.

Pode selecionar métodos de deteção de endereço da Internet maliciosos apenas na Consola de Administração (MMC) ou na interface local da aplicação. Não pode selecionar métodos de deteção de endereços da Internet maliciosos na Consola Web ou na Cloud Console. A opção predefinida é verificar os endereços da Internet em relação às bases de dados de endereços maliciosos com análise heurística (nível médio).

Verificação através da base de dados de endereços maliciosos

A verificação das ligações para determinar se estão incluídas na base de dados de endereços Web maliciosos permite localizar sites que foram adicionados à lista de bloqueio. A base de dados de endereços da Web maliciosos é mantida pela Kaspersky, incluída no pacote de instalação da aplicação e atualizada durante as atualizações da base de dados do Kaspersky Endpoint Security.

O Kaspersky Endpoint Security verifica todas as ligações para determinar se estão listadas em bases de dados de endereços Web maliciosos. As definições de verificação de ligação segura da aplicação não afetam a funcionalidade de verificação de ligações. Por outras palavras, se a verificação de ligações encriptadas estiver desativada, o Kaspersky Endpoint Security verifica as ligações por comparação com bases de dados de endereços Web maliciosos, ainda que o tráfego de rede seja transmitido através de uma ligação encriptada.

Como ativar ou desativar a verificação de endereços da Internet em relação à base de dados de endereços da Internet maliciosos através da Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças da web**.
4. No bloco **Nível de segurança**, clique no botão **Definições**.
5. Na janela que se abre, no bloco **Métodos de verificação**, selecione ou desmarque a caixa de verificação **Verificar o endereço da Internet contra a base de dados de endereços da Internet maliciosos**, para ativar ou desativar a verificação de endereços em relação à base de dados de endereços Web maliciosos.
6. Guarde as suas alterações.

Como ativar ou desativar a verificação de endereços em relação à base de dados de endereços maliciosos na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças da Web**.
3. Clique em **Definições avançadas**.
4. No bloco **Métodos de verificação**, selecione ou desmarque a caixa de verificação **Verificar o endereço da Internet contra a base de dados de endereços da internet maliciosos**, para ativar ou desativar a verificação de endereços em relação à base de dados de endereços Web maliciosos.
5. Guarde as suas alterações.

Análise heurística

Durante a análise heurística, o Kaspersky Endpoint Security analisa a atividade de aplicações no sistema operativo. A análise heurística pode detetar novas ameaças para as quais não existem atualmente registos nas bases de dados do Kaspersky Endpoint Security.

Quando o tráfego da Internet é verificado quanto a vírus e outras aplicações que apresentam uma ameaça, o analisador heurístico executa instruções nos ficheiros executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível da análise heurística garante um equilíbrio entre o detalhe das procuras de novas ameaças, a carga nos recursos do sistema operativo e a duração da análise heurística.

Como ativar ou desativar a utilização da análise heurística na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção essencial contra ameaças → Proteção contra ameaças da web**.
4. No bloco **Nível de segurança**, clique no botão **Definições**.
5. Na janela que se abre, no bloco **Métodos de verificação**, selecione a caixa de verificação **Utilizar análise heurística** se quiser que a aplicação utilize a análise heurística ao verificar o tráfego de Internet em busca de vírus e outro malware.
6. Utilize a barra de deslocamento para definir o nível da análise heurística: **nível superficial**, **nível médio** ou **nível aprofundado**.

   Quando o tráfego da Internet é verificado quanto a vírus e outras aplicações que apresentam uma ameaça, o analisador heurístico executa instruções nos ficheiros executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível da análise heurística garante um equilíbrio entre o detalhe das procuras de novas ameaças, a carga nos recursos do sistema operativo e a duração da análise heurística.
7. Guarde as suas alterações.

Como ativar ou desativar a utilização da análise heurística na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças da Web**.
3. Clique em **Definições avançadas**.
4. No bloco **Métodos de verificação**, selecione a caixa de verificação **Usar análise heurística** se quiser que a aplicação utilize a análise heurística ao verificar o tráfego de Internet em busca de vírus e outro malware.

   Quando o tráfego da Internet é verificado quanto a vírus e outras aplicações que apresentam uma ameaça, o analisador heurístico executa instruções nos ficheiros executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível da análise heurística garante um equilíbrio entre o detalhe das procuras de novas ameaças, a carga nos recursos do sistema operativo e a duração da análise heurística.
5. Guarde as suas alterações.

Anti-Phishing

A Proteção contra ameaças da web verifica as ligações para ver se elas pertencem a endereços da Internet de phishing. Isto 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 uma ligação para o site oficial do mesmo. Ao clicar nessa ligação, é direcionado para uma cópia exata do site do banco, onde até o endereço web verdadeiro do banco é apresentado no navegador, apesar de, na verdade, estar num site falsificado. A partir deste momento, todas as suas ações no site são registadas e podem ser utilizadas para roubar o seu dinheiro.

Uma vez que as ligações para sites de phishing podem ser recebidas através de outras fontes além das mensagens de e-mail, por exemplo, em aplicações de mensagens, o componente Proteção contra ameaças da Web monitoriza as tentativas de acesso a um site de phishing ao nível do tráfego de Internet e bloqueia o acesso a esses sites. São incluídas listas de URL de phishing no kit de distribuição do Kaspersky Endpoint Security.

Pode configurar o Anti-phishing apenas na Consola de Administração (MMC) ou na interface local da aplicação. Não pode configurar o Anti-phishing na Consola Web ou na Cloud Console. O Anti-phishing com análise heurística está ativado por defeito.

Como ativar ou desativar o Anti-phishing na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção essencial contra ameaças → Proteção contra ameaças da web**.
4. No bloco **Nível de segurança**, clique no botão **Definições**.

5. Na janela que se abre, no bloco **Definições de Anti-Phishing**, selecione ou desmarque a caixa de verificação **Verificar o endereço da Internet contra a base de dados de endereços da Internet de phishing**, para ativar ou desativar o Anti-phishing.

   A base de dados de endereços da Web de phishing inclui os endereços da Web de sites atualmente conhecidos, que são utilizados para iniciar ataques de phishing. A Kaspersky complementa esta base de dados de ligações de phishing com endereços obtidos da organização internacional Anti-Phishing Working Group. A base de dados de endereços de phishing está incluída no pacote de instalação da aplicação e é complementada com atualizações da base de dados do Kaspersky Endpoint Security.

6. Selecione a caixa de verificação **Utilizar análise heurística** se quiser que a aplicação utilize a análise heurística ao verificar as páginas Web em busca de ligações de phishing.

   Durante a análise heurística, o Kaspersky Endpoint Security analisa a atividade de aplicações no sistema operativo. A análise heurística pode detetar novas ameaças para as quais não existem atualmente registos nas bases de dados do Kaspersky Endpoint Security.

   Para verificar ligações, além de bases de dados anti-vírus e análise heurística, pode utilizar as bases de dados de reputação do Kaspersky Security Network.

7. Guarde as suas alterações.

Como ativar ou desativar o Anti-phishing na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças da Web**.

3. Clique em **Definições avançadas**.

4. Se quiser que o componente de Proteção Contra Ameaças da Web verifique as ligações por comparação com as bases de dados de endereço da Internet de phishing, selecione a caixa de verificação **Verificar o endereço da Internet contra a base de dados de endereços da Internet de phishing** no bloco **Anti-phishing**. A base de dados de endereços da Web de phishing inclui os endereços da Web de sites atualmente conhecidos, que são utilizados para iniciar ataques de phishing. A Kaspersky complementa esta base de dados de ligações de phishing com endereços obtidos da organização internacional Anti-Phishing Working Group. A base de dados de endereços de phishing está incluída no pacote de instalação da aplicação e é complementada com atualizações da base de dados do Kaspersky Endpoint Security.

5. Selecione a caixa de verificação **Usar análise heurística** se quiser que a aplicação utilize a análise heurística ao verificar as páginas Web em busca de ligações de phishing.

   Durante a análise heurística, o Kaspersky Endpoint Security analisa a atividade de aplicações no sistema operativo. A análise heurística pode detetar novas ameaças para as quais não existem atualmente registos nas bases de dados do Kaspersky Endpoint Security.

   Para verificar ligações, além de bases de dados anti-vírus e análise heurística, pode utilizar as bases de dados de reputação do Kaspersky Security Network.

6. Guarde as suas alterações.

Criar a lista de URL fiáveis

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 atende aos padrões RFC. Pode criar uma lista de URL cujo conteúdo considera fiável. O componente Proteção contra ameaças da Web não analisa as informações de endereços da Internet fiáveis para verificar a existência de vírus ou de outras ameaças. Esta opção pode ser útil nos casos em que, por exemplo, o componente Proteção contra ameaças da Web interfere com a transferência de um ficheiro a partir de um site conhecido.

Um URL pode ser o endereço de uma página de Internet específica ou o endereço de um site.

Como adicionar um endereço da Internet fiável através da Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças da web**.
5. No bloco **Nível de segurança**, clique no botão **Definições**.
6. Na janela que abre, selecione o separador **Endereços da Internet fiáveis**.
7. Selecione a caixa de verificação **Não verificar tráfego de Internet de URL fiáveis**.

   Se esta opção estiver selecionada, o componente Proteção contra ameaças da Web não verifica o conteúdo de páginas de Internet ou websites cujos endereços estejam incluídos na lista de URL fiáveis. Pode adicionar o endereço específico e a máscara de endereço de uma página de Internet/site à lista de URL fiáveis.
8. Criar uma lista de URL/páginas da Internet cujo conteúdo é fiável.

   O Kaspersky Endpoint Security suporta os caracteres `*` e `?` ao introduzir uma máscara.

   Também pode importar uma lista de endereços da Internet fiáveis a partir de um ficheiro XML.
9. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como adicionar um endereço Web fiável na Web Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda à secção **Trusted Zone**.
5. Na janela que abre, clique na ligação **Web addresses**.

   Abre-se uma janela que contém uma lista de endereços Web fiáveis.

6. Criar uma lista de URL/páginas da Internet cujo conteúdo é fiável.

   O Kaspersky Endpoint Security suporta os caracteres `*` e `?` ao introduzir uma máscara.

   Também pode importar uma lista de endereços da Internet fiáveis a partir de um ficheiro JSON.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como adicionar um endereço da Internet fiável na interface da aplicação

1. Na janela principal da aplicação, clique no botão .

2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças da Web**.

3. Clique em **Definições avançadas**.

4. Selecione a caixa de verificação **Não analisar tráfego de Internet em URL fiáveis**.

   Se esta opção estiver selecionada, o componente Proteção contra ameaças da Web não verifica o conteúdo de páginas de Internet ou websites cujos endereços estejam incluídos na lista de URL fiáveis. Pode adicionar o endereço específico e a máscara de endereço de uma página de Internet/site à lista de URL fiáveis.

5. Criar uma lista de URL/páginas da Internet cujo conteúdo é fiável.

   O Kaspersky Endpoint Security suporta os caracteres `*` e `?` ao introduzir uma máscara.

   Também pode importar uma lista de endereços da Internet fiáveis a partir de um ficheiro XML.

6. Guarde as suas alterações.

Como resultado, a Proteção contra ameaças da web não verifica o tráfego de endereços da Internet fiáveis. O utilizador pode sempre abrir um site fidedigno e transferir um ficheiro desse site. Se não conseguiu obter acesso ao site, verifique as definições dos componentes Verificação de ligações encriptadas, Controlo de Internet e Monitorização de portas de rede. Se o Kaspersky Endpoint Security detetar um ficheiro transferido de um site fidedigno como malicioso, poderá adicionar este ficheiro às exclusões.

Também pode criar uma lista de exclusões gerais para ligações encriptadas. Neste caso, o Kaspersky Endpoint Security não verifica o tráfego HTTPS de endereços da Internet fiáveis quando os componentes Proteção contra ameaças da web, Proteção contra ameaças de correio e Controlo de Internet estão a fazer o seu trabalho.

Exportar e importar a lista de endereços Web fiáveis

Pode exportar a lista de endereços de Internet fiáveis para um ficheiro XML. Em seguida, pode modificar o ficheiro para, por exemplo, adicionar um grande número de endereços da Internet do mesmo tipo. Também pode usar a função de exportação/importação para fazer uma cópia de segurança da lista de endereços da Internet fiáveis ou para migrar a lista para um servidor diferente.

Como exportar e importar uma lista de endereços da Internet fiáveis na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Proteção essencial contra ameaças → Proteção contra ameaças da web**.

4. No bloco **Nível de segurança**, clique no botão **Definições**.

5. Na janela que abre, selecione o separador **Endereços da Internet fiáveis**.

6. Para exportar a lista de endereços de Internet fiáveis:

   a. Selecione os endereços de Internet fiáveis que pretende exportar. Para selecionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.

   Se não tiver selecionado nenhum endereço de Internet fiável, o Kaspersky Endpoint Security exportará todos os endereços de Internet.

   b. Clique na hiperligação **Exportar**.

   c. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de endereços de Internet fiáveis e selecione a pasta onde pretende guardar este ficheiro.

   d. Guardar o ficheiro.

   O Kaspersky Endpoint Security exporta toda a lista de endereços de Internet fiáveis para o ficheiro XML.

7. Para importar a lista de endereços fiáveis:

   a. Clique na hiperligação **Importar**.

   Na janela que se abre, selecione o ficheiro XML a partir do qual pretende importar a lista de URL fiáveis.

   b. Abrir o ficheiro.

   Se o computador já tiver uma lista de URL fiáveis, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas a esta lista a partir do ficheiro XML.

8. Guarde as suas alterações.

Como exportar e importar uma lista de endereços de Internet fiáveis na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Communication & Web Protection** → **Web Threat Protection**.

5. Para exportar a lista de exclusões no bloco **Rules list**:

   a. Selecione os endereços de Internet fiáveis que pretende exportar.

   b. Selecione o botão → **Export**.

   O Kaspersky Endpoint Security exporta a lista de endereços Web fiáveis para um ficheiro JSON na pasta de transferências predefinida.

6. Para importar a lista de exclusões no bloco **Rules list**:

   a. Selecione o botão → **Import**.

   Na janela que se abre, selecione o ficheiro JSON a partir do qual pretende importar a lista de URL fiáveis.

b. Abrir o ficheiro.

Se o computador já tiver uma lista de URL fiáveis, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas a esta lista a partir do ficheiro JSON.

7. Guarde as suas alterações.

Proteção contra ameaças de correio

O componente Proteção contra ameaças de correio verifica a existência de vírus e outras ameaças nos anexos das mensagens de e-mail recebidas e enviadas. O componente fornece proteção ao computador com a ajuda das bases de dados antivírus, o serviço de nuvem da Kaspersky Security Network e análise heurística.

A proteção contra ameaças ao correio verifica as mensagens recebidas e enviadas. A aplicação suporta POP3, SMTP, IMAP e NNTP nos seguintes clientes de e-mail:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Para verificar o tráfego nos clientes de e-mail Mozilla Thunderbird, MyOffice Mail e R7-Office Organizer, tem de adicionar um certificado Kaspersky ao armazenamento de certificados e selecionar o próprio armazenamento de certificados.

A Proteção contra ameaças de correio não oferece suporte a outros protocolos e clientes de e-mail.

A Proteção contra ameaças de correio pode nem sempre ser capaz de obter acesso de *nível de protocolo* a mensagens (por exemplo, ao usar a solução Microsoft Exchange). Por este motivo, a Proteção contra ameaças de correio inclui uma extensão para Microsoft Office Outlook. A extensão permite verificar mensagens ao *nível do cliente de e-mail*. A extensão Proteção contra ameaças de correio suporta as versões de 32 bits e 64 bits do Outlook 2010, 2013, 2016, 2019, 2021, 2024 e 365. Em computadores baseados em Arm, a extensão Proteção contra ameaças de correio suporta as versões de 32 bits e 64 bits do Outlook 2016, Outlook 2021, Outlook 2024 e Outlook 365 para Arm64.

O componente Proteção contra ameaças de correio não verifica as mensagens se o cliente de correio estiver aberto num navegador.

Quando se deteta um ficheiro malicioso num anexo, o Kaspersky Endpoint Security adiciona as informações sobre a ação executada ao assunto da mensagem, por exemplo, *[A mensagem foi processada] <assunto da mensagem>*.

Ativar e desativar a Proteção contra ameaças de correio

Por predefinição, o componente Proteção contra ameaças de correio está ativado e é executado no modo recomendado pelos especialistas da Kaspersky. Para Proteção contra ameaças de correio, a aplicação pode aplicar diferentes grupos de definições. Estes grupos de definições armazenados na aplicação chamam-se *níveis de segurança*: **Alto**, **Recomendado**, **Baixo**. Considera-se que as definições de nível de segurança de correio **Recomendado** são as definições ideais recomendadas pelos especialistas da Kaspersky (consulte a tabela abaixo). Pode selecionar um dos níveis de segurança de e-mail pré-instalados ou configurar um nível de segurança de e-mail personalizado. Se tiver alterado as definições de nível de segurança de e-mail, pode sempre repor as definições de nível de segurança de e-mail recomendado.

Ao trabalhar com o cliente de e-mail Mozilla Thunderbird, o componente Proteção contra ameaças de correio não verifica a existência de vírus e outras ameaças nas mensagens transmitidas através do protocolo IMAP se forem utilizados filtros para mover as mensagens da pasta Caixa de entrada.

Como ativar ou desativar o componente Proteção contra ameaças de correio na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de correio**.
4. Use a caixa de verificação **Proteção contra ameaças de correio** para ativar ou desativar o componente.
5. Se ativou este componente, execute uma das seguintes ações no bloco **Nível de segurança**:
    - Se quiser aplicar um dos níveis de segurança predefinidos, selecione-o com o controlo de deslize:
        - **Elevado**. Quando este nível de segurança de e-mail é selecionado, o componente Proteção contra ameaças de correio verifica mensagens de e-mail o mais completamente. O componente Proteção contra ameaças de correio verifica mensagens de e-mail de entrada e de saída, e executa a análise heurística profunda. O nível de segurança de correio Elevado é recomendado para ambientes de alto risco. Um exemplo de um ambiente deste tipo é a ligação a um serviço de e-mail gratuito, a partir de uma rede doméstica que não está protegida por uma proteção de e-mail centralizada.
        - **Recomendado**. O nível de segurança do e-mail que fornece o equilíbrio ideal entre o desempenho da aplicação e a segurança do e-mail. O componente Proteção contra ameaças de correio verifica mensagens de e-mail de entrada e de saída e executa a análise heurística de nível médio. Este nível de segurança de tráfego de e-mail é recomendado pelos especialistas da Kaspersky. Os valores das definições para o nível de segurança recomendado são fornecidos na tabela abaixo.
        - **Baixo**. Quando este nível de segurança de e-mail está selecionado, o componente Proteção contra ameaças de correio verifica apenas mensagens de e-mail de entrada, executa uma análise heurística superficial e não verifica arquivos anexados a mensagens de e-mail. Com este nível de segurança de e-mail, o componente Proteção contra ameaças de correio verifica mensagens de e-mail à velocidade máxima, com uma utilização mínima dos recursos do sistema operativo. O nível Baixo de segurança de e-mail é recomendado para utilização num ambiente bem protegido. Um exemplo de um ambiente deste tipo pode ser a rede local (LAN) de uma empresa com segurança de e-mail centralizada.

- Se pretender configurar um nível de segurança personalizado, clique no botão **Definições** e defina as suas próprias definições do componente (consulte a tabela abaixo).

  Pode restaurar os valores dos níveis de segurança predefinidos ao clicar no botão **Por defeito**.

6. No bloco **Ação após deteção de ameaças**, selecione a ação executada pelo Kaspersky Endpoint Security em objetos maliciosos:

   - **Desinfetar, eliminar se a desinfeção falhar**. Quando um objeto infetado é detetado numa mensagem de entrada ou saída, a aplicação tenta desinfetar o objeto detetado. O utilizador poderá aceder à mensagem com um anexo seguro. Se não for possível desinfetar o objeto, a aplicação elimina o objeto infetado. A aplicação adiciona as informações sobre a ação executada ao assunto da mensagem, por exemplo, *[A mensagem foi processada] <assunto da mensagem>*.

   - **Desinfetar, bloquear se a desinfeção falhar**. Quando um objeto infetado é detetado numa mensagem de entrada, a aplicação tenta desinfetar o objeto detetado. O utilizador poderá aceder à mensagem com um anexo seguro. Se não for possível desinfetar o objeto, a aplicação adiciona um aviso ao assunto da mensagem. O utilizador poderá aceder à mensagem com o anexo original. Quando um objeto infetado é detetado numa mensagem de saída, a aplicação tenta desinfetar o objeto detetado. Se não for possível desinfetar o objeto, a aplicação bloqueia a transmissão da mensagem e o cliente de e-mail apresenta um erro.

   - **Bloquear**. Se for detetado um objeto infetado numa mensagem de entrada, a aplicação adiciona um aviso ao assunto da mensagem. O utilizador poderá aceder à mensagem com o anexo original. Se for detetado um objeto infetado numa mensagem de saída, a aplicação bloqueia a transmissão da mensagem e o cliente de e-mail apresenta um erro.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar ou desativar o componente Proteção contra ameaças de correio na Web Console

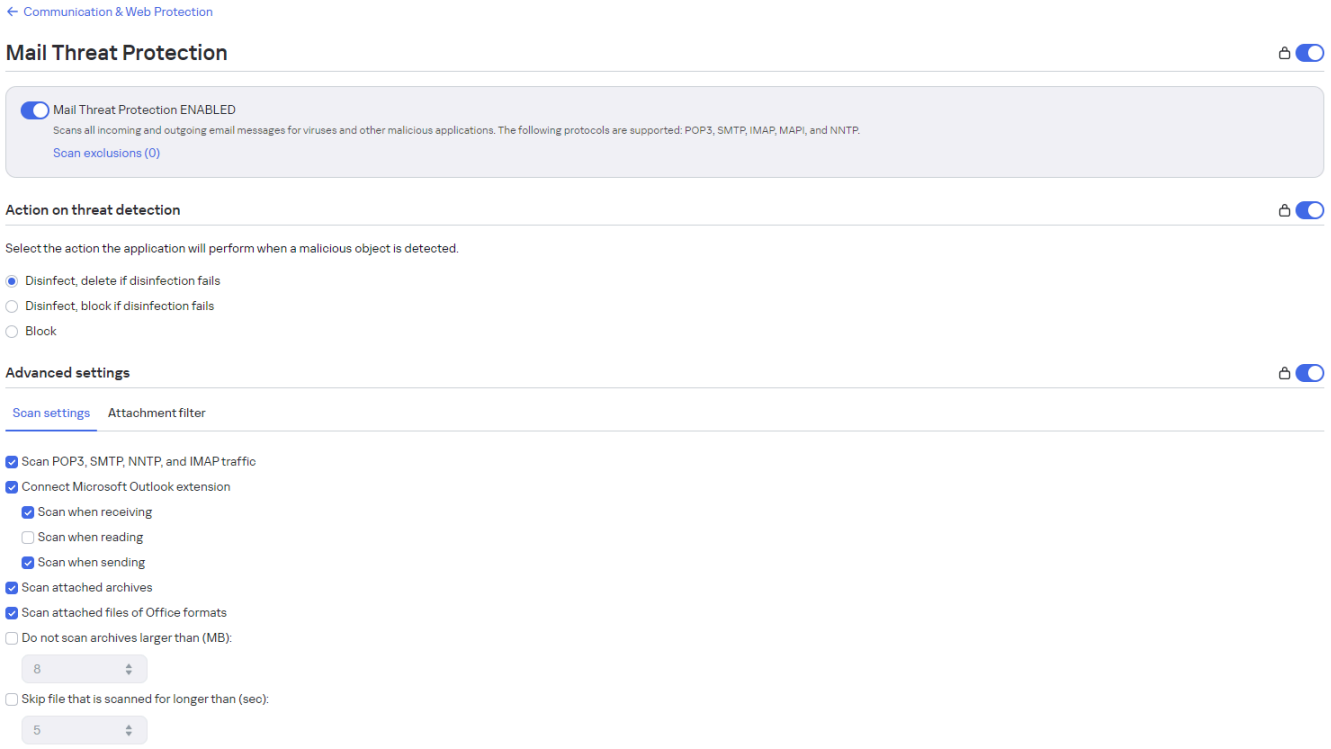
1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Communication & Web Protection** → **Mail Threat Protection**.



Definições da Proteção contra ameaças de correio

5. Use o botão de alternar da **Mail Threat Protection ENABLED** para ativar ou desativar o componente.

6. No bloco **Action on threat detection**, selecione a ação executada pelo Kaspersky Endpoint Security em objetos maliciosos:

   - **Disinfect, delete if disinfection fails**. Quando um objeto infetado é detetado numa mensagem de entrada ou saída, a aplicação tenta desinfetar o objeto detetado. O utilizador poderá aceder à mensagem com um anexo seguro. Se não for possível desinfetar o objeto, a aplicação elimina o objeto infetado. A aplicação adiciona as informações sobre a ação executada ao assunto da mensagem, por exemplo, *[A mensagem foi processada] <assunto da mensagem>*.

   - **Disinfect, block if disinfection fails**. Quando um objeto infetado é detetado numa mensagem de entrada, a aplicação tenta desinfetar o objeto detetado. O utilizador poderá aceder à mensagem com um anexo seguro. Se não for possível desinfetar o objeto, a aplicação adiciona um aviso ao assunto da mensagem. O utilizador poderá aceder à mensagem com o anexo original. Quando um objeto infetado é detetado numa mensagem de saída, a aplicação tenta desinfetar o objeto detetado. Se não for possível desinfetar o objeto, a aplicação bloqueia a transmissão da mensagem e o cliente de e-mail apresenta um erro.

   - **Block**. Se for detetado um objeto infetado numa mensagem de entrada, a aplicação adiciona um aviso ao assunto da mensagem. O utilizador poderá aceder à mensagem com o anexo original. Se for detetado um objeto infetado numa mensagem de saída, a aplicação bloqueia a transmissão da mensagem e o cliente de e-mail apresenta um erro.

7. Se necessário, edite as definições avançadas de Proteção contra ameaças de correio.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar ou desativar o componente Proteção contra ameaças de correio na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de correio**.
3. Use o botão de alternar da **Proteção contra ameaças de correio** para ativar ou desativar o componente.
4. Se ativou este componente, execute uma das seguintes ações no bloco **Nível de segurança**:
   - Se quiser aplicar um dos níveis de segurança predefinidos, selecione-o com o controlo de deslize:
     - **Alto**. Quando este nível de segurança de e-mail é selecionado, o componente Proteção contra ameaças de correio verifica mensagens de e-mail o mais completamente. O componente Proteção contra ameaças de correio verifica mensagens de e-mail de entrada e de saída, e executa a análise heurística profunda. O nível de segurança de correio Elevado é recomendado para ambientes de alto risco. Um exemplo de um ambiente deste tipo é a ligação a um serviço de e-mail gratuito, a partir de uma rede doméstica que não está protegida por uma proteção de e-mail centralizada.
     - **Recomendado**. O nível de segurança do e-mail que fornece o equilíbrio ideal entre o desempenho da aplicação e a segurança do e-mail. O componente Proteção contra ameaças de correio verifica mensagens de e-mail de entrada e de saída e executa a análise heurística de nível médio. Este nível de segurança de tráfego de e-mail é recomendado pelos especialistas da Kaspersky. Os valores das definições para o nível de segurança recomendado são fornecidos na tabela abaixo.
     - **Baixo**. Quando este nível de segurança de e-mail está selecionado, o componente Proteção contra ameaças de correio verifica apenas mensagens de e-mail de entrada, executa uma análise heurística superficial e não verifica arquivos anexados a mensagens de e-mail. Com este nível de segurança de e-mail, o componente Proteção contra ameaças de correio verifica mensagens de e-mail à velocidade máxima, com uma utilização mínima dos recursos do sistema operativo. O nível Baixo de segurança de e-mail é recomendado para utilização num ambiente bem protegido. Um exemplo de um ambiente deste tipo pode ser a rede local (LAN) de uma empresa com segurança de e-mail centralizada.
   - Se pretender configurar um nível de segurança personalizado, clique no botão **Definições avançadas** e defina as suas próprias definições do componente (consulte a tabela abaixo).

     Pode restaurar os valores dos níveis de segurança predefinidos ao clicar no botão **Restaurar nível de segurança recomendado**.

5. No bloco **Ação após deteção de ameaças**, selecione a ação executada pelo Kaspersky Endpoint Security em objetos maliciosos:

   - **Desinfetar, eliminar se a desinfeção falhar**. Quando um objeto infetado é detetado numa mensagem de entrada ou saída, a aplicação tenta desinfetar o objeto detetado. O utilizador poderá aceder à mensagem com um anexo seguro. Se não for possível desinfetar o objeto, a aplicação elimina o objeto infetado. A aplicação adiciona as informações sobre a ação executada ao assunto da mensagem, por exemplo, *[A mensagem foi processada] <assunto da mensagem>*.

   - **Desinfetar, bloquear se a desinfeção falhar**. Quando um objeto infetado é detetado numa mensagem de entrada, a aplicação tenta desinfetar o objeto detetado. O utilizador poderá aceder à mensagem com um anexo seguro. Se não for possível desinfetar o objeto, a aplicação adiciona um aviso ao assunto da mensagem. O utilizador poderá aceder à mensagem com o anexo original. Quando um objeto infetado é detetado numa mensagem de saída, a aplicação tenta desinfetar o objeto detetado. Se não for possível desinfetar o objeto, a aplicação bloqueia a transmissão da mensagem e o cliente de e-mail apresenta um erro.

   - **Bloquear**. Se for detetado um objeto infetado numa mensagem de entrada, a aplicação adiciona um aviso ao assunto da mensagem. O utilizador poderá aceder à mensagem com o anexo original. Se for detetado um objeto infetado numa mensagem de saída, a aplicação bloqueia a transmissão da mensagem e o cliente de e-mail apresenta um erro.

6. Guarde as suas alterações.

Definições de Proteção contra ameaças de correio recomendadas pelos especialistas da Kaspersky (nível de segurança recomendado)

Parâmetro	Valor	Descrição
Âmbito de proteção	**Mensagens de entrada e de saída**	O *Âmbito de proteção* inclui objetos que o componente verifica quando está em execução: Mensagens de entrada e de saída ou Apenas mensagens de entrada. Para proteger os seus computadores, precisa apenas de verificar as mensagens de entrada. Pode ativar a verificação de mensagens de saída para impedir que ficheiros infetados sejam enviados nos arquivos. Também pode ativar a verificação de mensagens de saída se quiser impedir que ficheiros em formatos específicos sejam enviados, como ficheiros de áudio e vídeo, por exemplo.
Ligar a extensão do Microsoft Outlook	**Ativado**	Se esta caixa de verificação estiver selecionada, a verificação de mensagens de e-mail transmitidas através dos protocolos POP3, SMTP, NNTP, IMAP é ativada na extensão integrada no Microsoft Outlook. Se o correio for verificado utilizando a extensão do Microsoft Outlook, recomenda-se a utilização do Cached Exchange Mode. Para obter informações mais detalhadas sobre o Modo Exchange em Cache e recomendações sobre a sua utilização, consulte a Base de Conhecimentos da Microsoft.
Verificar arquivos anexados	**Ativado**	A verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros arquivos. A aplicação verifica arquivos não só pela extensão, mas também pelo formato. Ao verificar os arquivos, a aplicação efetua uma descompactação recursiva. Isto permite a deteção de ameaças dentro de arquivos multinível (um arquivo dentro de um arquivo).
Analisar ficheiros anexados com formatos do Microsoft Office	**Ativado**	Verifica ficheiros do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Ficheiros de formato do Office incluem objetos OLE também. A aplicação verifica ficheiros em formato de escritório menores que 1 MB, independentemente de a caixa de seleção estar marcada ou não.
Filtro de anexo	**Mudar o nome dos anexos dos tipos selecionados**	Se esta opção for selecionada, o componente de Proteção contra ameaças de correio substituirá o último carácter de extensão encontrado nos ficheiros anexados dos tipos especificados pelo carácter de sublinhado (por exemplo, anexo.doc_). Portanto, para abrir o ficheiro, o utilizador deve renomear o ficheiro.

Parâmetro	Valor	Descrição
Análise heurística	**Nível médio**	A tecnologia foi desenvolvida para detetar ameaças que não é possível detetar utilizando a versão atual das bases de dados da aplicação da Kaspersky. Permite detetar ficheiros que podem estar infetados com um vírus desconhecido ou com uma variante de um vírus conhecido. Ao verificar ficheiros de códigos maliciosos, o analisador heurístico executa instruções nos ficheiros executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível da análise heurística garante um equilíbrio entre o detalhe das procuras de novas ameaças, a carga nos recursos do sistema operativo e a duração da análise heurística.
Ação após deteção de ameaças	**Desinfetar, eliminar se a desinfeção falhar**	Quando um objeto infetado é detetado numa mensagem de entrada ou saída, a aplicação tenta desinfetar o objeto detetado. O utilizador poderá aceder à mensagem com um anexo seguro. Se não for possível desinfetar o objeto, a aplicação elimina o objeto infetado. A aplicação adiciona as informações sobre a ação executada ao assunto da mensagem, por exemplo, *[A mensagem foi processada] <assunto da mensagem>*.

Alterar a ação a executar em mensagens de e-mail infetadas

Por predefinição, o componente Proteção contra ameaças de correio tenta automaticamente desinfetar todas as mensagens de e-mail infetadas detetadas. Se a desinfeção falhar, o componente Proteção contra ameaças de correio elimina as mensagens de e-mail infetadas.

Para alterar a ação a executar em mensagens de e-mail infetadas:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de correio**.
3. No bloco **Ação após deteção de ameaças**, selecione a ação a executar pelo Kaspersky Endpoint Security quando é detetada uma mensagem infetada:
   - **Desinfetar, eliminar se a desinfeção falhar**. Quando um objeto infetado é detetado numa mensagem de entrada ou saída, a aplicação tenta desinfetar o objeto detetado. O utilizador poderá aceder à mensagem com um anexo seguro. Se não for possível desinfetar o objeto, a aplicação elimina o objeto infetado. A aplicação adiciona as informações sobre a ação executada ao assunto da mensagem, por exemplo, *[A mensagem foi processada] <assunto da mensagem>*.
   - **Desinfetar, bloquear se a desinfeção falhar**. Quando um objeto infetado é detetado numa mensagem de entrada, a aplicação tenta desinfetar o objeto detetado. O utilizador poderá aceder à mensagem com um anexo seguro. Se não for possível desinfetar o objeto, a aplicação adiciona um aviso ao assunto da mensagem. O utilizador poderá aceder à mensagem com o anexo original. Quando um objeto infetado é detetado numa mensagem de saída, a aplicação tenta desinfetar o objeto detetado. Se não for possível desinfetar o objeto, a aplicação bloqueia a transmissão da mensagem e o cliente de e-mail apresenta um erro.
   - **Bloquear**. Se for detetado um objeto infetado numa mensagem de entrada, a aplicação adiciona um aviso ao assunto da mensagem. O utilizador poderá aceder à mensagem com o anexo original. Se for detetado um objeto infetado numa mensagem de saída, a aplicação bloqueia a transmissão da mensagem e o cliente de e-mail apresenta um erro.
4. Guarde as suas alterações.

Formar o âmbito de proteção do componente Proteção contra ameaças de correio

O *Âmbito da proteção* refere-se aos objetos verificados pelo componente quando este está ativado. Os âmbitos de proteção de componentes diferentes têm propriedades diferentes. As propriedades do âmbito de proteção do componente Proteção contra ameaças de correio incluem as definições para integrar o componente Proteção contra ameaças de correio nos clientes de correio, bem como o tipo de mensagens de e-mail e os protocolos de e-mail cujo tráfego é verificado pelo componente Proteção contra ameaças de correio. Por predefinição, o Kaspersky Endpoint Security verifica as mensagens de e-mail de entrada e de saída e o tráfego através dos protocolos POP3, SMTP, NNTP e IMAP, e está integrado no cliente de e-mail do Microsoft Office Outlook.

Para formar o âmbito de proteção do componente Proteção contra ameaças de correio:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de correio**.
3. Clique em **Definições avançadas**.
4. No bloco **Âmbito de proteção**, selecione as mensagens a verificar:
   - **Mensagens de entrada e de saída**.
   - **Apenas mensagens de entrada**.

   Para proteger os seus computadores, precisa apenas de verificar as mensagens de entrada. Pode ativar a verificação de mensagens de saída para impedir que ficheiros infetados sejam enviados nos arquivos. Também pode ativar a verificação de mensagens de saída se quiser impedir que ficheiros em formatos específicos sejam enviados, como ficheiros de áudio e vídeo, por exemplo.

   Se pretender verificar apenas as mensagens de entrada, recomendamos que efetue uma verificação única de todas as mensagens de saída, uma vez que poderão existir worms de e-mail no computador que se disseminam através do e-mail. Deste modo pode evitar problemas resultantes do envio em massa e não monitorizado de mensagens infetadas a partir do seu computador.
5. No bloco **Conetividade**, execute as seguintes ações:
   - Se pretender que o componente Proteção contra ameaças de correio verifique as mensagens transmitidas através dos protocolos POP3, SMTP, NNTP e IMAP antes de as mesmas chegarem ao computador do utilizador, selecione a caixa de verificação **Verificar tráfego POP3, SMTP, NNTP e IMAP**.

     Se não pretender que o componente Proteção contra ameaças de correio verifique as mensagens transmitidas através dos protocolos POP3, SMTP, NNTP e IMAP antes de as mesmas chegarem ao computador do utilizador, desmarque a caixa de verificação **Verificar tráfego POP3, SMTP, NNTP e IMAP**. Neste caso, as mensagens são verificadas pela extensão da Proteção contra ameaças de correio integrada no cliente de correio do Microsoft Office Outlook depois de serem recebidas no computador do utilizador se a caixa de verificação **Ligar a extensão do Microsoft Outlook** estiver selecionada.

Se usar um cliente de e-mail que não do Microsoft Office Outlook, o componente Proteção contra ameaças de correio não verifica as mensagens transmitidas pelos protocolos POP3, SMTP, NNTP e IMAP sempre que a caixa de verificação **Verificar tráfego POP3, SMTP, NNTP e IMAP** estiver selecionada.

- Se quiser permitir o acesso às definições do componente Proteção contra ameaças de correio a partir do Microsoft Office Outlook e ativar a verificação das mensagens transmitidas através dos protocolos POP3, SMTP, NNTP, IMAP e MAPI depois de chegarem ao computador através da extensão incorporada no Microsoft Office Outlook, selecione a caixa de verificação **Ligar a extensão do Microsoft Outlook**.

  Se quiser bloquear o acesso às definições do componente Proteção contra ameaças de correio a partir do Microsoft Office Outlook e desativar a verificação das mensagens transmitidas através dos protocolos POP3, SMTP, NNTP, IMAP e MAPI depois de chegarem ao computador através da extensão incorporada no Microsoft Office Outlook, desmarque a caixa de verificação **Ligar a extensão do Microsoft Outlook**.

  A extensão da Proteção contra ameaças de correio é incorporada no cliente de e-mail do Microsoft Office Outlook durante a instalação do Kaspersky Endpoint Security.

6. Guarde as suas alterações.

Verificação de ficheiros compostos anexados a mensagens de e-mail

Pode ativar ou desativar a verificação dos anexos das mensagens, limitar o tamanho máximo dos anexos das mensagens a serem verificados, bem como a duração máxima da verificação dos anexos.

Para configurar a verificação de ficheiros compostos anexados às mensagens de e-mail:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de correio**.
3. Clique em **Definições avançadas**.

4. No bloco **Verificação de ficheiros compostos**, configure as definições de verificação:

   - **Analisar ficheiros anexados com formatos do Microsoft Office**. Verifica ficheiros do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Ficheiros de formato do Office incluem objetos OLE também. A aplicação verifica ficheiros em formato de escritório menores que 1 MB, independentemente de a caixa de seleção estar marcada ou não.

   - **Verificar arquivos anexados**. A verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros arquivos. A aplicação verifica arquivos não só pela extensão, mas também pelo formato. Ao verificar os arquivos, a aplicação efetua uma descompactação recursiva. Isto permite a deteção de ameaças dentro de arquivos multinível (um arquivo dentro de um arquivo).

     Se, durante a verificação, a aplicação detetar uma password para um arquivo no texto da mensagem, esta password será utilizada para verificar o conteúdo do arquivo em busca de aplicações maliciosas. Neste caso, a password não é guardada. Um arquivo é descompactado durante a verificação. Se ocorrer um erro de aplicação durante o processo de descompactação, poderá eliminar manualmente os ficheiros descompactados que são guardados no caminho seguinte: %systemroot%\temp. Os ficheiros têm o prefixo PR.

   - **Não verificar arquivos com tamanho superior a N MB (de 1 a 9999)**. Se esta caixa de verificação estiver selecionada, o componente Proteção contra ameaças de correio exclui os arquivos anexados a mensagens de e-mail da verificação se o seu tamanho exceder o valor especificado. Se a caixa de verificação estiver desmarcada, o componente Proteção contra ameaças de correio verifica arquivos de qualquer tamanho anexados a mensagens de e-mail.

   - **Limite o tempo de verificação de arquivos a N segundos (de 1 a 9999)**. Se a caixa de verificação estiver selecionada, o tempo reservado para a verificação de arquivos anexados a mensagens de e-mail está limitado ao período especificado.

5. Guarde as suas alterações.

Filtrar anexos de mensagens de e-mail

A filtragem de anexos não é aplicada às mensagens de e-mail enviadas.

As aplicações maliciosas podem ser distribuídas sob a forma de anexos nas mensagens de e-mail. Pode configurar a filtragem por tipo de anexos da mensagem para que os ficheiros dos tipos especificados sejam automaticamente renomeados ou apagados. Alterando o nome de um anexo de determinado tipo, o Kaspersky Endpoint Security pode proteger o seu computador contra a execução automática de uma aplicação maliciosa.

Para configurar a filtragem de anexos:

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de correio**.

3. Clique em **Definições avançadas**.

4. No bloco **Filtro de anexo**, execute uma das seguintes ações:

   - **Desativar filtragem**. Se esta opção estiver selecionada, o componente Proteção contra ameaças de correio não filtra ficheiros anexados a mensagens de e-mail.

   - **Mudar o nome dos anexos dos tipos selecionados**. Se esta opção for selecionada, o componente de Proteção contra ameaças de correio substituirá o último carácter de extensão encontrado nos ficheiros anexados dos tipos especificados pelo carácter de sublinhado (por exemplo, anexo.doc_). Portanto, para abrir o ficheiro, o utilizador deve renomear o ficheiro.

   - **Eliminar anexos dos tipos selecionados**. Se esta opção estiver selecionada, o componente Proteção contra ameaças de correio elimina ficheiros anexados dos tipos especificados das mensagens de e-mail.

5. Se selecionou a opção **Mudar o nome dos anexos dos tipos selecionados** ou a opção **Eliminar anexos dos tipos selecionados** durante o passo anterior, selecione as caixas de verificação à frente dos tipos de ficheiros relevantes.

6. Guarde as suas alterações.

Exportar e importar extensões para filtragem de anexos

Pode exportar a lista de extensões de filtro de anexos para um ficheiro XML. Pode utilizar a função de exportação/importação para fazer uma cópia de segurança 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 na Consola de Administração (MMC)

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Communication & Web Protection** → **Mail Threat Protection**.

5. Para exportar a lista de extensões, no bloco **Attachment filter**:

   a. Selecione as extensões que pretende exportar.

   b. Clique na hiperligação **Export**.

   c. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de extensões e selecione a pasta onde pretende guardar este ficheiro.

   d. Guardar o ficheiro.

      O Kaspersky Endpoint Security exporta toda a lista de extensões para o ficheiro XML.

6. Para importar a lista de extensões, no bloco **Attachment filter**:

   a. Clique na hiperligação **Import**.

   b. Na janela que se abre, selecione o ficheiro XML a partir do qual pretende importar a lista de extensões.

   c. Abrir o ficheiro.

      Se o computador já tiver uma lista de extensões, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro XML.

7. Guarde as suas alterações.

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de correio**.

4. No bloco **Nível de segurança**, clique no botão **Definições**.

5. Esta ação abre uma janela; nessa janela, selecione o separador **Filtro de anexos**.

6. Para exportar a lista de extensões:

   a. Selecione as extensões que pretende exportar. Para selecionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.

   b. Clique na hiperligação **Exportar**.

   c. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de extensões e selecione a pasta onde pretende guardar este ficheiro.

   d. Guardar o ficheiro.

      O Kaspersky Endpoint Security exporta toda a lista de extensões para o ficheiro XML.

7. Para importar a lista de extensões:

   a. Clique na hiperligação **Importar**.

   b. Na janela que se abre, selecione o ficheiro XML a partir do qual pretende importar a lista de extensões.

   c. Abrir o ficheiro.

      Se o computador já tiver uma lista de extensões, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro XML.

8. Guarde as suas alterações.

Verificar e-mails no Microsoft Office Outlook

Durante a instalação do Kaspersky Endpoint Security, a extensão da Proteção contra ameaças de correio está integrada no Microsoft Office Outlook (doravante também referido como Outlook). A extensão permite a verificação de mensagens no nível de um cliente de e-mail em vez do nível do protocolo. Além das mensagens, a extensão permite verificar objetos recebidos por meio da interface MAPI dos repositórios do Microsoft Exchange (por exemplo, objetos no calendário). Esta verificação ocorre no cliente de e-mail.

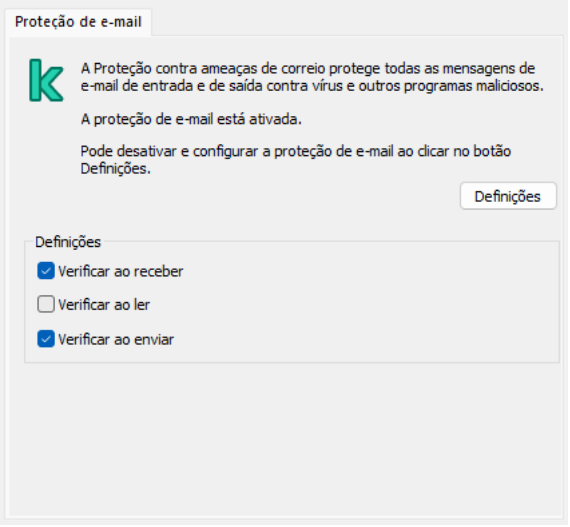
Esta extensão permite-lhe abrir as definições do componente Proteção contra ameaças de correio a partir do Outlook e especificar quando deve ser verificada a existência de vírus e de outras ameaças nas mensagens de e-mail.

A extensão Proteção contra ameaças de correio suporta as versões de 32 bits e 64 bits do Outlook 2010, 2013, 2016, 2019, 2021, 2024 e 365.

Em computadores baseados em Arm, a extensão Proteção contra ameaças de correio suporta as versões de 32 bits e 64 bits do Outlook 2016, Outlook 2021, Outlook 2024 e Outlook 365 para Arm64.

No Outlook, as mensagens recebidas são primeiro verificadas pelo componente de Proteção Contra Ameaças de Correio (se a caixa de verificação Verificar tráfego POP3, SMTP, NNTP e IMAP estiver selecionada na interface do Kaspersky Endpoint Security) e, em seguida, pela extensão da Proteção Contra Ameaças de Correio para Outlook. Se o componente Proteção contra ameaças de correio detetar um objeto malicioso numa mensagem, avisa-o sobre este evento.

As definições do componente de Proteção Contra Ameaças de Correio podem ser configuradas diretamente no Outlook se a extensão do Microsoft Outlook estiver ligada na interface do Kaspersky Endpoint Security (veja a figura abaixo).



Definições do componente Proteção contra ameaças de correio no Outlook

As mensagens enviadas são verificadas primeiro pela extensão da Proteção contra ameaças de correio para Outlook e, depois, pelo componente Proteção contra ameaças de correio.

Ao verificar e-mails com a extensão Proteção contra ameaças de correio para o Outlook, recomendamos a utilização do Modo em Cache do Exchange Server (Use Cached Exchange Mode). Para obter informações mais detalhadas sobre o Modo Exchange em Cache e recomendações sobre a sua utilização, consulte a Base de Conhecimentos da Microsoft.

Como configurar o modo operativo da extensão da Proteção contra ameaças de correio para Outlook na Administration Console (MMC)

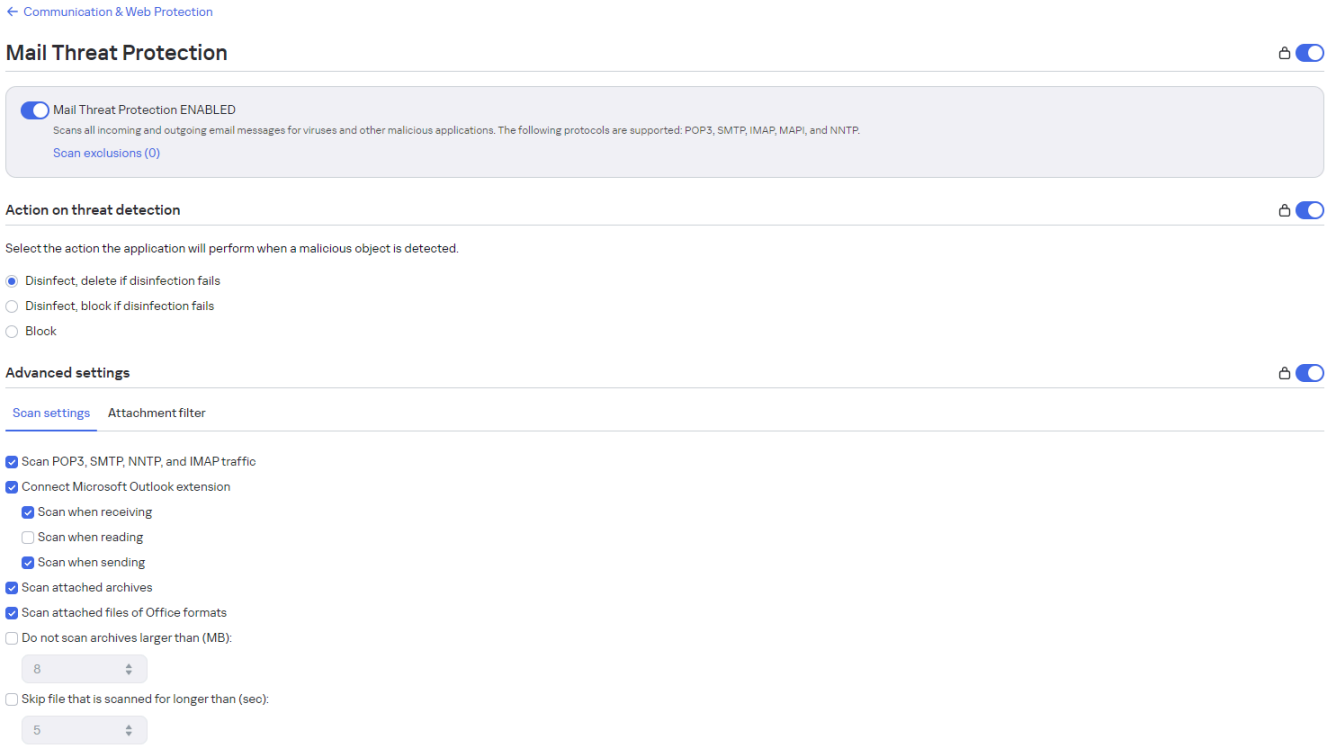
1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de correio**.
5. No bloco **Nível de segurança**, clique no botão **Definições**.
6. Na janela que surgir, no bloco **Conetividade**, selecione a caixa de seleção **Ligar a extensão do Microsoft Outlook**.
7. Clique em **Definições**.
8. Na janela **Proteção de e-mail**, execute uma das seguintes ações:
   - Selecione a caixa de verificação **Verificar ao receber** se pretender que a extensão da Proteção contra ameaças de correio para o Outlook verifique as mensagens de entrada quando estas chegam à caixa de correio.
   - Selecione a caixa de verificação **Verificar ao ler** se pretender que a extensão da Proteção contra ameaças de correio para o Outlook verifique as mensagens de entrada quando o utilizador as abre.
   - Selecione a caixa de verificação **Verificar ao enviar** se pretender que a extensão da Proteção contra ameaças de correio para o Outlook verifique as mensagens de saída quando estas são enviadas.
9. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como configurar o modo operativo da extensão da Proteção contra ameaças de correio para Outlook na Web Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.

4. Aceda a **Communication & Web Protection** → **Mail Threat Protection**.



Definições da Proteção contra ameaças de correio

5. Sob **Advanced settings**, selecione a aba **Scan settings**.

6. Selecione a caixa de verificação **Connect Microsoft Outlook extension**.

7. Configure o modo operativo da extensão:

   - Selecione a caixa de verificação **Scan when receiving** se pretender que a extensão da Proteção contra ameaças de correio para o Outlook verifique as mensagens de entrada quando estas chegam à caixa de correio.

   - Selecione a caixa de verificação **Scan when reading** se pretender que a extensão da Proteção contra ameaças de correio para o Outlook verifique as mensagens de entrada quando o utilizador as abre.

   - Selecione a caixa de verificação **Scan when sending** se pretender que a extensão da Proteção contra ameaças de correio para o Outlook verifique as mensagens de saída quando estas são enviadas.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Verificação de e-mails no Thunderbird, MyOffice, R7-Office

O componente Proteção contra ameaças de correio verifica a existência de vírus e outras ameaças nos anexos das mensagens de e-mail recebidas e enviadas. Para os clientes de e-mail Mozilla Thunderbird, MyOffice Mail e R7-Office Organizer, a aplicação obtém acesso às mensagens apenas no *nível de protocolo* (POP3, SMTP, IMAP, NNTP).

Para verificar o tráfego nos clientes de e-mail Mozilla Thunderbird, MyOffice Mail e R7-Office Organizer, tem de adicionar um certificado Kaspersky ao armazenamento de certificados e selecionar o próprio armazenamento de certificados.

O componente Proteção contra ameaças de correio não verifica as mensagens se o cliente de correio estiver aberto num navegador.

Proteção contra ameaças de correio

A proteção contra ameaças de correio verifica as mensagens recebidas e enviadas. Por predefinição, o componente Proteção contra ameaças de correio tenta automaticamente desinfetar todas as mensagens de e-mail infetadas detetadas. Se a desinfeção falhar, o componente Proteção contra ameaças de correio elimina as mensagens de e-mail infetadas. Quando se deteta um ficheiro malicioso num anexo, o Kaspersky Endpoint Security adiciona as informações sobre a ação executada ao assunto da mensagem, por exemplo, *[A mensagem foi processada] <assunto da mensagem>*.

Ao trabalhar com o cliente de e-mail Mozilla Thunderbird, o componente Proteção contra ameaças de correio não verifica a existência de vírus e outras ameaças nas mensagens transmitidas através do protocolo IMAP se forem utilizados filtros para mover as mensagens da pasta Caixa de entrada.

Verificação de software malicioso em bases de dados de correio

A Proteção contra ameaças de correio impede a infeção do computador ao nível do protocolo, mas, se o computador tiver sido infetado antes da instalação do Kaspersky Endpoint Security, a aplicação poderá detetar a ameaça nas bases de dados de e-mail através da tarefa *Verificação de software malicioso*. A aplicação não desinfeta nem elimina ficheiros infetados nas bases de dados de correio, independentemente das definições da tarefa. Isto deve-se ao facto de o Kaspersky Endpoint Security não dividir as mensagens do Thunderbird, MyOffice e P7-Office nos respetivos componentes (cabeçalho, corpo e anexos) da mesma forma que as mensagens do Microsoft Office Outlook. A aplicação apenas adiciona informações sobre os objetos detetados à lista de ameaças ativas.

Para eliminar ameaças ativas:

1. Encontre e elimine manualmente a mensagem com o objeto detetado na interface do cliente de e-mail.

   A aplicação exibe informações sobre o objeto detetado na lista de ameaças ativas.

   Exemplo de cartão de objeto detetado:

	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 da base de dados.

   Quando uma mensagem é eliminada na interface do utilizador, o cliente de e-mail apenas adiciona uma marca de eliminação. O cliente de e-mail só elimina a mensagem após uma compactação da base de dados. Para obter detalhes sobre a compactação da base de dados, consulte a ajuda do seu cliente de e-mail (por exemplo, Mozilla Thunderbird).

3. Execute a tarefa *Verificação de software malicioso* novamente e certifique-se de que a ameaça já não está presente.

Se, por qualquer motivo, a eliminação de mensagens com ficheiros infetados não estiver disponível nesse momento, pode processar essas ameaças na interface do utilizador do Kaspersky Endpoint Security. Para ficheiros de clientes de e-mail, existem duas opções para processar uma ameaça: **Ignorar** e **Adicionar às exclusões**. Para impedir que a aplicação adicione estes objetos à lista de ameaças ativas durante uma nova análise, adicione-os à lista de exclusões da análise.

Proteção contra ameaças de Rede

O componente *Proteção contra ameaças de Rede* (também chamado de Intrusion Detection System, IDS) monitoriza o tráfego de entrada da rede quanto à existência de atividade característica de ataques à rede. Quando a aplicação deteta uma tentativa de ataque à rede no computador do utilizador, bloqueia a ligação da rede a o computador atacante. As bases de dados da aplicação fornecem descrições dos tipos de ataques de rede conhecidos e das formas utilizadas para os combater. A lista de ataques à rede que o componente Proteção contra ameaças de Rede deteta é atualizada durante as atualizações da base de dados e do módulo da aplicação.

Ativar e desativar a Proteção contra ameaças de Rede

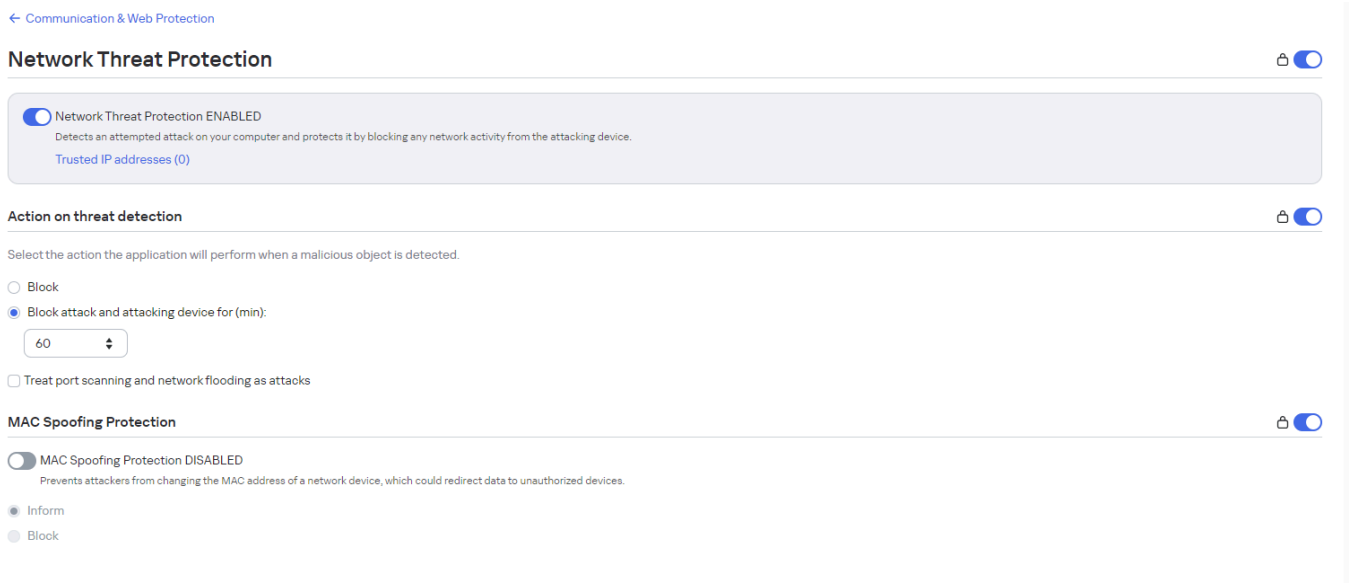
Por predefinição, a Proteção contra ameaças de Rede está ativada e é executada no modo otimizado. O Kaspersky Endpoint Security monitoriza o tráfego de rede de entrada quanto à existência de atividades características de ataques de rede e bloqueia os ataques.

Como ativar ou desativar o componente Proteção contra ameaças de Rede na Administration Console (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de rede**.
4. Use a caixa de verificação **Proteção contra ameaças de rede** para ativar ou desativar o componente.
5. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar ou desativar o componente Proteção contra ameaças de Rede na Web Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Communication & Web Protection** → **Network Threat Protection**.

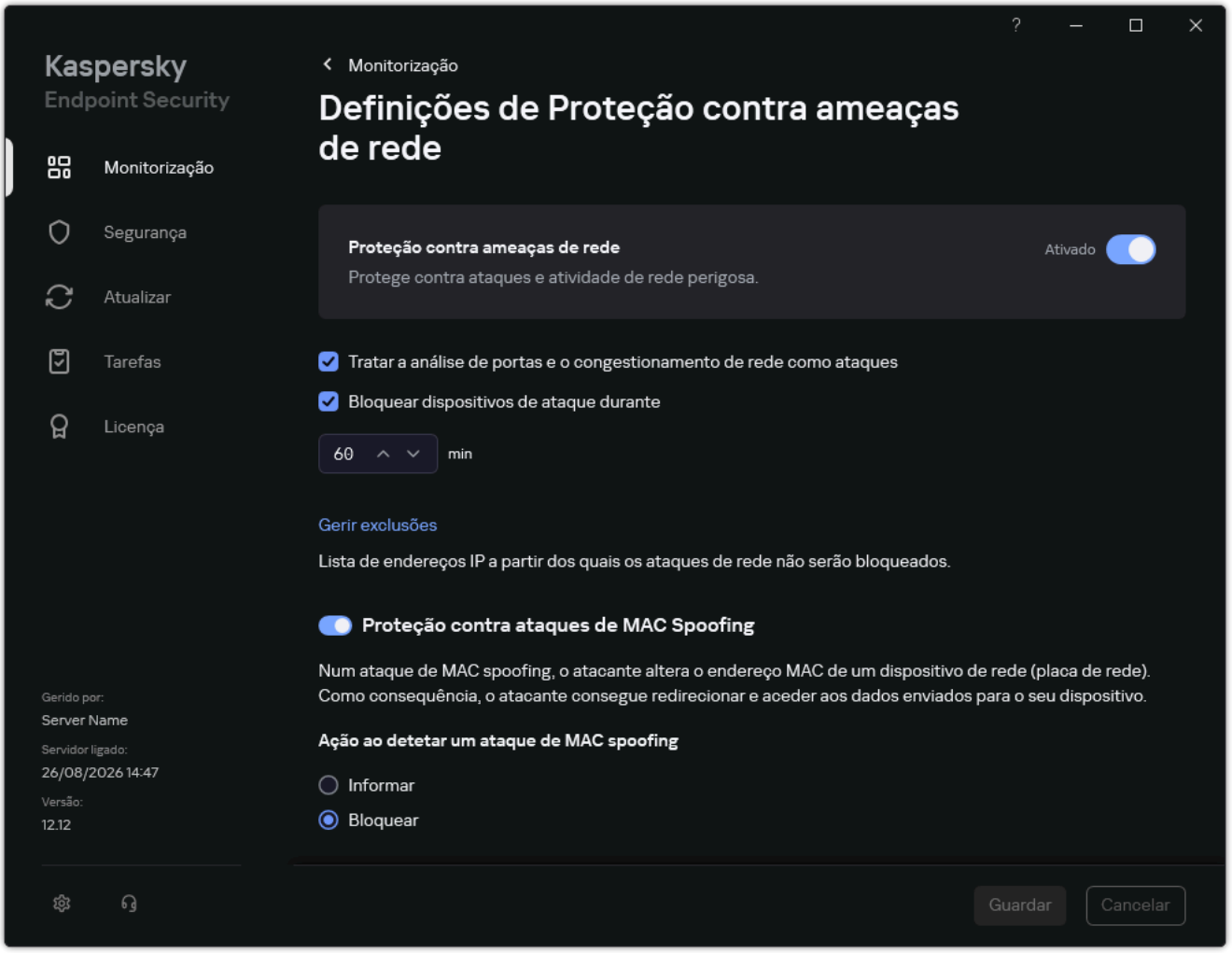


Definições da Proteção contra ameaças de Rede

5. Use o botão de alternar da **Network Threat Protection ENABLED** para ativar ou desativar o componente.
6. Guarde as suas alterações.

Como ativar ou desativar a Proteção contra ameaças de Rede na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de rede**.



Definições da Proteção contra ameaças de Rede

3. Use o botão de alternar da **Proteção contra ameaças de rede** para ativar ou desativar o componente.
4. Guarde as suas alterações.

Bloquear um computador atacante

Se o componente Proteção contra ameaças de Rede estiver ativado, o Kaspersky Endpoint Security bloqueia automaticamente as ameaças de rede. Além disso, a aplicação pode bloquear o computador de ataque e restringir o envio de pacotes de rede durante um determinado período. Por predefinição, o Kaspersky Endpoint Security bloqueia o computador durante uma hora.

Como bloquear um computador de ataque na Administration Console (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de rede**.

4. Em **Definições de Proteção contra ameaças de rede**, selecione a caixa de verificação **Bloquear dispositivos de ataque durante N min**.

   Se esta opção estiver ativada, o componente Proteção contra ameaças de Rede adiciona o computador de ataque à lista de bloqueios. Isto significa que o componente Proteção contra ameaças de Rede bloqueia a ligação de rede do computador atacante após a primeira tentativa de ataque de rede durante o período de tempo especificado. Este bloqueio protege automaticamente o computador do utilizador de possíveis ataques de rede no futuro, com origem no mesmo endereço. O tempo mínimo que um computador atacante deve passar na lista do bloco é de um minuto. O tempo máximo é de 999 minutos.

5. Defina uma duração de bloqueio diferente para um computador atacante no campo à direita da caixa de verificação **Bloquear dispositivos de ataque durante N min**.

6. Guarde as suas alterações.

Como bloquear um computador atacante na Web Console

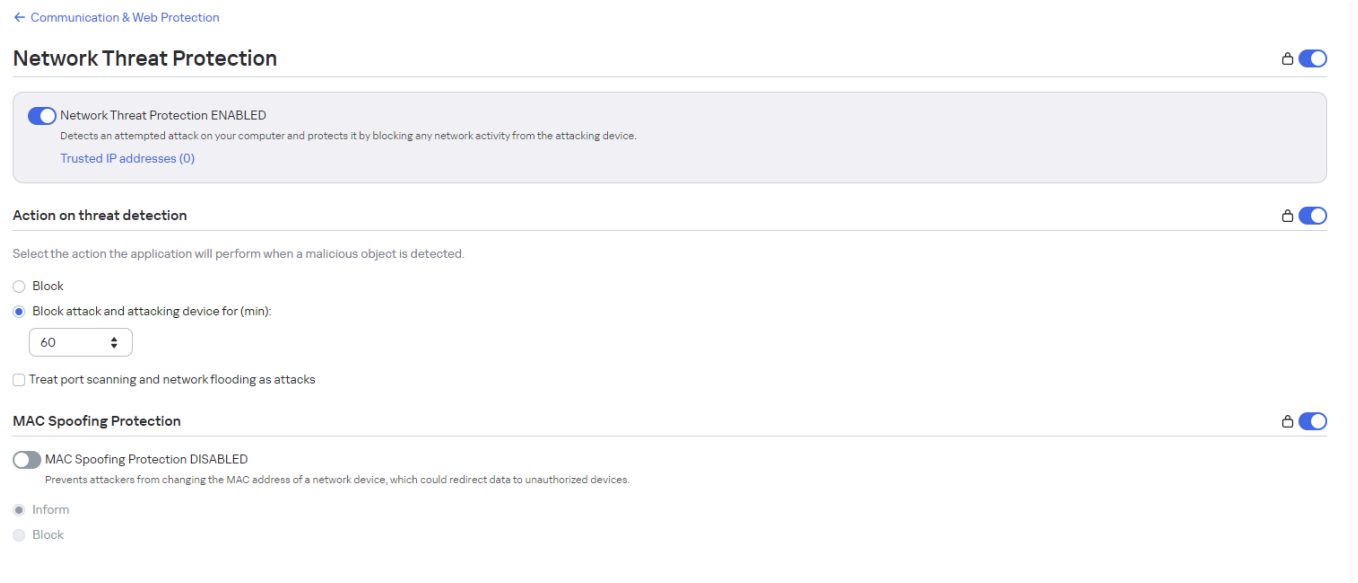
1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Communication & Web Protection** → **Network Threat Protection**.



Definições da Proteção contra ameaças de Rede

5. No bloco **Action on threat detection**, selecione a caixa de verificação **Block attack and attacking device for (min)**.

   Se esta opção estiver ativada, o componente Proteção contra ameaças de Rede adiciona o computador de ataque à lista de bloqueios. Isto significa que o componente Proteção contra ameaças de Rede bloqueia a ligação de rede do computador atacante após a primeira tentativa de ataque de rede durante o período de tempo especificado. Este bloqueio protege automaticamente o computador do utilizador de possíveis ataques de rede no futuro, com origem no mesmo endereço. O tempo mínimo que um computador atacante deve passar na lista do bloco é de um minuto. O tempo máximo é de 999 minutos.

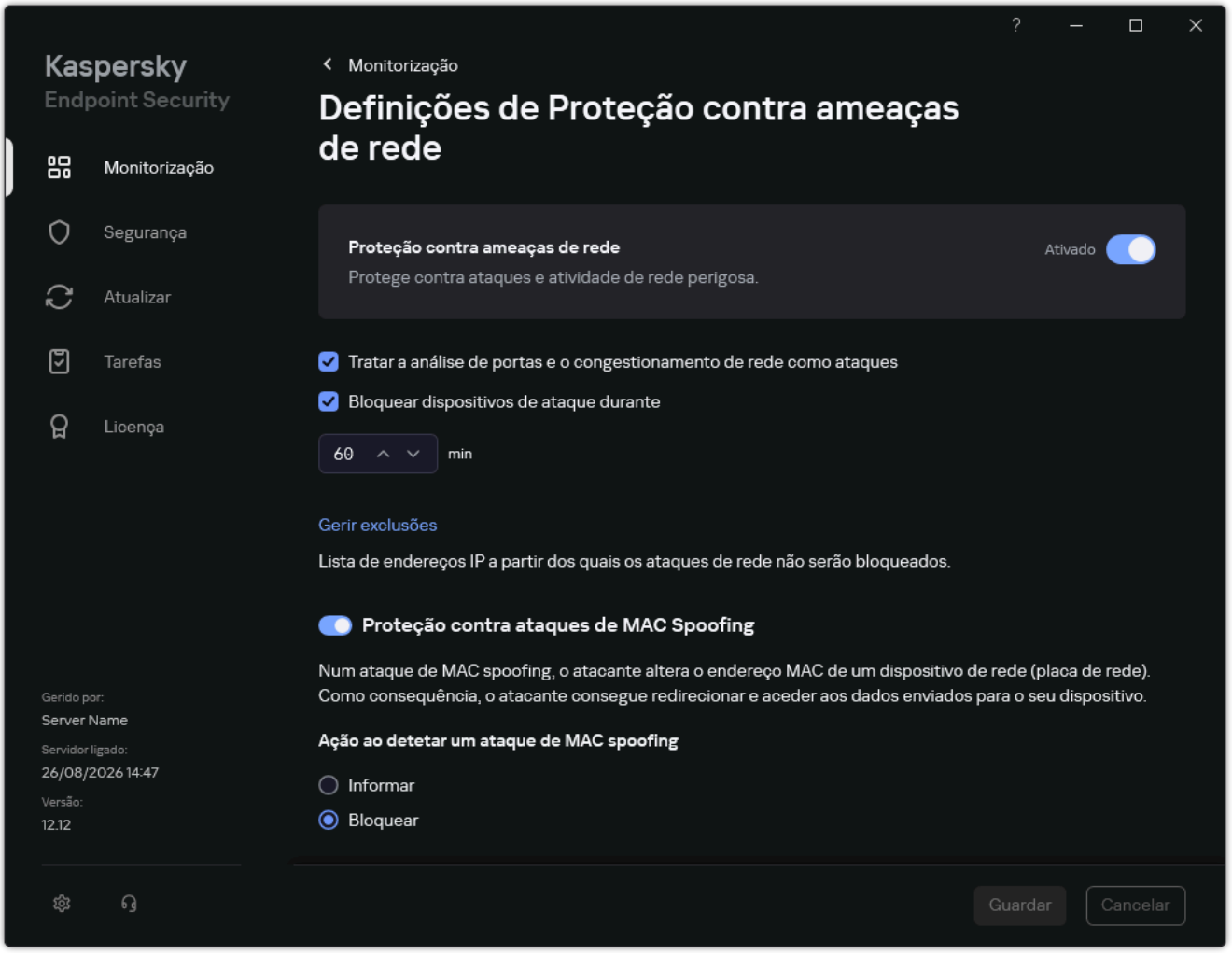
6. Altere a duração do bloqueio do computador atacante.

7. Guarde as suas alterações.

Como bloquear um computador de ataque na interface do utilizador na aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de rede**.



Definições da Proteção contra ameaças de Rede

3. Ative o botão de alternar **Bloquear dispositivos de ataque durante N min**.

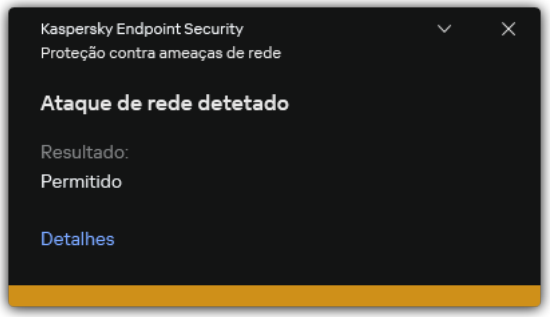
   Se esta opção estiver ativada, o componente Proteção contra ameaças de Rede adiciona o computador de ataque à lista de bloqueios. Isto significa que o componente Proteção contra ameaças de Rede bloqueia a ligação de rede do computador atacante após a primeira tentativa de ataque de rede durante o período de tempo especificado. Este bloqueio protege automaticamente o computador do utilizador de possíveis ataques de rede no futuro, com origem no mesmo endereço. O tempo mínimo que um computador atacante deve passar na lista do bloco é de um minuto. O tempo máximo é de 999 minutos.

4. Defina uma duração de bloqueio diferente para um computador de ataque no campo abaixo do botão de alternar **Bloquear dispositivos de ataque durante N min**.

5. Guarde as suas alterações.

Como resultado, quando o Kaspersky Endpoint Security deteta uma tentativa de ataque à rede contra o computador de um utilizador, bloqueia todas as ligações com o computador atacante. O Kaspersky Endpoint Security cria o evento *Network attack detected*. O evento contém informações sobre o computador atacante: endereços IP e MAC.

Pode ver o endereço MAC do computador invasor na interface do utilizador da aplicação ou na consola do Kaspersky Security Center versão 15.1 ou mais recente.



Notificação sobre a deteção de ataques de rede

O Kaspersky Endpoint Security desbloqueia o computador quando o tempo especificado terminar. A consola do Kaspersky Security Center não fornece ferramentas para monitorizar computadores bloqueados para além de os *Network attack detected* eventos no relatório. Apenas pode ver uma lista de computadores bloqueados na interface da aplicação. Esta funcionalidade é fornecida pela ferramenta *Monitor de Rede*. Também pode utilizar a ferramenta Monitor de Rede para desbloquear um computador.

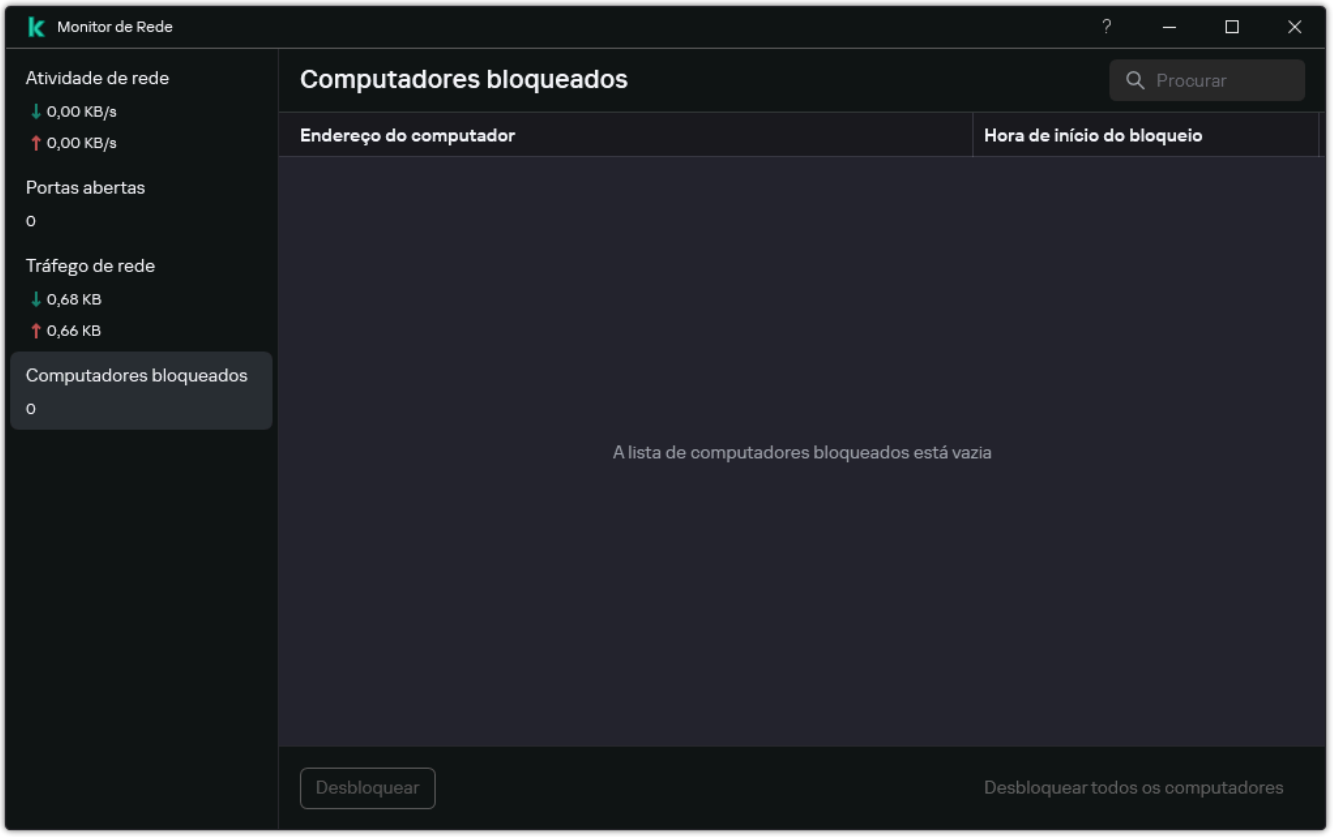
Para desbloquear um computador:

1. Na janela principal da aplicação, na secção **Monitorização**, clique em **Monitor de Rede**.
2. Aceda ao separador **Computadores bloqueados**.

   Esta ação abre uma lista de computadores boqueados (ver a figura abaixo).

   O Kaspersky Endpoint Security limpa a lista do bloco quando a aplicação é reiniciada e quando as definições da Proteção contra ameaças de Rede são alteradas.

3. Selecione o computador que pretende desbloquear e clique em **Desbloquear**.



Lista de computadores bloqueados

Configurar moradas de exclusões de bloqueio

O Kaspersky Endpoint Security pode reconhecer um ataque de rede e bloquear uma ligação de rede não segura que esteja a transmitir um grande número de pacotes (por exemplo, de câmaras de vigilância). Para trabalhar com dispositivos fiáveis, pode adicionar os endereços IP desses dispositivos à lista de exclusões. Também é possível selecionar o protocolo e a porta utilizados para a comunicação e permitir atividades de rede específicas.

Como configurar endereços de exclusões de bloqueio na Administration Console (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de rede**.
5. No bloco **Definições de Proteção contra ameaças de rede**, clique no botão **Exclusões**.
6. Na janela que abre, clique no botão **Adicionar**.
7. Introduza o endereço IP do computador para o qual não devem ser bloqueados os ataques de rede.

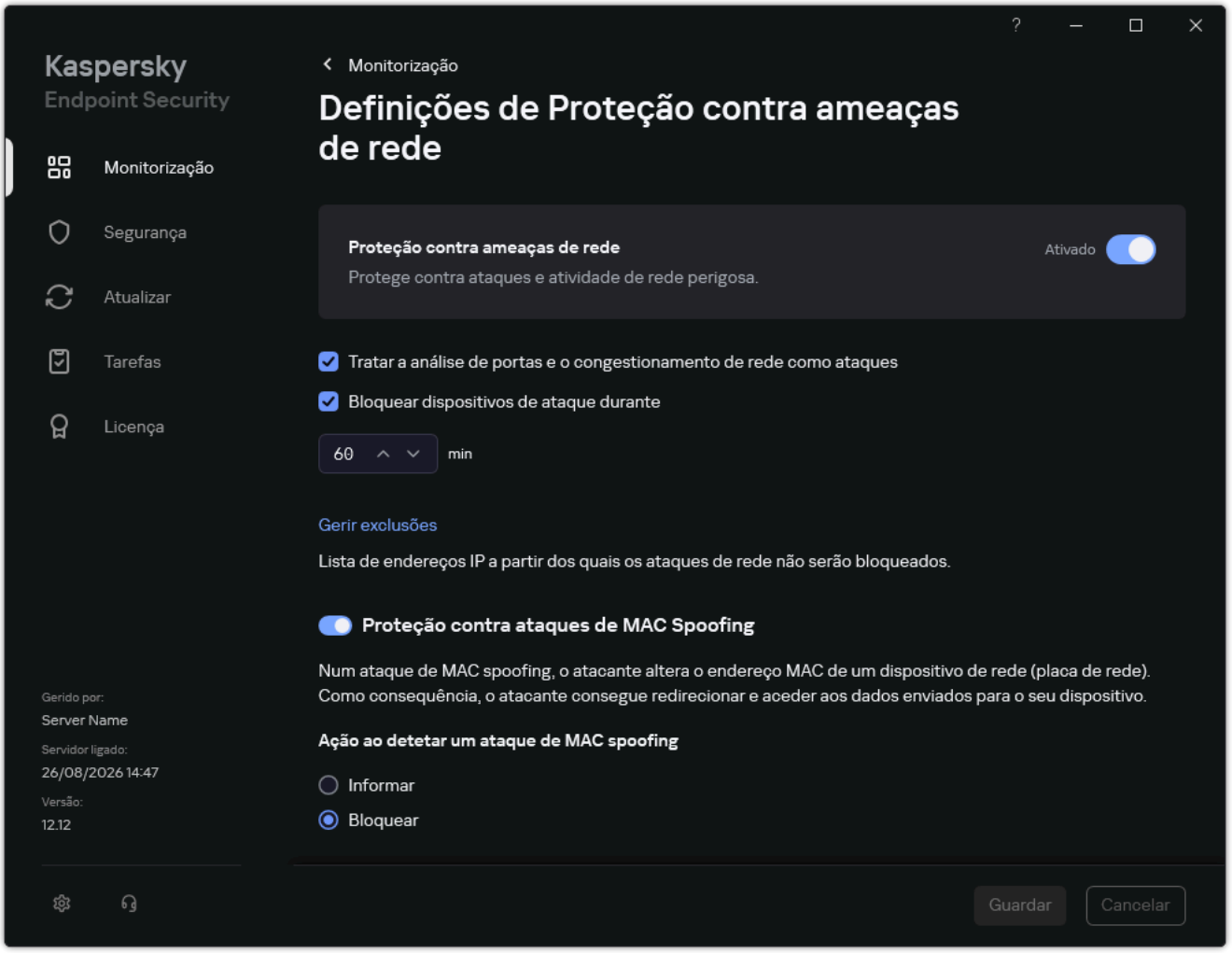
   Se necessário, selecione o protocolo e as portas pelas quais os dados são transmitidos.
8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como configurar endereços excluídos do bloqueio na Web Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda à secção **Trusted Zone**.
5. Na janela que abre, clique na ligação **IP addresses**.
   Esta ação abre uma janela que contém uma lista de endereços IP fiáveis.
6. Na janela que abre, clique no botão **Add**.
7. Introduza o endereço IP do computador para o qual não devem ser bloqueados os ataques de rede.
   Se necessário, especifique a sub-rede.
8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como configurar endereços de exclusões de bloqueio na interface do utilizador da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de rede**.



Definições da Proteção contra ameaças de Rede

3. Clique na hiperligação **Gerir exclusões**.
4. Na janela que abre, clique no botão **Adicionar**.
5. Introduza o endereço IP do computador para o qual não devem ser bloqueados os ataques de rede.

   Se necessário, selecione o protocolo e as portas pelas quais os dados são transmitidos.
6. Guarde as suas alterações.

Exportar e importar a lista de exclusões a partir do bloqueio

Pode exportar a lista de exclusões para um ficheiro XML. Em seguida, pode modificar o ficheiro para, por exemplo, adicionar um grande número de endereços do mesmo tipo. Também pode utilizar a função de exportação/importação para fazer uma cópia de segurança da lista de exclusões ou para migrar a lista para um servidor diferente.

Como exportar e importar uma lista de exclusões na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de rede**.
4. No bloco **Definições de Proteção contra ameaças de rede**, clique no botão **Exclusões**.
5. Para exportar a lista de regras:
   a. Selecione as exclusões que pretende exportar. Para selecionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.
      Se não tiver selecionado nenhuma exclusão, o Kaspersky Endpoint Security exportará todas as exclusões.
   b. Selecione o botão → **Exportar**.
   c. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de exclusões e selecione a pasta onde pretende guardar este ficheiro.
   d. Guardar o ficheiro.
      O Kaspersky Endpoint Security exporta toda a lista de exclusões para o ficheiro XML.
6. Para importar a lista de exclusões:
   a. Selecione o botão → **Importar**.
   b. Na janela que se abre, selecione o ficheiro XML do qual deseja importar a lista de exclusões.
   c. Abrir o ficheiro.
      Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security irá solicitar-lhe a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro XML.
7. Guarde as suas alterações.

Como exportar e importar uma lista de exclusões na Kaspersky Security Center Web Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Communication & Web Protection** → **Network Threat Protection**.
5. Na parte superior da janela, clique na ligação **Trusted IP addresses**.
   Abre-se a lista de exclusões.

6. Para exportar a lista de regras:

   a. Selecione as exclusões que pretende exportar.

   b. Selecione o botão → **Export**.

      O Kaspersky Endpoint Security exporta a lista de exclusões para um ficheiro JSON na pasta de transferências predefinida.

7. Para importar a lista de exclusões:

   a. Selecione o botão → **Import**.

      Na janela que se abre, selecione o ficheiro JSON do qual deseja importar a lista de exclusões.

   b. Abrir o ficheiro.

      Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security irá solicitar-lhe a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro JSON.

8. Guarde as suas alterações.

Configurar a Proteção contra ameaças de rede por tipo

O Kaspersky Endpoint Security permite fazer a gestão da proteção contra os seguintes tipos de ataques de rede:

- A *saturação de redes* é um ataque aos recursos da rede de uma organização (como os servidores de Internet). Este ataque consiste no envio de um grande número de solicitações, de modo a sobrecarregar a largura de banda dos recursos da rede. Quando tal acontece, os utilizadores não conseguem aceder aos recursos da rede da organização.

- Um ataque de *mapeamento de portas* consiste no mapeamento de portas UDP, portas TCP e serviços de rede no computador. Este ataque permite que o cibercriminoso identifique o grau de vulnerabilidade do computador antes de efetuar tipos mais perigosos de ataques à rede. O mapeamento de portas também permite que o cibercriminoso identifique o sistema operativo no computador e selecione os ataques de rede apropriados para tal sistema.

- Um *ataque de simulação MAC* consiste em mudar o endereço MAC de um dispositivo de rede (placa de rede). Como resultado, um criminoso pode redirecionar os dados enviados para um dispositivo para outro dispositivo e obter acesso a estes dados. O Kaspersky Endpoint Security permite bloquear ataques de simulação MAC e receber notificações sobre os ataques.

Pode desativar a detecção destes tipos de ataques no caso de algumas das suas aplicações permitidas executarem operações que são típicas para estes tipos de ataques. Esta ação ajudará a evitar falsos diagnósticos positivos.

Por predefinição, o Kaspersky Endpoint Security não monitoriza ataques de saturação de redes, de mapeamento de portas e de simulação MAC.

Não é possível configurar exclusões distintas para estes tipos de ataques. Isto significa que, mesmo que sejam adicionados endereços IP individuais à zona fiável, o Kaspersky Endpoint Security bloqueia o computador atacante se for detetado um ataque deste tipo. Pode ativar ou desativar a deteção desses ataques.

Não recomendamos a ativação da proteção contra simulação de MAC 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 devido a resultados falsos positivos.

Como configurar a Proteção contra ameaças de rede por tipo na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de rede**.
4. Use a caixa de verificação **Tratar a análise de portas e o congestionamento de rede como ataques** para ativar ou desativar a deteção destes ataques.

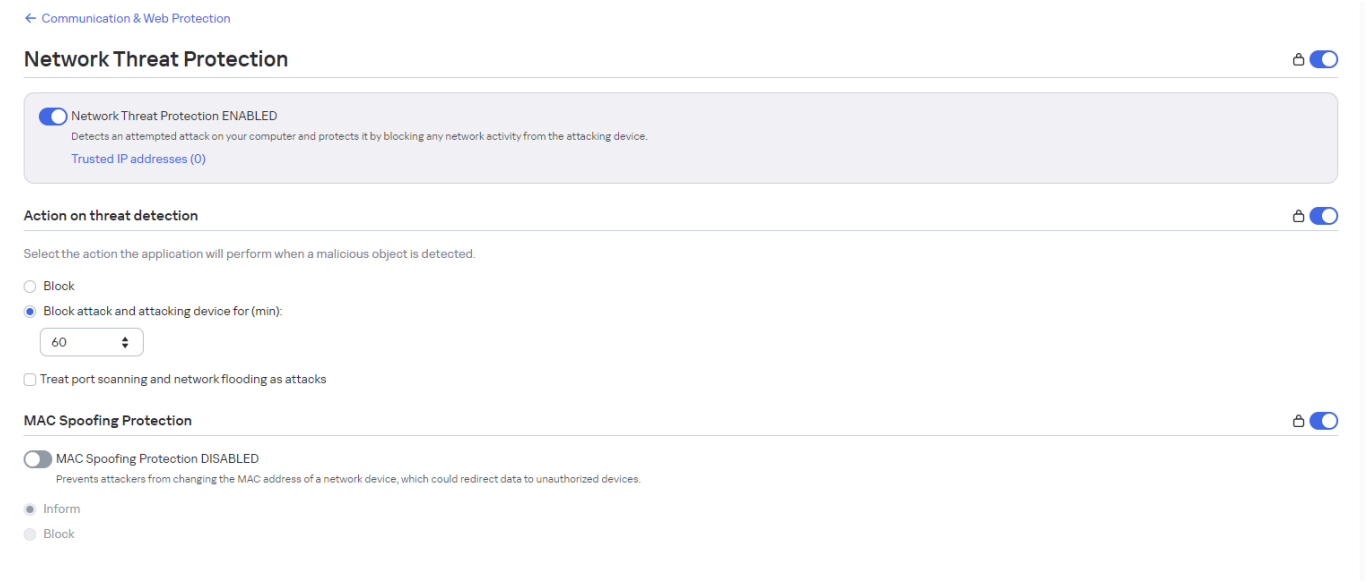
   Se esta funcionalidade estiver ativada, o Kaspersky Endpoint Security monitoriza o tráfego de rede para detetar o mapeamento de portas e saturação de rede. Se esse comportamento for detetado, a aplicação notifica o utilizador e envia o evento correspondente ao Kaspersky Security Center. A aplicação fornece informações sobre o computador que está a fazer os pedidos. Esta informação é necessária para uma resposta atempada. No entanto, o Kaspersky Endpoint Security não bloqueia o computador que está a fazer os pedidos porque esse tráfego pode ser uma ocorrência normal na rede corporativa.
5. No bloco **Modo de proteção contra falsificação de MAC**, selecione uma das seguintes opções:
   - **Não monitorizar falsificação de MAC**.
   - **Informar**.
   - **Bloquear**.
6. Guarde as suas alterações.

Como configurar a Proteção contra ameaças de Rede por tipo na Web Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.

4. Aceda a **Communication & Web Protection** → **Network Threat Protection**.



Definições da Proteção contra ameaças de Rede

5. Use a caixa de verificação **Treat port scanning and network flooding as attacks** para ativar ou desativar a deteção destes ataques.

   Se esta funcionalidade estiver ativada, o Kaspersky Endpoint Security monitoriza o tráfego de rede para detetar o mapeamento de portas e saturação de rede. Se esse comportamento for detetado, a aplicação notifica o utilizador e envia o evento correspondente ao Kaspersky Security Center. A aplicação fornece informações sobre o computador que está a fazer os pedidos. Esta informação é necessária para uma resposta atempada. No entanto, o Kaspersky Endpoint Security não bloqueia o computador que está a fazer os pedidos porque esse tráfego pode ser uma ocorrência normal na rede corporativa.

6. Em **MAC Spoofing Protection**, configure a deteção de ataques de MAC spoofing:

   a. Utilize o botão de alternar **MAC Spoofing Protection ENABLED** para ativar ou desativar a deteção destes ataques.

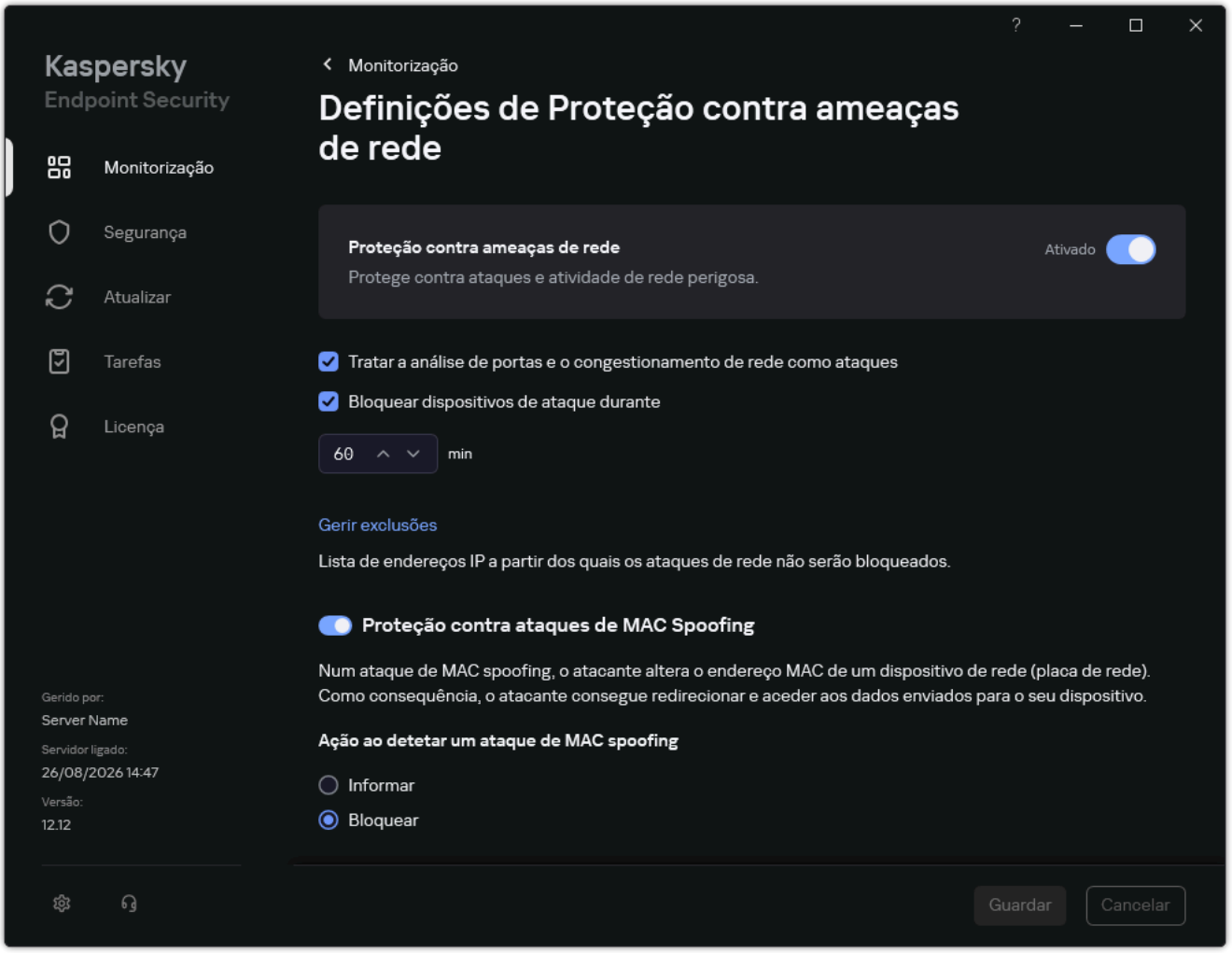
   b. Selecione a ação a executar quando for detetado um ataque de MAC spoofing:

   - **Inform**.
   - **Block**.

7. Guarde as suas alterações.

Como configurar a Proteção contra ameaças de rede por tipo na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Proteção contra ameaças de rede**.



Definições da Proteção contra ameaças de Rede

3. Utilize o botão de alternar **Tratar a análise de portas e o congestionamento de rede como ataques** para ativar ou desativar a deteção destes ataques.

   Se esta funcionalidade estiver ativada, o Kaspersky Endpoint Security monitoriza o tráfego de rede para detetar o mapeamento de portas e saturação de rede. Se esse comportamento for detetado, a aplicação notifica o utilizador e envia o evento correspondente ao Kaspersky Security Center. A aplicação fornece informações sobre o computador que está a fazer os pedidos. Esta informação é necessária para uma resposta atempada. No entanto, o Kaspersky Endpoint Security não bloqueia o computador que está a fazer os pedidos porque esse tráfego pode ser uma ocorrência normal na rede corporativa.

4. Utilize o botão de alternar **Proteção contra ataques de MAC Spoofing** para ativar ou desativar a deteção destes ataques.

5. No bloco **Ação ao detetar um ataque de MAC spoofing**, selecione uma das seguintes opções:

   - **Informar**.
   - **Bloquear**.

6. Guarde as suas alterações.

Firewall

O componente da Firewall bloqueia ligações não autorizadas a um computador enquanto trabalha na Internet ou numa rede local. A Firewall controla também a atividade de rede das aplicações no computador. Isto permite-lhe proteger a sua LAN empresarial contra roubo de identidade e outros ataques. O componente fornece proteção ao computador com a ajuda das bases de dados antivírus, o serviço de nuvem da Kaspersky Security Network e *regras de rede* predefinidas.

O Agente de Rede é utilizado para interação com o Kaspersky Security Center. A Firewall cria automaticamente regras de rede necessárias para o funcionamento da aplicação e do Agente de Rede. Por conseguinte, a Firewall abre várias portas no computador. A função do computador determina as portas que são abertas (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

Pode configurar as regras da rede aos seguintes níveis:

- *Regras de pacotes de rede*. As regras de pacotes de rede impõem restrições aos pacotes de rede, independentemente da aplicação. Estas regras restringem o tráfego de entrada e de saída de rede, 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 aplicações*. As regras de rede de aplicações impões restrições à atividade de rede de uma aplicação especificada. Estas influenciam não só as características do pacote de rede, mas também a aplicação específica à qual este pacote de rede se destina ou que emitiu este pacote de rede.

O acesso controlado de aplicações aos recursos, processos e dados pessoais do sistema operativo é fornecido pelo componente Prevenção contra invasões utilizando *direitos da aplicação*.

Durante a primeira inicialização da aplicação, a Firewall executa as seguintes ações:

1. Verifica a segurança da aplicação ao usar bases de dados antivírus transferidas.
2. Verifica a segurança da aplicação na Kaspersky Security Network.

   Recomenda-se a participação na Kaspersky Security Network para ajudar a Firewall a funcionar de forma mais eficiente.
3. Coloca a aplicação num dos grupos de confiança: *Fiáveis*, *Restrições baixas*, *Restrições altas*, *Não fiáveis*.

   Um grupo fiável define os direitos em que o Kaspersky Endpoint Security se baseia para controlar a atividade da aplicação. O Kaspersky Endpoint Security coloca uma aplicação num grupo fiável, dependendo do nível de perigo que essa aplicação pode representar para o computador.

O Kaspersky Endpoint Security coloca uma aplicação num grupo fiável para os componentes Firewall e Prevenção de Intrusão do Host. Não pode alterar o grupo fiável apenas para a Firewall ou Prevenção contra invasões.

Caso se tenha recusado participar na KSN ou não haja rede, o Kaspersky Endpoint Security coloca a aplicação num grupo fiável, dependendo das definições do componente Prevenção de Intrusão do Host. Após receber a reputação da aplicação da KSN, o grupo fiável pode ser alterado automaticamente.

4. Bloqueia a atividade de rede da aplicação, dependendo do grupo fiável. Por exemplo, as aplicações no grupo fiável de *Restrições altas* não têm permissão para utilizar nenhuma das ligações de rede.

Na próxima vez que a aplicação for iniciada, o Kaspersky Endpoint Security verifica a integridade da aplicação. Se a aplicação não tiver sido modificada, o componente utiliza as atuais regras da rede da aplicação. Se a aplicação tiver sido modificada, a Kaspersky Endpoint Security analisa a aplicação como se estivesse a ser iniciada pela primeira vez.

Prioridades de regra de rede

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

As regras de pacotes de rede têm uma prioridade mais elevada do que as regras de rede para aplicações. Se estiverem especificadas regras de pacotes de rede e regras de rede para aplicações para o mesmo tipo de atividade de rede, a atividade de rede é processada de acordo com as regras de pacotes de rede.

As regras de rede para aplicações funcionam de uma forma específica. Uma regra de rede para aplicações inclui regras de acesso com base no estado da rede: *Rede pública*, *Rede local* ou *Rede fiável*. Por exemplo, por predefinição, não é permitida nenhuma atividade de rede das aplicações no grupo fiável *Restrições altas* em redes de todos os estados. Se for especificada uma regra de rede para uma aplicação individual (aplicação principal), os processos secundários de outras aplicações serão executados de acordo com a regra de rede da aplicação principal. Se não houver uma regra de rede para a aplicação, os processos subordinados serão executados de acordo com a regra de acesso à rede do grupo fiável da aplicação.

Por exemplo, proibiu toda a atividade de rede nas redes de todos os estados para todas as aplicações, salvo para o navegador X. Se iniciar a instalação do navegador Y (processo subordinado) a partir do navegador X (aplicação principal), o instalador do navegador Y acederá à rede e transferirá os ficheiros necessários. Após a instalação, não será permitida ao navegador Y nenhuma ligação de rede de acordo com as definições da Firewall. Para proibir a atividade de rede do instalador do navegador Y como um processo secundário, deve adicionar uma regra de rede para o instalador do navegador Y.

Tipos da ligação de rede

A Firewall permite controlar a atividade da rede, dependendo do tipo da ligação de rede. O Kaspersky Endpoint Security recebe o tipo da ligação de rede a partir do sistema operativo do computador. O tipo da ligação de rede no sistema operacional é definido pelo utilizador ao configurar a ligação. Pode alterar o tipo da ligação de rede nas definições do Kaspersky Endpoint Security. A Firewall monitoriza a atividade da rede, dependendo do tipo de rede, especificado nas definições do Kaspersky Endpoint Security, e não do sistema operativo.

Estão disponíveis os seguintes tipos de ligação de rede:

- **Rede pública**. A rede não está protegida por aplicações antivírus, firewalls ou filtros (como Wi-Fi num café). Quando um utilizador utiliza um computador ligado a uma destas redes, a Firewall bloqueia o acesso aos ficheiros e às impressoras deste computador. Os utilizadores externos também não conseguem aceder aos dados através de pastas partilhadas e acesso remoto ao ambiente de trabalho deste computador. A Firewall filtra a atividade de rede de cada aplicação, de acordo com as regras de rede definidas para a mesma.

  Por predefinição, a Firewall atribui o tipo *Rede pública* à Internet. Não é possível alterar o tipo da Internet.

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

- **Rede fiável**. Uma rede segura na qual um computador não está exposto a ataques ou a tentativas não autorizadas de acesso aos dados. A Firewall permite qualquer atividade da rede nas redes que tenham este estado.

Compatibilidade com o Firewall do Windows Defender

O sistema operativo tem o seu próprio firewall incorporado, o *Firewall do Windows Defender*. A aplicação comporta-se de forma diferente consoante o tipo de sistema operativo:

- **Estação de trabalho**. A utilização do Firewall da Kaspersky em simultâneo com o Firewall do Windows Defender pode causar o funcionamento incorreto do sistema operativo. Por conseguinte, o Kaspersky Endpoint Security dispõe de um mecanismo que impede a utilização simultânea de ambos os firewalls. Quando ativa o Firewall da Kaspersky, o sistema operativo desativa automaticamente o Firewall do Windows Defender. Quando desativa o Firewall da Kaspersky, o sistema operativo 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 ao instalar a aplicação.

Ativar ou desativar a Firewall

Por predefinição, a Firewall está ativada e funciona no modo otimizado.

Como ativar ou desativar a Firewall na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção essencial contra ameaças → Firewall**.
4. Use a caixa de verificação **Firewall** para ativar ou desativar o componente.
5. Guarde as suas alterações.

Como ativar ou desativar a Firewall na Web Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Selecione **Communication & Web Protection** → **Firewall**.
5. Use o botão de alternar da **Firewall ENABLED** para ativar ou desativar o componente.
6. Guarde as suas alterações.

Como ativar ou desativar a Firewall na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças** → **Firewall**.
3. Use o botão de alternar da **Firewall** para ativar ou desativar o componente.
4. Guarde as suas alterações.

Como resultado, se a Firewall estiver ativada, o Kaspersky Endpoint Security controla a atividade de rede e bloqueia ligações de rede não autorizadas para o seu computador, e também bloqueia atividades de rede não autorizadas de aplicações no seu computador. A atividade de rede também é controlada pelo componente Proteção contra ameaças de rede. O componente Proteção contra ameaças de Rede (também denominado Intrusion Detection System, IDS) monitoriza o tráfego de entrada da rede quanto à existência de atividade característica de ataques à rede.

O Kaspersky Endpoint Security regista eventos de ataque de rede nos seus relatórios, independentemente das definições da Firewall. Mesmo que a Firewall bloqueie a ligação de rede utilizando regras e, assim, evite um ataque à rede, o componente Proteção contra ameaças de rede regista os eventos de ataque à rede. Este é necessário para gerar informações estatísticas sobre ataques de rede nos computadores da sua organização.

Alterar o tipo da ligação de rede

Por predefinição, a Firewall atribui o tipo *Rede pública* à Internet. Não é possível alterar o tipo da Internet.

Para alterar o tipo da ligação de rede:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças** → **Firewall**.
3. Clique em **Redes disponíveis**.
4. Selecione a ligação de rede cujo tipo pretende alterar.

5. Na coluna **Tipo de rede**, selecione o tipo da ligação de rede:

   - **Rede pública**. A rede não está protegida por aplicações antivírus, firewalls ou filtros (como Wi-Fi num café). Quando um utilizador utiliza um computador ligado a uma destas redes, a Firewall bloqueia o acesso aos ficheiros e às impressoras deste computador. Os utilizadores externos também não conseguem aceder aos dados através de pastas partilhadas e acesso remoto ao ambiente de trabalho deste computador. A Firewall filtra a atividade de rede de cada aplicação, de acordo com as regras de rede definidas para a mesma.

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

   - **Rede fiável**. Uma rede segura na qual um computador não está exposto a ataques ou a tentativas não autorizadas de acesso aos dados. A Firewall permite qualquer atividade da rede nas redes que tenham este estado.

6. Guarde as suas alterações.

Gerir regras de pacotes de rede

Pode executar as seguintes ações ao gerir regras de pacotes de rede:

- Criar uma nova regra de pacotes de rede.

  Pode criar uma nova regra de pacotes de rede, criando um conjunto de condições e ações que é aplicado aos pacotes e rede e aos fluxos de dados.

- Ativar ou desativar uma regra de pacotes de rede.

  Todas as regras de pacotes de rede criadas pela Firewall têm, por predefinição, o estado *Ativado*. Quando uma regra de pacotes de rede é ativada, a Firewall aplica esta regra.

  Pode desativar qualquer regra de pacotes de rede selecionada na lista de regras de pacotes de rede. Quando uma regra de pacotes de rede é desativada, a Firewall não aplica temporariamente esta regra.

  > É adicionada uma nova regra de pacotes de rede personalizada à lista de regras de pacotes de rede por predefinição, com o estado *Ativado*.

- Editar as definições de uma regra de pacotes de rede existente.

  Após criar uma nova regra de pacotes de rede, pode regressar à edição das respetivas definições e modificar as mesmas, conforme necessário.

- Alterar a ação da Firewall para uma regra de pacotes de rede.

  Na lista de regras de pacotes de rede, pode editar a ação executada pela Firewall ao detetar a atividade da rede que corresponde a uma regra de pacotes de rede específica.

- Alterar a prioridade de uma regra de pacotes de rede.

  Pode aumentar ou reduzir a prioridade de uma regra de pacotes de rede selecionada na lista.

- Remover uma regra de pacotes de rede.

  Pode remover uma regra de pacotes de rede para que a Firewall pare de aplicar esta regra ao detetar a atividade da rede e para que esta regra deixe de ser apresentada na lista de regras de pacotes de rede com o estado *Desativado*.

Criar uma regra de pacotes de rede

A firewall filtra toda a atividade de rede no computador de acordo com as regras de pacotes de rede. As regras de pacotes de rede contêm condições (por exemplo, direção, protocolo) que a Firewall aplica para controlar as ligações de rede do computador. As regras de pacotes de rede também especificam a ação que a Firewall executa com a ligação que corresponde à regra (permitir ou bloquear a ligação).

Recomendações para criar regras de pacotes de rede

Pode especificar um endereço IP ou um intervalo de endereços IP para filtrar a atividade da rede. Também pode especificar um nome DNS.

Se for utilizado um nome DNS numa regra, o Kaspersky Endpoint Security resolve esse nome DNS para um endereço IP e, posteriormente, trata a regra como se esse endereço IP tivesse sido especificado na mesma.

O Kaspersky Endpoint Security pode resolver nomes DNS nos seguintes casos:

- Arranque da aplicação
- Alteração das definições da Firewall

Quando a aplicação resolve nomes DNS a partir do computador no qual está instalada, pode ser efetuado um grande número de consultas ao servidor DNS. Para evitar esta situação, recomendamos que utilize endereços IP em vez de nomes DNS ao criar regras.

Em alguns casos, a utilização de nomes DNS em nomes de pacotes de rede pode não ser segura, porque o proprietário do servidor DNS pode modificar os parâmetros do registo DNS. Um agente malicioso também pode falsificar mensagens DNS e contornar as regras da Firewall.

É possível controlar as ligações de rede por nomes DNS utilizando as regras do Controlo de Internet. Se precisar de especificar um nome DNS nas regras da Firewall:

- Garanta a segurança da LAN corporativa.
- Garanta a segurança da cache e dos servidores DNS autoritativos.
- Ative a proteção do registo DNS contra modificações.

Ao criar regras de pacotes de rede, note que estas têm prioridade sobre as regras de rede para aplicações.

Métodos de criação de regras de pacotes de rede

Pode criar uma nova regra de pacotes de rede das seguintes formas:

- Utilize a ferramenta Monitor de Rede.

  O *Monitor de rede* é uma ferramenta concebida para visualizar informações sobre a atividade de rede do computador de um utilizador em tempo real. Isto é conveniente, dado que não é necessário configurar todas as definições da regra. Algumas definições da Firewall serão inseridas automaticamente a partir dos dados do Monitor de Rede. O Monitor de Rede apenas está disponível na interface da aplicação.

- Configure as definições da Firewall.

  Isto permite-lhe ajustar as definições da Firewall. Pode criar regras para qualquer atividade de rede, mesmo se não houver atividade de rede no momento.

Como utilizar a ferramenta Monitor de Rede para criar uma regra de pacotes de rede na interface da aplicação

1. Na janela principal da aplicação, na secção **Monitorização**, clique em **Monitor de Rede**.
2. Aceda ao separador **Atividade de rede**.

   O separador **Atividade de rede** apresenta todas as ligações de rede ativas atualmente com o computador. São apresentadas as ligações de rede de entrada e de saída.
3. No menu de contexto de uma ligação de rede, selecione **Criar regra para o pacote de rede**.

   Esta ação abre as propriedades da regra de rede.
4. Defina o estado **Ativo** para a regra de pacotes.
5. Introduza manualmente o nome do serviço de rede no campo **Nome**.
6. Configure as definições da regra de rede (consulte a tabela abaixo).

   Pode selecionar um modelo de regra predefinido ao clicar na ligação **Modelo de regra de rede**. Os modelos de regras descrevem as ligações de rede usadas com mais frequência.

   Todas as definições de regras de rede são preenchidas automaticamente.
7. Se pretender que as ações da regra de rede se reflitam no relatório, selecione a caixa de verificação **Registar eventos**.
8. Clique em **Guardar**.

   A nova regra de rede será adicionada à lista.
9. Utilize os botões **Para cima**/**Para baixo** para definir a prioridade da regra de rede.
10. Guarde as suas alterações.

Como utilizar as definições da Firewall para criar uma regra de pacotes de rede na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças** → **Firewall**.

3. Clique em **Regras de pacotes**.

   Esta ação abre a lista das regras de rede predefinidas definidas pela Firewall.

4. Na lista suspensa **Adicionar**, selecione o local da regra na lista: no topo da lista, 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 estado **Ativo** para a regra de pacotes.

6. Introduza manualmente o nome do serviço de rede no campo **Nome**.

7. Configure as definições da regra de rede (consulte a tabela abaixo).

   Pode selecionar um modelo de regra predefinido ao clicar na ligação **Modelo de regra de rede**. Os modelos de regras descrevem as ligações de rede usadas com mais frequência.

   Todas as definições de regras de rede são preenchidas automaticamente.

8. Se pretender que as ações da regra de rede se reflitam no relatório, selecione a caixa de verificação **Registar eventos**.

9. Clique em **Guardar**.

   A nova regra de rede será adicionada à lista.

10. Utilize os botões **Para cima**/**Para baixo** para definir a prioridade da regra de rede.

11. Guarde as suas alterações.

Como criar uma regra de pacotes de rede na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Proteção essencial contra ameaças** → **Firewall**.

4. No bloco **Definições da firewall**, clique no botão **Definições**.

   Esta ação abre a lista das regras de pacotes de rede e a lista das regras de rede da aplicação.

5. Aceda ao separador **Regras de pacotes de rede**.

   Esta ação abre a lista das regras de rede predefinidas definidas pela Firewall.

6. Na lista suspensa **Adicionar**, selecione o local da regra na lista: no topo da lista, 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. Introduza manualmente o nome do serviço de rede no campo **Nome**.

8. Configure as definições da regra de rede (consulte a tabela abaixo).

   Pode selecionar um modelo de regra predefinido ao clicar no botão . Os modelos de regras descrevem as ligações de rede usadas com mais frequência.

   Todas as definições de regras de rede são preenchidas automaticamente.

9. Se pretender que as ações da regra de rede se reflitam no relatório, selecione a caixa de verificação **Registar eventos**.

10. Guardar a nova regra de rede.
11. Utilize os botões **Para cima**/**Para baixo** para definir a prioridade da regra de rede.
12. Guarde as suas alterações.

A Firewall controlará os pacotes de rede de acordo com a regra. Pode desativar uma regra de pacotes da operação da Firewall sem eliminá-la da lista. Para o fazer, desmarque a caixa de verificação ao lado do objeto.

Como criar uma regra de pacotes de rede na Web Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Selecione **Communication & Web Protection** → **Firewall**.
5. Selecione o separador **Network packet rules**.

   Esta ação abre a lista das regras de rede predefinidas definidas pela Firewall.
6. Clique em **Add**.

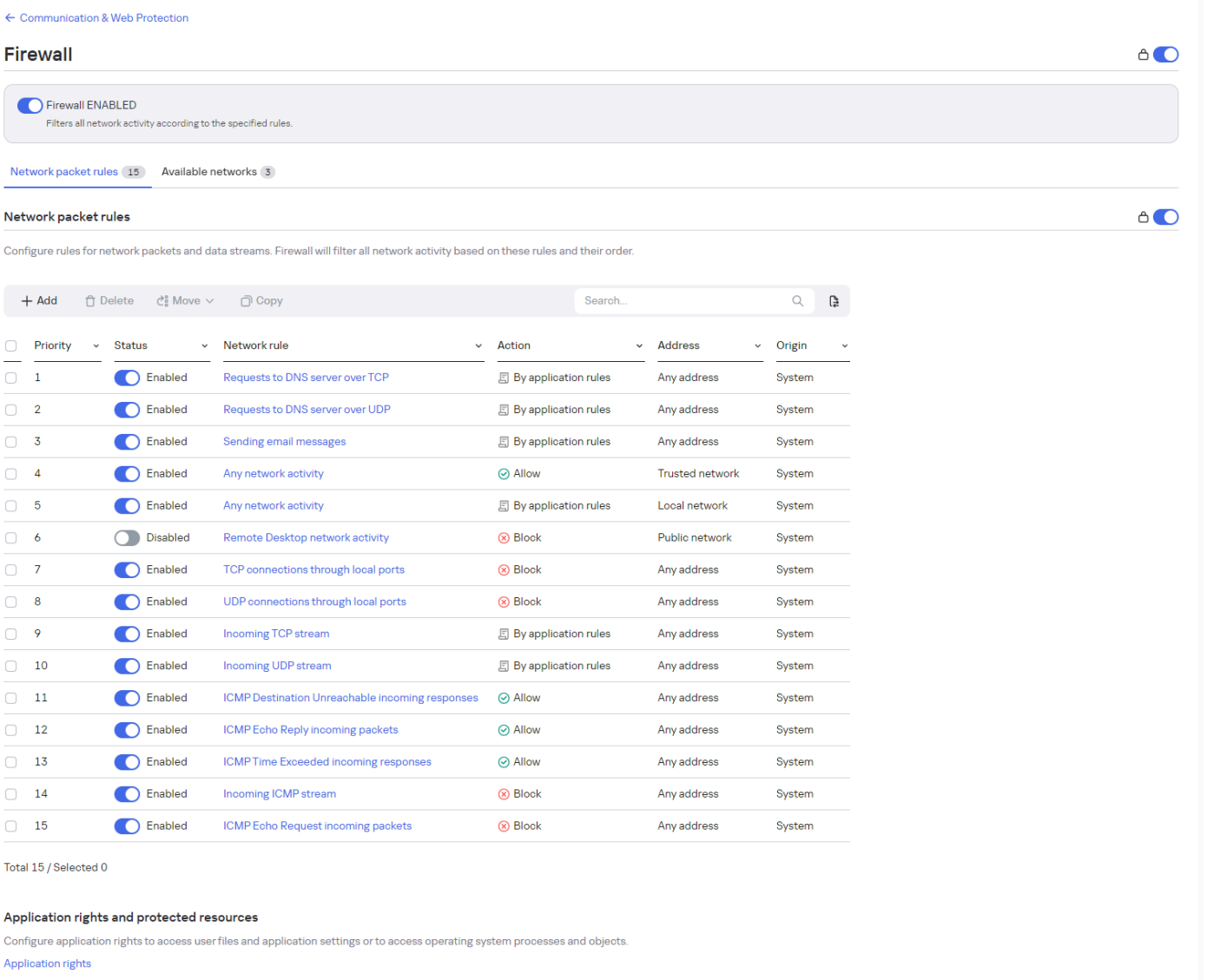
   Esta ação abre o formulário para uma nova regra de rede.
7. Introduza manualmente o nome do serviço de rede no campo **Rule name**.
8. Configure as definições da regra de rede (consulte a tabela abaixo).

   Pode selecionar um modelo de regra predefinido ao clicar na ligação **Select rule template**. Os modelos de regras descrevem as ligações de rede usadas com mais frequência.

   Todas as definições de regras de rede são preenchidas automaticamente.
9. Se pretender que as ações da regra de rede se reflitam no relatório, selecione a caixa de verificação **Log events**.
10. Guardar a regra de rede.

    A nova regra de rede será adicionada à lista.
11. Utilize o botão **Move** para definir a prioridade da regra de rede.
12. Guarde as suas alterações.

A Firewall controlará os pacotes de rede de acordo com a regra. Pode desativar uma regra de pacotes da operação da Firewall sem eliminá-la da lista. Utilize o botão de alternar na coluna **Status** para ativar ou desativar a regra do pacote.



Regras de pacotes da Firewall

Definições da regra de pacotes de rede

Parâmetro	Descrição
Ação	**Permitir**. **Bloquear**. **Segundo as regras da aplicação**. Se esta opção estiver selecionada, a Firewall aplica as regras de rede de aplicações à ligação de rede.
Protocolo	Controle a atividade de rede executada através do protocolo selecionado: TCP, UDP, ICMP, ICMPv6, IGMP e GRE. Se ICMP ou ICMPv6 estiver selecionado como protocolo, pode definir o código e o tipo de pacote ICMP. Se TCP ou UDP estiver selecionado como o tipo de protocolo, pode especificar os números de porta dos computadores locais e remotos entre os quais a ligação deve ser monitorizada. Intervalo de valores possíveis para os números de porta: 0–65535. Em cada campo, pode inserir vários valores separados por `,` ou especificar um intervalo de valores utilizando `-`. Por exemplo: • `100,101` • `100-130` • `100,110-130`

Parâmetro	Descrição
Direção	**Entrada (pacote)**. A Firewall aplica a regra de rede a todos os pacotes de rede de entrada. **Entrada**. A Firewall aplica a regra de rede a todos os pacotes de rede enviados através de uma ligação iniciada por um computador remoto. **Entrada/Saída**. A Firewall aplica a regra de rede a todos os pacotes de rede de entrada e de saída. **Saída (pacote)**. A Firewall aplica a regra de rede a todos os pacotes de rede de saída. **Saída**. A Firewall aplica a regra de rede a todos os pacotes de rede enviados através de uma ligação iniciada pelo computador do utilizador.
Adaptadores de rede	Adaptadores de rede que podem enviar e/ou receber pacotes de rede. A especificação das definições dos adaptadores de rede permite diferenciar entre pacotes de rede enviados ou recebidos por adaptadores de rede com endereços IP idênticos.
Time to live (TTL)	Limitar o controlo dos pacotes de rede pelo seu tempo de vida (Time to Live, TTL).
Endereços remotos	Endereços de rede de computadores remotos que podem enviar e/ou receber pacotes de rede. A Firewall aplica a regra de rede ao intervalo especificado de endereços de rede remotos. Pode incluir todos os endereços IP numa regra de rede, criar uma lista separada de endereços IP, especificar um intervalo de endereços IP ou selecionar uma sub-rede (redes fiáveis, redes locais, redes públicas). Também pode especificar um nome DNS de um computador em vez do seu endereço IP. Apenas deve usar nomes DNS para computadores da rede local ou serviços internos. A interação com os serviços em nuvem (como Microsoft Azure) e outros recursos da Internet deve ser tratada pelo componente Controlo de Internet. Se na regra de pacote de rede adicionou um nome DNS para o qual não seja possível determinar o endereço IP, o Kaspersky Endpoint Security apresentará um aviso. Na lista de regras de pacote de rede na Consola Web, é adicionada uma coluna com uma descrição do erro. Na Administration Console (MMC), a descrição do erro não está disponível. Estas regras de pacotes são realçadas a cores.
Endereços locais	Endereços de rede de computadores que podem enviar e receber pacotes de rede. A Firewall aplica uma regra de rede ao intervalo especificado de endereços de rede locais. Pode incluir todos os endereços IP numa regra de rede, criar uma lista separada de endereços IP ou especificar um intervalo de endereços IP. A aplicação armazena endereços locais apenas se for especificada uma lista de endereços remotos. Ou seja, foi selecionado o valor **Endereços da lista** para **Endereços remotos** e foi adicionado, pelo menos, um endereço. Por vezes, o endereço local não pode ser obtido para aplicações. Se for este o caso, este 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 da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Firewall**.
3. Clique em **Regras de pacotes**.
   Abre-se uma lista predefinida de regras de pacotes de rede definidas pela Firewall.
4. Na lista, selecione a regra de pacotes de rede necessária.
5. Utilize o botão de alternar na coluna **Estado** para ativar ou desativar a regra.
6. Guarde as suas alterações.

Alterar a ação da Firewall para uma regra de pacotes de rede

Para alterar a ação da Firewall aplicada a uma regra de pacotes de rede:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Firewall**.
3. Clique em **Regras de pacotes**.

   Abre-se uma lista predefinida de regras de pacotes de rede definidas pela Firewall.
4. Selecione a regra na lista de regras de pacotes de rede e clique no botão **Editar**.
5. Na lista suspensa **Ação**, selecione a ação a ser executada pela Firewall ao detetar este tipo de atividade de rede:

   - **Permitir**.
   - **Bloquear**.
   - **Segundo as regras da aplicação**. Se esta opção estiver selecionada, a Firewall aplica as regras de rede de aplicações à ligação de rede.
6. Guarde as suas alterações.

Alterar a prioridade de uma regra de pacotes de rede

A prioridade de uma regra de pacotes de rede é determinada pela respetiva posição na lista de regras de pacotes de rede. A primeira regra de pacote de rede na lista de regras de pacotes de rede tem a prioridade mais elevada.

As regras de pacotes de rede criadas manualmente são adicionadas ao fim da lista de regras de pacotes de rede e têm a prioridade mais baixa.

A firewall executa as regras pela ordem na qual são apresentadas na lista de regras de pacotes de rede, de forma descendente. De acordo com cada regra de pacote de rede processada aplicável a uma determinada ligação de rede, a firewall permite ou bloqueia o acesso da rede ao endereço e porta especificados nas definições desta ligação de rede.

Para alterar a prioridade da regra de pacotes de rede:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Firewall**.
3. Clique em **Regras de pacotes**.

   Abre-se uma lista predefinida de regras de pacotes de rede definidas pela Firewall.
4. Na lista, selecione a regra de pacotes de rede cuja prioridade pretende alterar.

5. Utilize os botões **Para cima**/**Para baixo** para definir a prioridade da regra de rede.

6. Guarde as suas alterações.

Exportar e importar regras de pacotes de rede

Pode exportar a lista de regras de pacotes de rede para um ficheiro XML. Em seguida, pode modificar o ficheiro para, por exemplo, adicionar um grande número de regras do mesmo tipo. Pode utilizar a função de exportação/importação para fazer uma cópia de segurança 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 na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Proteção essencial contra ameaças** → **Firewall**.

4. No bloco **Definições da firewall**, clique no botão **Definições**.

   Esta ação abre a lista das regras de pacotes de rede e a lista das regras de rede da aplicação.

5. Aceda ao separador **Regras de pacotes de rede**.

6. Para exportar a lista de regras de pacotes de rede:

   a. Selecione as regras que pretende exportar. Para selecionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.

      Se não tiver selecionado nenhuma regra, o Kaspersky Endpoint Security exportará todas as regras.

   b. Clique na hiperligação **Exportar**.

   c. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de regras e selecione a pasta onde pretende guardar este ficheiro.

   d. Guardar o ficheiro.

      O Kaspersky Endpoint Security exporta a lista de regras para o ficheiro XML.

7. Para importar uma lista de regras de pacotes de rede:

   a. Clique na hiperligação **Importar**.

      Na janela que se abre, selecione o ficheiro XML a partir do qual pretende importar a lista de regras.

   b. Abrir o ficheiro.

      Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro XML.

8. Guarde as suas alterações.

Como exportar e importar uma lista de regras de pacotes de rede na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Selecione **Communication & Web Protection** → **Firewall**.
5. Para exportar a lista de regras, no bloco **Network packet rules**:

   a. Selecione as regras que pretende exportar.

   b. Selecione o botão → **Export**.

   O Kaspersky Endpoint Security exporta a lista de regras para um ficheiro JSON na pasta de transferências predefinida.
6. Para importar a lista de regras, no bloco **Network packet rules**:

   a. Selecione o botão → **Import**.

   Na janela que se abre, selecione o ficheiro JSON a partir do qual pretende importar a lista de regras.

   b. Abrir o ficheiro.

   Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro JSON.
7. Guarde as suas alterações.

Definição de regras de pacotes de rede em XML

A firewall permite a exportação de regras de pacotes de rede no formato XML. Em seguida, pode modificar o ficheiro para, por exemplo, adicionar um grande número de regras do mesmo tipo.

O ficheiro XML contém dois nós principais: `Rules` e `Resources`. O nó `Rules` lista as regras de pacotes de rede. Este nó contém regras configuradas por padrão (*regras predefinidas*), bem como regras adicionadas pelo utilizador (*regras personalizadas*).

Marcação da regra de pacotes 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>
```

Definições da regra de pacotes de rede no formato XML

Parâmetro	Descrição	Valor
`<key name="0000">`	Prioridade da regra. Quanto menor for o valor, maior será a prioridade.	Número inteiro O valor prioritário tem de consistir em 4 dígitos. Os nós no ficheiro XML têm de ser organizados por valor de prioridade, começando por `0000`.
`RuleId`	ID da regra.	**Regras predefinidas** `100` – **Pedidos para o servidor de DNS por TCP**. `101` – **Pedidos para o servidor de DNS por UDP**. `102` – **Enviar mensagens de e-mail**. `110` – **Qualquer atividade de rede** (Redes fiáveis). `125` – **Qualquer atividade de rede** (Redes locais). `130` – **Atividade de rede do ambiente remoto**. `131` – **Ligações TCP por portas locais**. `132` – **Ligações UDP por portas locais**. `133` – **Fluxo TCP de entrada**. `134` – **Fluxo UDP de entrada**. `137` – **Respostas de entrada de ICMP Destination Unreachable**. `138` – **Pacotes de entrada de ICMP Echo Reply**. `140` – **Respostas de entrada de ICMP Time Exceeded**. `142` – **Fluxo ICMP de entrada**. `266` – **Pacotes de entrada de ICMPv6 Echo Request**.
`RuleState`	Estado 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 da aplicação a que pertence a regra do pacote de rede.	Se a regra não pertencer a nenhuma aplicação, o valor é `0`.
`ResIdEx`	ID principal do recurso com definições de regras. Pode utilizar este identificador para localizar um bloco com definições de regras no nó `Resources`.	Número inteiro
`ResIdEx2`	ID do tipo de rede.	`0` – **Qualquer endereço**. `50` – **Redes fiáveis**. `51` – **Redes locais**. `52` – **Redes públicas**. `<Network Identifier>` – **Endereços da lista** (os endereços são definidos manualmente).
`AccessFlag`	Valor do parâmetro **Ação**.	`0` – **Permitir**. `2` – **Segundo as regras da aplicação**. `3` – **Bloquear**. `4` – **Permitir** e **Registar eventos**. `6` – **Segundo as regras da aplicação** e **Registar eventos**. `7` – **Bloquear** e **Registar eventos**.
`</key>`		

O nó `Resources` contém definições de regras de pacotes de rede. As definições personalizadas das regras de pacotes de rede estão listadas no bloco `<key name="0004">`.

Marcação da regra de pacote de rede personalizado

```
<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>
```

Definições da regra de pacotes de rede personalizada

Parâmetro	Descrição	Valor
`<key name="Data">`	ID do bloco de parâmetros.	Número inteiro
`RemotePorts`	Valor do parâmetro **Portas remotas**.	Lista das gamas de portas remotas.
`LocalPorts`	Valor do parâmetro **Portas locais**.	Lista das gamas 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` – **Outra**. • `1` – **LoopBack**. • `2` – **Rede com fios (Ethernet)**. • `3` – **Rede sem fios (Wi-Fi)**. • `4` – **Túnel**. • `5` – **Ligação PPP**. • `6` – **Ligação PPPoE**. • `7` – **Ligação VPN**. • `8` – **Ligação 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` – **Echo Reply** (ICMP) ou desativado. `3` – **Destino inacessível** (ICMP). `4` – **Atraso de Origem**. `5` – **Redirecionar**. `6` – **Endereço de Anfitrião Alternativo**. `8` – **Echo Request**. `9` – **Anúncio de Router**. `10` – **Solicitação de Router**. `11` – **Tempo excedido**. `12` – **Problema de Parâmetro**. `13` – **Marca de hora**. `14` – **Resposta de Marca de hora**. `15` – **Pedido de Informação**. `16` – **Resposta de Informação**. `17` – **Pedido de Máscara de Endereço**. `18` – **Resposta de Máscara de Endereço**. `30` – **Traceroute**. `31` – **Erro de Conversão de Datagrama**. `32` – **Redirecionar Anfitrião Móvel**. `33` – **IPv6 Where-Are-You**. `34` – **IPv6 I-Am-Here**. `35` – **Pedido de Registo Móvel**. `36` – **Resposta de Registo Móvel**. `37` – **Pedido de Nome de Domínio**. `38` – **Resposta de Nome de Domínio**. `40` – **Photuris**. **Protocolo ICMPv6** `1` – **Destino inacessível**. `2` – **Pacote Demasiado Grande**. `3` – **Tempo excedido**. `4` – **Problema de Parâmetro**. `128` – **Echo Request**. `129` – **Echo Reply**. `130` – **Consulta de Recetor de Difusão**. `131` – **Relatório de Recetor de Difusão**. `132` – **Recetor de Difusão Concluído**. `133` – **Solicitação de Router**. `134` – **Anúncio de Router**. `135` – **Solicitação de Vizinho**. `136` – **Anúncio de Vizinho**. `137` – **Redirecionar Mensagem**. `138` – **Renumeração de Router**. `139` – **Consulta de Informação de Nó ICMP**. `141` – **Mensagem de Solicitação de Identificação de Vizinhança Inversa**. `142` – **Mensagem de Anúncio de Identificação de Vizinhança Inversa**. `143` – **Relatório de Recetor de Difusão Versão 2**.

Parâmetro	Descrição	Valor
		`144` – **Mensagem de Pedido de Identificação de Endereço de Agente Interno**. `145` – **Mensagem de Resposta de Identificação de Endereço de Agente Interno**. `146` – **Solicitação de Prefixo Móvel**. `147` – **Publicação de Prefixo Móvel**. `148` – **Mensagem de Solicitação do Caminho de Certificação**. `149` – **Mensagem de Publicação do Caminho de Certificação**. `151` – **Anúncio de Router de Difusão**. `152` – **Solicitação de Router de Difusão**. `153` – **Encerramento do Router de Difusão**.
`IcmpCode`	Valor do parâmetro **Código ICMP**.	`0` – **Código 0** ou desativado. `1` – **Código 1**. `2` – **Código 2**.
`Flags`	Ponteiro de atributos de estrutura.	Número inteiro Recomenda-se deixar este parâmetro inalterado.
`TTL`	Valor do parâmetro **Time to live (TTL)**.	Valor em segundos. Se desativado, o valor é `0`.
`</key>`		
`Id`	ID principal do recurso (veja o nó `Rules`).	Número inteiro
`ParentID`	ID do grupo principal.	Número inteiro Recomenda-se deixar este parâmetro inalterado.
`Flags`	Estado da regra.	`6` – a regra está desativada. `38` – a regra está ativada.
`Name`	Nome da regra de pacote de rede.	Cadeia

Gerir regras de rede de aplicações

Por predefinição, o Kaspersky Endpoint Security agrupa todas as aplicações instaladas no computador pelo nome do fornecedor do software cuja atividade dos ficheiros ou da rede está a monitorizar. Por sua vez, os grupos de aplicações são categorizados em grupos fiáveis. Todas as aplicações e grupos de aplicações herdam as propriedades dos respetivos grupos principais: as regras de controlo das aplicações, as regras de rede de aplicações e a respetiva prioridade de execução.

À semelhança do componente Prevenção contra invasões, por predefinição, o componente Firewall aplica as regras de rede de um grupo de aplicações ao filtrar a atividade da rede de todas as aplicações no grupo. As regras de rede de grupo de aplicações definem os direitos que permitem às aplicações no grupo aceder a ligações de rede diferentes.

Por predefinição, a Firewall cria um conjunto de regras de rede para cada grupo de aplicações detetado pelo Kaspersky Endpoint Security no computador. Pode alterar a ação da Firewall aplicada às regras de rede de grupo de aplicações criadas por predefinição. Não pode editar, remover, desativar ou alterar a prioridade das regras de rede do grupo de aplicações criadas por predefinição.

Também pode criar uma regra de rede para uma aplicação individual. Essa regra terá uma prioridade mais elevada do que a regra de rede do grupo ao qual a aplicação pertence.

Criar uma regra de rede de aplicações

Por predefinição, a atividade das aplicações é controlada por regras de rede definidas para o grupo fiável ao qual o Kaspersky Endpoint Security atribuiu a aplicação na primeira vez em que foi iniciada. Se necessário, pode criar regras de rede para um grupo fiável completo, para uma aplicação individual ou para um grupo de aplicações dentro de um grupo fiável.

As regras de rede definidas manualmente têm uma prioridade mais alta do que as regras de rede que foram determinadas para um grupo fiável. Ou seja, se as regras de aplicações definidas manualmente forem diferentes das regras de aplicações determinadas para um grupo fiável, a Firewall controla a atividade das aplicações de acordo com as regras de aplicações definidas manualmente.

Por predefinição, a Firewall cria as seguintes regras de rede para cada aplicação:

- Qualquer atividade de rede em redes fiáveis.
- Qualquer atividade de rede em redes locais.
- Qualquer atividade de rede em redes públicas.

O Kaspersky Endpoint Security controla a atividade de rede das aplicações de acordo com as regras de rede predefinidas da seguinte forma:

- Fiável e Restrições baixas: toda a atividade de rede é permitida.
- Restrições altas e Não fiável: toda a atividade de rede é bloqueada.

As regras de aplicações predefinidas não podem ser editadas ou eliminadas.

Pode criar uma regra de rede de aplicações das seguintes formas:

- Utilize a ferramenta Monitor de Rede.

  O *Monitor de rede* é uma ferramenta concebida para visualizar informações sobre a atividade de rede do computador de um utilizador em tempo real. Isto é conveniente, dado que não é necessário configurar todas as definições da regra. Algumas definições da Firewall serão inseridas automaticamente a partir dos dados do Monitor de Rede. O Monitor de Rede apenas está disponível na interface da aplicação.

- Configure as definições da Firewall.

  Isto permite-lhe ajustar as definições da Firewall. Pode criar regras para qualquer atividade de rede, mesmo se não houver atividade de rede no momento.

Ao criar regras de rede de aplicações, note que as regras de pacotes de rede têm prioridade sobre as regras de rede de aplicações.

Como utilizar a ferramenta Monitor de Rede para criar uma regra de rede de aplicações na interface da aplicação

1. Na janela principal da aplicação, na secção **Monitorização**, clique em **Monitor de Rede**.
2. Aceda ao separador **Atividade de rede** ou **Portas abertas**.

   O separador **Atividade de rede** apresenta todas as ligações de rede ativas atualmente com o computador. São apresentadas as ligações de rede de entrada e de saída.

   O separador **Portas abertas** indica todas as portas de rede abertas do computador.
3. No menu de contexto de uma ligação de rede, selecione **Criar uma regra de rede para a aplicação**.

   Abre-se a janela de regras e propriedades da aplicação.
4. Selecione o separador **Regras de rede**.

   Esta ação abre a lista das regras de rede predefinidas definidas pela Firewall.
5. Clique em **Adicionar**.

   Esta ação abre as propriedades da regra de rede.
6. Introduza manualmente o nome do serviço de rede no campo **Nome**.
7. Configure as definições da regra de rede (consulte a tabela abaixo).

   Pode selecionar um modelo de regra predefinido ao clicar na ligação **Modelo de regra de rede**. Os modelos de regras descrevem as ligações de rede usadas com mais frequência.

   Todas as definições de regras de rede são preenchidas automaticamente.
8. Se pretender que as ações da regra de rede se reflitam no relatório, selecione a caixa de verificação **Registar eventos**.
9. Clique em **Guardar**.

   A nova regra de rede será adicionada à lista.
10. Utilize os botões **Para cima**/**Para baixo** para definir a prioridade da regra de rede.
11. Guarde as suas alterações.

Como utilizar as definições da Firewall para criar uma regra de rede de aplicações na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Firewall**.
3. Clique em **Regras de aplicações**.

   Esta ação abre a lista das regras de rede predefinidas definidas pela Firewall.

4. Na lista de aplicações, selecione a aplicação ou o grupo de aplicações para as quais pretende criar uma regra de rede.

5. Clique com o botão direito do rato para abrir o menu de contexto e selecione **Detalhes e regras**.

   Abre-se a janela de regras e propriedades da aplicação.

6. Selecione o separador **Regras de rede**.

7. Clique em **Adicionar**.

   Esta ação abre as propriedades da regra de rede.

8. Introduza manualmente o nome do serviço de rede no campo **Nome**.

9. Configure as definições da regra de rede (consulte a tabela abaixo).

   Pode selecionar um modelo de regra predefinido ao clicar na ligação **Modelo de regra de rede**. Os modelos de regras descrevem as ligações de rede usadas com mais frequência.

   Todas as definições de regras de rede são preenchidas automaticamente.

10. Se pretender que as ações da regra de rede se reflitam no relatório, selecione a caixa de verificação **Registar eventos**.

11. Clique em **Guardar**.

    A nova regra de rede será adicionada à lista.

12. Utilize os botões **Para cima**/**Para baixo** para definir a prioridade da regra de rede.

13. Guarde as suas alterações.

Como criar uma regra de rede de aplicações na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Proteção essencial contra ameaças** → **Firewall**.

4. No bloco **Definições da firewall**, clique no botão **Definições**.

   Esta ação abre a lista das regras de pacotes de rede e a lista das regras de rede da aplicação.

5. Aceda ao separador **Regras de rede de aplicações**.

6. Clique em **Adicionar**.

7. Na janela que abre, introduza os critérios de pesquisa da aplicação para a qual pretende criar uma regra de rede.

   Pode introduzir o nome da aplicação ou do fornecedor. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.

8. Clique em **Atualizar**.

   O Kaspersky Endpoint Security pesquisa a aplicação na lista consolidada de aplicações instaladas nos computadores geridos. O Kaspersky Endpoint Security apresenta uma lista de aplicações que satisfazem os seus critérios de pesquisa.

9. Selecione a aplicação necessária.

10. Na lista suspensa **Adicionar a aplicação selecionada ao grupo fiável**, selecione **Grupos predefinidos** e clique em **Ok**.

    A aplicação será adicionada ao grupo predefinido.

11. Selecione a aplicação relevante e, em seguida, selecione **Direitos de aplicações** no menu de contexto da aplicação.

    Abre-se a janela de regras e propriedades da aplicação.

12. Selecione o separador **Regras de rede**.

    Esta ação abre a lista das regras de rede predefinidas definidas pela Firewall.

13. Clique em **Adicionar**.

    Esta ação abre as propriedades da regra de rede.

14. Introduza manualmente o nome do serviço de rede no campo **Nome**.

15. Configure as definições da regra de rede (consulte a tabela abaixo).

    Pode selecionar um modelo de regra predefinido ao clicar no botão . Os modelos de regras descrevem as ligações de rede usadas com mais frequência.

    Todas as definições de regras de rede são preenchidas automaticamente.

16. Se pretender que as ações da regra de rede se reflitam no relatório, selecione a caixa de verificação **Registar eventos**.

17. Guardar a nova regra de rede.

18. Utilize os botões **Para cima**/**Para baixo** para definir a prioridade da regra de rede.

19. Guarde as suas alterações.

Como criar uma regra de rede de aplicações na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Selecione **Communication & Web Protection** → **Firewall**.

5. No bloco **Application rights and protected resources**, clique na ligação **Application rights**.

   Esta ação abre a janela de configuração dos direitos de aplicações e a lista de recursos protegidos.

6. Aceda ao separador **Application rights**.

   Uma lista de grupos fiáveis será apresentada no lado esquerdo da janela e as respetivas propriedades serão apresentadas no lado direito.

7. No bloco **Applications**, clique no botão **Add**.

   É iniciado o Assistente para adicionar uma aplicação a um grupo fiável.

8. Selecione o grupo fiável relevante para a aplicação.

9. Selecione o tipo de **Application**. Avance para o passo seguinte.

   Se pretender criar uma regra de rede para várias aplicações, selecione o tipo de **Group** e defina um nome para o grupo de aplicações.

10. Na lista aberta de aplicações, selecione as aplicações para as quais pretende criar uma regra de rede.

    Utilize um filtro. Pode introduzir o nome da aplicação ou do fornecedor. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.

11. Conclua o assistente.

    A aplicação será adicionada ao grupo fiável.

12. Na parte esquerda da janela, selecione a aplicação relevante.

13. Na parte direita da janela, selecione **Network rules** na lista suspensa.

    Esta ação abre a lista das regras de rede predefinidas definidas pela Firewall.

14. Clique em **Add**.

    Esta ação abre as propriedades da regra de aplicações.

15. Introduza manualmente o nome do serviço de rede no campo **Rule name**.

16. Configure as definições da regra de rede (consulte a tabela abaixo).

    Pode selecionar um modelo de regra predefinido ao clicar na ligação **Select rule template**. Os modelos de regras descrevem as ligações de rede usadas com mais frequência.

    Todas as definições de regras de rede são preenchidas automaticamente.

17. Se pretender que as ações da regra de rede se reflitam no relatório, selecione a caixa de verificação **Log events**.

18. Guardar a regra de rede.

    A nova regra de rede será adicionada à lista.

19. Utilize o botão **Move** para definir a prioridade da regra de rede.

20. Guarde as suas alterações.

Definições da regra de rede de aplicações

Parâmetro	Descrição
Ação	**Permitir**. **Bloquear**.
Protocolo	Controle a atividade de rede executada através do protocolo selecionado: TCP, UDP, ICMP, ICMPv6, IGMP e GRE. Se ICMP ou ICMPv6 estiver selecionado como protocolo, pode definir o código e o tipo de pacote ICMP. Se TCP ou UDP estiver selecionado como o tipo de protocolo, pode especificar os números de porta dos computadores locais e remotos entre os quais a ligação deve ser monitorizada. Intervalo de valores possíveis para os números de porta: 0–65535. Em cada campo, pode inserir vários valores separados por `,` ou especificar um intervalo de valores utilizando `-`. Por exemplo: • `100,101` • `100-130` • `100,110-130`
Direção	**Entrada**. **Entrada/Saída**. **Saída**.

Parâmetro	Descrição
Endereços remotos	Endereços de rede de computadores remotos que podem enviar e/ou receber pacotes de rede. A Firewall aplica a regra de rede ao intervalo especificado de endereços de rede remotos. Pode incluir todos os endereços IP numa regra de rede, criar uma lista separada de endereços IP, especificar um intervalo de endereços IP ou selecionar uma sub-rede (redes fiáveis, redes locais, redes públicas). Também pode especificar um nome DNS de um computador em vez do seu endereço IP. Apenas deve usar nomes DNS para computadores da rede local ou serviços internos. A interação com os serviços em nuvem (como Microsoft Azure) e outros recursos da Internet deve ser tratada pelo componente Controlo de Internet. Se na regra de pacote de rede adicionou um nome DNS para o qual não seja possível determinar o endereço IP, o Kaspersky Endpoint Security apresentará um aviso. Na lista de regras de pacote de rede na Consola Web, é adicionada uma coluna com uma descrição do erro. Na Administration Console (MMC), a descrição do erro não está disponível. Estas regras de pacotes são realçadas a cores.
Endereços locais	Endereços de rede de computadores que podem enviar e receber pacotes de rede. A Firewall aplica uma regra de rede ao intervalo especificado de endereços de rede locais. Pode incluir todos os endereços IP numa regra de rede, criar uma lista separada de endereços IP ou especificar um intervalo de endereços IP. A aplicação armazena endereços locais apenas se for especificada uma lista de endereços remotos. Ou seja, foi selecionado o valor **Endereços da lista** para **Endereços remotos** e foi adicionado, pelo menos, um endereço. Por vezes, o endereço local não pode ser obtido para aplicações. Se for este o caso, este parâmetro é ignorado.

Ativar e desativar uma regra de rede de aplicações

Para ativar ou desativar uma regra de rede de aplicações:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Firewall**.
3. Clique em **Regras de aplicações**.

   Abre-se a lista de regras de aplicações.
4. Na lista de aplicações, selecione a aplicação ou o grupo de aplicações para os quais pretende criar ou editar uma regra de rede.
5. Clique com o botão direito do rato para abrir o menu de contexto e selecione **Detalhes e regras**.

   Abre-se a janela de regras e propriedades da aplicação.
6. Selecione o separador **Regras de rede**.
7. Na lista de regras de rede para um grupo de aplicações, selecione a regra de rede relevante.

   Abre-se a janela de propriedades da regra de rede.
8. Defina o estado **Ativo** ou **Inativo** da regra de rede.

   Não é possível desativar uma regra de rede de grupos de aplicações que seja criada, por predefinição, pela Firewall.
9. Guarde as suas alterações.

Alterar a ação da Firewall para uma regra de rede de aplicações

Pode alterar a ação da Firewall aplicada a todas as regras de rede para uma aplicação ou grupo de aplicações criadas por predefinição e alterar a ação da Firewall para uma única regra de rede personalizada para uma aplicação ou grupo de aplicações.

Para alterar a ação da Firewall para todas as regras de rede para uma aplicação ou grupo de aplicações:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Firewall**.
3. Clique em **Regras de aplicações**.

   Abre-se a lista de regras de aplicações.
4. Se pretender alterar a ação da Firewall aplicada a todas as regras de rede que criadas por predefinição, selecione uma aplicação ou grupo de aplicações na lista. As regras de rede criadas manualmente permanecem inalteradas.
5. Clique com o botão direito para abrir o menu de contexto, selecione **Regras de rede** e depois selecione a ação que quer atribuir:
   - **Herdar**.
   - **Permitir**.
   - **Bloquear**.
6. Guarde as suas alterações.

Para alterar a resposta da Firewall para uma regra de rede, para uma aplicação ou grupo de aplicações:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Firewall**.
3. Clique em **Regras de aplicações**.

   Abre-se a lista de regras de aplicações.
4. Na lista, selecione a aplicação ou o grupo de aplicações para os quais pretende alterar a ação para uma regra de rede.
5. Clique com o botão direito do rato para abrir o menu de contexto e selecione **Detalhes e regras**.

   Abre-se a janela de regras e propriedades da aplicação.
6. Selecione o separador **Regras de rede**.
7. Selecione a regra de rede para a qual pretende alterar a ação da Firewall.

8. Na coluna **Permissão**, clique com o botão direito do rato para visualizar o menu de contexto e selecione a ação que pretende atribuir:
   - **Herdar**.
   - **Permitir**.
   - **Recusar**.
   - **Registar eventos**.
9. Guarde as suas alterações.

Alterar a prioridade de uma regra de rede de aplicações

A prioridade de uma regra de rede é determinada pela respetiva posição na lista de regras de rede. A Firewall executa regras pela ordem na qual são apresentadas na lista de regras de rede, de forma descendente. De acordo com cada regra de rede processada aplicável a uma determinada ligação de rede, a Firewall permite ou bloqueia o acesso da rede ao endereço e porta indicados nas definições desta ligação de rede.

As regras de rede criadas manualmente têm uma prioridade mais alta do que as regras de rede predefinidas.

Não pode alterar a prioridade das regras de rede do grupo de aplicações criadas por predefinição.

Para alterar a prioridade de uma regra de rede de aplicações:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção essencial contra ameaças → Firewall**.
3. Clique em **Regras de aplicações**.
   Abre-se a lista de regras de aplicações.
4. Na lista de aplicações, selecione a aplicação ou o grupo de aplicações para os quais pretende alterar a prioridade de uma regra de rede.
5. Clique com o botão direito do rato para abrir o menu de contexto e selecione **Detalhes e regras**.
   Abre-se a janela de regras e propriedades da aplicação.
6. Selecione o separador **Regras de rede**.
7. Selecione a regra de rede cuja prioridade pretende editar.
8. Utilize os botões **Para cima**/**Para baixo** para definir a prioridade da regra de rede.
9. Guarde as suas alterações.

Monitor de Rede

O *Monitor de rede* é uma ferramenta concebida para visualizar informações sobre a atividade de rede do computador de um utilizador em tempo real.

Para iniciar o Monitor de Rede:

Na janela principal da aplicação, na secção **Monitorização**, clique em **Monitor de Rede**.

A janela Monitor de Rede abre-se. Nesta janela, as informações sobre a atividade de rede do computador são apresentadas em quatro separadores:

- O separador **Atividade de rede** apresenta todas as ligações de rede ativas atualmente com o computador. São apresentadas as ligações de rede de entrada e de saída. Neste separador, pode também criar regras de pacotes de rede para a operação da Firewall.
- O separador **Portas abertas** indica todas as portas de rede abertas do computador. Neste separador, pode também criar regras de pacotes de rede e regras de aplicações para a operação da Firewall.
- O separador **Tráfego de rede** indica o volume de tráfego de rede de entrada e de saída entre o computador do utilizador e os outros computadores na rede aos quais o utilizador está atualmente ligado.
- O separador **Computadores bloqueados** indica os endereços IP dos computadores remotos cuja atividade de rede foi bloqueada pelo componente Proteção contra ameaças de Rede, após detetar tentativas de ataque de rede provenientes desses endereços IP.

Prevenção de explorações

O componente Prevenção de explorações deteta o código de programa que aproveita vulnerabilidades no computador para explorar privilégios de administrador ou realizar atividades maliciosas. Por exemplo, as explorações podem utilizar um ataque de capacidade da memória intermédia excedida. Para tal, a exploração envia uma grande quantidade de dados para uma aplicação vulnerável. Ao processar estes dados, a aplicação vulnerável executa código malicioso. Como resultado deste ataque, a exploração pode iniciar uma instalação não autorizada de software malicioso. Ao detetar que uma tentativa para executar um ficheiro executável a partir de uma aplicação vulnerável não foi executada pelo utilizador, o Kaspersky Endpoint Security bloqueia a execução desse ficheiro ou notifica o utilizador.

O componente Prevenção de explorações também monitoriza portas de rede em busca de processos de aplicações que podem ameaçar a segurança do computador. A aplicação obtém informações sobre tais processos com bases de dados de antivírus.

Ativar e desativar a prevenção de explorações

Por predefinição, a Prevenção de explorações está ativada e funciona no modo otimizado. O Kaspersky Endpoint Security monitoriza os ficheiros executáveis que são executados por aplicações vulneráveis. Se o Kaspersky Endpoint Security detetar que um ficheiro executável de uma aplicação vulnerável foi executado por outro elemento que não o utilizador, o Kaspersky Endpoint Security executará a ação selecionada (por exemplo, bloqueia a operação).

Como ativar ou desativar a Prevenção de explorações na Administration Console (MMC)

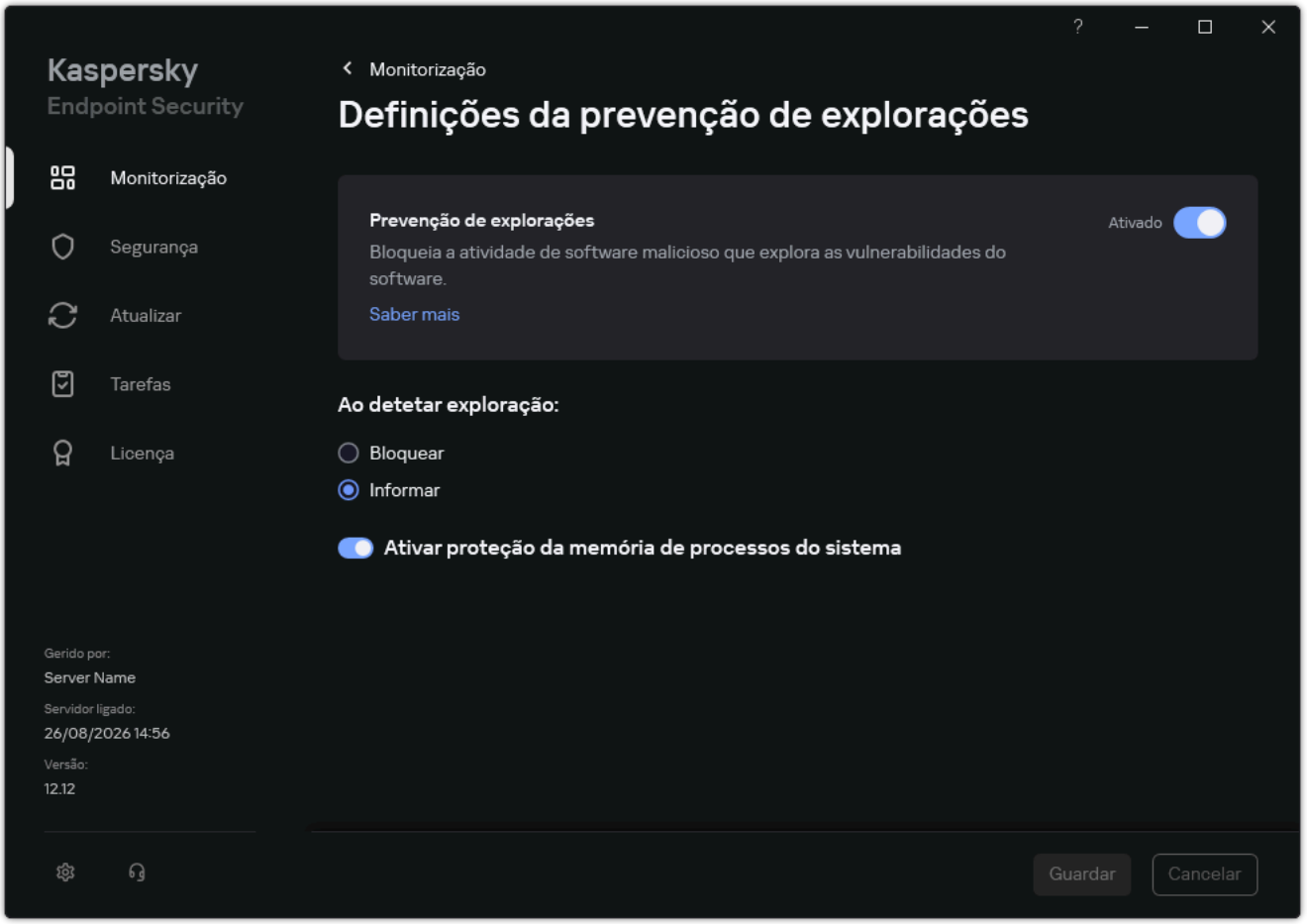
1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção avançada contra ameaças** → **Prevenção de explorações**.
4. Use a caixa de verificação **Prevenção de explorações** para ativar ou desativar o componente.
5. Selecione a ação relevante no bloco **Ao detetar exploração**:
   - **Bloquear**. Se este item for selecionado, ao detetar uma exploração, o Kaspersky Endpoint Security bloqueia as operações desta exploração e cria uma entrada no registo com informação sobre a exploração.
   - **Informar**. Se este item for selecionado, o Kaspersky Endpoint Security, ao detetar uma exploração, cria uma entrada no registo com informação sobre a exploração e adiciona informação sobre esta à lista de ameaças ativas.
6. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar ou desativar a Prevenção de explorações na Web Console e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **Behavior Analysis** → **Exploit Prevention**.
5. Use o botão de alternar da **Exploit Prevention** para ativar ou desativar o componente.
6. Selecione a ação relevante no bloco **Action on threat detection**:
   - **Block**. Se este item for selecionado, ao detetar uma exploração, o Kaspersky Endpoint Security bloqueia as operações desta exploração e cria uma entrada no registo com informação sobre a exploração.
   - **Inform**. Se este item for selecionado, o Kaspersky Endpoint Security, ao detetar uma exploração, cria uma entrada no registo com informação sobre a exploração e adiciona informação sobre esta à lista de ameaças ativas.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar ou desativar a Prevenção de explorações na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção avançada contra ameaças → Prevenção de explorações**.



Definições da Prevenção de explorações

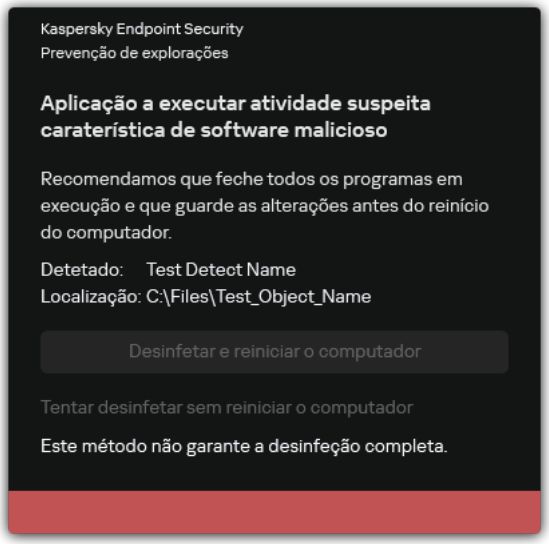
3. Use o botão de alternar da **Prevenção de explorações** para ativar ou desativar o componente.

4. Selecione a ação relevante no bloco **Ao detetar exploração**:

   - **Bloquear**. Se este item for selecionado, ao detetar uma exploração, o Kaspersky Endpoint Security bloqueia as operações desta exploração e cria uma entrada no registo com informação sobre a exploração.

   - **Informar**. Se este item for selecionado, o Kaspersky Endpoint Security, ao detetar uma exploração, cria uma entrada no registo com informação sobre a exploração e adiciona informação sobre esta à lista de ameaças ativas.

5. Guarde as suas alterações.



Notificação sobre ameaça ativa

Proteção da memória de processos do sistema

Por predefinição, 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 o componente proteção da memória de processos do sistema na Administration Console (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Proteção avançada contra ameaças → Prevenção de explorações**.

4. Use a caixa de verificação **Ativar proteção da memória de processos do sistema** para ativar ou desativar a opção.

5. Guarde as suas alterações.

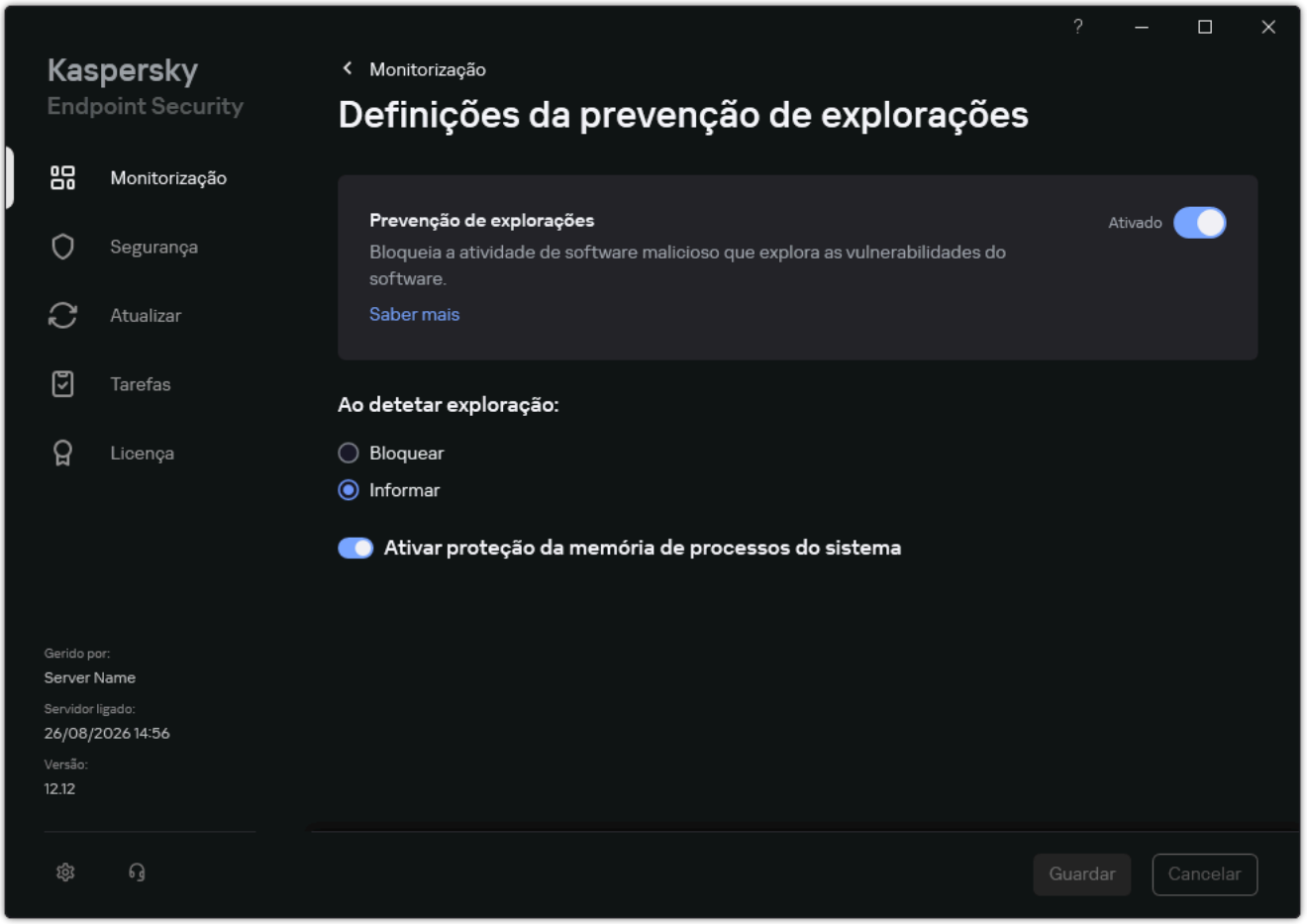
Como ativar ou desativar a proteção da memória de processos do sistema na Web Console e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **Behavior Analysis** → **Exploit Prevention**.
5. Use o botão de alternar **System process memory protection ENABLED** para ativar ou desativar esta funcionalidade.
6. Guarde as suas alterações.

Como ativar ou desativar a proteção da memória de processos do sistema na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Prevenção de explorações**.



Definições da Prevenção de explorações

3. Use o botão de alternar **Ativar proteção da memória de processos do sistema** para ativar ou desativar esta funcionalidade.
4. Guarde as suas alterações.

Deteção de comportamento

O componente Deteção de comportamento recebe dados sobre as ações das aplicações no computador e transmite essas informações para outros componentes de proteção, de modo a melhorar o respetivo desempenho. O componente Deteção de comportamento utiliza Assinaturas de Fluxos de Comportamento (BSS) para aplicações. Se a atividade das aplicações corresponder uma assinatura de fluxo de comportamento, o Kaspersky Endpoint Security irá executar a ação de resposta selecionada. A funcionalidade do Kaspersky Endpoint Security é baseado em assinaturas de fluxos de comportamento e proporciona defesa proativa ao computador.

O componente Deteção de comportamento também monitoriza portas de rede em busca de processos de aplicações que podem ameaçar a segurança do computador. A aplicação obtém informações sobre tais processos com bases de dados de antivírus.

Por predefinição, a Deteção de comportamento está ativada e é executada no modo recomendado pelos especialistas da Kaspersky. Quando uma atividade maliciosa é detetada, o Kaspersky Endpoint Security elimina o ficheiro executável da aplicação maliciosa.

Não é recomendado desativar a Deteção de comportamento exceto quando absolutamente necessário, uma vez que reduz a eficácia dos componentes de proteção. Os componentes de proteção podem solicitar dados recolhidos pelo componente Deteção de comportamento para detetar ameaças.

Como ativar ou desativar a Deteção de Comportamento na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Proteção avançada contra ameaças** → **Deteção de comportamento**.
5. Use a caixa de verificação **Deteção de comportamento** para ativar ou desativar o componente.
6. Selecione a ação relevante no bloco **Ação ao detetar atividade de malware**:
   - **Eliminar**. Se este item estiver selecionado, ao detetar atividade maliciosa, o Kaspersky Endpoint Security elimina o ficheiro executável da aplicação maliciosa e cria uma cópia de segurança do ficheiro na Cópia de segurança.
   - **Bloquear**. Se este item estiver selecionado, ao detetar atividade maliciosa, o Kaspersky Endpoint Security encerra a aplicação em questão.
   - **Informar**. Se este item for selecionado e se for detetada atividade de software malicioso de uma aplicação, o Kaspersky Endpoint Security adiciona informação sobre a atividade do software malicioso da aplicação à lista de ameaças ativas.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar ou desativar a Deteção de Comportamento na Consola Web e na Cloud Console

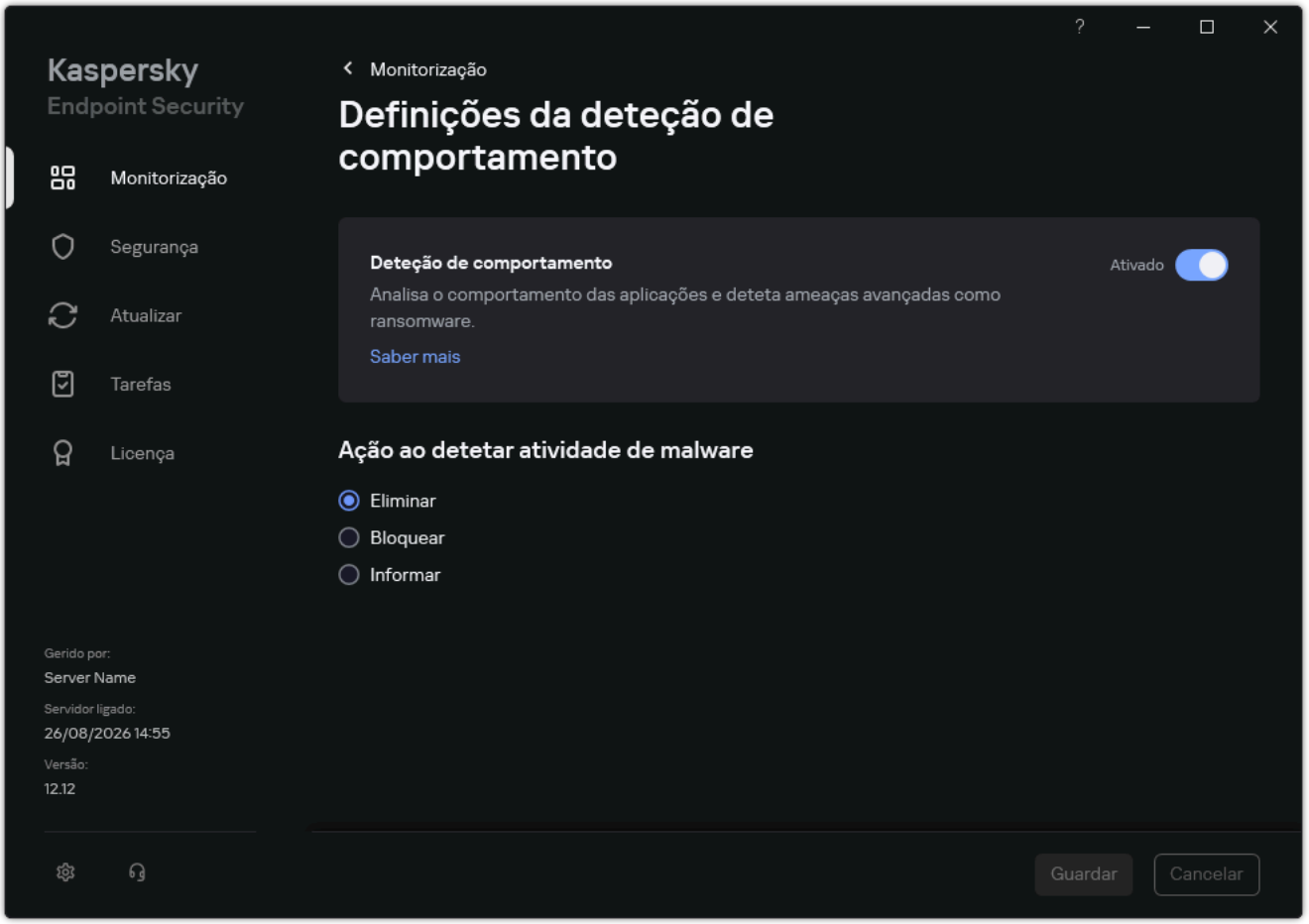
1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **Behavior Analysis** → **Behavior Detection**
5. Use o botão de alternar da **Behavior Detection ENABLED** para ativar ou desativar o componente.
6. Selecione a ação relevante no bloco **Action on threat detection**:

   - **Delete**. Se este item estiver selecionado, ao detetar atividade maliciosa, o Kaspersky Endpoint Security elimina o ficheiro executável da aplicação maliciosa e cria uma cópia de segurança do ficheiro na Cópia de segurança.
   - **Block**. Se este item estiver selecionado, ao detetar atividade maliciosa, o Kaspersky Endpoint Security encerra a aplicação em questão.
   - **Inform**. Se este item for selecionado e se for detetada atividade de software malicioso de uma aplicação, o Kaspersky Endpoint Security adiciona informação sobre a atividade do software malicioso da aplicação à lista de ameaças ativas.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar ou desativar a Deteção de Comportamento na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção avançada contra ameaças → Deteção de comportamento**.



Definições da Deteção de comportamento

3. Use o botão de alternar da **Deteção de comportamento** para ativar ou desativar o componente.
4. Selecione a ação relevante no bloco **Ação ao detetar atividade de malware**:

   - **Eliminar**. Se este item estiver selecionado, ao detetar atividade maliciosa, o Kaspersky Endpoint Security elimina o ficheiro executável da aplicação maliciosa e cria uma cópia de segurança do ficheiro na Cópia de segurança.
   - **Bloquear**. Se este item estiver selecionado, ao detetar atividade maliciosa, o Kaspersky Endpoint Security encerra a aplicação em questão.
   - **Informar**. Se este item for selecionado e se for detetada atividade de software malicioso de uma aplicação, o Kaspersky Endpoint Security adiciona informação sobre a atividade do software malicioso da aplicação à lista de ameaças ativas.

5. Guarde as suas alterações.

Como resultado, se a Deteção de Comportamento estiver ativada, o Kaspersky Endpoint Security utilizará assinaturas de fluxo de comportamento para analisar a atividade das aplicações no sistema operativo.

Anti-Cryptor

A partir do Kaspersky Endpoint Security 12.12 para Windows, a proteção de pastas partilhadas contra encriptação externa, que antes fazia parte do componente Deteção de Comportamento, passou a ser um componente separado, o Anti-Cryptor.

O componente monitoriza as operações realizadas apenas com os ficheiros armazenados em dispositivos de armazenamento em massa com o sistema de ficheiros NTFS e não encriptados com EFS.

O componente Anti-Cryptor analisa a atividade em pastas partilhadas. Se esta atividade corresponder a uma assinatura de fluxo de comportamento que seja comum para encriptação externa, o Kaspersky Endpoint Security executa a ação selecionada.

Para que o componente Anti-Cryptor funcione, tem de ativar o componente Deteção de comportamento.

Se o Kaspersky Endpoint Security detetar uma tentativa de modificação dos ficheiros nas pastas partilhadas, realiza as seguintes ações:

- Bloqueia o acesso à modificação de ficheiros para a sessão que iniciou a atividade maliciosa (o ficheiro será apenas de leitura).
- Cria cópias de segurança dos ficheiros que estão a ser modificados.
- Adiciona uma entrada aos relatórios de interface da aplicação local e envia informações sobre a atividade maliciosa detetada para o Kaspersky Security Center.
- De igual modo, se o componente Motor de remediação está ativado, o Kaspersky Endpoint Security restaura os ficheiros modificados a partir das cópias de segurança.

Ativar ou desativar a proteção de pastas partilhadas contra encriptação externa

Por padrão, a proteção de pastas partilhadas contra encriptação externa está ativada e a funcionar conforme recomendado pelos especialistas da Kaspersky. Para configurar esta funcionalidade, pode criar um âmbito de proteção e configurar exclusões, se necessário. Por padrão, a aplicação identifica automaticamente pastas partilhadas e monitoriza a atividade de ficheiros em todas as pastas. Quando uma tentativa de encriptar ficheiros externamente em pastas partilhadas é detetada, o Kaspersky Endpoint Security bloqueia a sessão do utilizador remoto por uma hora (por padrão).

Após a instalação do Kaspersky Endpoint Security, a proteção de pastas partilhadas contra encriptação externa estará limitada até o computador ser reiniciado.

Como ativar ou desativar a proteção de pastas partilhadas contra encriptação externa na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção avançada contra ameaças** → **Anti-Cryptor**.
4. Use a caixa de verificação **Anti-Cryptor** para ativar ou desativar a deteção de atividade típica da encriptação externa.
5. Selecione a ação relevante que a aplicação irá tomar quando uma tentativa de modificar ficheiros em pastas partilhadas for detetada:
   - **Bloquear ligação durante N min**. Se esta opção for selecionada, quando o Kaspersky Endpoint Security detetar uma tentativa de modificar ficheiros em pastas partilhadas, ele irá bloquear o acesso à modificação do ficheiro para a sessão que iniciou a atividade maliciosa e irá criar cópias de segurança dos ficheiros modificados.

     Se o componente Motor de remediação for ativado e a opção **Bloquear ligação durante N minutos** for selecionada, os ficheiros modificados são restaurados de cópias de segurança.

   - **Informar**. Se esta opção for selecionada, ao detetar uma tentativa de modificar ficheiros em pastas partilhadas, o Kaspersky Endpoint Security adiciona informações sobre esta tentativa à lista de ameaças ativas, adiciona uma entrada a relatórios de interface de aplicação local e envia informações sobre a atividade maliciosa detetada ao Kaspersky Security Center.
6. Se necessário, edite um âmbito de proteção e defina exclusões.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar ou desativar a proteção de pastas partilhadas contra encriptação externa na consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. Use o botão de alternar **Anti-Cryptor ENABLED** para ativar ou desativar a deteção de atividade típica da encriptação externa.

6. Selecione a ação relevante que a aplicação irá tomar quando uma tentativa de modificar ficheiros em pastas partilhadas for detetada:

   - **Block connection for (min) N min**. Se esta opção for selecionada, quando o Kaspersky Endpoint Security detetar uma tentativa de modificar ficheiros em pastas partilhadas, ele irá bloquear o acesso à modificação do ficheiro para a sessão que iniciou a atividade maliciosa e irá criar cópias de segurança dos ficheiros modificados.

     Se o componente Motor de remediação for ativado e a opção **Block connection for (min) N minutos** for selecionada, os ficheiros modificados são restaurados de cópias de segurança.

   - **Inform**. Se esta opção for selecionada, ao detetar uma tentativa de modificar ficheiros em pastas partilhadas, o Kaspersky Endpoint Security adiciona informações sobre esta tentativa à lista de ameaças ativas, adiciona uma entrada a relatórios de interface de aplicação local e envia informações sobre a atividade maliciosa detetada ao Kaspersky Security Center.

7. Se necessário, edite um âmbito de proteção e defina exclusões.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar ou desativar a proteção de pastas partilhadas contra a gestão externa na interface da aplicação

1. Na janela principal da aplicação, clique no botão .

2. Na janela Application settings, selecione **Proteção avançada contra ameaças → Anti-Cryptor**.

3. Use a caixa de verificação **Proteção de pastas partilhadas contra encriptação externa** para ativar ou desativar a deteção de atividade típica da encriptação externa.

4. Use a caixa de verificação **Proteção de pastas partilhadas contra encriptação externa** para ativar ou desativar a deteção de atividade típica da encriptação externa.

5. Selecione a ação relevante que a aplicação irá tomar quando uma tentativa de modificar ficheiros em pastas partilhadas for detetada:

   - **Bloquear ligação durante (min) N min**. Se esta opção for selecionada, quando o Kaspersky Endpoint Security detetar uma tentativa de modificar ficheiros em pastas partilhadas, ele irá bloquear o acesso à modificação do ficheiro para a sessão que iniciou a atividade maliciosa e irá criar cópias de segurança dos ficheiros modificados.

     Se o componente Motor de remediação for ativado e a opção **Bloquear ligação durante (min) N minutos** for selecionada, os ficheiros modificados são restaurados de cópias de segurança.

   - **Informar**. Se esta opção for selecionada, ao detetar uma tentativa de modificar ficheiros em pastas partilhadas, o Kaspersky Endpoint Security adiciona informações sobre esta tentativa à lista de ameaças ativas, adiciona uma entrada a relatórios de interface de aplicação local e envia informações sobre a atividade maliciosa detetada ao Kaspersky Security Center.

6. Se necessário, edite um âmbito de proteção e defina exclusões.

7. Guarde as suas alterações.

Configurar o período de bloqueio de um computador não fiável

Um *computador não fiável* é um computador remoto que está envolvido em atividades maliciosas ou encriptação de dados. Por predefinição, o Kaspersky Endpoint Security bloqueia a sessão do utilizador remoto durante 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 partilhada.

Como configurar o período de bloqueio de um computador não fiável na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção avançada contra ameaças → Anti-Cryptor**.
4. No bloco **Ação após deteção de ameaças**, selecione **Bloquear ligação durante N min**.
5. Configure o período de bloqueio de um computador não fiável que esteja envolvido em atividades maliciosas ou encriptação de dados.
6. Guarde as suas alterações.

Como configurar o período de bloqueio de um computador não fiável na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection → Behavior Analysis → Anti-Cryptor**.
5. Em **Action on threat detection**, configure o período de bloqueio de um computador não fiável que esteja envolvido em atividades maliciosas ou encriptação de dados.
6. Guarde as suas alterações.

Como configurar o período de bloqueio de um computador não fiável na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção avançada contra ameaças → Anti-Cryptor**.
3. No bloco **Ação após deteção de ameaças**, selecione **Bloquear ligação durante (min)**.
4. Configure o período de bloqueio de um computador não fiável que esteja envolvido em atividades maliciosas ou encriptação de dados.
5. Guarde as suas alterações.

Como resultado, o computador remoto será bloqueado. Para desbloquear o computador remoto, pode reiniciar o Kaspersky Endpoint Security.

Editar o âmbito da proteção

O *âmbito de proteção* é uma lista de caminhos para pastas partilhadas nas quais o Kaspersky Endpoint Security monitoriza a atividade de ficheiros. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara. Por padrão, a aplicação identifica automaticamente pastas partilhadas e monitoriza a atividade de ficheiros em todas as pastas.

A exclusão de uma pasta de um âmbito de proteção pode reduzir a quantidade de falsos positivos se a sua organização utilizar encriptação de dados ao trocar ficheiros utilizando pastas partilhadas. Por exemplo, a Deteção de comportamento pode levantar falsos positivos quando o utilizador trabalha com ficheiros com a extensão ENC numa pasta partilhada. Essa atividade corresponde a um padrão de comportamento típico da encriptação externa. Se tiver ficheiros encriptados numa pasta partilhada para proteger dados, adicione essa pasta às exclusões.

Também pode excluir computadores dos quais tentativas de encriptação externa não podem ser manipuladas.

Como editar um âmbito de proteção na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção avançada contra ameaças** → **Anti-Cryptor**.
4. No bloco **Âmbito de Proteção**, selecione **Apenas as pastas partilhadas especificadas**.
5. Na lista de pastas, clique em **Adicionar**.
6. Esta ação abre uma janela; nessa janela, insira o caminho para a pasta partilhada que deseja incluir no âmbito de proteção (por exemplo, `C:\Share`).

   Para adicionar uma pasta partilhada ao âmbito de proteção, use um caminho local.

7. Clique em **OK**.
8. Se necessário, defina exclusões do âmbito de proteção:

   a. No bloco **Exclusões de verificação**, clique no botão **Por máscara**.

   b. Na janela que abre, clique no botão **Adicionar**.

   c. Na janela apresentada, especifique uma extensão de ficheiro no formato `*.<file extension>` ou um caminho da pasta. O Kaspersky Endpoint Security suporta os caracteres `*` e `?` ao introduzir uma máscara.

   A aplicação não suporta algumas extensões de ficheiros de exclusão. Desta forma, pode especificar uma exclusão como `*.docx` ou `**\Folder\**`.

   Pode excluir um objeto das verificações sem o remover da lista de objetos no âmbito de proteção. Para o fazer, desmarque a caixa de verificação ao lado do objeto.

9. Guarde as suas alterações.

Como editar o âmbito de proteção na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. No bloco **Protection scope**, selecione **Only specified shared folders**.
6. Na lista de pastas, clique em **Add**.
7. Esta ação abre uma janela; nessa janela, insira o caminho para a pasta partilhada que deseja incluir no âmbito de proteção (por exemplo, `C:\Share`).

   > Para adicionar uma pasta partilhada ao âmbito de proteção, use um caminho local.
8. Clique em **OK**.
9. Se necessário, defina exclusões do âmbito de proteção:

   a. Na parte superior da janela, clique na ligação **Scan exclusions**.

   b. Na janela que abre, clique no botão **Add**.

   c. Na janela apresentada, especifique uma extensão de ficheiro no formato `*.<file extension>` ou um caminho da pasta. O Kaspersky Endpoint Security suporta os caracteres `*` e `?` ao introduzir uma máscara.

   A aplicação não suporta algumas extensões de ficheiros de exclusão. Desta forma, pode especificar uma exclusão como `*.docx` ou `**\Folder\**`.

   Pode excluir um objeto das verificações sem o remover da lista de objetos no âmbito de proteção. Para o fazer, desmarque a caixa de verificação ao lado do objeto.
10. Guarde as suas alterações.

Como editar o âmbito de proteção na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Anti-Cryptor**.
3. No bloco **Âmbito de proteção**, selecione **Apenas as pastas partilhadas especificadas**.
4. Na lista de pastas, clique em **Adicionar**.
5. Esta ação abre uma janela; nessa janela, insira o caminho para a pasta partilhada que deseja incluir no âmbito de proteção (por exemplo, `C:\Share`).

   > Para adicionar uma pasta partilhada ao âmbito de proteção, use um caminho local.

6. Clique em **OK**.

7. Se necessário, defina exclusões do âmbito de proteção:

   a. Na parte superior da janela, clique na ligação **Exclusões por máscara**.

   b. Na janela que abre, clique no botão **Adicionar**.

   c. Na janela apresentada, especifique uma extensão de ficheiro no formato `*.<file extension>` ou um caminho da pasta. O Kaspersky Endpoint Security suporta os caracteres `*` e `?` ao introduzir uma máscara.

      A aplicação não suporta algumas extensões de ficheiros de exclusão. Desta forma, pode especificar uma exclusão como `*.docx` ou `**\Folder\**`.

   Pode excluir um objeto das verificações sem o remover da lista de objetos no âmbito de proteção. Para o fazer, desmarque a caixa de verificação ao lado do objeto.

8. Guarde as suas alterações.

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Definições gerais → Exclusões e tipos de objetos detetados**.

3. No bloco **Exclusões**, clique na ligação **Gerir exclusões**.

4. Clique em **Adicionar**.

5. Clique em **Procurar** e selecione a pasta partilhada.

   Também pode introduzir o caminho manualmente. O Kaspersky Endpoint Security suporta os caracteres `*` e `?` ao introduzir uma máscara:

   - O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.

   - Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

   - O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.

   Pode utilizar máscaras no início, no meio ou no final do caminho do ficheiro. Por exemplo, se quiser adicionar uma pasta para todos os utilizadores às exclusões, introduza a máscara `?:\Users\*\Folder\`.

6. No bloco **Componentes de proteção**, selecione o componente **Deteção de comportamento**.

7. Se necessário, no campo **Comentário**, introduza um breve comentário na exclusão de verificação que está a criar.

8. Selecione o estado **Ativo** para a exclusão.

   Pode usar o botão de alternar para parar uma exclusão a qualquer momento.

9. Guarde as suas alterações.

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda à secção **Trusted Zone**.

5. Na janela que abre, clique na ligação **Malware Scan exclusions**.

6. Selecione a caixa de verificação **Merge values when inheriting** se quiser criar uma lista consolidada de exclusões para todos os computadores da empresa. As listas de exclusões nas políticas principal e subordinadas serão unidas. As listas serão unidas, desde que a união de valores ao herdar esteja ativada. As exclusões da política principal são apresentadas nas políticas subordinadas numa vista apenas de leitura. Não é possível alterar ou eliminar exclusões da política principal.

7. Selecione a caixa de verificação **Allow use of local exclusions** se pretender permitir que o utilizador crie uma lista local de exclusões. Desta forma, um utilizador pode criar a sua própria lista local de exclusões, além da lista geral de exclusões gerada na política. Um administrador pode usar o Kaspersky Security Center para ver, adicionar, editar ou eliminar itens da lista nas propriedades do computador.

   Se a caixa de verificação estiver desmarcada, o utilizador só consegue aceder à lista geral de exclusões gerada na política. Além disso, se esta caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security oculta a lista consolidada de exclusões de verificação na interface de utilizador da aplicação.

8. Clique em **Add** e selecione uma ação:

   - **Category**. Pode agrupar exclusões de verificação em categorias separadas. Para criar uma nova categoria, insira o nome da categoria e adicione, pelo menos, uma exclusão de verificação à categoria.
   - **New exclusion**. O Kaspersky Endpoint Security adiciona uma nova exclusão de verificação à raiz da lista.
   - **Select exclusion from list**. Para configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e o System Center Configuration Manager, a aplicação inclui *exclusões de verificação predefinidas*. Também foram adicionadas exclusões de verificação predefinidas para suportar a configuração de aplicações em ambientes virtuais Citrix e VMware. Tem de selecionar exclusões de verificação predefinidas dependendo da finalidade do servidor protegido.

9. Selecione como pretende adicionar a exclusão: **Path to the file or folder**.

10. Introduza o caminho para a pasta partilhada.

Também pode introduzir o caminho manualmente. O Kaspersky Endpoint Security suporta os caracteres `*` e `?` ao introduzir uma máscara:

- O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.

- Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

- O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.

Pode utilizar máscaras no início, no meio ou no final do caminho do ficheiro. Por exemplo, se quiser adicionar uma pasta para todos os utilizadores às exclusões, introduza a máscara `C:\Users\*\Folder\`.

11. No bloco **Apply exclusion to**, selecione o componente **Behavior Detection**.

12. Se necessário, no campo **Comment**, introduza um breve comentário na exclusão de verificação que está a criar.

13. Selecione o estado **Add to exclusions** para a exclusão.

    Pode usar o botão de alternar para parar uma exclusão a qualquer momento.

14. Guarde as suas alterações.

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Definições gerais → Exclusões e tipos de objetos**.

4. No bloco **Analisar exclusões e aplicações fiáveis → Exclusões de verificação**, clique no botão **Definições**.

   Abre-se uma janela que contém uma lista de exclusões.

5. Selecione a caixa de verificação **Unir valores ao herdar** se quiser criar uma lista consolidada de exclusões para todos os computadores da empresa. As listas de exclusões nas políticas principal e subordinadas serão unidas. As listas serão unidas, desde que a união de valores ao herdar esteja ativada. As exclusões da política principal são apresentadas nas políticas subordinadas numa vista apenas de leitura. Não é possível alterar ou eliminar exclusões da política principal.

6. Selecione a caixa de verificação **Permitir a utilização de exclusões locais** se pretender permitir que o utilizador crie uma lista local de exclusões. Desta forma, um utilizador pode criar a sua própria lista local de exclusões, além da lista geral de exclusões gerada na política. Um administrador pode usar o Kaspersky Security Center para ver, adicionar, editar ou eliminar itens da lista nas propriedades do computador.

   Se a caixa de verificação estiver desmarcada, o utilizador só consegue aceder à lista geral de exclusões gerada na política. Além disso, se esta caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security oculta a lista consolidada de exclusões de verificação na interface de utilizador da aplicação.

7. Clique em **Adicionar** e selecione uma ação:

   - **Categoria**. Pode agrupar exclusões de verificação em categorias separadas. Para criar uma nova categoria, insira o nome da categoria e adicione, pelo menos, uma exclusão de verificação à categoria.

   - **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 em servidores SQL, servidores Microsoft Exchange e o System Center Configuration Manager, a aplicação inclui *exclusões de verificação predefinidas*. Também foram adicionadas exclusões de verificação predefinidas para suportar a configuração de aplicações em ambientes virtuais Citrix e VMware. Tem de selecionar exclusões de verificação predefinidas dependendo da finalidade do servidor protegido.

8. Clique em **Adicionar**.

9. No bloco **Propriedades**, selecione a caixa de verificação **Ficheiro ou pasta**.

10. Clique na ligação **Selec. ficheiro ou pasta** no bloco **Descrição da exclusão de verificação (clique nos itens sublinhados para editar os mesmos)** para abrir a janela **Nome do ficheiro ou pasta**.

11. Clique em **Procurar** e selecione a pasta partilhada.

    Também pode introduzir o caminho manualmente. O Kaspersky Endpoint Security suporta os caracteres `*` e `?` ao introduzir uma máscara:

    - O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.

    - Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

    - O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.

    Pode utilizar máscaras no início, no meio ou no final do caminho do ficheiro. Por exemplo, se quiser adicionar uma pasta para todos os utilizadores às exclusões, introduza a máscara `?:\Users\*\Folder\`.

12. Se necessário, no campo **Comentário**, introduza um breve comentário na exclusão de verificação que está a criar.

13. Clique no bloco **Descrição da exclusão de verificação (clique nos itens sublinhados para editar os mesmos)** para abrir a janela **Componentes de proteção**.

14. Selecione a caixa de verificação junto ao componente **Deteção de comportamento**.

15. Guarde as suas alterações.

Adicionar computadores fiáveis para encriptação de dados externos

Se a sua organização usa encriptação de dados externos no seu fluxo de trabalho de troca de ficheiros, tem de criar uma lista de computadores fiáveis. O Kaspersky Endpoint Security não monitoriza a encriptação de dados por computadores fiáveis.

O serviço Auditar Início de Sessão tem de estar ativado para ativar as exclusões de endereços da proteção de pastas partilhadas contra encriptação externa. Por predefinição, o serviço Auditar início de sessão está desativado (para informação detalhada sobre o serviço Auditar início de sessão, visite o site da Microsoft).

A funcionalidade de exclusão de endereços da proteção de pastas partilhadas não funciona num computador remoto se este tiver sido ligado antes de o Kaspersky Endpoint Security ter sido iniciado. Pode reiniciar este computador remoto após o Kaspersky Endpoint Security ser iniciado, de modo a garantir que a funcionalidade de exclusão de endereços da proteção de pastas partilhadas funciona neste computador remoto.

Como adicionar um computador fiável para encriptação de dados externos na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Proteção avançada contra ameaças** → **Anti-Cryptor**.
5. No bloco **Exclusões de verificação**, clique no botão **Por nome ou endereço IP**.
6. Na janela que abre, clique no botão **Por nome ou endereço IP**.
7. Introduza os endereços IP, o intervalo de endereços IP ou os nomes dos computadores a partir dos quais as tentativas de encriptação externa não devem ser tratadas.

   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 guarde as suas alterações.

Como adicionar um computador fiável para a encriptação externa de dados na Kaspersky Security Center Web Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda à secção **Trusted Zone**.
5. Na parte direita da janela, clique na ligação **Anti-Cryptor exclusions**.
6. Na janela que abre, clique no botão **Add**.
7. Introduza os endereços IP, o intervalo de endereços IP ou os nomes dos computadores a partir dos quais as tentativas de encriptação externa não devem ser tratadas.

   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 guarde as suas alterações.

Como adicionar um computador fiável para encriptação de dados externos na interface da aplicação

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Anti-Cryptor**.
3. Na parte superior da janela, clique na ligação **Exclusões por nome ou endereço IP**.
4. Na janela que abre, clique no botão **Adicionar**.
5. Introduza os endereços IP, o intervalo de endereços IP ou os nomes dos computadores a partir dos quais as tentativas de encriptação externa não devem ser tratadas.

   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. Guarde as suas alterações.

Exportar e importar uma lista de exclusões da proteção de pastas partilhadas contra encriptação externa

Pode exportar a lista de exclusões para um ficheiro XML. Em seguida, pode modificar o ficheiro para, por exemplo, adicionar um grande número de endereços do mesmo tipo. Também pode utilizar a função de exportação/importação para fazer uma cópia de segurança da lista de exclusões ou para migrar a lista para um servidor diferente.

Como exportar e importar uma lista de exclusões na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção avançada contra ameaças** → **Anti-Cryptor**.
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 pretende exportar. Para selecionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.
      Se não tiver selecionado nenhuma exclusão, o Kaspersky Endpoint Security exportará todas as exclusões.
   b. Selecione o botão → **Exportar**.
   c. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de exclusões e selecione a pasta onde pretende guardar este ficheiro.
   d. Guardar o ficheiro.
      O Kaspersky Endpoint Security exporta toda a lista de exclusões para o ficheiro XML.
6. Para importar a lista de exclusões:
   a. Selecione o botão → **Importar**.
   b. Na janela que se abre, selecione o ficheiro XML do qual deseja importar a lista de exclusões.
   c. Abrir o ficheiro.
      Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security irá solicitar-lhe a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro XML.
7. Guarde as suas alterações.

Como exportar e importar uma lista de exclusões na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. Clique na hiperligação **Exclusions by name or IP address**.
6. Para exportar a lista de regras:

   a. Selecione as exclusões que pretende exportar.

   b. Selecione o botão → **Export**.

   O Kaspersky Endpoint Security exporta a lista de exclusões para um ficheiro JSON na pasta de transferências predefinida.
7. Para importar a lista de exclusões:

   a. Selecione o botão → **Import**.

   Na janela que se abre, selecione o ficheiro JSON do qual deseja importar a lista de exclusões.

   b. Abrir o ficheiro.

   Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security irá solicitar-lhe a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro JSON.
8. Guarde as suas alterações.

Motor de remediação

O componente Motor de remediação permite que o Kaspersky Endpoint Security reverta ações que foram executadas por software malicioso no sistema operativo.

Ao reverter a atividade de software malicioso no sistema operativo, o Kaspersky Endpoint Security controla os seguintes tipos de atividade de software malicioso:

- **Atividade de ficheiros**

  O Kaspersky Endpoint Security executar as seguintes ações:

  - Elimina ficheiros executáveis que foram criados pelo malware (em toda a multimédia exceto unidades de rede).
  - Elimina ficheiros executáveis que foram criados por programas que foram infiltrados por software malicioso.
  - Restaura ficheiros que foram modificados ou eliminados por malware.

  A funcionalidade de recuperação de ficheiros possui um certo número de limitações.

- **Atividade de registo**

  O Kaspersky Endpoint Security executar as seguintes ações:

  - Elimina chaves de registo que foram criadas por malware.
  - Não restaura chaves de registo que foram modificadas ou eliminadas por malware.

- **Atividade de sistema**

  O Kaspersky Endpoint Security executar as seguintes ações:

  - Termina processos que foram iniciados por malware.
  - Termina processos nos quais tenha penetrado uma aplicação maliciosa.
  - Não retoma processos que tenham sido interrompidos por malware.

- **Atividade de rede**

  O Kaspersky Endpoint Security executar as seguintes ações:

  - Bloqueia a atividade da rede de malware.
  - Bloqueia a atividade da rede de processos que foram infiltrados por malware.

A reversão das ações do software malicioso pode ser iniciada pelo componente Proteção contra ameaças de ficheiros ou Deteção de comportamentos, ou durante uma verificação de software malicioso.

A reversão das operações de software malicioso afeta um conjunto de dados estritamente definido. A reversão não tem efeitos adversos no sistema operativo nem na integridade dos dados do seu computador.

Como ativar ou desativar o componente Motor de remediação na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção avançada contra ameaças → Motor de remediação**.
4. Use a caixa de verificação **Motor de remediação** para ativar ou desativar o componente.
5. Guarde as suas alterações.

Como ativar ou desativar o componente Motor de remediação na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Host Threat Protection → Behavior Analysis → Remediation Engine**.
5. Use o botão de alternar da **Remediation Engine ENABLED** para ativar ou desativar o componente.
6. Guarde as suas alterações.

Como ativar ou desativar o componente Motor de remediação na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Motor de remediação**.
3. Use o botão de alternar da **Motor de remediação** para ativar ou desativar o componente.
4. Guarde as suas alterações.

Como resultado, se o Motor de remediação estiver ativado, o Kaspersky Endpoint Security reverterá as ações executadas por aplicações maliciosas no sistema operativo.

Kaspersky Security Network



Para proteger o seu computador de forma mais eficaz, o Kaspersky Endpoint Security utiliza dados recebidos de utilizadores em todo o mundo. A Kaspersky Security Network foi concebida 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 na nuvem que fornece o acesso à Base de Conhecimento online da Kaspersky, que contém informações sobre a reputação de ficheiros, recursos da Internet e software. A utilização de dados da Kaspersky Security Network permite uma resposta mais rápida do Kaspersky Endpoint Security a novas ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos diagnósticos positivos. Se participar na Kaspersky Security Network, os serviços da KSN irão fornecer ao Kaspersky Endpoint Security informações sobre a reputação dos endereços Web verificados, bem como informações sobre a categoria e a reputação dos ficheiros verificados. Para obter mais informações sobre como configurar o acesso ao KSN, consulte a Ajuda do Kaspersky Security Center.

A utilização da Kaspersky Security Network é voluntária. A aplicação solicita que utilize a KSN durante a configuração inicial da aplicação. Os utilizadores podem começar ou interromper a participação na KSN em qualquer momento.

Para obter informações mais detalhadas sobre a informação estatística da Kaspersky gerada durante a participação na KSN e sobre o armazenamento e a destruição de tal, consulte a Declaração de Recolha de Dados da KSN e o site da Kaspersky. O ficheiro ksn_<ID do idioma>.txt com o texto da Declaração de Recolha de Dados da KSN está incluído no kit de distribuição da aplicação.

A infraestrutura das bases de dados de reputação da Kaspersky

O Kaspersky Endpoint Security suporta as seguintes soluções de infraestrutura para trabalhar com as bases de dados de reputação da Kaspersky:

- *Kaspersky Security Network (KSN)* é a solução usada pela maioria das aplicações da Kaspersky. Os participantes na KSN recebem informações da Kaspersky e enviam as informações à Kaspersky sobre os objetos detetados no computador do utilizador para fins de análise adicional pelos analistas da Kaspersky e inclusão nas bases de dados estatísticas e de reputação da Kaspersky Security Network.

- *Kaspersky Private Security Network (KPSN)* é uma solução que permite que utilizadores de computadores que alojam o Kaspersky Endpoint Security ou outras aplicações da Kaspersky tenham acesso às bases de dados de reputação do Kaspersky Security Network e a outros dados estatísticos sem enviar dados para o KSN a partir de seus próprios computadores. O KPSN foi criado para clientes empresariais que não podem participar na Kaspersky Security Network por qualquer um dos seguintes motivos:

  - As estações de trabalho locais não estão ligadas à Internet.

  - A transmissão de quaisquer dados para fora do país ou para fora da LAN empresarial é proibida por lei ou restringida por políticas de segurança empresariais.

Ativar e desativar a utilização da Kaspersky Security Network

Por predefinição, o Kaspersky Endpoint Security usa o modo KSN avançado. *O modo KSN avançado* é um modo no qual o Kaspersky Endpoint Security envia dados adicionais à Kaspersky.

Como ativar ou desativar a Utilização KSN na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Proteção avançada contra ameaças** → **Kaspersky Security Network**.

4. Use o botão de alternar da **Kaspersky Security Network** para ativar ou desativar o componente.

   Se ativou o uso de KSN, o Kaspersky Endpoint Security apresentará a Declaração da Kaspersky Security Network. Leia e aceite os termos da Declaração da Kaspersky Security Network (KSN) se concordar com estes.

5. Se necessário, desmarque a caixa de verificação **Ativar o modo KSN alargado**. Por predefinição, o KSN avançado está ativado.

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

Como ativar ou desativar a Utilização KSN na Web Console e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **General Settings** → **Kaspersky Security Network**.

5. Use o botão de alternar da **Use of Kaspersky Security Network (KSN) ENABLED** para ativar ou desativar o componente.

   Se ativou o uso de KSN, o Kaspersky Endpoint Security apresentará a Declaração da Kaspersky Security Network. Leia e aceite os termos da Declaração da Kaspersky Security Network (KSN) se concordar com estes.

6. Se necessário, desligue o botão de alternar **Use extended KSN mode**. Por predefinição, o KSN avançado está ativado.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar ou desativar a Utilização KSN na interface da aplicação

1. Na janela principal da aplicação, clique no botão .

2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Kaspersky Security Network**.

3. Use o botão de alternar da **Kaspersky Security Network** para ativar ou desativar o componente.

   Se ativou o uso de KSN, o Kaspersky Endpoint Security apresentará a Declaração da Kaspersky Security Network. Leia e aceite os termos da Declaração da Kaspersky Security Network (KSN) se concordar com estes.

4. Se necessário, desligue o botão de alternar **Ativar o modo KSN alargado**. Por predefinição, o KSN avançado está ativado.

5. Guarde as suas alterações.

Como resultado, se o uso da KSN estiver ativado, o Kaspersky Endpoint Security utiliza informações sobre a reputação dos ficheiros, recursos Web e aplicações recebidas da Kaspersky Security Network.

Limitações do Kaspersky Private Security Network

Kaspersky Private Security Network (KPSN) é uma solução que permite que utilizadores de computadores que alojam o Kaspersky Endpoint Security ou outras aplicações da Kaspersky tenham acesso às bases de dados de reputação do Kaspersky Security Network e a outros dados estatísticos sem enviar dados para o KSN a partir de seus próprios computadores. A Kaspersky Private Security Network permite que utilize a sua própria base de dados de reputação local para verificar a reputação de objetos (ficheiros ou endereços de Internet). A reputação de um objeto adicionado à base de dados de reputação local tem uma prioridade mais elevada do que uma adicionada à KSN/KPSN. Por exemplo, imagine que o Kaspersky Endpoint Security está a verificar um computador e solicita a reputação de um ficheiro na KSN/KPSN. Se o ficheiro tiver uma reputação de *Não fiáveis* na base de dados de reputação local, mas tiver uma reputação de *Fiáveis* na KSN/KPSN, o Kaspersky Endpoint Security detetará o ficheiro como *Não fiáveis* e executará a ação definida para ameaças detetadas.

No entanto, em alguns casos, o Kaspersky Endpoint Security pode não solicitar a reputação de um objeto na KSN/KPSN. Se for este o caso, o Kaspersky Endpoint Security não receberá dados da base de dados de reputação local da KPSN. O Kaspersky Endpoint Security poderá não solicitar a reputação de um objeto na KSN/KPSN pelos seguintes motivos:

- As aplicações da Kaspersky estão a utilizar bases de dados de reputação offline. As bases de dados de reputação offline são concebidas para otimizar recursos durante a operação das aplicações Kaspersky e para proteger objetos extremamente importantes no computador. As bases de dados de reputação offline são criadas por especialistas da Kaspersky com base nos dados da Kaspersky Security Network. As aplicações Kaspersky atualizam as bases de dados de reputação offline com bases de dados de antivírus da aplicação específica. Se as bases de dados de reputação offline contiverem informações sobre um objeto que está a ser verificado, a aplicação não solicita a reputação deste objeto à KSN/KPSN.

- As exclusões de verificação (zona fiável) são configuradas nas definições da aplicação. Se for este o caso, a aplicação não tem em consideração a reputação do objeto na base de dados de reputação local.

- A aplicação utiliza tecnologias de otimização de verificação, como iSwift ou iChecker, ou está a armazenar na cache as solicitações de reputação na KSN/KPSN. Se for este o caso, a aplicação pode não solicitar a reputação de objetos verificados anteriormente.

- Para otimizar a sua carga de trabalho, a aplicação verifica ficheiros de um determinado formato e tamanho. A lista de formatos relevantes e limites de tamanho é determinada pelos especialistas da Kaspersky. Esta lista é atualizada com as bases de dados de antivírus da aplicação. Também pode definir as definições de otimização da verificação na interface da aplicação, por exemplo, para o componente Proteção contra ameaças de ficheiros.

- O Kaspersky Endpoint Security no modo Light Agent comunica com os Servidores KSN através de um servidor proxy KSN. A comunicação direta com o KSN não é suportada.

Ativar e desativar o modo de nuvem para componentes de proteção

O Modo de nuvem refere-se ao modo operacional da aplicação no qual o Kaspersky Endpoint Security utiliza uma versão simplificada das bases de dados antivírus. A Kaspersky Security Network suporta a operação da aplicação quando estão a ser usadas bases de dados antivírus simplificadas. A versão simplificada das bases de dados antivírus permite-lhe utilizar cerca de metade da RAM do computador que de outra forma seria utilizada com as bases de dados habituais. Se não participar na Kaspersky Security Network ou se o Modo de nuvem estiver desativado, o Kaspersky Endpoint Security transfere a versão completa das bases de dados antivírus dos servidores da Kaspersky.

Quando utilizar a Kaspersky Private Security Network, a funcionalidade do cloud mode está disponível, começando com a versão 3.0 da Kaspersky Private Security Network.

Se a aplicação estiver a funcionar no modo Light Agent, o modo de Nuvem não está disponível.

Como ativar ou desativar o modo de nuvem para componentes de proteção na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Proteção avançada contra ameaças → Kaspersky Security Network**.
4. Use a caixa de verificação **Ativar o modo de nuvem** para ativar ou desativar o componente.
5. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar ou desativar o modo de nuvem para componentes de proteção na Web Console e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings → Kaspersky Security Network**.
5. Use o botão de alternar da **Use cloud mode** para ativar ou desativar o componente.
6. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar ou desativar o modo de nuvem para componentes de proteção na interface da aplicação

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Proteção avançada contra ameaças → Kaspersky Security Network**.
3. Use o botão de alternar da **Ativar o modo de nuvem** para ativar ou desativar o componente.
4. Guarde as suas alterações.

Como resultado, o Kaspersky Endpoint Security transfere uma versão simplificada ou uma versão completa das bases de dados de antivírus durante a atualização seguinte.

Se a versão simplificada das bases de dados de antivírus não estiver disponível para utilização, o Kaspersky Endpoint Security muda automaticamente para a versão premium das bases de dados de antivírus.

Definições do KSN Proxy

Os computadores de utilizador geridos pelo Servidor de Administração do Kaspersky Security Center podem interagir com a KSN diretamente ou através do serviço KSN Proxy.

Se a aplicação estiver a ser executada no modo Light Agent, não é suportada a comunicação direta com o KSN. O Kaspersky Endpoint Security comunica com servidores KSN por meio de um servidor proxy KSN.

O serviço KSN Proxy permite o seguinte:

- O computador do utilizador pode enviar consultas para a KSN e submeter informações na KSN, mesmo sem acesso direto à Internet.
- O serviço KSN Proxy armazena dados processados, reduzindo a carga no canal de comunicação da rede externa e tornando mais rápida a receção de informação solicitada pelo computador do utilizador.

Por defeito, após a KSN estar ativada e a Declaração da KSN ser aceite, a aplicação utiliza um servidor proxy para se ligar à Kaspersky Security Network. O servidor proxy utilizado pela aplicação é o Servidor de Administração do Kaspersky Security Center via porta TCP 13111. Por conseguinte, se o KSN Proxy não estiver disponível, tem de verificar o seguinte:

- O serviço `ksnproxy` está a ser executado no Servidor de Administração.
- A Firewall no computador não está a bloquear a porta 13111.

Pode configurar a utilização do KSN Proxy da seguinte forma: ativar ou desativar o KSN Proxy, e configurar a porta para a ligação. Para o fazer, tem de abrir as propriedades do Servidor de Administração. Para obter mais informações sobre a configuração, consulte a Ajuda do Kaspersky Security Center. Também pode ativar ou desativar o KSN Proxy para computadores individuais na política do Kaspersky Endpoint Security.

Como ativar ou desativar o KSN Proxy na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Proteção avançada contra ameaças → Kaspersky Security Network**.
4. No bloco **Definições de proxy da KSN**, utilize a caixa de verificação **Usar um Servidor de administração como um servidor proxy KSN** para ativar ou desativar o KSN Proxy.
5. Se necessário, selecione a caixa de verificação **Usar os servidores do Kaspersky Security Network se o servidor KSN proxy estiver indisponível**.

   Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security utiliza os servidores da KSN quando o serviço KSN Proxy estiver indisponível. Os servidores da KSN podem estar localizados quer na Kaspersky quer em terceiros (quando a Kaspersky Private Security Network é utilizada).
6. Guarde as suas alterações.

Como ativar ou desativar o KSN Proxy na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings → Kaspersky Security Network**.
5. Use a caixa de verificação **Use Administration Server as a KSN proxy server** para ativar ou desativar o KSN Proxy.

6. Se necessário, selecione a caixa de verificação **Use Kaspersky Security Network servers if the KSN proxy server is unavailable**.

   Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security utiliza os servidores da KSN quando o serviço KSN Proxy estiver indisponível. Os servidores da KSN podem estar localizados quer na Kaspersky quer em terceiros (quando a Kaspersky Private Security Network é utilizada). Por padrão, a caixa de verificação está desmarcada.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

O endereço do KSN Proxy corresponde ao endereço do Servidor de Administração. Quando o nome de domínio do Servidor de Administração é alterado, tem de atualizar manualmente o endereço do KSN Proxy.

Para configurar o endereço do KSN Proxy:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione a pasta **Remote installation** → **Advanced** → **Installation packages**.
3. No menu de contexto da pasta **Installation packages**, selecione **Properties**.
4. No separador **General** na janela aberta, especifique o novo endereço do servidor do KSN proxy.
5. Guarde as suas alterações.

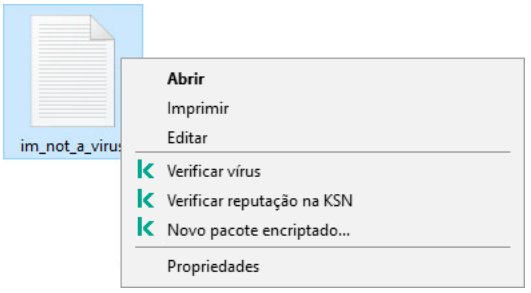
Verificar a reputação de um ficheiro na Kaspersky Security Network

Se duvidar da segurança de um ficheiro, pode verificar a sua reputação na Kaspersky Security Network.

Pode verificar a reputação de um ficheiro se tiver aceite os termos da Declaração da Kaspersky Security Network.

Para verificar a reputação de um ficheiro na Kaspersky Security Network:

Abra o menu de contexto do ficheiro e selecione a opção **Verificar a reputação na KSN** (ver a figura abaixo).



Menu de contexto do ficheiro

O Kaspersky Endpoint Security apresenta a reputação do ficheiro:

Fiável (Kaspersky Security Network). A aplicação considera um ficheiro confiável se uma ou mais das seguintes condições forem cumpridas:

- o ficheiro está assinado digitalmente por um fornecedor confiável;
- o ficheiro tem uma reputação confiável na Kaspersky Security Network;
- o utilizador adicionou a aplicação ao grupo Confiável.

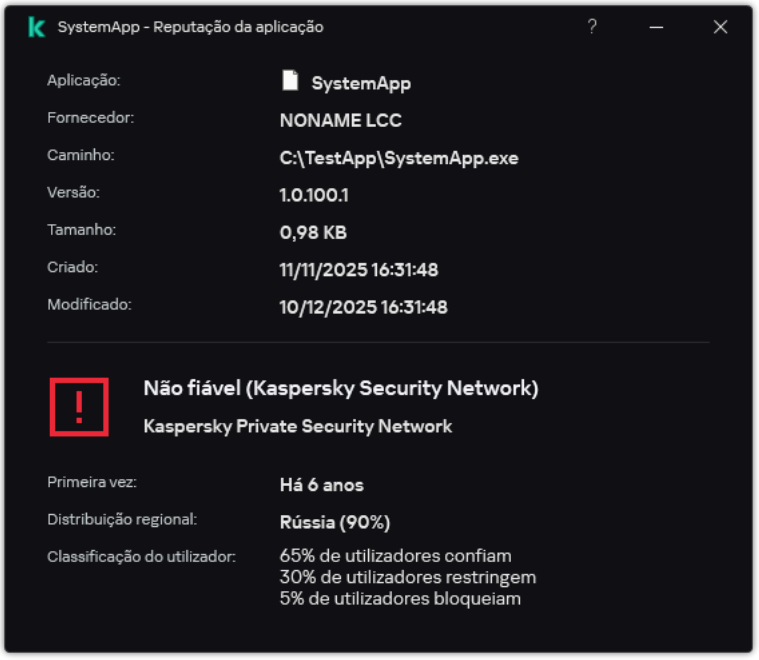
Software legítimo que pode ser utilizado por intrusos para danificar o seu computador ou dados pessoais. Embora não tenham funções maliciosas, estas aplicações podem ser exploradas por intrusos. Para mais informações sobre software legítimo que pode ser utilizado por criminosos para danificar o computador ou os dados pessoais dos utilizadores, visite o website da Kaspersky IT Encyclopedia. Pode adicionar estas aplicações à lista fiável.

Não fiável (Kaspersky Security Network). Um vírus ou outra aplicação que constitui uma ameaça.

Desconhecido (Kaspersky Security Network). A Kaspersky Security Network não possui informações acerca do ficheiro. Pode verificar um ficheiro utilizando bases de dados de antivírus (a opção **Verificar vírus** no menu do contexto).

O Kaspersky Endpoint Security apresenta a solução KSN utilizada para determinar a reputação do ficheiro: *Kaspersky Security Network* or *Kaspersky Private Security Network*.

O Kaspersky Endpoint Security apresenta também informações adicionais sobre o ficheiro (ver a figura abaixo).



Reputação de um ficheiro na Kaspersky Security Network

Verificação de ligações encriptadas

Após a instalação, o Kaspersky Endpoint Security adiciona um certificado da Kaspersky ao armazenamento do sistema para certificados fiáveis (loja de certificados Windows). O Kaspersky Endpoint Security utiliza este certificado para verificar ligações encriptadas. O Kaspersky Endpoint Security inclui também a utilização do armazenamento do sistema de certificados fiáveis no Firefox e Thunderbird para verificar o tráfego dessas aplicações.

Os componentes Controlo de Internet, Proteção contra ameaças de correio, Proteção contra ameaças da Web, Deteção de comportamento e Prevenção de explorações podem desencriptar e verificar o tráfego de rede transmitido através de ligações encriptadas que utilizam os seguintes protocolos:

- SSL 3.0.
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Ativar a verificação de ligações encriptadas

Por predefinição, o Kaspersky Endpoint Security nem sempre verifica ligações encriptadas, mas apenas quando solicitado pelos componentes de proteção.

Como ativar a verificação de ligações encriptadas na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Definições gerais** → **Definições de Rede**.
5. No bloco **Verificação de ligações encriptadas**, selecione o modo de verificação de ligação encriptada:
   - **Verificar ligações encriptadas**. O Kaspersky Endpoint Security não terá acesso aos conteúdos de sites cujos endereços começam por `https://`.
   - **Verificar ligações encriptadas a pedido dos componentes de proteção**. O Kaspersky Endpoint Security só procederá à verificação de tráfego encriptado quando tal for solicitado pelos componentes Proteção Contra Ameaças da Web, Proteção Contra Ameaças de Correio e Controlo de Internet.
   - **Verificar sempre ligações encriptadas**. O Kaspersky Endpoint Security procederá à verificação do tráfego de rede encriptada ainda que os componentes de proteção estejam desativados.

O Kaspersky Endpoint Security não verifica ligações encriptadas estabelecidas por aplicações fiáveis para as quais a verificação de tráfego está desativada. O Kaspersky Endpoint Security não verifica ligações encriptadas da lista predefinida de sites fiáveis. A lista predefinida de sites fiáveis é criada por especialistas da Kaspersky. Esta lista é atualizada com as bases de dados de antivírus da aplicação. Só pode ver a lista predefinida de sites fiáveis na interface do Kaspersky Endpoint Security. Não pode ver a lista na Consola do Kaspersky Security Center.

6. Se necessário, adicione exclusões de verificação: endereços e aplicações fiáveis.

7. Configure as definições para a verificação das ligações encriptadas (consulte a tabela abaixo).

8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar a verificação de ligações encriptadas na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **General Settings** → **Network Settings**.

5. Sob **Encrypted Connections Scan**, ative a opção **Encrypted Connections Scan ENABLED**.

   Se o botão estiver desativado, o Kaspersky Endpoint Security não terá acesso aos conteúdos de sites cujos endereços começam por `https://`.

6. Clique em **Settings** e selecione o modo de verificação de ligação encriptada:

   - **Scan encrypted connections upon request from protection components**. O Kaspersky Endpoint Security só procederá à verificação de tráfego encriptado quando tal for solicitado pelos componentes Proteção Contra Ameaças da Web, Proteção Contra Ameaças de Correio e Controlo de Internet.

   - **Always scan encrypted connections**. O Kaspersky Endpoint Security procederá à verificação do tráfego de rede encriptada ainda que os componentes de proteção estejam desativados.

   O Kaspersky Endpoint Security não verifica ligações encriptadas estabelecidas por aplicações fiáveis para as quais a verificação de tráfego está desativada. O Kaspersky Endpoint Security não verifica ligações encriptadas da lista predefinida de sites fiáveis. A lista predefinida de sites fiáveis é criada por especialistas da Kaspersky. Esta lista é atualizada com as bases de dados de antivírus da aplicação. Só pode ver a lista predefinida de sites fiáveis na interface do Kaspersky Endpoint Security. Não pode ver a lista na Consola do Kaspersky Security Center.

7. Se necessário, adicione exclusões de verificação: endereços e aplicações fiáveis.

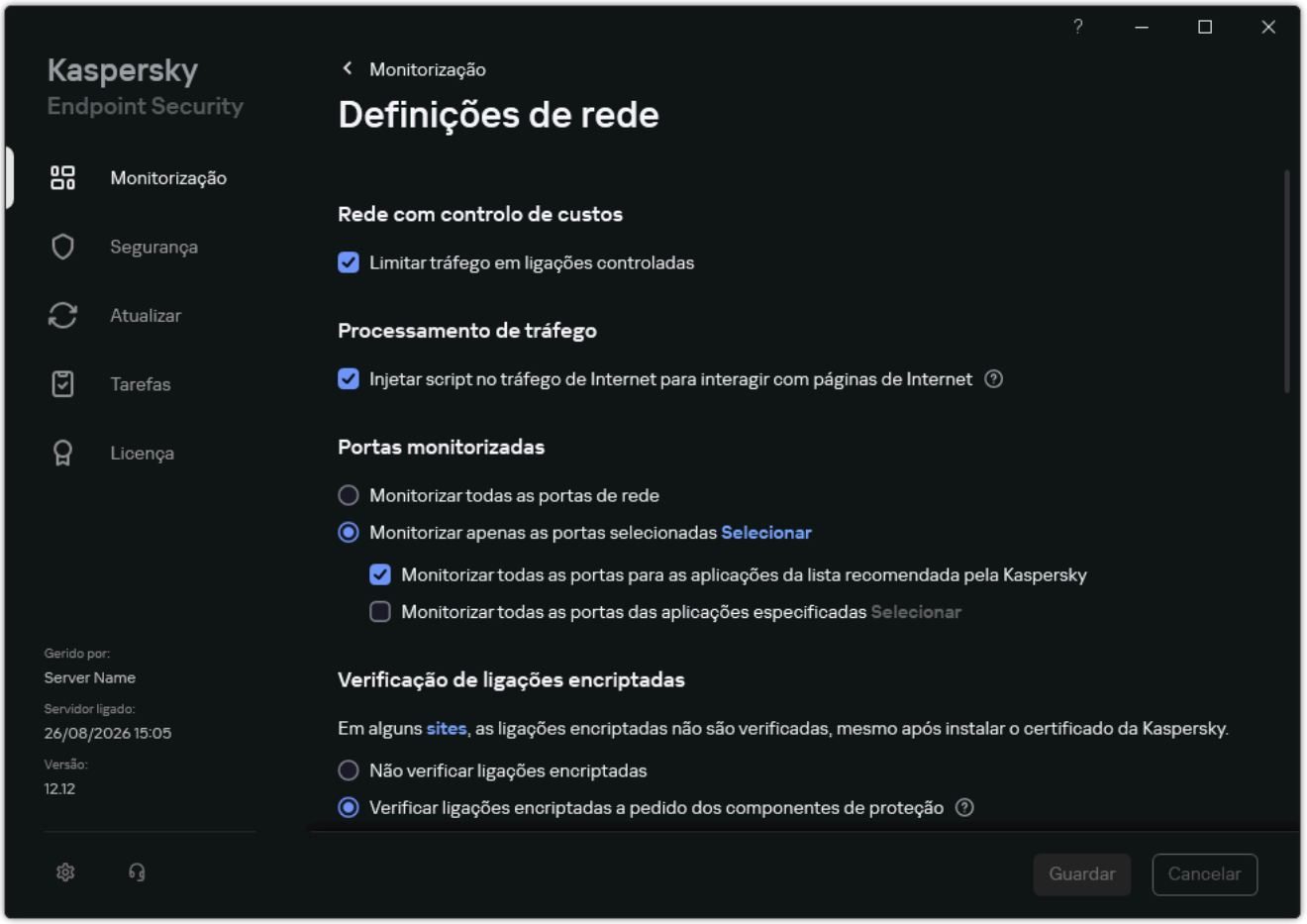
8. Configure as definições para a verificação das ligações encriptadas (consulte a tabela abaixo).

9. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar a verificação de ligações encriptadas na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Definições gerais** → **Definições de rede**.



Definições de verificação das ligações encriptadas

3. No bloco **Verificação de ligações encriptadas**, selecione o modo de verificação de ligação encriptada:

   - **Não verificar ligações encriptadas**. O Kaspersky Endpoint Security não terá acesso aos conteúdos de sites cujos endereços começam por `https://`.

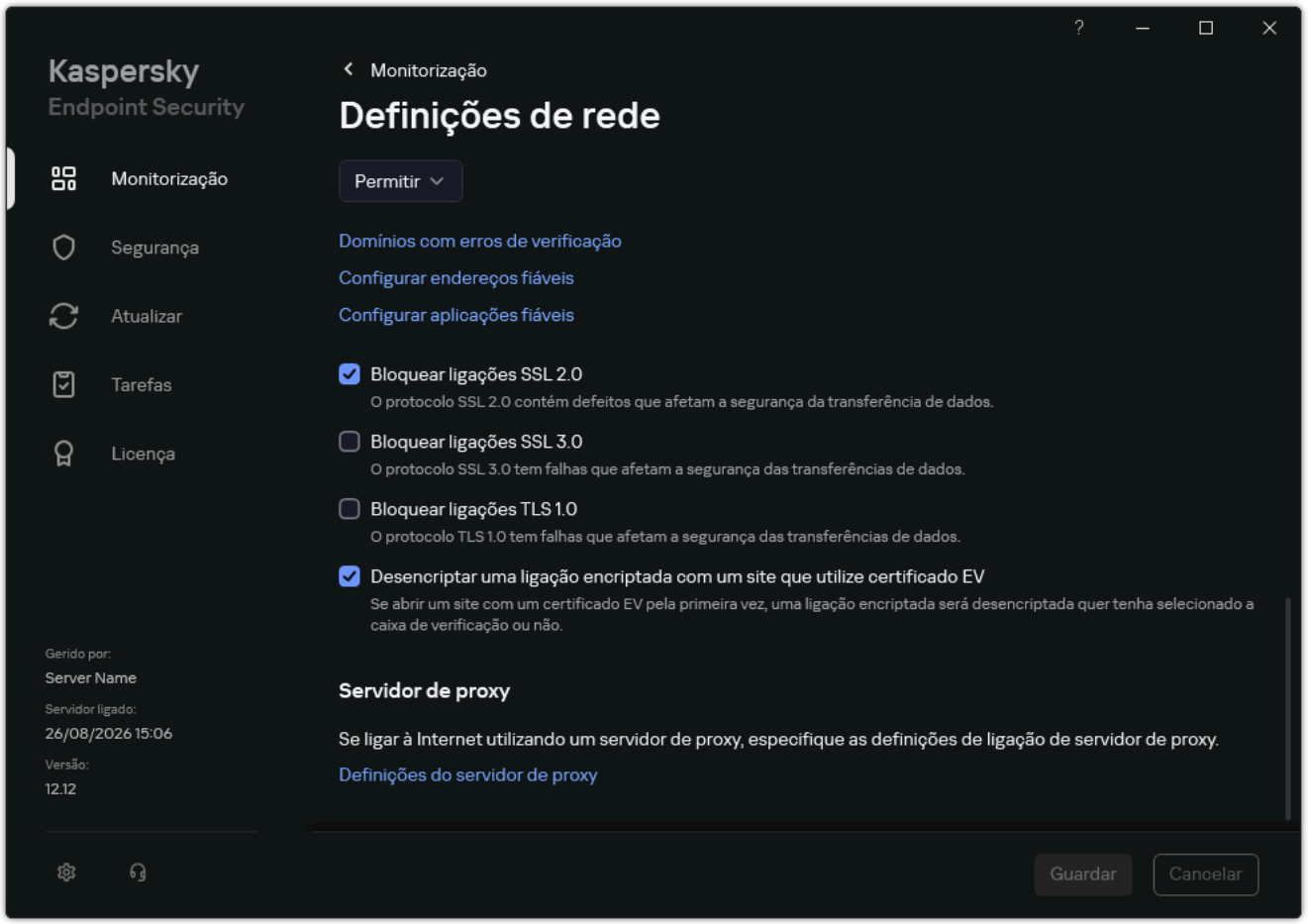
   - **Verificar ligações encriptadas a pedido dos componentes de proteção**. O Kaspersky Endpoint Security só procederá à verificação de tráfego encriptado quando tal for solicitado pelos componentes Proteção Contra Ameaças da Web, Proteção Contra Ameaças de Correio e Controlo de Internet.

   - **Verificar sempre ligações encriptadas**. O Kaspersky Endpoint Security procederá à verificação do tráfego de rede encriptada ainda que os componentes de proteção estejam desativados.

   O Kaspersky Endpoint Security não verifica ligações encriptadas estabelecidas por aplicações fiáveis para as quais a verificação de tráfego está desativada. O Kaspersky Endpoint Security não verifica ligações encriptadas da lista predefinida de sites fiáveis. A lista predefinida de sites fiáveis é criada por especialistas da Kaspersky. Esta lista é atualizada com as bases de dados de antivírus da aplicação. Só pode ver a lista predefinida de sites fiáveis na interface do Kaspersky Endpoint Security. Não pode ver a lista na Consola do Kaspersky Security Center.

4. Se necessário, adicione exclusões de verificação: endereços e aplicações fiáveis.

5. Configure as definições para a verificação das ligações encriptadas (consulte a tabela abaixo).



Definições adicionais para verificação de ligações encriptadas

6. Guarde as suas alterações.

Definições de verificação das ligações encriptadas

Parâmetro	Descrição
Certificados de raiz fiável	Lista de certificados de raiz fiável. O Kaspersky Endpoint Security permite-lhe instalar certificados de raiz fiáveis em computadores de utilizadores se, por exemplo, precisar de implementar um novo centro de certificação. A aplicação permite-lhe adicionar um certificado a uma loja especial de certificados do Kaspersky Endpoint Security. Neste caso, o certificado é considerado de confiança apenas para a aplicação do Kaspersky Endpoint Security. Por outras palavras, o utilizador pode ter acesso a um site com o novo certificado no navegador. Se outra aplicação tentar obter acesso ao site, pode obter um erro de ligação devido à emissão de um certificado. Para adicionar à loja de certificados do sistema, pode utilizar as políticas de grupo do Active Directory.
Visitar um domínio com um certificado não fiável	• **Permitir**. Quando visita um domínio com um certificado não fiável, o Kaspersky Endpoint Security permite a ligação à rede. Ao abrir um domínio com um certificado não fiável com um navegador, o Kaspersky Endpoint Security apresenta uma página HTML com um aviso e o motivo porque não é recomendável visitar esse domínio. Um utilizador pode clicar na ligação da página HTML de aviso para obter acesso ao recurso da Internet solicitado. Se uma aplicação ou serviço de terceiros estabelecer uma ligação com um domínio com um certificado não fiável, o Kaspersky Endpoint Security cria o seu próprio certificado para verificar o tráfego. O novo certificado tem o estado *Não fiável*. Isto é necessário para avisar a aplicação de terceiros sobre a ligação não fiável, uma vez que a página HTML não pode ser apresentada neste caso e a ligação pode ser estabelecida no modo de segundo plano. • **Bloquear**. Quando visita um domínio com um certificado não fiável, o Kaspersky Endpoint Security bloqueia a ligação à rede. Ao visitar um domínio com um certificado não fiável com um navegador, o Kaspersky Endpoint Security apresenta uma página HTML com o motivo porque o domínio específico está bloqueado.
Visitar um domínio com um erro de verificação de ligações encriptadas	• **Bloquear**. Se ocorrer um erro de verificação das ligações encriptadas, o Kaspersky Endpoint Security bloqueia a ligação de rede. • **Permitir e adicionar domínio às exclusões**. Se ocorrer um erro de verificação de ligações encriptadas, o Kaspersky Endpoint Security adiciona o domínio que resultou no erro à lista de domínios com erros de verificação e não monitoriza o tráfego de rede encriptado quando visita este domínio. Poder ver uma lista de domínios com erros de verificação de ligações encriptadas apenas na interface local da aplicação. Para limpar o conteúdo da lista, deve selecionar **Bloquear**. O Kaspersky Endpoint Security também gera um evento para o erro de verificação de ligações encriptadas.

Parâmetro	Descrição
Bloquear ligações SSL 2.0	Se a caixa de verificação estiver selecionada, a aplicação monitoriza e bloqueia as ligações de rede estabelecidas através do protocolo SSL 2.0. Se a caixa de verificação não estiver selecionada, a aplicação não bloqueia as ligações de rede estabelecidas através do protocolo SSL 2.0. No entanto, a aplicação não monitoriza o tráfego de rede através deste protocolo.
Bloquear ligações SSL 3.0	Se a caixa de verificação estiver selecionada, a aplicação bloqueia as ligações de rede estabelecidas através do protocolo SSL 3.0. Se a caixa de verificação não estiver selecionada, a aplicação não bloqueia as ligações de rede estabelecidas através do protocolo SSL 3.0. A aplicação não monitoriza o tráfego de rede através deste protocolo. Todos os componentes da aplicação funcionam sem restrições.
Bloquear ligações TLS 1.0	Se a caixa de verificação estiver selecionada, a aplicação bloqueia as ligações de rede estabelecidas através do protocolo TLS 1.0. Se a caixa de verificação não estiver selecionada, a aplicação não bloqueia as ligações de rede estabelecidas através do protocolo TLS 1.0. A aplicação não monitoriza o tráfego de rede através deste protocolo. Todos os componentes da aplicação funcionam sem restrições.
Desencriptar uma ligação encriptada com um site que utilize certificado EV	Certificados EV (Extended Validation Certificate) confirmam a autenticidade dos sites e melhoram a segurança da ligação. Os navegadores usam um ícone de cadeado na barra de endereços para indicar que um site tem um certificado EV. Os navegadores também podem colorir total ou parcialmente a barra de endereço a verde. Se a caixa de seleção estiver selecionada, a aplicação desencripta e monitoriza as ligações encriptadas com sites que utilizem um certificado EV. Se a caixa de seleção estiver desmarcada, a aplicação não terá acesso ao conteúdo do tráfego HTTPS. Por este motivo, a aplicação monitoriza o tráfego HTTPS apenas com base no endereço do site, por exemplo, `https://bing.com`. Se estiver a abrir um site com um certificado EV pela primeira vez, a ligação encriptada será desencriptada, independentemente de a caixa de seleção estar selecionada ou não.

Instalar certificados de raiz fiáveis

O Kaspersky Endpoint Security permite-lhe instalar certificados de raiz fiáveis em computadores de utilizadores se, por exemplo, precisar de implementar um novo centro de certificação. A aplicação permite-lhe adicionar um certificado a uma loja especial de certificados do Kaspersky Endpoint Security. Neste caso, o certificado é considerado de confiança apenas para a aplicação do Kaspersky Endpoint Security. Por outras palavras, o utilizador pode ter acesso a um site com o novo certificado no navegador. Se outra aplicação tentar obter acesso ao site, pode obter um erro de ligação devido à emissão de um certificado. Para adicionar à loja de certificados do sistema, pode utilizar as políticas de grupo do Active Directory.

Como instalar certificados de raiz fiável na Consola de administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais → Definições de Rede**.
4. No bloco **Certificados de raiz fiável**, clique no botão **Adicionar**.
5. Esta ação abre uma janela; nessa janela, selecione um certificado de raiz fiável.

   O Kaspersky Endpoint Security suporta certificados com extensões PEM, DER e CRT.
6. Guarde as suas alterações.

Como instalar certificados de raiz fiável na Web Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **Network Settings**.
5. Clique na hiperligação **Trusted root certificates**.
6. Esta ação abre uma janela; nessa janela, clique em **Add** e selecione um certificado de raiz fiável.

   O Kaspersky Endpoint Security suporta certificados com extensões PEM, DER e CRT.
7. Guarde as suas alterações.

Como instalar certificados de raiz fiável na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Definições de rede**.
3. No bloco **Verificação de ligações encriptadas**, clique no botão **Mostrar certificados**.
4. Esta ação abre uma janela; nessa janela, clique em **Adicionar** e selecione um certificado de raiz fiável.

   O Kaspersky Endpoint Security suporta certificados com extensões PEM, DER e CRT.
5. Guarde as suas alterações.

Como resultado, ao verificar o tráfego, para além do arquivo de certificados do sistema, o Kaspersky Endpoint Security utiliza o seu próprio arquivo de certificados.

Verificar ligações encriptadas com um certificado não fiável

Após a instalação, o Kaspersky Endpoint Security adiciona um certificado da Kaspersky ao armazenamento do sistema para certificados fiáveis (loja de certificados Windows). O Kaspersky Endpoint Security utiliza este certificado para verificar ligações encriptadas. Ao visitar um domínio com um certificado não fiável, pode permitir ou negar o acesso do utilizador a esse domínio (consulte as instruções abaixo).

Se permitiu que o utilizador visite domínios com certificados não fiáveis, o Kaspersky Endpoint Security executa as seguintes ações:

- Ao visitar um domínio com um certificado não fiável no *navegador*, o Kaspersky Endpoint Security utiliza o certificado Kaspersky para verificar o tráfego. O Kaspersky Endpoint Security mostra 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 utilizador pode clicar na ligação da página HTML de aviso para obter acesso ao recurso da Internet solicitado. Depois de seguir esta ligação, durante a próxima hora, o Kaspersky Endpoint Security não apresenta avisos sobre um certificado não fiável ao visitar outros recursos no mesmo domínio. O Kaspersky Endpoint Security também gera um evento sobre o estabelecimento de uma ligação encriptada com um certificado não fiável.

  Em alguns casos, o Kaspersky Endpoint Security não consegue exibir tecnicamente uma página HTML com um aviso no navegador (veja a figura abaixo). Por exemplo, se um recurso da Web usa uma versão desatualizada de um protocolo de rede e uma porta não padrão. Nestes casos, o Kaspersky Endpoint Security bloqueia o acesso a este domínio e o navegador irá mostrar a janela predefinida `ERR_CONNECTION_RESET`. Para aceder a um recurso da Web, pode adicionar o domínio às exclusões ou utilizar um certificado fiável.

- Se *uma aplicação ou serviço de terceiros* estabelecer uma ligação com um domínio com um certificado não fiável, o Kaspersky Endpoint Security cria o seu próprio certificado para verificar o tráfego. O novo certificado tem o estado *Não fiável*. Isto é necessário para avisar a aplicação de terceiros sobre a ligação não fiável, uma vez que a página HTML não pode ser apresentada neste caso e a ligação pode ser estabelecida no modo de segundo plano. Portanto, se uma aplicação de terceiros tiver ferramentas de verificação de certificado integradas, a ligação poderá ser terminada. Nesse caso, deve entrar em contacto com o proprietário do domínio e configurar uma ligação fiável. Se não for possível configurar uma ligação fiável, pode adicionar essa aplicação de terceiros à lista de aplicações fiáveis. O Kaspersky Endpoint Security também gera um evento sobre o estabelecimento de uma ligação encriptada com um certificado não fiável.

Como configurar a verificação de ligações encriptadas com um certificado não fiável na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais** → **Definições de Rede**.
4. No bloco **Verificação de ligações encriptadas**, clique no botão **Definições avançadas**.
5. Na janela que se abre, selecione o modo operacional da aplicação ao visitar um domínio com um certificado não fiável: **Permitir** ou **Bloquear**.
6. Guarde as suas alterações.

Como configurar a verificação de ligações encriptadas com um certificado não fiável na Web Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **Network Settings**.

5. No bloco **Encrypted Connections Scan**, clique na ligação **Settings**.

6. Na janela que se abre, selecione o modo operacional da aplicação ao visitar um domínio com um certificado não fiável: **Allow connection** ou **Block connection**.

7. Guarde as suas alterações.

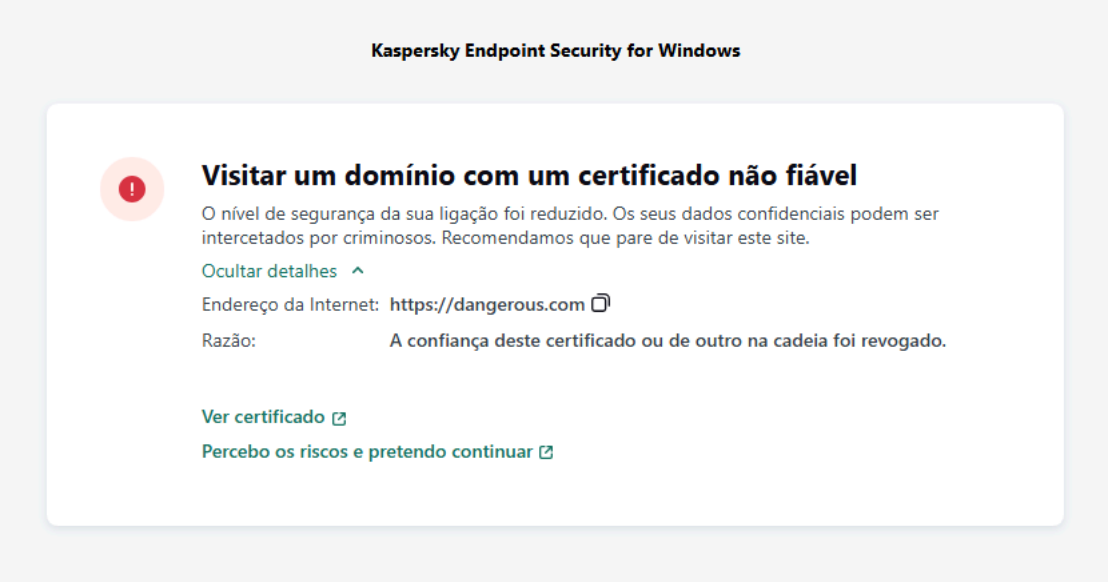
Como configurar a verificação de ligações encriptadas com um certificado não fiável na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Definições gerais** → **Definições de rede**.

3. No bloco **Verificação de ligações encriptadas**, selecione o modo operacional da aplicação ao visitar um domínio com um certificado não fiável: **Permitir** ou **Bloquear**.

4. Guarde as suas alterações.



Aviso sobre visitar um domínio com um certificado não fiável

Adicionar um certificado Kaspersky ao próprio armazenamento de certificados

Os navegadores e clientes de e-mail usam o certificado para verificar a segurança e a autenticidade dos recursos da Web. O certificado também fornece encriptação de dados entre os recursos da Web e o utilizador. A maioria dos navegadores e clientes de e-mail utilizam o armazenamento de certificados fiável (loja de certificados do Windows). Por exemplo, o Google Chrome. Alguns navegadores e clientes de e-mail usam o seu próprio armazenamento de certificados por padrão, em vez da loja de certificados do Windows. Por exemplo, o Firefox e o Thunderbird.

Após a instalação, o Kaspersky Endpoint Security adiciona um certificado da Kaspersky ao armazenamento do sistema para certificados fiáveis (loja de certificados Windows). Se o Kaspersky Security Center for implementado na sua organização e uma política estiver a ser aplicada a um computador, o Kaspersky Endpoint Security ativa automaticamente o uso do armazenamento de certificados do Windows nos navegadores e nos clientes de e-mail para verificar o tráfego dessas aplicações. Se não estiver a ser aplicada uma política no computador, pode escolher o armazenamento de certificados que será utilizado pelos navegadores e clientes de e-mail. Se selecionou o próprio armazenamento de certificados, adicione o certificado Kaspersky ao armazenamento manualmente. Isso ajudará a evitar erros ao trabalhar com tráfego HTTPS.

Para verificar tráfego no navegador Mozilla Firefox e no cliente de e-mail Thunderbird, tem de ativar a Verificação de ligações encriptadas. Se a Verificação de ligações encriptadas estiver desativada, a aplicação não verifica o tráfego no navegador Mozilla Firefox e no cliente de e-mail Thunderbird. A verificação de ligações encriptadas também deve ser ativada para verificar o tráfego nos clientes 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 Kaspersky do Painel de Controlo do Windows (propriedades da Internet). Pode aprender mais sobre como adicionar um certificado ao armazenamento, por exemplo, no Site de suporte técnico da Mozilla.

Pode escolher o armazenamento de certificados apenas na interface local da aplicação.

Para escolher um armazenamento de certificados para verificar ligações encriptadas nos navegadores e clientes de e-mail:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Definições de rede**.
3. No bloco **Verificação de ligações encriptadas**, selecione a caixa de verificação **Para verificar as ligações encriptadas em aplicações com o armazenamento de certificados do mesmo, utilize**.
4. Selecionar um armazenamento de certificados:
   - **Armazenamento de certificados do Windows (recomendado)**. O certificado raiz da Kaspersky é adicionado a este armazenamento durante a instalação do Kaspersky Endpoint Security.
   - **Armazenamento de certificados próprio**. O Mozilla Firefox e Thunderbird utilizam os seus próprios armazenamentos de certificados. Se o armazenamento de certificados Mozilla for selecionado, precisará de adicionar manualmente o certificado raiz da Kaspersky a este armazenamento através das propriedades do navegador.

     Os clientes de e-mail MyOffice Mail e R7-Office Organizer também usam o seu próprio armazenamento de certificados.
5. Guarde as suas alterações.

Excluir ligações encriptadas da verificação

A maioria dos recursos da web utiliza ligações encriptadas. Os especialistas da Kaspersky recomendam que ative a Verificação de ligações encriptadas. Se a verificação de ligações encriptadas interferir com as atividades relacionadas ao trabalho, pode adicionar um website a exclusões conhecidas como *endereços fiáveis*. Neste caso, o Kaspersky Endpoint Security não verifica o tráfego HTTPS de endereços da Internet fiáveis quando os componentes Proteção contra ameaças da web, Proteção contra ameaças de correio e Controlo de Internet estão a fazer o seu trabalho.

Se uma aplicação fiável utilizar uma ligação encriptada, pode desativar a verificação de ligações encriptadas para esta aplicação. Por exemplo, pode desativar a verificação de ligações encriptadas para aplicações de armazenamento em nuvem que utilizam autenticação de dois fatores com o seu próprio certificado.

Como excluir um endereço da Web de verificações de ligação encriptada na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Definições gerais** → **Definições de Rede**.
5. No bloco **Verificação de ligações encriptadas**, clique no botão **Configurar endereços fiáveis**.
6. Clique em **Adicionar**.
7. Introduza um nome de domínio ou um endereço IP se não quiser que o Kaspersky Endpoint Security verifique as ligações encriptadas estabelecidas ao visitar esse domínio.

   O Kaspersky Endpoint Security suporta o caractere `*` para a introdução de uma máscara no nome de domínio.

   > O Kaspersky Endpoint Security não suporta o símbolo `*` para endereços IP. Pode selecionar um intervalo de endereços IP com uma máscara de sub-rede (por exemplo, 198.51.100.0/24).

   Exemplos:

   - `domain.com` - o registo inclui os seguintes endereços: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. O registo não inclui subdomínios (por exemplo, `subdomain.domain.com`)
   - `subdomain.domain.com` - o registo inclui os seguintes endereços: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. O registo não inclui o domínio `domain.com`.
   - `*.domain.com` - o registo inclui os seguintes endereços: `https://movies.domain.com`, `https://images.domain.com/page123`. O registo não inclui o domínio `domain.com`.
8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como excluir um endereço Web das verificações de ligações encriptadas na Web Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **Network Settings**.
5. No bloco **Encrypted Connections Scan**, clique no botão **Trusted domains**.
6. Clique em **Add**.
7. Introduza um nome de domínio ou um endereço IP se não quiser que o Kaspersky Endpoint Security verifique as ligações encriptadas estabelecidas ao visitar esse domínio.

   O Kaspersky Endpoint Security suporta o caractere `*` para a introdução de uma máscara no nome de domínio.

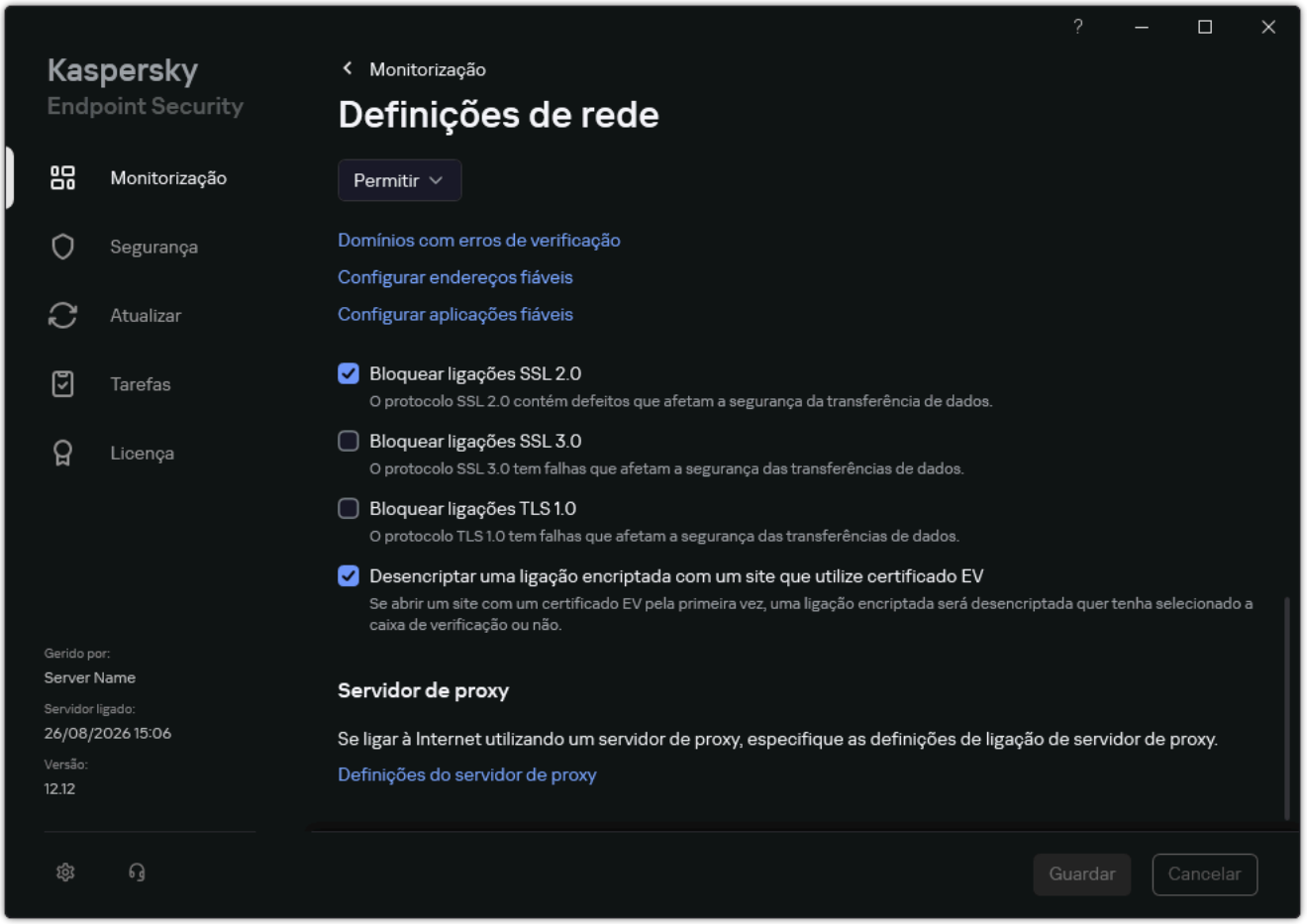
   > O Kaspersky Endpoint Security não suporta o símbolo `*` para endereços IP. Pode selecionar um intervalo de endereços IP com uma máscara de sub-rede (por exemplo, 198.51.100.0/24).

   Exemplos:

   - `domain.com` - o registo inclui os seguintes endereços: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. O registo não inclui subdomínios (por exemplo, `subdomain.domain.com`)
   - `subdomain.domain.com` - o registo inclui os seguintes endereços: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. O registo não inclui o domínio `domain.com`.
   - `*.domain.com` - o registo inclui os seguintes endereços: `https://movies.domain.com`, `https://images.domain.com/page123`. O registo não inclui o domínio `domain.com`.
8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como excluir um endereço da Web de verificações de ligação encriptada na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Definições de rede**.



Definições da rede de aplicações

3. No bloco **Verificação de ligações encriptadas**, clique no botão **Configurar endereços fiáveis**.
4. Clique em **Adicionar**.
5. Introduza um nome de domínio ou um endereço IP se não quiser que o Kaspersky Endpoint Security verifique as ligações encriptadas estabelecidas ao visitar esse domínio.

   O Kaspersky Endpoint Security suporta o caractere `*` para a introdução de uma máscara no nome de domínio.

   O Kaspersky Endpoint Security não suporta o símbolo `*` para endereços IP. Pode selecionar um intervalo de endereços IP com uma máscara de sub-rede (por exemplo, 198.51.100.0/24).

Exemplos:

- `domain.com` - o registo inclui os seguintes endereços: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. O registo não inclui subdomínios (por exemplo, `subdomain.domain.com`)
- `subdomain.domain.com` - o registo inclui os seguintes endereços: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. O registo não inclui o domínio `domain.com`.
- `*.domain.com` - o registo inclui os seguintes endereços: `https://movies.domain.com`, `https://images.domain.com/page123`. O registo não inclui o domínio `domain.com`.

6. Guarde as suas alterações.

Por predefinição, o Kaspersky Endpoint Security não verifica conexões encriptadas quando ocorrem erros e adiciona o website a uma lista especial de *Domínios com erros de verificação*. O Kaspersky Endpoint Security compila uma lista separada para cada utilizador e não envia dados para o Kaspersky Security Center. Pode ativar o bloqueio da ligação quando ocorrer um erro de verificação. Poder ver uma lista de domínios com erros de verificação de ligações encriptadas apenas na interface local da aplicação.

Para ver a lista de domínios com erros de verificação:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais → Definições de rede**.
3. No bloco **Verificação de ligações encriptadas**, clique no botão **Domínios com erros de verificação**.

   Abre-se uma lista de domínios com erros de verificação. Para redefinir a lista, ative a ligação de bloqueio quando ocorrem erros de verificação na política, aplique a política, em seguida, redefina o parâmetro para o seu valor inicial e aplique a política novamente.

Os especialistas da Kaspersky fazem uma lista de *exceções globais* - websites fiáveis que o Kaspersky Endpoint Security não verifica, independentemente das configurações da aplicação.

Para ver as exclusões globais de verificações de tráfego encriptado:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais → Definições de rede**.
3. No bloco **Verificação de ligações encriptadas**, clique na ligação da lista de sites fidedignos.

   Abre-se uma lista de sites compilada por especialistas da Kaspersky. O Kaspersky Endpoint Security não verifica ligações protegidas para sites da lista. A lista pode ser atualizada quando as bases de dados e os módulos do Kaspersky Endpoint Security são atualizados.

Bloquear o acesso a domínios com certificados não fidedignos

Em alguns casos, ao bloquear o acesso a um domínio com um certificado não fidedigno, o Kaspersky Endpoint Security apresenta no navegador uma página de aviso HTML sem a ligação para o recurso Web solicitado.

Isto pode acontecer pelos seguintes motivos:

- O administrador bloqueou o acesso a um domínio com um certificado não fidedigno.
- O domínio tem um certificado não fidedigno ou inválido e o servidor Web utiliza o mecanismo HTTP Strict Transport Security (HSTS). O *HSTS* é um mecanismo de segurança que impõe a utilização do protocolo HTTPS seguro para a comunicação entre um cliente e um servidor Web. Neste caso, não pode aceder ao domínio, mesmo que o tenha adicionado à lista de endereços fidedignos. O mecanismo HSTS está descrito na RFC 6797.

  Em alguns casos, o website pode ser aberto diretamente num navegador sem utilizar o Kaspersky Endpoint Security. Os navegadores nem sempre detetam certificados revogados, ao passo que o Kaspersky Endpoint Security verifica online a revogação de certificados ao estabelecer uma ligação. Isto permite que a aplicação detete um problema com o certificado antes do navegador e apresente a mensagem de erro correspondente.



Aviso sobre visitar um domínio com um certificado não fiável

Eliminar dados

O Kaspersky Endpoint Security permite o uso de uma tarefa para eliminar remotamente os dados dos computadores dos utilizadores.

O Kaspersky Endpoint Security elimina os dados da seguinte forma:

- Em modo não assistido;
- Em discos rígidos e unidades amovíveis;
- Para todas as contas de utilizador no computador.

O Kaspersky Endpoint Security executa a tarefa *Eliminar dados* independentemente do tipo de licença usado, mesmo após a expiração da licença.

Modos de Limpeza de Dados

Esta tarefa permite-lhe eliminar dados nos seguintes modos:

- Eliminação imediata de dados.

  Neste modo, pode, por exemplo, eliminar dados desatualizados para libertar espaço no disco.

- Eliminação de dados adiada.

  Este modo destina-se, por exemplo, a proteger os dados num computador portátil, caso seja perdido ou roubado. Pode configurar a eliminação automática de dados se o computador portátil ultrapassar os limites da rede empresarial e não estiver sincronizado com o Kaspersky Security Center há muito tempo.

Não é possível agendar a eliminação de dados nas propriedades da tarefa. Só pode eliminar dados imediatamente depois de iniciar a tarefa manualmente ou depois de configurar a eliminação de dados com atraso se não existir ligação ao Kaspersky Security Center.

Limitações

A Limpeza de Dados tem as seguintes limitações:

- Somente um administrador do Kaspersky Security Center pode gerir a tarefa de *Eliminar dados*. Não pode configurar ou iniciar uma tarefa na interface local do Kaspersky Endpoint Security.
- Para o sistema de ficheiros NTFS, o Kaspersky Endpoint Security elimina apenas os nomes dos principais fluxos de dados. Não é possível eliminar nomes de fluxo de dados alternativos.
- Quando eliminar um ficheiro de ligação simbólica, o Kaspersky Endpoint Security também elimina os ficheiros cujos caminhos são especificados na ligação simbólica.

Criar uma tarefa de limpeza de dados

Para eliminar dados nos computadores dos utilizadores:

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **Wipe data**.

c. No campo **Task name**, introduza uma breve descrição, por exemplo, *Eliminar dados (Antirroubo)*.

d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Avance para o passo seguinte.

   Se forem adicionados novos computadores a um grupo de administração no âmbito da tarefa, a tarefa de eliminação 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.

   Será apresentada uma nova tarefa na lista de tarefas.

6. Clique na tarefa **Wipe data** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

7. Selecione o separador **Application settings**.

8. Selecione o método de eliminação de dados:

   - **Delete by means of the operating system**. O Kaspersky Endpoint Security usa os recursos do sistema operativo para eliminar ficheiros sem os enviar para a reciclagem.
   - **Delete completely, no recovery possible**. O Kaspersky Endpoint Security substitui os ficheiros com dados aleatórios. É praticamente impossível restaurar dados depois de eles serem excluídos.

9. Se quiser adiar a eliminação de dados, selecione a caixa de verificação **Automatically wipe data when there is no connection to Kaspersky Security Center for more than N days**. Configure o número de dias.

   A tarefa de eliminação de dados adiada será realizada sempre que não houver uma ligação ao Kaspersky Security Center durante o período de tempo definido.

   Ao configurar a exclusão de dados adiada, lembre-se de que os funcionários podem ter horários de trabalho diferentes. Considere também o horário de trabalho dos utilizadores offline. Para obter mais informações sobre como trabalhar com computadores offline e utilizadores fora do escritório, consulte a Ajuda Online do Kaspersky Security Center.

   Se o computador estiver desligado e a ligação estiver ausente por mais tempo do que o tempo configurado, após ligá-lo, o Kaspersky Endpoint Security não excluirá os dados imediatamente. A aplicação aguarda a sincronização com o Kaspersky Security Center durante uma hora. Isto é necessário para evitar a exclusão não autorizada de dados em computadores de utilizadores que desligaram os seus computadores, por exemplo, antes de irem de férias.

   Se a caixa de verificação estiver desmarcada, a tarefa será realizada imediatamente após a sincronização com o Kaspersky Security Center.

10. Crie uma lista de objetos a eliminar:

    - **Pastas**. O Kaspersky Endpoint Security elimina todos os ficheiros da pasta e das suas subpastas. O Kaspersky Endpoint Security não suporta máscaras e variáveis de ambiente para introduzir um caminho de pasta.

    - **Ficheiros por extensão**. O Kaspersky Endpoint Security procura ficheiros com as extensões especificadas em todas as unidades locais do computador, incluindo unidades amovíveis. Utilize os carateres "`;`" ou "`,`" para especificar várias extensões.

    - **Âmbito predefinido**. O Kaspersky Endpoint Security eliminará os ficheiros das seguintes áreas:

        - **Documents**. Ficheiros na pasta *Documentos* padrão do sistema operativo e as respetivas subpastas.

        - **Cookies**. Ficheiros em que o navegador guarda os dados dos websites visitados pelo utilizador (por exemplo, dados de autorização do utilizador).

        - **Desktop**. Ficheiros na pasta *Ambiente de trabalho* padrão do sistema operativo e respetivas subpastas.

        - **Temporary Internet Explorer files**. Ficheiros temporários relacionados com o funcionamento do Internet Explorer, por exemplo, cópias de páginas Web, imagens e ficheiros multimédia.

        - **Temporary files**. Ficheiros temporários relacionados com o funcionamento das aplicações instaladas no computador. Por exemplo, as aplicações do Microsoft Office criam ficheiros temporários que contêm cópias de segurança dos documentos.

        - **Outlook files**. Ficheiros relacionados com o funcionamento do cliente de e-mail do Outlook: ficheiros de dados (PST), ficheiros de dados offline (OST), ficheiros do livro de endereços offline (OAB) e ficheiros do livro de endereços pessoal (PAB).

        - **User profile**. Conjunto de ficheiros e pastas que armazenam as definições do sistema operativo para a conta do utilizador local.

    Pode criar uma lista de objetos para eliminar em cada separador. O Kaspersky Endpoint Security criará uma lista consolidada e eliminará os ficheiros desta lista quando uma tarefa estiver concluída.

    > Não pode eliminar ficheiros que sejam necessários para o funcionamento do Kaspersky Endpoint Security.

11. Guarde as suas alterações.

12. Selecione a caixa de verificação junto à tarefa.

13. Clique em **Start**.

    Como resultado, os dados nos computadores dos utilizadores serão eliminados de acordo com o modo selecionado: imediato ou quando a ligação estiver ausente. Se o Kaspersky Endpoint Security não conseguir eliminar um ficheiro, tal como quando um utilizador estiver a usar um ficheiro, a aplicação não tentará eliminar esse ficheiro novamente. Execute a tarefa novamente para concluir a eliminação dos dados.

Controlo de computador

Controlo de Internet

O Controlo de Internet gere o acesso do utilizador aos recursos da Web. Isto ajuda a reduzir o tráfego e o uso inadequado do tempo de trabalho. Quando um utilizador tenta abrir um website restrito pelo Controlo de Internet, o Kaspersky Endpoint Security bloqueia o acesso ou apresenta um aviso (consulte a figura abaixo).

Para utilizar o Controlo de Internet, tem de concluir a configuração inicial da aplicação:

- Para monitorização do tráfego HTTPS, ative a verificação de ligações encriptadas (ativado por padrão).
- Selecione as portas que o Kaspersky Endpoint Security deve monitorizar (por defeito, a aplicação monitoriza todas as portas).
- Selecione as aplicações cujo tráfego pretende que o Kaspersky Endpoint Security monitorize. A maioria dos navegadores já está presente na lista de aplicações recomendadas pela Kaspersky. Se o seu navegador não estiver na lista, adicione-o manualmente.
- Recomendamos que injete um script de interação de página de Internet no tráfego de Internet (por padrão, a injeção de script está desativada). Este script permite o registo de eventos do Controlo de Internet para o registo de eventos da aplicação, registo de eventos do SO e relatórios.

Métodos de gestão do acesso a sites

O Controlo de Internet permite-lhe configurar o acesso a sites usando os seguintes métodos:

- **Categoria do site**. Os sites são categorizados de acordo com o serviço de nuvem do Kaspersky Security Network, a análise heurística e a base de dados de sites conhecidos (incluídos nas bases de dados da aplicação). Por exemplo, pode restringir o acesso do utilizador à categoria *Redes sociais* ou a outras categorias.
- **Tipo de dados**. Pode restringir o acesso do utilizador aos dados num site e ocultar imagens, por exemplo. O Kaspersky Endpoint Security determina o tipo de dados com base no formato do ficheiro e não com base na sua extensão.

  O Kaspersky Endpoint Security não verifica ficheiros dentro de arquivos. Por exemplo, se os ficheiros de imagem forem colocados num arquivo, o Kaspersky Endpoint Security identifica o tipo de dados *Arquivos* e não *Gráficos*.

- **Endereço individual**. Pode introduzir um endereço da Web ou usar máscaras.

Pode usar simultaneamente vários métodos para regular o acesso a sites. Por exemplo, pode restringir o acesso ao tipo de dados *Ficheiros de aplicações de escritório* apenas para a categoria do site *E-mail baseado na Web*.

Regras de acesso a sites

O Controlo de Internet regula o acesso do utilizador a sites através das *regras de acesso*. Pode configurar as seguintes definições avançadas para uma regra de acesso ao site:

- Utilizadores aos quais a regra se aplica.

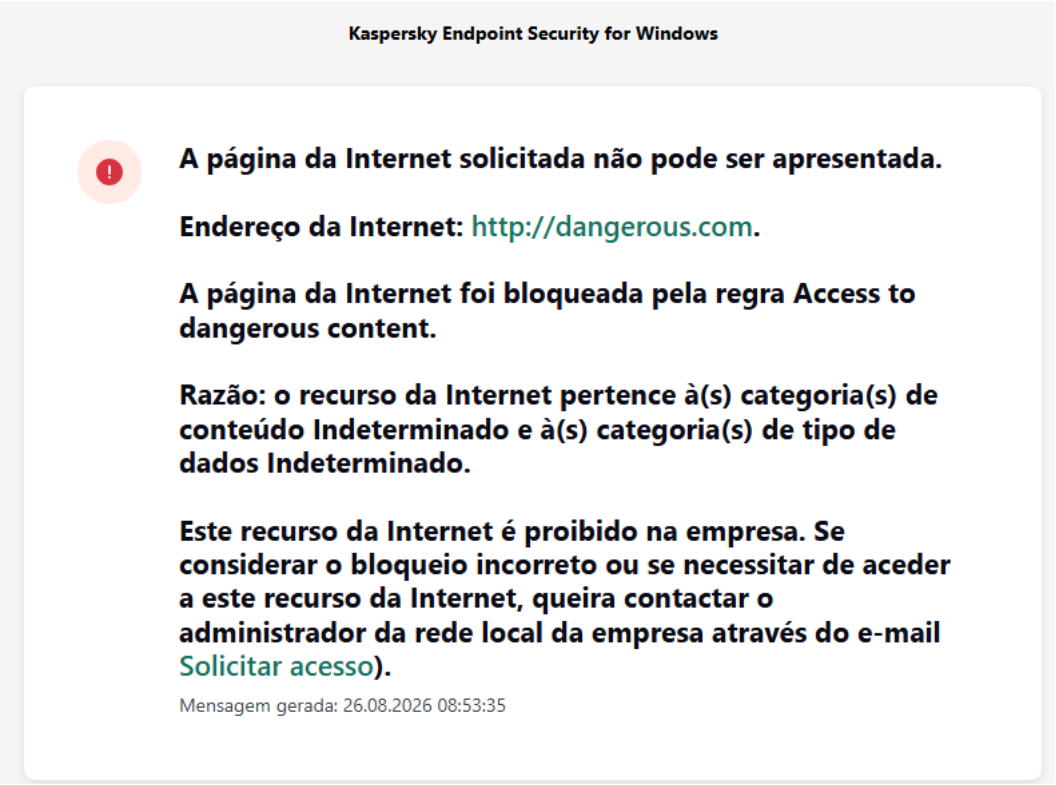
  Por exemplo, pode restringir o acesso à Internet através de um navegador para todos os utilizadores da empresa, exceto o departamento de TI.

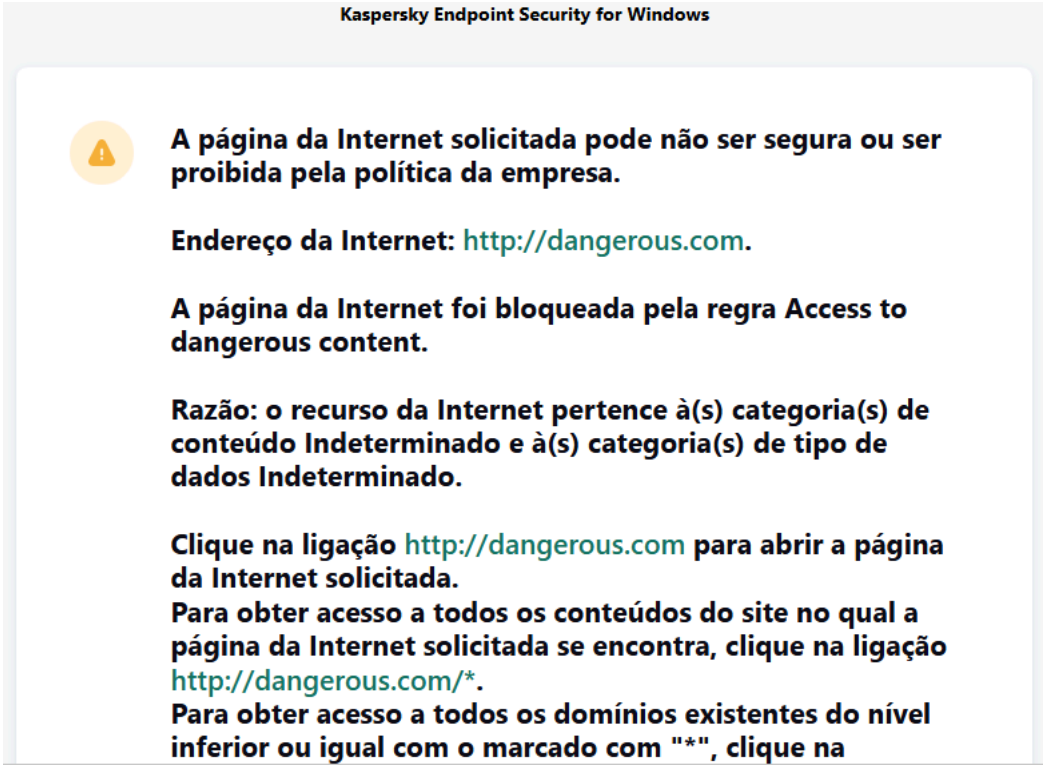
- Agendamento de regras.

  Por exemplo, pode restringir o acesso à Internet através de um navegador apenas durante o horário de expediente.

Prioridades das regras de acesso

Cada regra tem uma prioridade. Quanto mais alta for a posição de uma regra na lista, mais alta será a sua prioridade. Se um site for adicionado a várias regras, o Controlo de Internet regula o acesso ao site com base na regra com a prioridade mais alta. Por exemplo, o Kaspersky Endpoint Security pode identificar um portal empresarial como uma rede social. Para restringir o acesso a redes sociais e fornecer acesso ao portal da Web empresarial, crie duas regras: uma regra de bloqueio para a categoria de site *Redes sociais* e uma regra de permissão para o portal da Web empresarial. A regra de acesso para o portal da Web empresarial deve ter uma prioridade mais alta que a regra de acesso para redes sociais.





Mensagens do Controlo de Internet

Adicionar uma regra de acesso a recursos da Internet

Uma *regra de acesso aos recursos da Web* é um conjunto de filtros e ações que o Kaspersky Endpoint Security aplica quando os utilizadores visitam recursos da Web. As regras de acesso podem incluir um agendamento de regras.

Não recomendamos que crie mais de 1000 regras de acesso a recursos da Internet, uma vez que poderia causar instabilidade do sistema.

Uma regra de acesso a recursos da Internet consiste num conjunto de filtros e ações que o Kaspersky Endpoint Security executa quando o utilizador visita recursos da Internet descritos na regra durante o período de tempo indicado no agendamento da regra. Os filtros permitem especificar de forma precisa um conjunto de recursos da Internet para os quais o acesso é controlado pelo componente Controlo de Internet.

Estão disponíveis os seguintes filtros:

- **Filtro por conteúdo**. O Controlo de Internet categoriza os recursos da Internet por conteúdo e tipo de dados. Pode controlar o acesso de utilizadores a recursos da Internet com conteúdo e tipos de dados definidos por estas categorias. Quando os utilizadores visitam recursos da Internet que pertençam à categoria de conteúdo e/ou categoria de tipo de dados selecionada, o Kaspersky Endpoint Security executa a ação especificada na regra.

- **Filtro por endereços de recursos da Internet**. Pode controlar o acesso de utilizadores a todos os endereços de recursos da Internet ou a endereços de recursos da Internet individuais e/ou grupos de endereços de recursos da Internet.

  Se a filtragem por conteúdo e a filtragem por endereços de recursos da Internet forem especificadas e os endereços de recursos da Internet e/ou grupos de endereços de recursos da Internet especificados pertencerem às categorias de conteúdo ou categorias de tipos de dados selecionadas, o Kaspersky Endpoint Security não controla o acesso a todos os recursos da Internet nas categorias de conteúdo e/ou tipo de dados selecionadas. Em vez disso, a aplicação controla o acesso apenas aos endereços de recursos da Internet e/ou grupos de endereços de recursos da Internet especificados.

- **Filtrar por nomes de utilizadores e grupos de utilizadores**. Pode especificar os nomes dos utilizadores e/ou dos grupos de utilizadores para os quais o acesso aos recursos da Internet é controlado de acordo com a regra.

- **Agendamento de regras**. Pode especificar o agendamento de regra. O agendamento de regra determina o período durante o qual o Kaspersky Endpoint Security monitoriza o acesso aos recursos da Internet abrangidos pela regra.

Após a instalação do Kaspersky Endpoint Security, a lista de regras do componente Controlo de Internet não está vazia. A *Regra predefinida* está predefinida. Esta regra é aplicada a quaisquer recursos da Web que não estão abrangidos por outras regras e permite ou bloqueia o acesso a estes recursos da Web a todos os utilizadores.

Cada regra tem uma prioridade. Quanto mais alta for a posição de uma regra na lista, mais alta será a sua prioridade. Se um site for adicionado a várias regras, o Controlo de Internet regula o acesso ao site com base na regra com a prioridade mais alta. Por exemplo, o Kaspersky Endpoint Security pode identificar um portal empresarial como uma rede social. Para restringir o acesso a redes sociais e fornecer acesso ao portal da Web empresarial, crie duas regras: uma regra de bloqueio para a categoria de site *Redes sociais* e uma regra de permissão para o portal da Web empresarial. A regra de acesso para o portal da Web empresarial deve ter uma prioridade mais alta que a regra de acesso para redes sociais.

Como adicionar uma regra de recurso da Web na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança** → **Controlo de Internet**.
4. Selecione a caixa de verificação **Controlo de Internet**.
5. No bloco **Definições do Controlo de Internet**, clique no botão **Adicionar**.

   Abre-se a janela **Regra de acesso a recursos da Internet**.
6. Configure a regra de acesso aos recursos da Web (consulte a tabela abaixo).
7. Se pretender que o Controlo de Internet termine a ligação com o recurso da Web proibido imediatamente após a aplicação da política, selecione a caixa de verificação **Termine as sessões do navegador do utilizador ativas depois de a regra ser aplicada**.

O Controlo de Internet permite desconectar imediatamente recursos da Web apenas em navegadores. Para outras aplicações, o Controlo de Internet restringe apenas novas ligações.

Se a caixa de verificação estiver desmarcada, o Controlo de Internet restringe apenas as novas ligações a recursos da Web proibidos. O Controlo de Internet não encerra ligações ativas.

8. Guarde as suas alterações.

Como adicionar uma regra de acesso aos recursos da Web na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

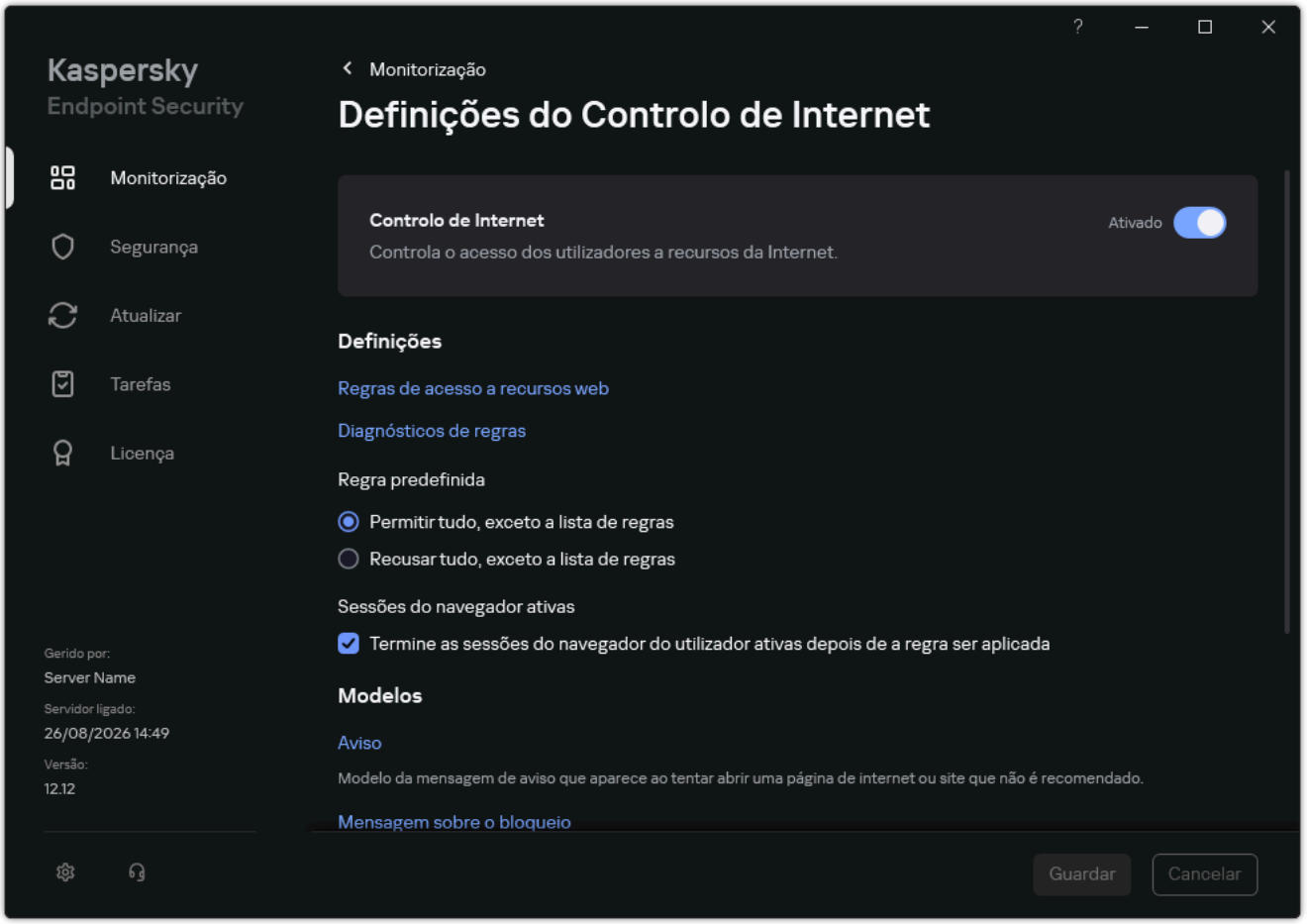
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Security Controls** → **Web Control**.
5. Ative o botão de alternar **Web Control ENABLED**.
6. No bloco **Rules list**, clique no botão **Add**.
7. Configure a regra de acesso aos recursos da Web (consulte a tabela abaixo).
8. Se pretender que o Controlo de Internet termine a ligação com o recurso da Web proibido imediatamente após a aplicação da política, selecione a caixa de verificação **Terminate active user browser sessions after the rule is applied**.

   O Controlo de Internet permite desconectar imediatamente recursos da Web apenas em navegadores. Para outras aplicações, o Controlo de Internet restringe apenas novas ligações.

   Se a caixa de verificação estiver desmarcada, o Controlo de Internet restringe apenas as novas ligações a recursos da Web proibidos. O Controlo de Internet não encerra ligações ativas.
9. Guarde as suas alterações.

Como adicionar uma regra de acesso de recurso da Web na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Internet**.



Definições do Controlo de Internet

3. Ative o botão de alternar **Controlo de Internet**.
4. No bloco **Definições**, clique no botão **Regras de acesso a recursos web**.
5. Na janela que abre, clique no botão **Adicionar**.

   Abre-se a janela **Regra de acesso a recursos da Internet**.
6. Configure a regra de acesso aos recursos da Web (consulte a tabela abaixo).
7. Se pretender que o Controlo de Internet termine a ligação com o recurso da Web proibido imediatamente após a aplicação da política, selecione a caixa de verificação **Termine as sessões do navegador do utilizador ativas depois de a regra ser aplicada**.

   > O Controlo de Internet permite desconectar imediatamente recursos da Web apenas em navegadores. Para outras aplicações, o Controlo de Internet restringe apenas novas ligações.

   Se a caixa de verificação estiver desmarcada, o Controlo de Internet restringe apenas as novas ligações a recursos da Web proibidos. O Controlo de Internet não encerra ligações ativas.
8. Guarde as suas alterações.

Como resultado, a nova regra do Controlo de Internet é adicionada à lista. Se necessário, altere a prioridade da regra do Controlo de Internet. Também pode utilizar o botão de alternar para desativar a regra de acesso a recursos Web em qualquer altura sem a remover da lista.

Parâmetros da regra do Controlo de Internet

Parâmetro	Descrição
Nome da regra	Nome da regra do Controlo de Internet.
Condição	• **Ativada**. • **Desativada**. Pode usar o botão de alternar para desativar a regra de acesso a recursos da Internet a qualquer momento.
Ação	• **Permitir**. O Controlo de Internet permite o acesso ao recursos da Web que correspondem aos parâmetros da regra. • **Bloquear**. O Controlo da Internet bloqueia o acesso aos recursos da Web que correspondem aos parâmetros da regra e apresenta uma mensagem de acesso negado ao site. • **Avisar**. Quando o utilizador tenta obter acesso a um recurso da Web que corresponde à regra, o Controlo de Internet exibe um aviso de que não é aconselhável visitar o recurso de Internet. Utilizando as ligações da mensagem de aviso, o utilizador pode obter acesso ao recurso da Internet solicitado.
Conteúdo do filtro	• **Por categorias de conteúdo**. Pode controlar o acesso dos utilizadores aos recursos da Internet por categoria (por exemplo, a categoria *Redes sociais*). • **Por tipos de dados**. Pode controlar o acesso dos utilizadores aos recursos da Internet com base no tipo específico dos dados publicados (por exemplo, *Gráficos*).
Endereços	• **A todos os endereços**. O Controlo de Internet não filtra recursos da Internet por endereço. • **Aos endereços individuais**. O Controlo de Internet filtra apenas os endereços de recursos da Internet da lista. Pode introduzir um endereço da Web ou usar máscaras. Também pode exportar uma lista de endereços de recursos da Internet a partir de um ficheiro TXT. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio. Se a Verificação de ligações encriptadas estiver desativada, para o protocolo HTTPS só pode filtrar por nome do servidor.
Utilizadores	• **A todos os utilizadores**. O Controlo de Internet não filtra recursos da Internet para utilizadores específicos. • **A utilizadores individuais e/ou grupos**. O Controlo de Internet filtra recursos da Internet apenas para utilizadores específicos. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.
Agendamento de regras	O agendamento de regra determina o período durante o qual o Kaspersky Endpoint Security monitoriza o acesso aos recursos da Internet abrangidos pela regra. Por exemplo, pode restringir o acesso à Internet através de um navegador apenas durante o horário de expediente.

Filtro por endereços de recursos da Internet

Para controlar o acesso a recursos da Web individuais, tem de criar uma regra de Controlo de Internet, criar uma lista de endereços da Internet e selecionar uma ação de Controlo de Internet. Ao criar uma lista de endereços da Internet, pode introduzir endereços URL ou utilizar máscaras.

As regras podem incluir um agendamento de regras e uma lista de utilizadores aos quais a regra se aplica. Por exemplo, pode restringir o acesso a sites apenas durante o horário de trabalho ou permitir a visita a sites a utilizadores de determinados grupos.

Como ativar um filtro de endereço de recurso da Internet na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança → Controlo de Internet**.

4. Selecione a caixa de verificação **Controlo de Internet**.

5. No bloco **Definições do Controlo de Internet**, clique no botão **Adicionar**.

   Abre-se a janela **Regra de acesso a recursos da Internet**.

6. Configure a regra de acesso a recursos da Internet:

   a. No campo **Nome**, introduza o nome da regra.

   b. Na lista pendente **Aplicar aos endereços**, selecione **Aos endereços individuais**.

   c. Criar uma lista de endereços de recursos da Internet. Pode introduzir um endereço da Web ou usar máscaras. Também pode exportar uma lista de endereços de recursos da Internet a partir de um ficheiro TXT.

   > Se a Verificação de ligações encriptadas estiver desativada, para o protocolo HTTPS só pode filtrar por nome do servidor.

   d. Na lista pendente **Aplicar aos utilizadores**, selecione o filtro relevante para os utilizadores:

   - **A todos os utilizadores**. O Controlo de Internet não filtra recursos da Internet por endereço.
   - **Para utilizadores individuais ou grupos**. O Controlo de Internet filtra apenas os endereços de recursos da Internet da lista. Pode introduzir um endereço da Web ou usar máscaras. Também pode exportar uma lista de endereços de recursos da Internet a partir de um ficheiro TXT. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

   e. Na lista pendente **Ação**, selecione uma opção:

   - **Permitir**. O Controlo de Internet permite o acesso ao recursos da Web que correspondem aos parâmetros da regra.
   - **Bloquear**. O Controlo da Internet bloqueia o acesso aos recursos da Web que correspondem aos parâmetros da regra e apresenta uma mensagem de acesso negado ao site.
   - **Avisar**. Quando o utilizador tenta obter acesso a um recurso da Web que corresponde à regra, o Controlo de Internet exibe um aviso de que não é aconselhável visitar o recurso de Internet. Utilizando as ligações da mensagem de aviso, o utilizador pode obter acesso ao recurso da Internet solicitado.

   f. Na lista pendente **Agendamento de regras**, selecione um agendamento ou crie um novo agendamento.

7. Se pretender que o Controlo de Internet termine a ligação com o recurso da Web proibido imediatamente após a aplicação da política, selecione a caixa de verificação **Termine as sessões do navegador do utilizador ativas depois de a regra ser aplicada**.

   > O Controlo de Internet permite desconectar imediatamente recursos da Web apenas em navegadores. Para outras aplicações, o Controlo de Internet restringe apenas novas ligações.

Se a caixa de verificação estiver desmarcada, o Controlo de Internet restringe apenas as novas ligações a recursos da Web proibidos. O Controlo de Internet não encerra ligações ativas.

8. Guarde as suas alterações.

Como ativar um filtro de endereço de recurso da Internet na Consola Web e Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Security Controls** → **Web Control**.
5. Ative o botão de alternar **Web Control ENABLED**.
6. No bloco **Rules list**, clique no botão **Add**.
7. Configure a regra de acesso a recursos da Internet:
   a. No campo **Rule name**, introduza o nome da regra.
   b. Selecione o estado **Enabled** para a regra de acesso a recursos da Internet.

      Pode utilizar o botão de alternar para desativar a regra de acesso a recursos Web em qualquer altura sem a remover da lista.
   c. No bloco **Action**, selecione a opção relevante:
      - **Allow**. O Controlo de Internet permite o acesso ao recursos da Web que correspondem aos parâmetros da regra.
      - **Block**. O Controlo da Internet bloqueia o acesso aos recursos da Web que correspondem aos parâmetros da regra e apresenta uma mensagem de acesso negado ao site.
      - **Inform**. Quando o utilizador tenta obter acesso a um recurso da Web que corresponde à regra, o Controlo de Internet exibe um aviso de que não é aconselhável visitar o recurso de Internet. Utilizando as ligações da mensagem de aviso, o utilizador pode obter acesso ao recurso da Internet solicitado.
   d. Em **Scope**, selecione **Individual websites**.
   e. Configure o filtro de conteúdos:
      - **Individual address**. Criar uma lista de endereços de recursos da Internet. Pode introduzir um endereço da Web ou usar máscaras. Também pode exportar uma lista de endereços de recursos da Internet a partir de um ficheiro TXT.

        Se a Verificação de ligações encriptadas estiver desativada, para o protocolo HTTPS só pode filtrar por nome do servidor.
      - **Data type**. Pode controlar o acesso dos utilizadores aos recursos da Internet com base no tipo específico dos dados publicados (por exemplo, *Gráficos*).

f. Sob **User or group**, selecione os utilizadores aos quais pretende que o Controlo de Internet aplique a regra.

O Controlo de Internet filtra apenas os endereços de recursos da Internet da lista. Pode introduzir um endereço da Web ou usar máscaras. Também pode exportar uma lista de endereços de recursos da Internet a partir de um ficheiro TXT. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

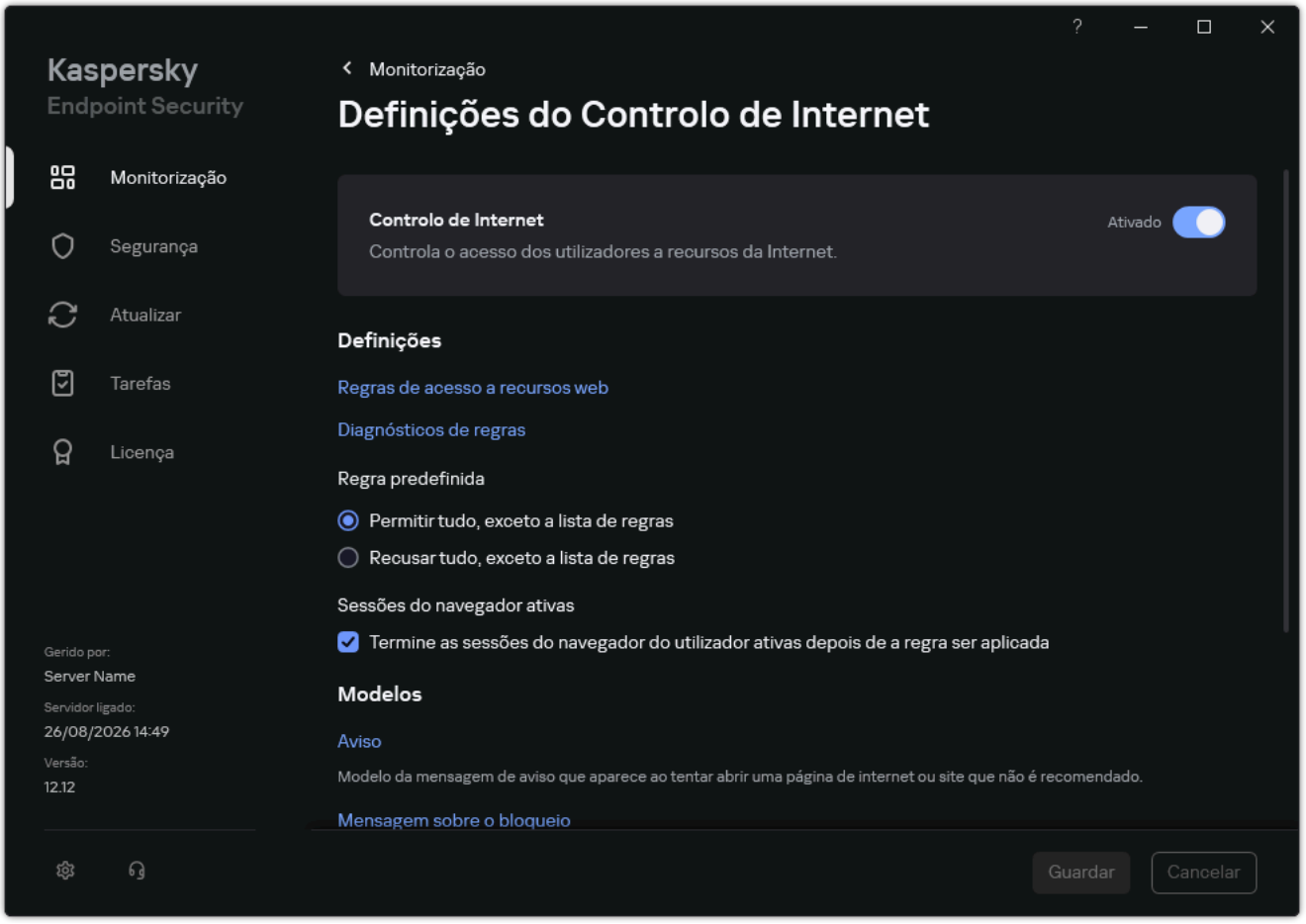
g. No bloco **Access schedule**, selecione um agendamento ou crie um novo agendamento.

8. Guarde as suas alterações.

Como ativar um filtro de endereço de recurso da Internet na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Internet**.



Definições do Controlo de Internet

3. No bloco **Definições**, clique no botão **Regras de acesso a recursos web**.

4. Na janela que abre, clique no botão **Adicionar**.

Abre-se a janela **Regra de acesso a recursos da Internet**.

5. No campo **Nome da regra**, introduza o nome da regra.

6. Selecione o estado **Ativada** para a regra de acesso a recursos da Internet.

Pode usar o botão de alternar para desativar a regra de acesso a recursos da Internet a qualquer momento.

7. No bloco **Ação**, selecione a opção relevante:

   - **Permitir**. O Controlo de Internet permite o acesso ao recursos da Web que correspondem aos parâmetros da regra.
   - **Bloquear**. O Controlo da Internet bloqueia o acesso aos recursos da Web que correspondem aos parâmetros da regra e apresenta uma mensagem de acesso negado ao site.
   - **Avisar**. Quando o utilizador tenta obter acesso a um recurso da Web que corresponde à regra, o Controlo de Internet exibe um aviso de que não é aconselhável visitar o recurso de Internet. Utilizando as ligações da mensagem de aviso, o utilizador pode obter acesso ao recurso da Internet solicitado.

8. Em **Endereços**, selecione **Aos endereços individuais**.

   Criar uma lista de endereços de recursos da Internet. Pode introduzir um endereço da Web ou usar máscaras. Também pode exportar uma lista de endereços de recursos da Internet a partir de um ficheiro TXT.

   > Se a Verificação de ligações encriptadas estiver desativada, para o protocolo HTTPS só pode filtrar por nome do servidor.

9. No bloco **Utilizadores**, selecione o filtro relevante para os utilizadores:

   - **A todos os utilizadores**. O Controlo de Internet não filtra recursos da Internet para utilizadores específicos.
   - **A utilizadores individuais e/ou grupos**. O Controlo de Internet filtra apenas os endereços de recursos da Internet da lista. Pode introduzir um endereço da Web ou usar máscaras. Também pode exportar uma lista de endereços de recursos da Internet a partir de um ficheiro TXT. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

10. Na lista pendente **Agendamento de regras**, selecione um agendamento ou crie um novo agendamento.

11. Se pretender que o Controlo de Internet termine a ligação com o recurso da Web proibido imediatamente após a aplicação da política, selecione a caixa de verificação **Termine as sessões do navegador do utilizador ativas depois de a regra ser aplicada**.

    > O Controlo de Internet permite desconectar imediatamente recursos da Web apenas em navegadores. Para outras aplicações, o Controlo de Internet restringe apenas novas ligações.

    Se a caixa de verificação estiver desmarcada, o Controlo de Internet restringe apenas as novas ligações a recursos da Web proibidos. O Controlo de Internet não encerra ligações ativas.

12. Guarde as suas alterações.

Como resultado, a nova regra do Controlo de Internet é adicionada à lista. Se necessário, altere a prioridade da regra do Controlo de Internet. Também pode utilizar o botão de alternar para desativar a regra de acesso a recursos Web em qualquer altura sem a remover da lista.

Filtro por conteúdo de recursos da Internet

Para controlar o acesso por conteúdo de recursos da Web, o Controlo de Internet fornece um filtro de categoria e um filtro de tipo de dados.

Os sites são categorizados de acordo com o serviço de nuvem do Kaspersky Security Network, a análise heurística e a base de dados de sites conhecidos (incluídos nas bases de dados da aplicação). Por exemplo, pode restringir o acesso do utilizador à categoria *Redes sociais* ou a outras categorias.

Pode restringir o acesso do utilizador a um site com base no tipo de dados, por exemplo, para ocultar imagens. O Kaspersky Endpoint Security determina o tipo de dados com base no formato do ficheiro e não com base na sua extensão. O Controlo de Internet distingue os seguintes tipos de dados:

- Vídeo
- Som
- Ficheiros de aplicações de escritório
- Ficheiros executáveis
- Arquivos
- Gráficos
- Scripts

O Kaspersky Endpoint Security não verifica ficheiros dentro de arquivos. Por exemplo, se os ficheiros de imagem forem colocados num arquivo, o Kaspersky Endpoint Security identifica o tipo de dados *Arquivos* e não *Gráficos*.

As regras podem incluir um agendamento de regras e uma lista de utilizadores aos quais a regra se aplica. Por exemplo, pode restringir o acesso a sites apenas durante o horário de trabalho ou permitir a visita a sites a utilizadores de determinados grupos.

Como ativar um filtro de conteúdo de recursos da Web na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança** → **Controlo de Internet**.
4. Selecione a caixa de verificação **Controlo de Internet**.
5. No bloco **Definições do Controlo de Internet**, clique no botão **Adicionar**.

   Abre-se a janela **Regra de acesso a recursos da Internet**.

6. Configure a regra de acesso a recursos da Internet:

   a. No campo **Nome**, introduza o nome da regra.

   b. Na lista pendente **Conteúdo de filtro**, selecione o filtro de conteúdo relevante:

   - **Por categorias de conteúdo**. Pode controlar o acesso dos utilizadores aos recursos da Internet por categoria (por exemplo, a categoria *Redes sociais*).
   - **Por tipos de dados**. Pode controlar o acesso dos utilizadores aos recursos da Internet com base no tipo específico dos dados publicados (por exemplo, *Gráficos*).
   - **Por categorias de conteúdo e tipos de dados**. Os filtros por categorias de conteúdo e tipos de dados estão ativados.

   Depois de selecionar os filtros, configure os parâmetros de filtragem.

   c. Na lista pendente **Aplicar aos utilizadores**, selecione o filtro relevante para os utilizadores:

   - **A todos os utilizadores**. O Controlo de Internet não filtra recursos da Internet por endereço.
   - **Para utilizadores individuais ou grupos**. O Controlo de Internet filtra apenas os endereços de recursos da Internet da lista. Pode introduzir um endereço da Web ou usar máscaras. Também pode exportar uma lista de endereços de recursos da Internet a partir de um ficheiro TXT. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

   d. Na lista pendente **Ação**, selecione uma opção:

   - **Permitir**. O Controlo de Internet permite o acesso ao recursos da Web que correspondem aos parâmetros da regra.
   - **Bloquear**. O Controlo da Internet bloqueia o acesso aos recursos da Web que correspondem aos parâmetros da regra e apresenta uma mensagem de acesso negado ao site.
   - **Avisar**. Quando o utilizador tenta obter acesso a um recurso da Web que corresponde à regra, o Controlo de Internet exibe um aviso de que não é aconselhável visitar o recurso de Internet. Utilizando as ligações da mensagem de aviso, o utilizador pode obter acesso ao recurso da Internet solicitado.

   e. Na lista pendente **Agendamento de regras**, selecione um agendamento ou crie um novo agendamento.

7. Se pretender que o Controlo de Internet termine a ligação com o recurso da Web proibido imediatamente após a aplicação da política, selecione a caixa de verificação **Termine as sessões do navegador do utilizador ativas depois de a regra ser aplicada**.

   O Controlo de Internet permite desconectar imediatamente recursos da Web apenas em navegadores. Para outras aplicações, o Controlo de Internet restringe apenas novas ligações.

   Se a caixa de verificação estiver desmarcada, o Controlo de Internet restringe apenas as novas ligações a recursos da Web proibidos. O Controlo de Internet não encerra ligações ativas.

8. Guarde as suas alterações.

Como ativar um filtro de conteúdo de recursos da Web na Consola Web e Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

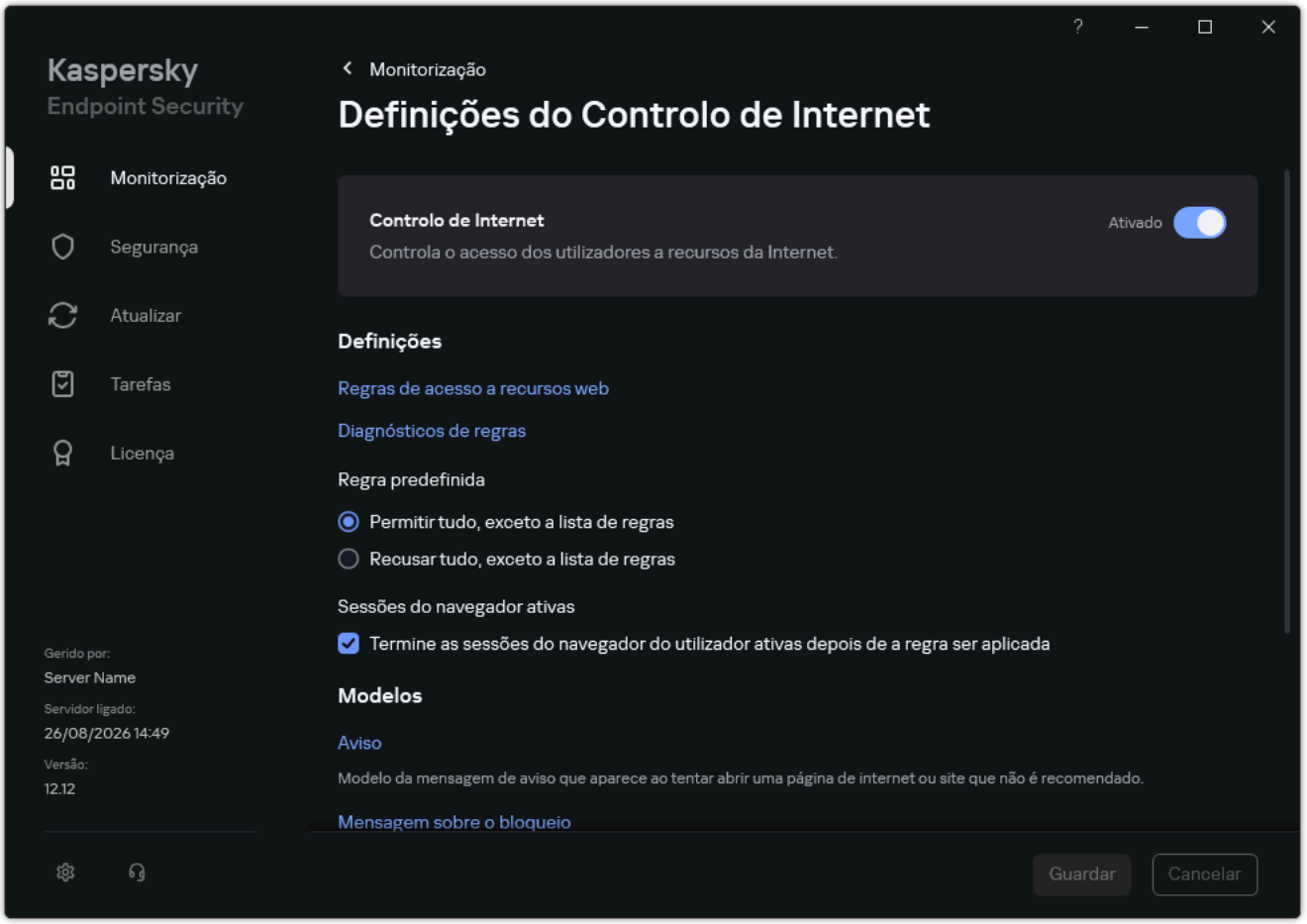
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Security Controls** → **Web Control**.
5. Ative o botão de alternar **Web Control ENABLED**.
6. No bloco **Rules list**, clique no botão **Add**.
7. Configure a regra de acesso a recursos da Internet:
   a. No campo **Rule name**, introduza o nome da regra.
   b. Selecione o estado **Enabled** para a regra de acesso a recursos da Internet.

      Pode usar o botão de alternar para desativar a regra de acesso a recursos da Internet a qualquer momento.
   c. No bloco **Action**, selecione a opção relevante:
      - **Allow**. O Controlo de Internet permite o acesso ao recursos da Web que correspondem aos parâmetros da regra.
      - **Block**. O Controlo da Internet bloqueia o acesso aos recursos da Web que correspondem aos parâmetros da regra e apresenta uma mensagem de acesso negado ao site.
      - **Inform**. Quando o utilizador tenta obter acesso a um recurso da Web que corresponde à regra, o Controlo de Internet exibe um aviso de que não é aconselhável visitar o recurso de Internet. Utilizando as ligações da mensagem de aviso, o utilizador pode obter acesso ao recurso da Internet solicitado.
   d. Em **Scope**, selecione **Content category**.
   e. Configure o filtro de conteúdos:
      - **Content category**. Pode controlar o acesso dos utilizadores aos recursos da Internet por categoria (por exemplo, a categoria *Redes sociais*).
      - **Data type**. Pode controlar o acesso dos utilizadores aos recursos da Internet com base no tipo específico dos dados publicados (por exemplo, *Gráficos*).
   f. Sob **User or group**, selecione os utilizadores aos quais pretende que o Controlo de Internet aplique a regra.

      O Controlo de Internet filtra apenas os endereços de recursos da Internet da lista. Pode introduzir um endereço da Web ou usar máscaras. Também pode exportar uma lista de endereços de recursos da Internet a partir de um ficheiro TXT. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.
   g. No bloco **Access schedule**, selecione um agendamento ou crie um novo agendamento.
8. Guarde as suas alterações.

Como ativar um filtro de conteúdo de recursos da Web na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Internet**.



Definições do Controlo de Internet

3. No bloco **Definições**, clique no botão **Regras de acesso a recursos web**.
4. Na janela que abre, clique no botão **Adicionar**.

   Abre-se a janela **Regra de acesso a recursos da Internet**.
5. No campo **Nome da regra**, introduza o nome da regra.
6. Selecione o estado **Ativada** para a regra de acesso a recursos da Internet.

   Pode usar o botão de alternar para desativar a regra de acesso a recursos da Internet a qualquer momento.
7. No bloco **Ação**, selecione a opção relevante:

   - **Permitir**. O Controlo de Internet permite o acesso ao recursos da Web que correspondem aos parâmetros da regra.
   - **Bloquear**. O Controlo da Internet bloqueia o acesso aos recursos da Web que correspondem aos parâmetros da regra e apresenta uma mensagem de acesso negado ao site.
   - **Avisar**. Quando o utilizador tenta obter acesso a um recurso da Web que corresponde à regra, o Controlo de Internet exibe um aviso de que não é aconselhável visitar o recurso de Internet. Utilizando as ligações da mensagem de aviso, o utilizador pode obter acesso ao recurso da Internet solicitado.

8. No bloco **Conteúdo do filtro**, selecione o filtro de conteúdos relevante:

   - **Por categorias de conteúdo**. Pode controlar o acesso dos utilizadores aos recursos da Internet por categoria (por exemplo, a categoria *Redes sociais*).
   - **Por tipos de dados**. Pode controlar o acesso dos utilizadores aos recursos da Internet com base no tipo específico dos dados publicados (por exemplo, *Gráficos*).

   Para configurar o filtro de conteúdos:

   a. Clique na hiperligação **Definições**.

   b. Selecione as caixas de verificação junto dos nomes das categorias de conteúdo e/ou tipos de dados pretendidas.

   Selecionar a caixa de verificação junto ao nome de uma categoria de conteúdo e/ou tipo de dados significa que o Kaspersky Endpoint Security aplica a regra para controlar o acesso aos recursos da Internet que pertencem às categorias de conteúdo selecionadas e/ou categorias de tipos de dados.

   c. Regresse à janela para configurar a regra de acesso a recursos da Internet.

9. No bloco **Utilizadores**, selecione o filtro relevante para os utilizadores:

   - **A todos os utilizadores**. O Controlo de Internet não filtra recursos da Internet por endereço.
   - **A utilizadores individuais e/ou grupos**. O Controlo de Internet filtra apenas os endereços de recursos da Internet da lista. Pode introduzir um endereço da Web ou usar máscaras. Também pode exportar uma lista de endereços de recursos da Internet a partir de um ficheiro TXT. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio. Para criar uma lista de utilizadores aos quais pretende aplicar a regra:

     a. Clique em **Adicionar**.

     b. Na janela que abre, selecione os utilizadores ou os grupos de utilizadores aos quais pretende aplicar a regra de acesso a recursos da Internet.

     c. Regresse à janela para configurar a regra de acesso a recursos da Internet.

10. Na lista pendente **Agendamento de regras**, selecione o nome da agenda necessária ou crie uma agenda nova com base no agendamento de regra selecionado. Para tal:

    a. Clique em **Editar ou adicionar novo**.

    b. Na janela que abre, clique no botão **Adicionar**.

    c. Na janela que abre, insira o nome do agendamento da regra.

    d. Configure o agendamento de acesso a recursos da Internet para os utilizadores.

    e. Regresse à janela para configurar a regra de acesso a recursos da Internet.

11. Se pretender que o Controlo de Internet termine a ligação com o recurso da Web proibido imediatamente após a aplicação da política, selecione a caixa de verificação **Termine as sessões do navegador do utilizador ativas depois de a regra ser aplicada**.

O Controlo de Internet permite desconectar imediatamente recursos da Web apenas em navegadores. Para outras aplicações, o Controlo de Internet restringe apenas novas ligações.

Se a caixa de verificação estiver desmarcada, o Controlo de Internet restringe apenas as novas ligações a recursos da Web proibidos. O Controlo de Internet não encerra ligações ativas.

12. Guarde as suas alterações.

Como resultado, a nova regra do Controlo de Internet é adicionada à lista. Se necessário, altere a prioridade da regra do Controlo de Internet. Também pode utilizar o botão de alternar para desativar a regra de acesso a recursos Web em qualquer altura sem a remover da lista.

Testar regras de acesso a recursos da Internet

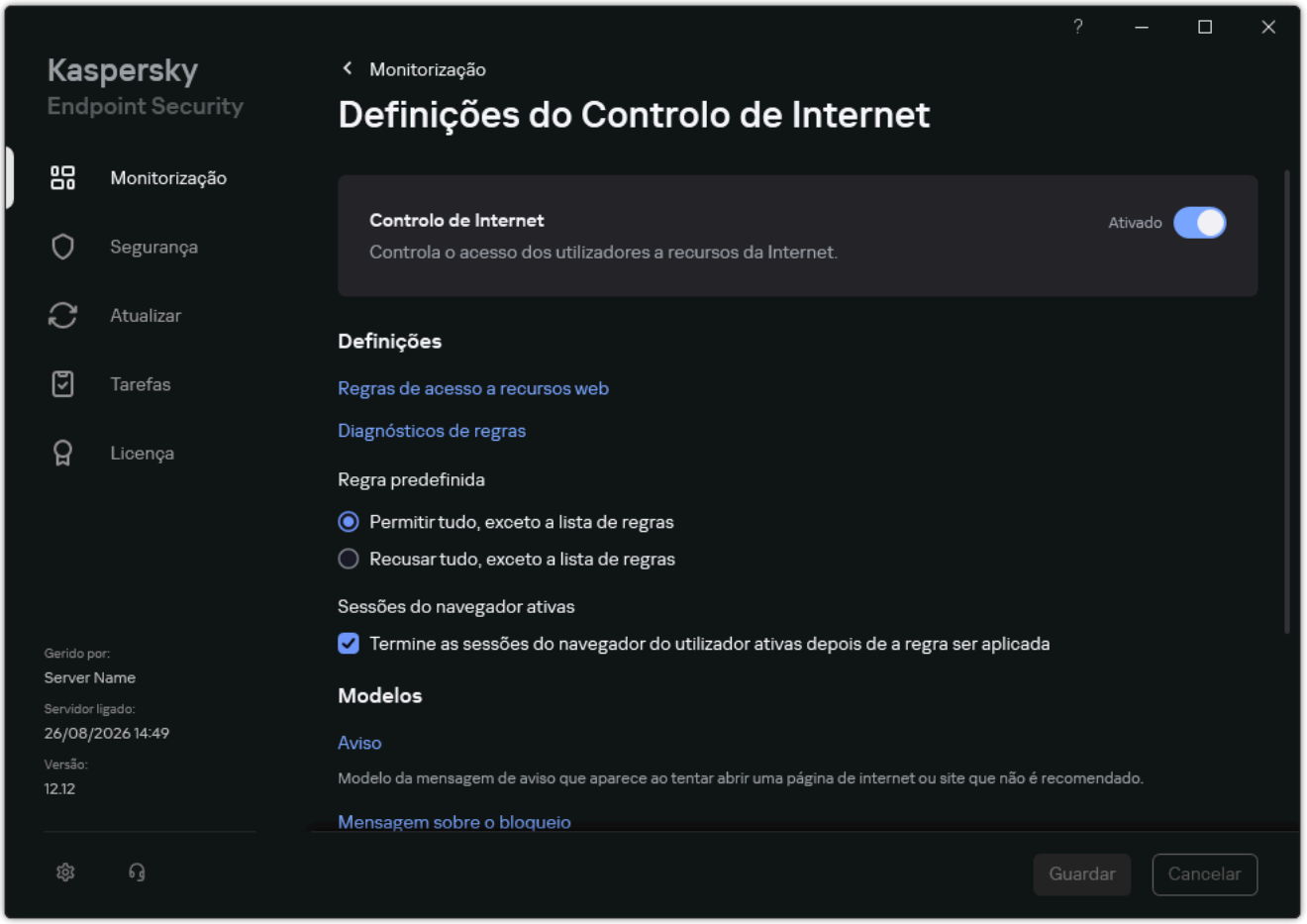
Ao configurar o Controlo de Internet, poderá bloquear inadvertidamente o acesso aos recursos de Internet de que os utilizadores necessitam para o seu trabalho. Para descobrir qual é a regra de Controlo de Internet que está a bloquear o acesso aos recursos da Web, pode utilizar a ferramenta *Diagnóstico de regras do Controlo de Internet*. A ferramenta Diagnósticos de regras do Controlo de Internet está disponível apenas na interface do Kaspersky Endpoint Security. Na consola do Kaspersky Security Center, não é possível descobrir que regra de Controlo de Internet inclui um determinado recurso.

Se o utilizador considerar que o recurso da Internet está bloqueado indevidamente, pode clicar na ligação na mensagem de notificação de bloqueio do recurso da Internet para enviar uma mensagem pré-gerada para o administrador local da rede da empresa.

Para testar as regras de acesso do recurso da Internet:

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Internet**.



Definições do Controlo de Internet

3. No bloco **Definições**, clique na ligação **Diagnósticos de regras**.

   Abre-se a janela **Diagnósticos de regras**.

4. Se pretender testar as regras que o Kaspersky Endpoint Security utiliza para controlar o acesso a um recurso da Internet específico, selecione a caixa de verificação **Especifique o endereço**. Introduza o endereço do recurso da Web no campo abaixo.

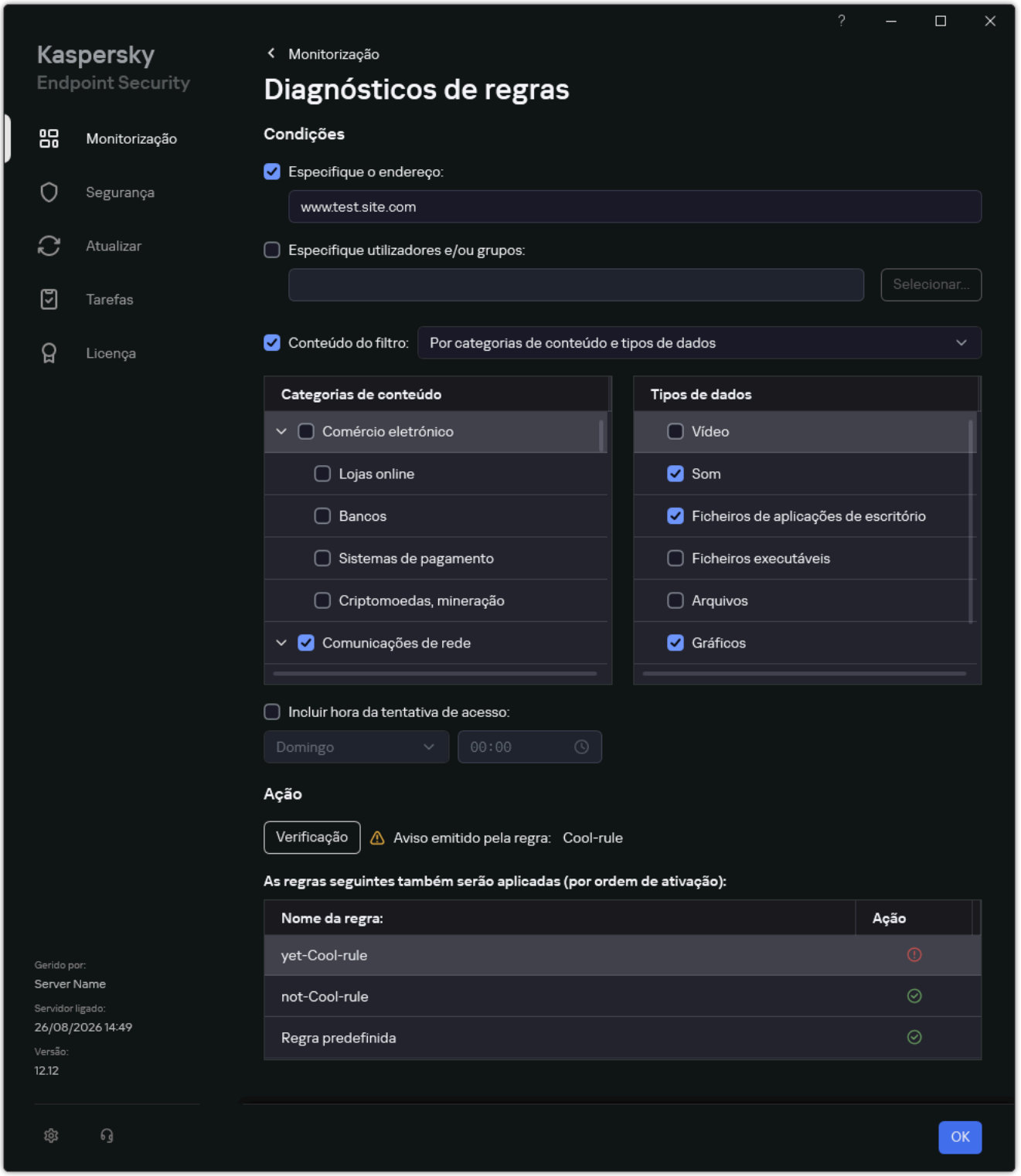
5. Se pretender testar as regras que o Kaspersky Endpoint Security utiliza para controlar o acesso aos recursos da Internet para utilizadores e/ou grupos de utilizadores especificados, indique uma lista de utilizadores e/ou grupos de utilizadores.

6. Se pretender testar as regras que o Kaspersky Endpoint Security utiliza para controlar o acesso a recursos da Internet de determinadas categorias de conteúdo e/ou categorias de tipos de dados, selecione a caixa de verificação **Conteúdo do filtro** e escolha a opção relevante na lista pendente (**Por categorias de conteúdo**, **Por tipos de dados** ou **Por categorias de conteúdo e tipos de dados**).

7. Se pretender testar as regras tendo em conta a hora e o dia da semana em que é efetuada uma tentativa de acesso aos recursos de Internet especificados nas condições de diagnósticos de regras, selecione a caixa de verificação **Incluir hora da tentativa de acesso**. Em seguida, especifique o dia da semana e a hora.

8. Clique em **Verificação**.

A conclusão do teste é seguida por uma mensagem com informações sobre a ação realizada pelo Kaspersky Endpoint Security, de acordo com a primeira regra ativada com a tentativa de aceder ao recurso da Internet especificado (permitir, bloquear ou aviso). A primeira regra a ser ativada é a regra com a classificação na lista de regras de Controlo de Internet mais elevada do que as restantes regras que correspondem às condições de diagnóstico. A mensagem é apresentada à direita do botão **Verificação**. A tabela seguinte indica as restantes regras ativadas, especificando a ação realizada pelo Kaspersky Endpoint Security. As regras são indicadas por ordem de prioridade decrescente.



Exportar e importar regras de Controlo de Internet

Pode exportar a lista de regras de Controlo de Internet para um ficheiro XML ou JSON. Em seguida, pode modificar o ficheiro para, por exemplo, adicionar um grande número de endereços do mesmo tipo. Pode utilizar a função de exportação/importação para fazer uma cópia de segurança da lista de regras de Controlo de Internet ou para migrar a lista para um servidor diferente.

Como exportar e importar uma lista de regras de Controlo de Internet na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança → Controlo de Internet**.
4. Para exportar a lista de regras de Controlo de Internet:
   a. Selecione as regras que pretende exportar. Para selecionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.
      Se não tiver selecionado nenhuma regra, o Kaspersky Endpoint Security exportará todas as regras.
   b. Clique na hiperligação **Exportar**.
   c. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de regras e selecione a pasta onde pretende guardar este ficheiro.
   d. Guardar o ficheiro.
      O Kaspersky Endpoint Security exporta a lista de regras para o ficheiro XML.
5. Para importar a lista de regras de Controlo de Internet:
   a. Clique na hiperligação **Importar**.
      Na janela que se abre, selecione o ficheiro XML a partir do qual pretende importar a lista de regras.
   b. Abrir o ficheiro.
      Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro XML.
6. Guarde as suas alterações.

Como exportar e importar uma lista de regras de Controlo de Internet na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Security Controls → Web Control**.

5. Para exportar a lista de regras, no bloco **Rules list**:

   a. Selecione as regras que pretende exportar.

   b. Selecione o botão → **Export**.

      O Kaspersky Endpoint Security exporta a lista de regras para um ficheiro JSON na pasta de transferências predefinida.

6. Para importar a lista de regras, no bloco **Rules list**:

   a. Selecione o botão → **Import**.

      Na janela que se abre, selecione o ficheiro JSON a partir do qual pretende importar a lista de regras.

   b. Abrir o ficheiro.

      Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro JSON.

7. Guarde as suas alterações.

Exportar e importar endereços de recursos da Internet da regra de Controlo de Internet

Se tiver criado uma lista de endereços de recursos da Internet numa regra de acesso a recursos da Internet, pode exportá-la para um ficheiro:

- Em formato TXT na Consola de Administração (MMC)
- Em formato JSON na Web Console
- Em formato CSV na interface da aplicação

Posteriormente, pode importar a lista deste ficheiro, de modo a evitar ter de criar manualmente uma nova lista de endereços de recursos da Internet ao configurar uma regra de acesso. A opção de exportação e importação da lista de endereços de recursos da Internet pode ser útil se, por exemplo, criar regras de acesso com parâmetros semelhantes.

Também pode exportar/importar todas as regras de Controlo de Internet e não apenas os endereços dos recursos da Internet de uma regra individual.

Como exportar/importar endereços dos recursos da Internet da regra de Controlo de Internet na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Controlos de segurança** → **Controlo de Internet**.

5. No bloco **Definições do Controlo de Internet**, selecione a regra cuja lista de endereços de recursos da Internet pretende exportar ou importar.

   São apresentadas as propriedades da regra de Controlo de Internet.

6. Para exportar a lista de recursos da Internet, faça o seguinte na lista de endereços:

   a. Selecione os endereços que pretende exportar.

      Se não tiver selecionado nenhum endereço, o Kaspersky Endpoint Security exportará todos os endereços.

   b. Selecione o botão .

   c. Na janela que abre, introduza o nome do ficheiro TXT para o qual pretende exportar a lista de endereços de recursos de Internet e selecione a pasta onde pretende guardar este ficheiro.

   d. Guardar o ficheiro.

      O Kaspersky Endpoint Security exporta a lista de endereços de recursos da Internet para um ficheiro TXT.

7. Para importar a lista de recursos da Internet, faça o seguinte na lista de endereços:

   a. Selecione o botão .

      Na janela que se abre, selecione o ficheiro TXT do qual deseja importar a lista de recursos da Internet.

   b. Abrir o ficheiro.

      Se o computador já tiver uma lista de endereços, o Kaspersky Endpoint Security solicita-lhe a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro TXT.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como exportar/importar endereços dos recursos da Internet da regra de Controlo de Internet na Web Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Security Controls** → **Web Control**.

5. No bloco **Rules list**, selecione a regra cuja lista de endereços de recursos da Internet pretende exportar ou importar.

   São apresentadas as propriedades da regra de Controlo de Internet.

6. No bloco **Scope** → **Individual websites**, clique no botão **Edit**.

7. Para exportar a lista de recursos da Internet, faça o seguinte na lista de endereços:

   a. Selecione os endereços que pretende exportar.

   b. Selecione o botão → **Export**.

      O Kaspersky Endpoint Security exporta a lista de endereços dos recursos da Internet para um ficheiro JSON na pasta de transferências predefinida.

8. Para importar a lista de recursos da Internet, faça o seguinte na lista de endereços:

   a. Selecione o botão → **Import**.

      Na janela que se abre, selecione o ficheiro JSON do qual pretende importar a lista de endereços dos recursos da Internet.

   b. Abrir o ficheiro.

      Se o computador já tiver uma lista de endereços, o Kaspersky Endpoint Security solicita-lhe a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro JSON.

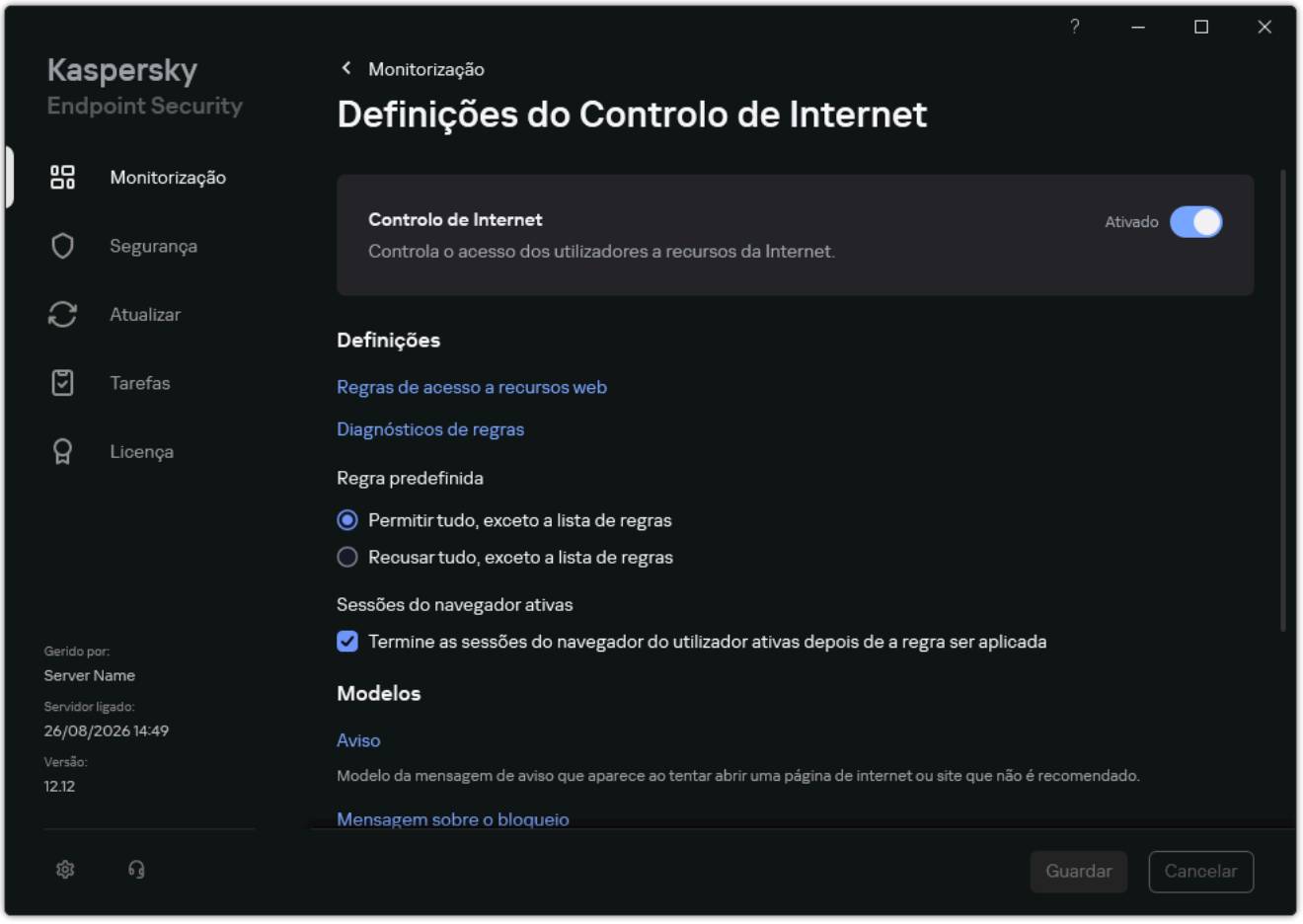
   Pode exportar e importar grupos de sites da mesma forma.

9. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como exportar/importar endereços dos recursos da Internet da regra de Controlo de Internet na interface da aplicação

1. Na janela principal da aplicação, clique no botão .

2. Na janela Application settings, selecione **Controlos de segurança** → **Controlo de Internet**.



Definições do Controlo de Internet

3. No bloco **Definições**, clique no botão **Regras de acesso a recursos web**.

4. Selecione a regra cuja lista de endereços de recursos da Internet pretende exportar ou importar.

5. Para exportar a lista de endereços da Internet fiáveis, faça o seguinte no bloco **Endereços**:

   a. Selecione os endereços que pretende exportar.

      Se não tiver selecionado nenhum endereço, o Kaspersky Endpoint Security exportará todos os endereços.

   b. Clique em **Exportar**.

   c. Na janela que abre, introduza o nome do ficheiro CSV para o qual pretende exportar a lista de endereços de recursos de Internet e selecione a pasta onde pretende guardar este ficheiro.

   d. Guardar o ficheiro.

      O Kaspersky Endpoint Security exporta a lista de endereços de recursos da Internet para um ficheiro CSV.

6. Para importar a lista de recursos da Internet, faça o seguinte no bloco **Endereços**:

   a. Clique em **Importar**.

      Na janela que se abre, selecione o ficheiro CSV do qual deseja importar a lista de recursos da Internet.

   b. Abrir o ficheiro.

      Se o computador já tiver uma lista de endereços, o Kaspersky Endpoint Security solicita-lhe a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro CSV.

7. Guarde as suas alterações.

Monitorizar atividade da Internet do utilizador

O Kaspersky Endpoint Security permite-lhe registar dados sobre visitas de utilizadores a todos os sites, incluindo sites permitidos. Isto permite-lhe obter o histórico completo das visualizações do navegador. O Kaspersky Endpoint Security envia eventos de atividade do utilizador para o Kaspersky Security Center, para o registo local do Kaspersky Endpoint Security e para o registo de eventos do Windows. Para receber eventos no Kaspersky Security Center, precisa de configurar as definições dos eventos numa política na Consola de Administração ou na Consola da Web. Pode também configurar a transmissão de eventos do Controlo de Internet por email e a apresentação de notificações no ecrã no computador do utilizador.

Navegadores que suportam a função de monitorização: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. A monitorização da atividade do utilizador não funciona noutros navegadores.

O Kaspersky Endpoint Security cria os seguintes eventos de atividade da Internet do utilizador:

- Bloquear o site (estado *Critical*).
- Visita a um site não recomendado (*Warning* estado).
- Visita a um site permitido (estado *Info*).

Antes de ativar o monitorização da atividade do utilizador na Internet, deve fazer o seguinte:

- Injetar um script de interação de página de Internet no tráfego de Internet (consulte as instruções abaixo). O script permite o registo de eventos do Controlo de Internet.
- Para monitorização do tráfego HTTPS, precisa de ativar a verificação de ligações encriptadas.

Injetar um script de interação de página de Internet

Como injetar um script de interação de página de Internet no tráfego de internet na Administration Console (MMC)

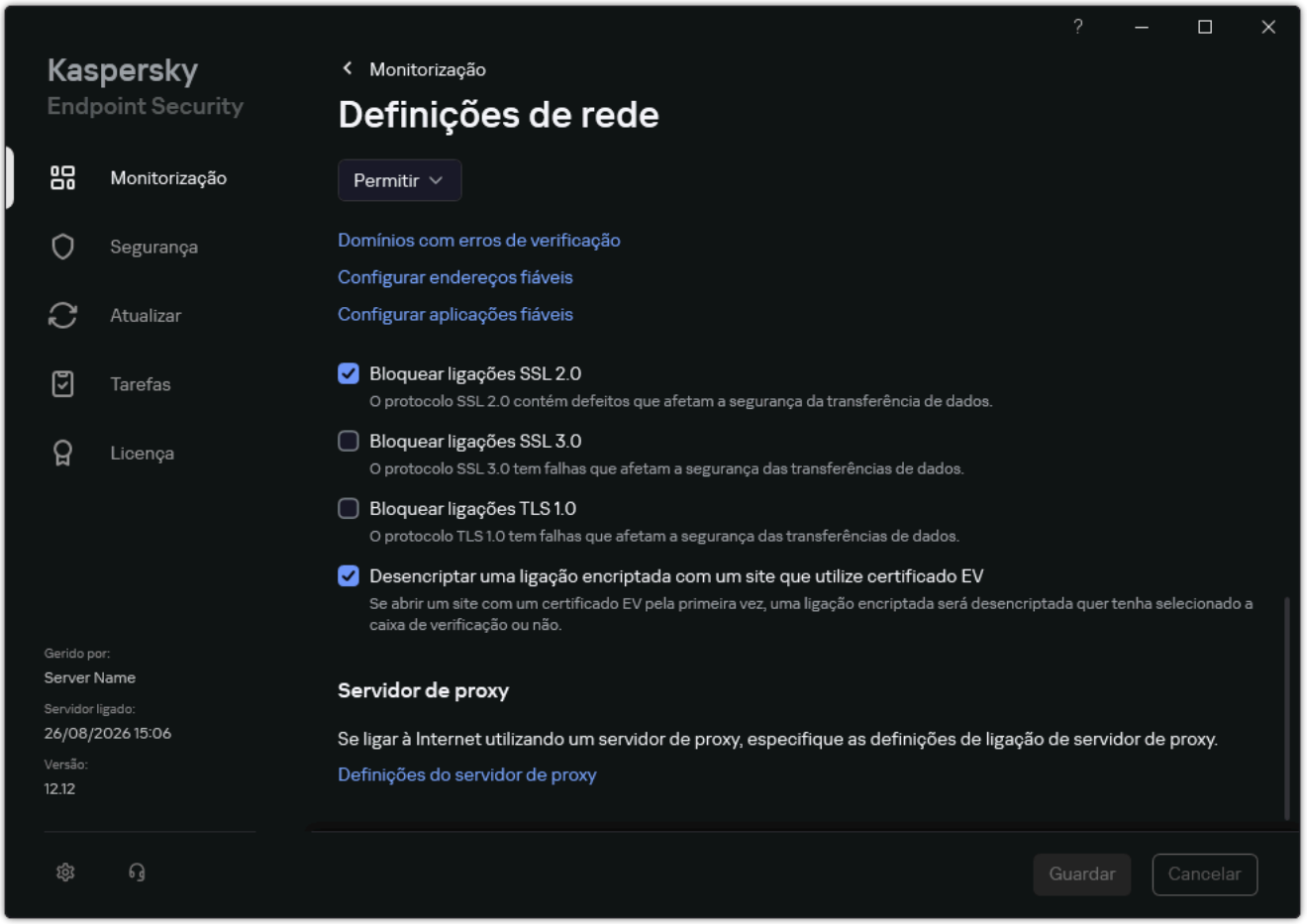
1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais** → **Definições de Rede**.
4. No bloco **Verificação de ligações encriptadas**, selecione a caixa de verificação **Injetar script no tráfego de Internet para interagir com páginas de Internet**.
5. Guarde as suas alterações.

Como injetar um script de interação de página de Internet no tráfego de internet na Web Console e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Na janela de política, selecione **General Settings** → **Network Settings**.
5. Sob **Monitoring of internet connections**, ative a opção **Monitoring of internet connections ENABLED**.
6. Guarde as suas alterações.

Como injetar um script de interação de página de Internet no tráfego de internet na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Definições de rede**.



Definições da rede de aplicações

3. No bloco **Processamento de tráfego**, selecione a caixa de verificação **Injetar script no tráfego de Internet para interagir com páginas de Internet**.
4. Guarde as suas alterações.

Como resultado, o Kaspersky Endpoint Security injetará um script de interação de página de Internet no tráfego de Internet. Este script permite o registo de eventos do Controlo de Internet para o registo de eventos da aplicação, registo de eventos do SO e relatórios.

Configurar o registo de eventos do Controlo de Internet

Para configurar o registo de eventos do Controlo de Internet no computador do utilizador:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Interface**.
3. No bloco **Notificações**, clique no botão **Configurar notificações**.

4. Na janela que surgir, selecione a secção **Controlo de Internet**.

   Isto abre a tabela de eventos do Controlo de Internet e métodos de notificação.

5. Configure o método de notificação para cada evento: **Guardar no relatório local** ou **Guardar no Registo de Eventos do Windows**.

   Para registar eventos de visita ao site permitidos, precisa igualmente de configurar o Controlo de Internet (consulte as instruções abaixo).

   Na tabela de eventos, pode também ativar uma notificação no ecrã e uma notificação por e-mail. Para enviar notificações por e-mail, precisa de definir as definições do servidor SMTP. Para obter mais informações detalhadas sobre o envio de notificações por e-mail, consulte a Ajuda do Kaspersky Security Center.

6. Guarde as suas alterações.

Como resultado, o Kaspersky Endpoint Security começa a registar eventos de atividades da Internet do utilizador.

O Controlo de Internet envia eventos da atividade do utilizador ao Kaspersky Security Center da seguinte maneira:

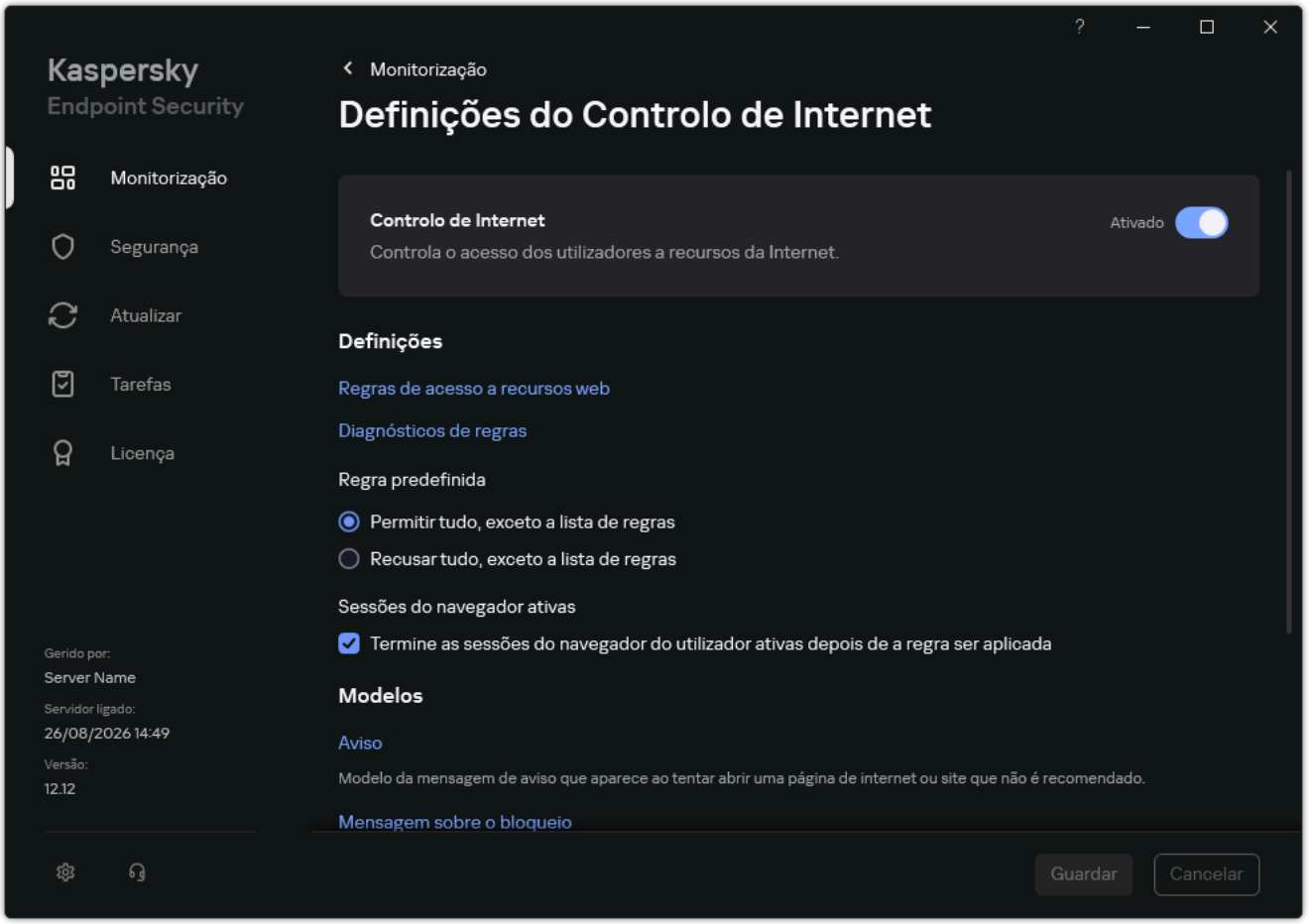
- Se utilizar o Kaspersky Security Center, o Controlo de Internet envia eventos para todos os objetos que compõem a página Web. Por este motivo, podem ser criados vários eventos quando uma página da Web é bloqueada. Por exemplo, ao bloquear a página da Web http://www.example.com, o Kaspersky Endpoint 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 utilizar a Consola de Nuvem do Kaspersky Security Center, o Controlo de Internet agrupa eventos e envia apenas o protocolo e o domínio do website. Por exemplo, se um utilizador visitar as páginas da Web não recomendadas http://www.example.com/main, http://www.example.com/contact, http://www.example.com/gallery, o Kaspersky Endpoint Security só enviará um evento com o objeto http://www.example.com.

Ativar os eventos quando visitar sites permitidos

Para ativar o registo de eventos quando visitar sites permitidos:

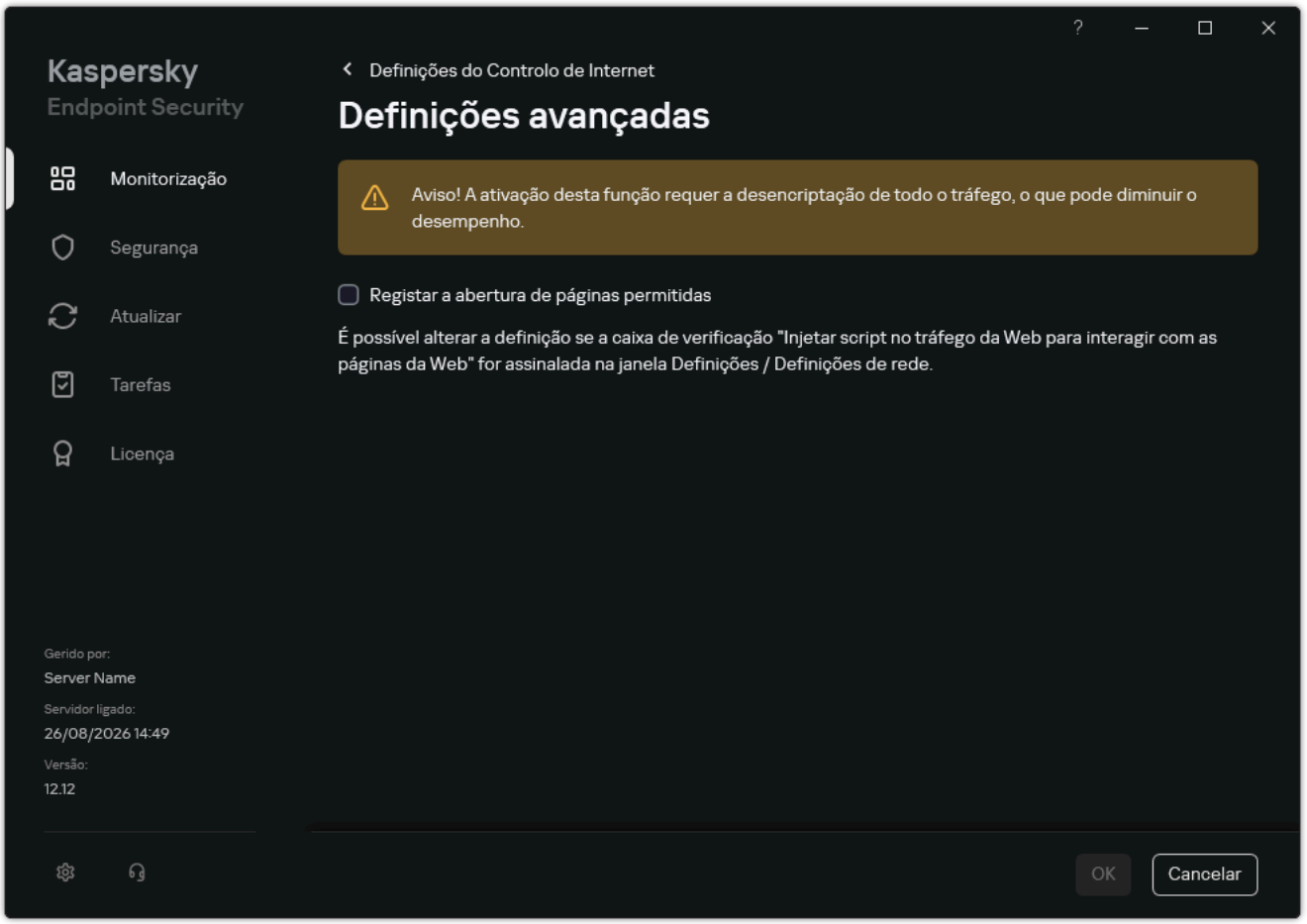
1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Internet**.



Definições do Controlo de Internet

3. No bloco **Adicional**, clique no botão **Definições avançadas**.

4. Na janela que abre, selecione a caixa de verificação **Registar a abertura de páginas permitidas**.



Definições avançadas do Controlo de Internet

5. Guarde as suas alterações.

Como resultado, poderá ver o histórico completo do navegador.

Editar modelos de mensagens de Controlo de Internet

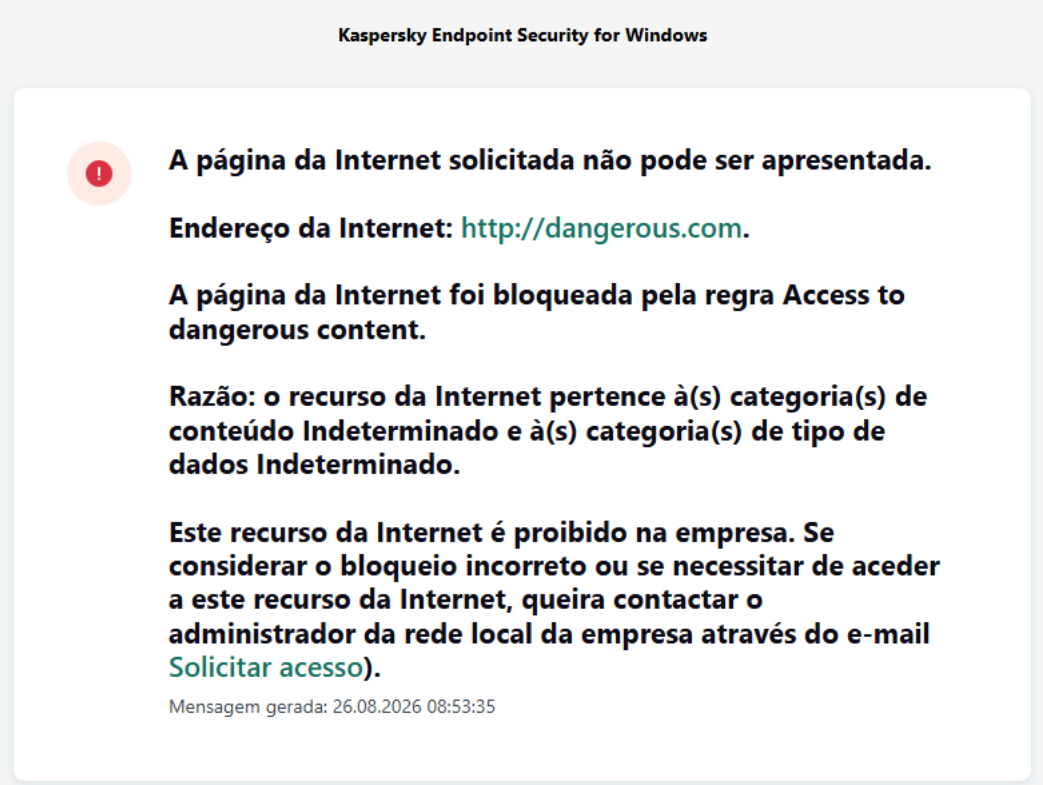
Conforme o tipo de ação especificada nas propriedades das regras de Controlo de Internet, o Kaspersky Endpoint Security apresenta uma mensagem de um dos tipos seguintes quando os utilizadores tentam aceder aos recursos da Internet (a aplicação substitui uma página HTML com a mensagem da resposta do servidor HTTP):

- Mensagem de Aviso. Esta mensagem avisa o utilizador de que visitar o recurso da Internet não é recomendado e/ou viola a política de segurança da empresa. O Kaspersky Endpoint Security apresenta uma mensagem de aviso se a opção **Avisar** estiver selecionada nas definições da regra que descreve este recurso da Internet.

  Se o utilizador considerar o aviso incorreto, pode clicar na ligação da mensagem de aviso para enviar uma mensagem pré-criada para o administrador local da rede da empresa.

- Mensagem a informar o bloqueio de um recurso da Internet. O Kaspersky Endpoint Security apresenta uma mensagem a informar que um recurso da Internet está bloqueado (consulte a figura abaixo), se a opção **Bloquear** estiver selecionada nas definições da regra que descreve este recurso da Internet.

Se o utilizador considerar que o recurso da Internet está bloqueado indevidamente, pode clicar na ligação na mensagem de notificação de bloqueio do recurso da Internet para enviar uma mensagem pré-gerada para o administrador local da rede da empresa.



Mensagem sobre o bloqueio de recursos Web

São fornecidos modelos especiais para a mensagem de aviso, para a mensagem que informa que um recurso da Internet está bloqueado e para uma mensagem enviada ao administrador da rede local. São fornecidas variáveis especiais para gerir os modelos da mensagem (por exemplo, %USER_NAME%). As variáveis permitem que um único modelo de mensagem seja usado para diferentes computadores. Ao gerar uma mensagem, o Kaspersky Endpoint Security recupera o valor da variável das definições do sistema operativo e insere-o na mensagem correspondente ao computador, utilizador e evento específicos.

Como alterar o modelo de mensagem do Controlo de Internet na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança** → **Controlo de Internet**.
4. No bloco **Definições dos modelos de mensagem**, clique no botão **Modelos**.

5. Configure os modelos de mensagens do Controlo de Internet:

   - **Aviso**. O campo de entrada é constituído por um modelo da mensagem apresentada quando é acionada uma regra de aviso de tentativas de acesso a um recurso da Internet indesejado.

   - **Mensagem sobre o bloqueio**. O campo de registo contém o modelo da mensagem que é apresentada caso seja acionada uma regra que bloqueie o acesso a um recurso da Internet.

   - **Mensagem para o administrador**. Modelo da mensagem a enviar ao administrador da rede local, caso o utilizador considere que o bloqueio foi um erro. Depois de o utilizador solicitar acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio do acesso à página da Web para o administrador**. A descrição do evento contém uma mensagem para o administrador com variáveis substituídas. Pode visualizar estes eventos na consola do Kaspersky Security Center utilizando a seleção de eventos predefinida **User requests**. Se a sua organização não tiver o Kaspersky Security Center implementado ou não houver uma ligação ao Servidor de Administração, a aplicação irá enviar uma mensagem ao administrador para o endereço de e-mail especificado.

   Para adicionar uma variável ao texto do modelo, coloque o cursor na posição desejada, clique em **Variável** e selecione a variável necessária na lista de opções disponíveis.

   Também pode restaurar o texto do modelo padrão ao clicar em **Por defeito**.

6. Guarde as suas alterações.

Como alterar o modelo de mensagem do Controlo de Internet na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Security Controls** → **Web Control**.

5. No bloco **Message templates**, clique na ligação **Message about website blocking** e configure modelos para mensagens do Controlo de Internet:

   - **Warning**. O campo de entrada é constituído por um modelo da mensagem apresentada quando é acionada uma regra de aviso de tentativas de acesso a um recurso da Internet indesejado.

   - **Message about blocking**. O campo de registo contém o modelo da mensagem que é apresentada caso seja acionada uma regra que bloqueie o acesso a um recurso da Internet.

   - **Message to administrator**. Modelo da mensagem a enviar ao administrador da rede local, caso o utilizador considere que o bloqueio foi um erro. Depois de o utilizador solicitar acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio do acesso à página da Web para o administrador**. A descrição do evento contém uma mensagem para o administrador com variáveis substituídas. Pode visualizar estes eventos na consola do Kaspersky Security Center utilizando a seleção de eventos predefinida **User requests**. Se a sua organização não tiver o Kaspersky Security Center implementado ou não houver uma ligação ao Servidor de Administração, a aplicação irá enviar uma mensagem ao administrador para o endereço de e-mail especificado.

   Para adicionar uma variável ao texto do modelo, coloque o cursor na posição desejada, clique em **Add variable** e selecione a variável necessária na lista de opções disponíveis.

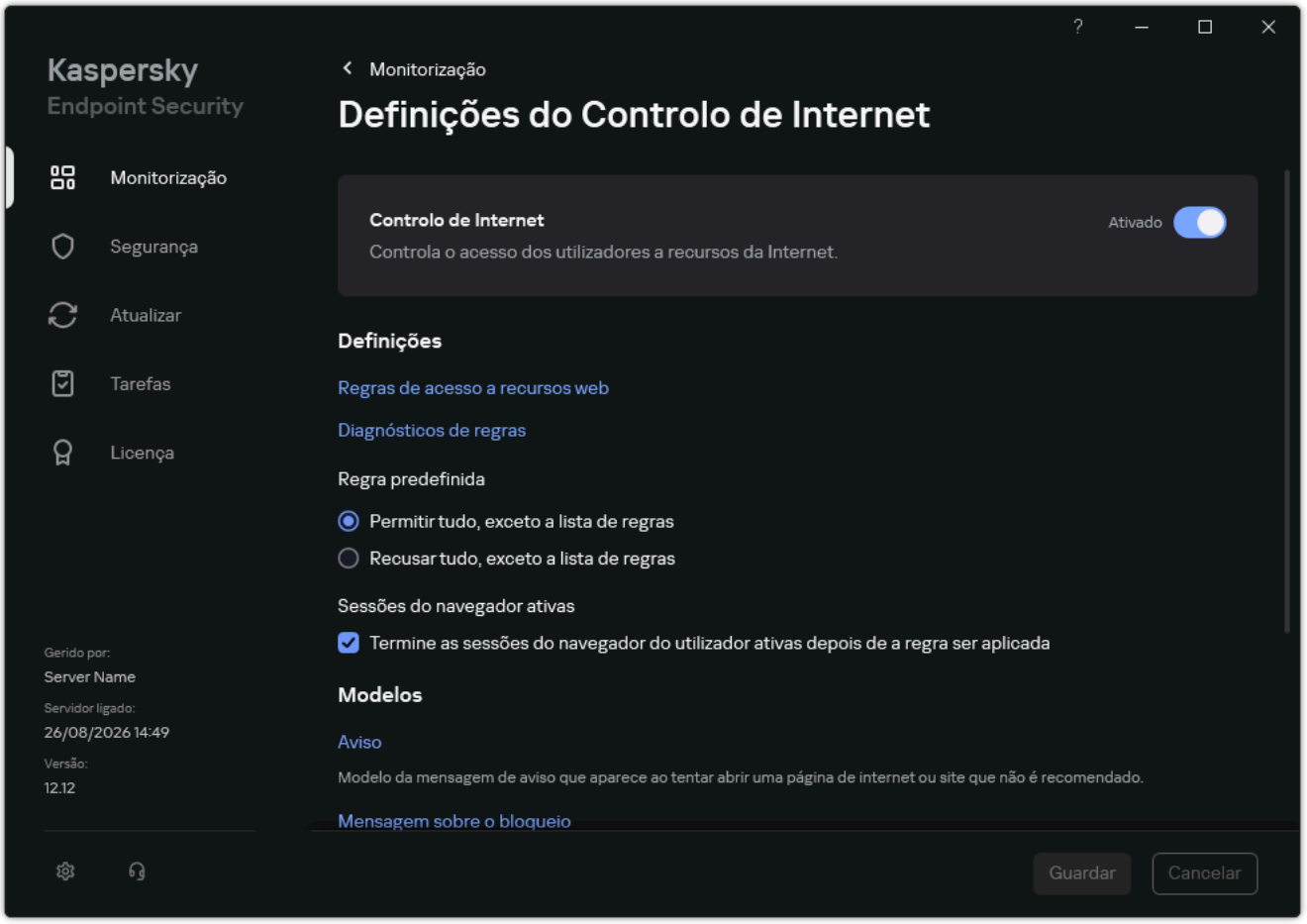
Também pode restaurar o texto do modelo padrão ao clicar em **Reset to default**.

6. Guarde as suas alterações.

Como alterar o modelo de mensagem do Controlo de Internet na interface de aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Internet**.



Definições do Controlo de Internet

3. No bloco **Modelos**, configure os modelos para mensagens de Controlo de Internet:

   - **Aviso**. O campo de entrada é constituído por um modelo da mensagem apresentada quando é acionada uma regra de aviso de tentativas de acesso a um recurso da Internet indesejado.

   - **Mensagem sobre o bloqueio**. O campo de registo contém o modelo da mensagem que é apresentada caso seja acionada uma regra que bloqueie o acesso a um recurso da Internet.

   - **Mensagem para o administrador**. Modelo da mensagem a enviar ao administrador da rede local, caso o utilizador considere que o bloqueio foi um erro. Depois de o utilizador solicitar acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio do acesso à página da Web para o administrador**. A descrição do evento contém uma mensagem para o administrador com variáveis substituídas. Pode visualizar estes eventos na consola do Kaspersky Security Center utilizando a seleção de eventos predefinida **User requests**. Se a sua organização não tiver o Kaspersky Security Center implementado ou não houver uma ligação ao Servidor de Administração, a aplicação irá enviar uma mensagem ao administrador para o endereço de e-mail especificado.

   Para adicionar uma variável ao texto do modelo, coloque o cursor na posição desejada, clique em **Adicionar variável** e selecione a variável necessária na lista de opções disponíveis.

Também pode restaurar o texto do modelo padrão ao clicar em **Repor**.

4. Guarde as suas alterações.

Editar máscaras para endereços de recursos da Internet

A utilização de uma *máscara de endereço de recurso da Internet* (também designada por "máscara de endereço") pode ser útil se necessitar de introduzir vários endereços de recursos da Internet ao criar uma regra de acesso a recursos da Internet. Se corretamente concebida, uma máscara de endereço pode substituir um grande número de endereços de recursos da Internet.

Ao criar uma máscara de endereço, siga estas regras:

1. O carácter `*` substitui qualquer sequência que contenha zero caracteres ou mais.

   Por exemplo, se introduzir a máscara de endereço `*abc*`, a regra de acesso é aplicada a todos os recursos da Internet que contenham a sequência `abc`. Exemplo: `http://www.example.com/page_0-9abcdef.html`.

2. Uma sequência de caracteres `*.` (conhecidos como *máscara de domínio*) permite selecionar todos os domínios de um endereço. A máscara de domínio `*.` representa qualquer nome de domínio, nome de subdomínio ou uma 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 `www.example.com` é interpretada como `*.example.com`. Esta máscara abrange os endereços `www2.example.com` e `www.pictures.example.com`.

4. Se uma máscara de endereço não começar com o carácter `*`, o conteúdo da máscara de endereço é equivalente ao mesmo conteúdo com o prefixo `*.`

5. Se uma máscara de endereço terminar com um carácter que não `/` 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`, em que `a`, `b` e `c` correspondem a quaisquer caracteres.

6. Se uma máscara de endereço terminar com o carácter `/`, 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 uma cadeia vazia.

8. Os endereços de recursos da Internet são comparados com uma máscara de endereço, tendo em conta o protocolo (http ou https):

   - Se a máscara de endereço não contiver qualquer protocolo de rede, esta máscara de endereço abrange os 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 contiver um protocolo de rede, esta máscara de endereço abrange apenas endereços com o mesmo protocolo de rede que a máscara de endereço.

     Exemplo: a máscara de endereço `http://*.example.com` abrange o endereço `http://www.example.com` mas não o endereço `https://www.example.com`.

9. Uma máscara de endereço entre aspas é processada sem considerar quaisquer substituições adicionais, exceto o carácter `*`, se tiver sido inicialmente incluído na máscara de endereço. As regras 5 e 7 não se aplicam a máscaras de endereço entre aspas duplas (ver exemplos 14 – 18 na tabela abaixo).

10. O nome de utilizador e a password, a porta de ligação e a utilização de maiúsculas ou minúsculas nos caracteres não são tidos em consideração durante a comparação com a máscara de endereço de um recurso da Internet.

Exemplos de como utilizar regras para criar máscaras de endereço

N.º	Máscara de endereço	Endereço de recurso da Internet a verificar	O endereço é abrangido pela máscara de endereço	Comentário
1	*.exemplo.com	http://www.123exemplo.com	Não	Ver regra 1.
2	*.exemplo.com	http://www.123.exemplo.com	Sim	Ver regra 2.
3	*exemplo.com	http://www.123exemplo.com	Sim	Ver regra 1.
4	*exemplo.com	http://www.123.exemplo.com	Sim	Ver regra 1.
5	http://www.*.exemplo.com	http://www.123exemplo.com	Não	Ver regra 1.
6	www.exemplo.com	http://www.exemplo.com	Sim	Ver regras 3, 2, 1.
7	www.exemplo.com	https://www.exemplo.com	Sim	Ver regras 3, 2, 1.
8	http://www.*.exemplo.com	http://123.exemplo.com	Sim	Ver regras 3, 4, 1.
9	www.exemplo.com	http://www.exemplo.com/abc	Sim	Ver regras 3, 5, 1.
10	exemplo.com	http://www.exemplo.com	Sim	Ver regras 3, 1.
11	http://exemplo.com/	http://exemplo.com/abc	Sim	Ver regra 6.
12	http://exemplo.com/*	http://example.com	Sim	Ver regra 7.
13	http://example.com	https://exemplo.com	Não	Ver regra 8.
14	"exemplo.com"	http://www.exemplo.com	Não	Ver regra 9.
15	"http://www.exemplo.com"	http://www.exemplo.com/abc	Não	Ver regra 9.
16	"*.exemplo.com"	http://www.exemplo.com	Sim	Ver regras 1, 9.
17	"http://www.exemplo.com/*"	http://www.exemplo.com/abc	Sim	Ver regras 1, 9.
18	"www.exemplo.com"	http://www.example.com; https://www.example.com	Sim	Ver regras 9, 8.
19	www.exemplo.com/abc/123	http://www.exemplo.com/abc	Não	Uma máscara de endereço contém mais informações do que o endereço de um recurso da Internet.

Controlo de Internet para máquinas virtuais

O Controlo de Internet controla o tráfego no computador, bem como numa máquina virtual que é implementada localmente no computador. Isto funciona sem ter de instalar a aplicação Kaspersky Endpoint Security na máquina virtual local. Isto significa que se o utilizador tentar abrir um site bloqueado por uma regra de Controlo de Internet num navegador na *máquina virtual*, a aplicação instalada no sistema operativo anfitrião do *computador* nega o acesso a esse site.

O Controlo de Internet funciona de forma diferente em máquinas virtuais diferentes.

Oracle VM VirtualBox

O Kaspersky Endpoint Security suporta regras de Controlo de Internet em máquinas virtuais Oracle VM VirtualBox sem limitações. A aplicação pode controlar todo o tráfego da máquina virtual. Se estiver configurado um filtro por utilizador nas regras de Controlo de Internet, a aplicação funciona corretamente porque todos os processos das máquinas virtuais são iniciados pelo utilizador local.

VMware Workstation

O Kaspersky Endpoint Security suporta regras de Controlo de Internet em máquinas virtuais VMware Workstation com limitações. A aplicação não suporta regras com um filtro por utilizador configurado. Os processos da máquina virtual são executados sob o utilizador do sistema (SYSTEM). Isto torna impossível identificar o utilizador que está a tentar abrir o site na máquina virtual.

Microsoft Hyper-V

O Kaspersky Endpoint Security não suporta regras de Controlo de Internet em máquinas virtuais Microsoft Hyper-V.

Configure os modelos de mensagens do Controlo de Internet:

Pode utilizar as seguintes variáveis nos modelos de mensagens do utilizador ou nos modelos de mensagens do administrador:

- **Nome de utilizador** – `%USER_NAME%`.

  Nome da conta de utilizador atual no computador em que a mensagem foi gerada, no formato `<device name>\<user alias>` (por exemplo, `DESKTOP-123\John.Smith`).

- **Endereço do recurso da Internet** – `%CANONIC_REQUEST_URL%`.

  Endereço do recurso da Internet bloqueado.

- **Nome da regra** – %RULE%.

  Nome da regra que bloqueou o recurso da Internet.

- **E-mail para enviar uma mensagem** – %COMPLAIN_EMAIL%.

  Endereço de e-mail para envio de feedback sobre blocos de recursos da Internet. Ao clicar no endereço de e-mail, abre-se uma janela na qual o utilizador pode escrever uma mensagem para o administrador.

- **Nome da categoria de conteúdo** – %CONTENT_CATEGORY_LIST%.

  Categoria do site à qual pertence o recurso bloqueado (por exemplo, *Sistemas de pagamento*).

- **Nome da categoria de tipo de dados** – %TYPE_CATEGORY_LIST%.

  Categoria do tipo de dados no recurso da Internet bloqueado (por exemplo, *Gráficos*).

- **Ligação para o recurso da Internet solicitado** – %CONTINUE_PAGE%.

  Ligação para a página de Internet solicitada (por exemplo, `http://www.example.com/pagename.html`).

- **Ligação para o site** – %CONTINUE_SITE%.

  Ligação para o site que contém a página de Internet solicitada (por exemplo, `http://www.example.com/`).

- **Ligação para acesso aos domínios** – %CONTINUE_DOMAIN%.

  Ligação que pode ser clicada para obter acesso a todas as páginas de Internet existentes do nome de domínio. Por exemplo, se o endereço da página de Internet bloqueada for `http://www.example.com`, a variável %CONTINUE_DOMAIN% é substituída pela ligação `http://*.example.com`. Clicar nesta ligação permite o acesso a todos os endereços de Internet do nome de domínio base `http://www.example.com/` incluindo subdomínios, por exemplo, `http://start.example.com/*` ou `http://domain.domain.example.com/*`, onde o carácter * representa qualquer sequência de caracteres (incluindo uma cadeia vazia).

Controlo de Dispositivos

O Controlo de Dispositivos gere o acesso de utilizador a dispositivos que são instalados no ou ligados ao computador (por exemplo, discos rígidos, câmaras ou módulos Wi-Fi). Tal permite proteger o computador da infeção quando os dispositivos são ligados, e impede a perda ou fuga de dados.

Se o Controlo de Dispositivos estiver ativado, a aplicação transmitirá informações sobre os dispositivos ligados ao Kaspersky Security Center. Pode ver a lista de dispositivos ligados no Kaspersky Security Center na pasta **Advanced** → **Repositories** → **Hardware**.

Níveis de acesso ao dispositivo

O Controlo de Dispositivos controla o acesso aos seguintes níveis:

- **Tipo de dispositivo**. Por exemplo, impressoras, unidades amovíveis e unidades de CD/DVD.

  Pode configurar o acesso ao dispositivo do seguinte modo:

  - Permitir – ✓.
  - Bloquear – ⊘.

- Por regras (apenas impressoras e dispositivos portáteis) – .
- Depende do barramento de ligação (exceto Wi-Fi) – .
- Bloquear com exceções (apenas Wi-Fi) - .

- **Barramento de ligação**. Um *barramento de ligação* é uma interface utilizada para ligar dispositivos ao computador (por exemplo, USB ou FireWire). Se o modo **Depende do barramento de ligação** for selecionado para o tipo de dispositivo, a aplicação permite ou nega o acesso ao dispositivo, dependendo da interface de ligação (por exemplo, USB).

  Pode configurar o acesso ao dispositivo do seguinte modo:

  - Permitir – .
  - Bloquear – .

- **Dispositivos fiáveis**. *Dispositivos fiáveis* são dispositivos aos quais os utilizadores especificados nas definições de dispositivo fiável têm acesso total, em qualquer altura.

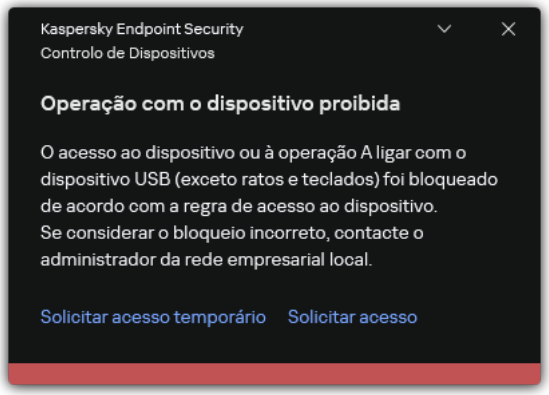
  Pode adicionar dispositivos fiáveis com base nos seguintes dados:

  - **Dispositivos por ID**. Cada dispositivo possui um identificador exclusivo (Hardware ID ou HWID). Pode ver a ID nas propriedades de dispositivo utilizando ferramentas do sistema operativo. Exemplo de um ID do dispositivo: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Se desejar adicionar vários dispositivos específicos, é conveniente adicionar dispositivos por ID.
  - **Dispositivos por modelo**. Cada dispositivo possui um Vendor ID (VID) e um Product ID (PID). Pode examinar os IDs nas propriedades do dispositivo utilizando ferramentas do sistema operativo. Modelo para inserir o VID e o PID: `VID_1234&PID_5678`. Se usar dispositivos de um determinado modelo na sua organização, é conveniente adicionar dispositivos por modelo. Deste modo, pode adicionar todos os dispositivos deste modelo.
  - **Dispositivos por máscara de ID**. Se estiver a utilizar vários dispositivos com IDs semelhantes, pode utilizar máscaras para adicionar dispositivos à lista fiável. O caráter `*` substitui qualquer conjunto de carateres. O Kaspersky Endpoint Security não suporta o caráter `?` ao introduzir uma máscara. Por exemplo, `WDC_C*`.
  - **Dispositivos por máscara de modelo**. Se estiver a utilizar vários dispositivos com VIDs ou PIDs semelhantes (por exemplo, dispositivos do mesmo fabricante), pode utilizar máscaras para adicionar dispositivos à lista fiável. O caráter `*` substitui qualquer conjunto de carateres. O Kaspersky Endpoint Security não suporta o caráter `?` ao introduzir uma máscara. Por exemplo, `VID_05AC&PID_*`.

O Controlo de Dispositivos regula o acesso do utilizador a dispositivos através de *regras de acesso*. O Controlo de Dispositivos também o permite guardar eventos de ligação/desconexão de dispositivo. Para guardar eventos, tem de configurar o registo de eventos numa política.

Se o acesso a um dispositivo depender do barramento de ligação (o estado), o Kaspersky Endpoint Security não guarda eventos de ativação/desativação de dispositivos. Para ativar o Kaspersky Endpoint Security para guardar eventos de ativação/desativação de dispositivos, permita o acesso ao tipo correspondente de dispositivo (o estado) ou adicione o dispositivo à lista fiável.

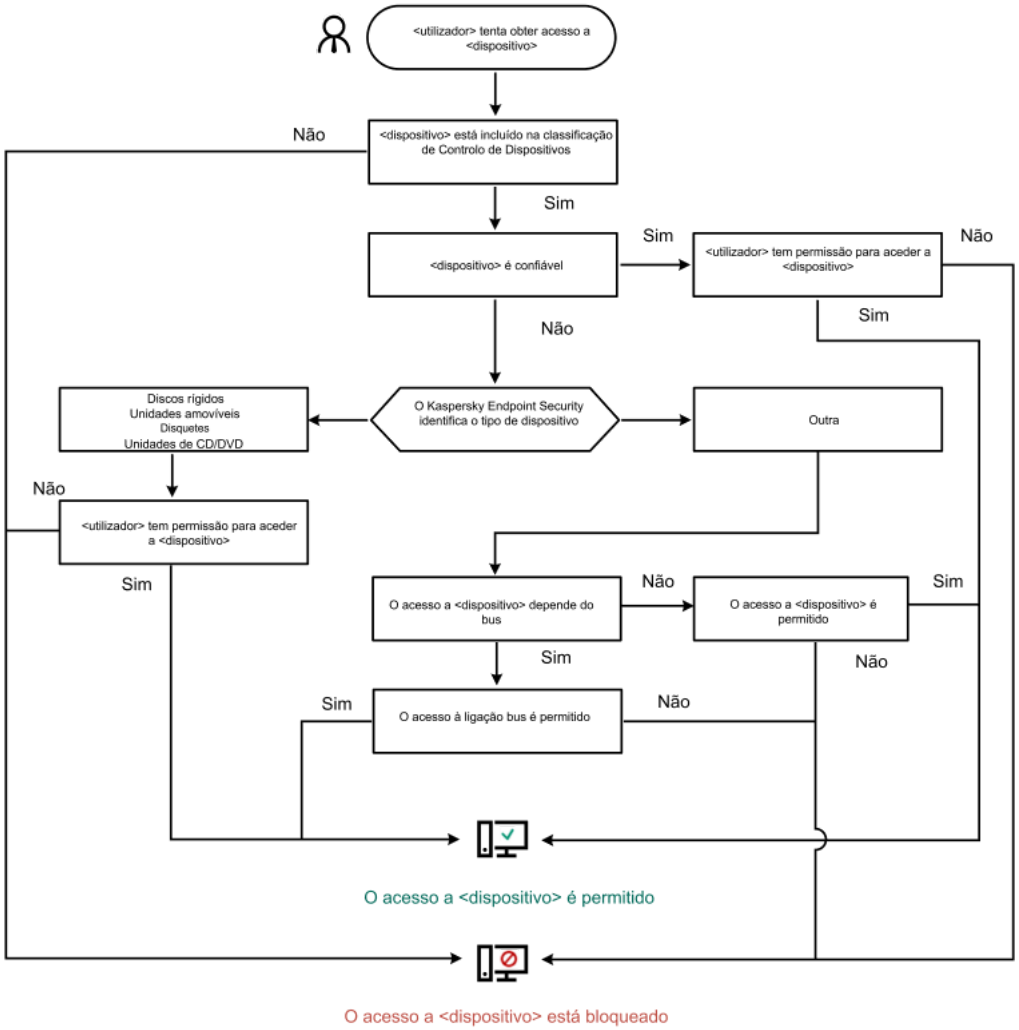
Quando um dispositivo que está bloqueado pelo Controlo de Dispositivos é ligado ao computador, o Kaspersky Endpoint Security bloqueará o acesso e apresentará uma notificação (ver a figura abaixo).



Notificação de Controlo de Dispositivos

Algoritmo operacional do Controlo de Dispositivos

O Kaspersky Endpoint Security toma uma decisão sobre se é permitido o acesso a um dispositivo depois do utilizador ligar o mesmo ao computador (ver figura abaixo).



Algoritmo operacional do Controlo de Dispositivos

Se um dispositivo estiver ligado e o acesso for permitido, pode editar a regra de acesso e bloquear o acesso. Neste caso, na próxima vez que alguém tentar aceder ao dispositivo (tal como para visualizar a árvore de pastas ou executar operações de leitura ou escrita), o Kaspersky Endpoint Security bloqueia o acesso. Um dispositivo sem sistema de ficheiros apenas é bloqueado na próxima vez que o dispositivo for ligado.

Se um utilizador do computador com Kaspersky Endpoint Security instalado tiver de solicitar acesso a um dispositivo que o utilizador acredite ter sido bloqueado por engano, envie ao utilizador as instruções de pedido de acesso.

Sobre as regras de acesso

Uma *regra de acesso a dispositivos* é um grupo de definições que determina a forma como os utilizadores podem aceder aos dispositivos instalados ou ligados ao computador. Estas definições incluem acesso a um dispositivo específico, um agendamento de acesso e permissões de leitura ou gravação. Não pode adicionar um dispositivo que esteja fora da classificação do Controlo de Dispositivos. O acesso a tais dispositivos é permitido a todos os utilizadores.

Regras de acesso a dispositivo

O grupo de definições para uma regra de acesso é diferente dependendo do tipo de dispositivo (ver tabela abaixo).

Aceder a definições de regras

Dispositivos	Controlo de acesso	Agendamento de acesso a um dispositivo	Atribuição de utilizadores e/ou um grupo de utilizadores	Prioridade	Ler/escrever permissão
Discos rígidos	✓	✓	✓	✓	✓
Unidades amovíveis (incluindo unidades flash USB)	✓	✓	✓	✓	✓
Disquetes	✓	✓	✓	✓	✓
Unidades de CD/DVD	✓	✓	✓	✓	✓
Dispositivos portáteis (MTP)	✓	✓	✓	✓	✓
Impressoras locais	✓	–	✓	✓	–
Impressoras de rede	✓	–	✓	✓	–
Modems	✓	–	–	–	–
Dispositivos de fita	✓	–	–	–	–
Dispositivos multifunções	✓	–	–	–	–
Leitores de cartões	✓	–	–	–	–
Dispositivos Windows CE USB ActiveSync	✓	–	–	–	–
Adaptadores de rede externos	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
Câmaras e scanners	✓	–	–	–	–

Regras de acesso para redes Wi-Fi

Uma regra de acesso à rede Wi-Fi determina se a utilização de redes Wi-Fi é permitida (o estado) ou proibida (o estado). Pode adicionar uma *rede Wi-Fi fiável* (o estado) a uma regra. A utilização de uma rede Wi-Fi fiável é permitida sem limitações. Por defeito, uma regra de acesso a rede Wi-Fi permite o acesso a qualquer rede Wi-Fi.

Regras de acesso a barramentos de ligação

Se o valor **Depende do barramento de ligação** for selecionado para a regra de acesso por tipo de dispositivo, a aplicação permite ou nega o acesso ao dispositivo, dependendo da interface de ligação. São criadas, por predefinição, regras que permitem o acesso a barramentos para todos os barramentos de ligação existentes na classificação do componente Controlo de Dispositivos.

As regras de acesso a barramentos de ligação determinam se a ligação de dispositivos é permitida (o estado) ou proibida (o estado). A prioridade das regras de acesso por tipo de dispositivo é superior à prioridade das regras de acesso a barramentos de ligação.

O teclado e o rato não podem ser bloqueados com o Controlo de Dispositivos. Se proibir o acesso ao barramento de ligação USB, o utilizador continuará a trabalhar com o teclado e o rato ligados por USB. O componente Prevenção de ataques BadUSB destina-se a evitar a ligação ao computador de dispositivos USB infetados que simulam teclados.

Obter informações sobre os dispositivos instalados

O Kaspersky Security Center recebe informações sobre os dispositivos instalados das seguintes fontes: Agente de Rede e Kaspersky Endpoint Security. As informações sobre os dispositivos instalados são necessárias para a gestão do acesso e a criação de uma lista de dispositivos fiáveis.

Informações sobre o hardware do computador

Se o Agente de Rede estiver instalado num dispositivo Windows, envia as seguintes informações sobre o hardware do dispositivo para o Servidor de Administração:

- RAM
- dispositivos de armazenamento (incluindo discos rígidos)
- placa principal
- CPU
- adaptador de rede
- monitores

- GPU
- placa de som

O Agente de Rede fornece estas informações em cada sincronização com o Kaspersky Security Center. Pode ver o hardware de um computador nas respetivas propriedades (**Registo de hardware**).

Informações de hardware

O Kaspersky Endpoint Security fornece informações sobre o hardware instalado: impressoras, unidades amovíveis, dispositivos portáteis (MTP), entre outros. Para receber informações de hardware, tem de aplicar uma política ativa que permita a transmissão de informações sobre os dispositivos instalados (esta transmissão está ativada por predefinição).

Como ativar a transmissão de dados sobre os dispositivos instalados na Consola de Gestão (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Definições gerais** → **Relatórios e armazenamento**.
5. No bloco **Transferência de dados para o Servidor de administração**, clique no botão **Definições**.
6. Selecione a caixa de verificação **Dispositivos instalados**.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar a transmissão de dados sobre os dispositivos instalados na Web Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **KSC Integration**.
5. No bloco **Data transfer to Administration Server**, clique no botão **Advanced settings**.
6. Selecione a caixa de verificação **About installed devices**.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como resultado, pode ver a lista de dispositivos instalados na consola do Kaspersky Security Center (**Repositories** → **Hardware**).

Gerir o acesso aos dispositivos por tipo

O Controlo de Dispositivos permite gerir o acesso a dispositivos por tipo. O tipo do dispositivo é determinado pelo sistema operativo quando o dispositivo é ligado. Pode procurar o tipo de dispositivo utilizando a ferramenta Gestor de Dispositivos integrada no sistema operativo. Para gerir o acesso aos dispositivos, deve configurar regras. Uma *regra de acesso a dispositivos* é um grupo de definições que determina a forma como os utilizadores podem aceder aos dispositivos instalados ou ligados ao computador. Estas definições incluem acesso a um dispositivo específico, um agendamento de acesso e permissões de leitura ou gravação. Não pode adicionar um dispositivo que esteja fora da classificação do Controlo de Dispositivos. O acesso a tais dispositivos é permitido a todos os utilizadores.

Por defeito, o Controlo de Dispositivos permite acesso a todos os dispositivos para todos os utilizadores.

Pode configurar o acesso aos dispositivos da seguinte maneira:

- **Permitir**.

  O Kaspersky Endpoint Security concede a todos os utilizadores acesso total aos dispositivos.

- **Bloquear**.

  O Kaspersky Endpoint Security bloqueia ligações de dispositivos. A aplicação permite apenas dispositivos fiáveis para ligar.

- **Depende do barramento de ligação**.

  O Kaspersky Endpoint Security determina a interface de ligação dos dispositivos e restringe o acesso aos dispositivos de acordo com seu estado de ligação de barramento. A aplicação também permite ligar dispositivos fiáveis.

- **Por regras**.

  Para alguns tipos de dispositivos, pode designar utilizadores individuais ou um grupo de utilizadores que têm permissão para utilizar os dispositivos, definir um agendamento de acesso aos dispositivos e configurar permissões de leitura e gravação. A aplicação também permite ligar dispositivos fiáveis.

Tenha atenção ao configurar o acesso aos dispositivos do tipo **Discos rígidos**. Se bloquear o acesso ao disco do sistema, a aplicação poderá causar uma falha (BSOD) ao iniciar o sistema operativo.

Se um dispositivo não se enquadrar no esquema de classificação de Controlo de Dispositivos, o acesso a tal dispositivo não pode ser restringido.

Como gerir o acesso a dispositivos por tipo na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Controlos de segurança** → **Controlo de Dispositivos**.

5. Sob **Definições do Controlo de Dispositivos**, selecione a aba **Tipos de dispositivos**.

   O separador **Tipos de dispositivos** mostra as regras de acesso para todos os dispositivos incluídos na classificação de componentes do Controlo de Dispositivos.

6. Configurar regras de acesso para os dispositivos:

   a. Selecione o modo de acesso: **Permitir**, **Bloquear**, **Depende do barramento de ligação**, **Por regras**.

      Para selecionar o modo de acesso **Por regras**, tem de clicar duas vezes para abrir as propriedades da regra de acesso.

   b. Se selecionar o modo de acesso **Depende do barramento de ligação**, tem de configurar as regras de acesso para as interfaces de ligação no separador **Barramentos de ligação**.

   c. No caso de dispositivos de armazenamento (por exemplo, suportes amovíveis), pode configurar permissões de acesso para utilizadores individuais. Também pode definir um agendamento de acesso aos dispositivos e configurar permissões de leitura e gravação.

      Pode adicionar dispositivos à lista fiável. *Dispositivos fiáveis* são dispositivos aos quais os utilizadores especificados nas definições de dispositivo fiável têm acesso total, em qualquer altura.

   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 ligação Wi-Fi do computador.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como gerir o acesso a dispositivos por tipo na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Security Controls** → **Device Control**.

5. Sob **Device access rules**, selecione a aba **Devices and Wi-Fi networks**.

   A tabela lista as regras de acesso para todos os dispositivos que estão presentes na classificação do componente Controlo de Dispositivos.

6. Configurar regras de acesso para os dispositivos:

   a. Selecione o modo de acesso: **Allow**, **Block**, **Depends on bus**, **Custom**.

      Se o modo de acesso não estiver no menu suspenso, abra as propriedades da regra de acesso clicando duas vezes no tipo de dispositivo.

   b. Se selecionar o modo de acesso **Depends on bus**, tem de configurar as regras de acesso para as interfaces de ligação no separador **Connection buses**.

c. No caso de dispositivos de armazenamento (por exemplo, suportes amovíveis), pode configurar permissões de acesso para utilizadores individuais. Também pode definir um agendamento de acesso aos dispositivos e configurar permissões de leitura e gravação.

Pode adicionar dispositivos à lista fiável. *Dispositivos fiáveis* são dispositivos aos quais os utilizadores especificados nas definições de dispositivo fiável têm acesso total, em qualquer altura.

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 ligação Wi-Fi do computador.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como gerir o acesso aos dispositivos na interface da aplicação

1. Na janela principal da aplicação, clique no botão .

2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Dispositivos**.

3. No bloco **Definições de acesso**, clique na ligação **Dispositivos e redes Wi-Fi**.

A tabela lista as regras de acesso para todos os dispositivos que estão presentes na classificação do componente Controlo de Dispositivos.

4. Configurar regras de acesso para os dispositivos:

a. Selecione o modo de acesso: **Permitir**, **Bloquear**, **Depende do barramento de ligação**, **Por regras**.

Se o modo de acesso não estiver no menu suspenso, abra as propriedades da regra de acesso clicando duas vezes no tipo de dispositivo.

b. Se selecionar o modo de acesso **Depende do barramento de ligação**, tem de configurar as regras de acesso para as interfaces de ligação no separador **Barramentos de ligação**.

c. No caso de dispositivos de armazenamento (por exemplo, suportes amovíveis), pode configurar permissões de acesso para utilizadores individuais. Também pode definir um agendamento de acesso aos dispositivos e configurar permissões de leitura e gravação.

Pode adicionar dispositivos à lista fiável. *Dispositivos fiáveis* são dispositivos aos quais os utilizadores especificados nas definições de dispositivo fiável têm acesso total, em qualquer altura.

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 ligação Wi-Fi do computador.

5. Guarde as suas alterações.

Como resultado, quando um utilizador tenta obter acesso a um dispositivo, a aplicação bloqueia o acesso de acordo com as regras. O Kaspersky Endpoint Security também regista um evento correspondente. Se deseja conceder acesso a dispositivos individuais, pode adicionar estes dispositivos à lista de dispositivos fiáveis.

Gerir o acesso aos dispositivos pelo barramento de ligação

Para editar uma regra de acesso a barramentos de ligação:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança** → **Controlo de Dispositivos**.
3. No bloco **Definições de acesso**, clique no botão **Barramentos de ligação**.

   A janela aberta mostra as regras de acesso para todos os barramentos de ligação incluídos na classificação do componente Controlo de Dispositivos.
4. Selecione a regra de acesso que pretende editar.
5. Na coluna **Acesso**, selecione se deseja ou não permitir o acesso ao barramento de ligação: **Permitir** ou **Bloquear**.

   Se alterou o acesso ao barramento de ligação **Porta Série** (COM) ou **Portal Paralela** (LPT), tem de reiniciar o computador para ativar a regra de acesso.
6. Guarde as suas alterações.

Diferenciação de direitos de acesso do utilizador aos dispositivos

Pode configurar os direitos de acesso do utilizador por tipo de dispositivo ou para dispositivos fiáveis.

Diferenciação dos direitos de acesso do utilizador por tipo de dispositivo

O Controlo de Dispositivos permite configurar os direitos de acesso do utilizador aos dados em *dispositivos de armazenamento*. Para tais dispositivos, configurar permissões de leitura e gravação. O Controlo de Dispositivos suporta os seguintes tipos de *dispositivos de armazenamento*:

- Discos rígidos
- Unidades amovíveis (incluindo unidades flash USB)
- Disquetes
- Unidades de CD/DVD
- Dispositivos portáteis (MTP) Dispositivos portáteis (MTP) incluem, por exemplo, dispositivos móveis, câmaras fotográficas, reprodutores de multimédia e assim por diante.

Desta forma, pode, por exemplo, permitir a utilização de suportes amovíveis apenas para o grupo de administradores. Para outros tipos de dispositivos, pode negar ou permitir acesso para todos os utilizadores. Também pode configurar direitos de acesso do utilizador para utilizar impressoras.

Como configurar direitos de acesso do utilizador a dados em dispositivos de armazenamento na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Controlos de segurança** → **Controlo de Dispositivos**.
5. Sob **Definições do Controlo de Dispositivos**, selecione a aba **Tipos de dispositivos**.

   O separador **Tipos de dispositivos** mostra as regras de acesso para todos os dispositivos incluídos na classificação de componentes do Controlo de Dispositivos.
6. Para configurar regras de acesso a dispositivos de armazenamento, clique duas vezes para abrir a lista de regras.
7. Configurar a regra de acesso ao dispositivo de armazenamento:

   a. No bloco **Regras de acesso**, clique no botão **Adicionar**.

      Abre-se uma janela para adicionar uma nova regra de acesso aos dispositivos de armazenamento.

   b. No campo **Prioridade da regra**, defina a prioridade de *gravação da regra*. Uma regra inclui os seguintes atributos: conta de utilizador, agendamento, permissões (leitura/gravação) e prioridade.

      Uma regra tem uma prioridade específica. Se um utilizador tiver sido adicionado a vários grupos, o Kaspersky Endpoint Security regula o acesso a dispositivos com base na regra com a prioridade mais alta. O Kaspersky Endpoint Security permite-lhe atribuir prioridade de 0 a 10 000. Quanto maior for o valor, maior será a prioridade. Por outras palavras, uma entrada com o valor 0 tem a prioridade mais baixa.

      Por exemplo, pode conceder permissões apenas de leitura ao grupo Todos e conceder permissões de leitura/gravação ao grupo de administradores. Para tal, atribua uma prioridade de 1 ao grupo de administradores e atribua uma prioridade de 0 ao grupo Todos.

      A prioridade de uma regra de bloqueio é superior à prioridade de uma regra de permissão. Por outras palavras, se um utilizador tiver sido adicionado a vários grupos e a prioridade de todas as regras for a mesma, o Kaspersky Endpoint Security regula o acesso a dispositivos com base em qualquer regra de bloqueio existente.

   c. Sob **Regra para utilizadores e grupos**, selecione utilizadores ou grupos de utilizadores. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

   d. Clique em **OK**.
8. Sob **Agendas para a regra de acesso selecionada**, configure um agendamento de acesso a dispositivos de armazenamento para os utilizadores.

   Por exemplo, pode permitir que os utilizadores utilizem dispositivos de armazenamento apenas durante o horário de trabalho.
9. Configure as permissões de acesso dos utilizadores a dispositivos de armazenamento no gestor de ficheiros (**Ler** / **Escrever**).
10. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como configurar direitos de acesso do utilizador a dados em dispositivos de armazenamento na Consola Web e no Cloud Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Security Controls** → **Device Control**.
5. No bloco **Device access rules**, na tabela de regras de acesso, abra as propriedades das regras de acesso para dispositivos de armazenamento.
6. No bloco **Device access rules**, selecione **Custom**.
7. Configurar a regra de acesso ao dispositivo de armazenamento:

   a. No bloco **Users and their rights**, clique no botão **Add**.

   Abre-se uma janela para adicionar uma nova regra de acesso aos dispositivos de armazenamento.

   b. No campo **Priority**, defina a prioridade de *gravação da regra*. Uma regra inclui os seguintes atributos: conta de utilizador, agendamento, permissões (leitura/gravação) e prioridade.

   Uma regra tem uma prioridade específica. Se um utilizador tiver sido adicionado a vários grupos, o Kaspersky Endpoint Security regula o acesso a dispositivos com base na regra com a prioridade mais alta. O Kaspersky Endpoint Security permite-lhe atribuir prioridade de 0 a 10 000. Quanto maior for o valor, maior será a prioridade. Por outras palavras, uma entrada com o valor 0 tem a prioridade mais baixa.

   Por exemplo, pode conceder permissões apenas de leitura ao grupo Todos e conceder permissões de leitura/gravação ao grupo de administradores. Para tal, atribua uma prioridade de 1 ao grupo de administradores e atribua uma prioridade de 0 ao grupo Todos.

   A prioridade de uma regra de bloqueio é superior à prioridade de uma regra de permissão. Por outras palavras, se um utilizador tiver sido adicionado a vários grupos e a prioridade de todas as regras for a mesma, o Kaspersky Endpoint Security regula o acesso a dispositivos com base em qualquer regra de bloqueio existente.

   c. Sob **User or group**, selecione utilizadores ou grupos de utilizadores. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

   d. Sob **Access schedule**, configure um agendamento de acesso a dispositivos de armazenamento para os utilizadores.

   Por exemplo, pode permitir que os utilizadores utilizem dispositivos de armazenamento apenas durante o horário de trabalho.

   e. Configure as permissões de acesso dos utilizadores a dispositivos de armazenamento no gestor de ficheiros (**Read** / **Write**).

   f. Clique em **Save**.
8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como configurar direitos de acesso do utilizador aos dados em dispositivos de armazenamento na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Dispositivos**.
3. No bloco **Definições de acesso**, clique na ligação **Dispositivos e redes Wi-Fi**.

   A tabela lista as regras de acesso para todos os dispositivos que estão presentes na classificação do componente Controlo de Dispositivos.
4. Para configurar regras de acesso a dispositivos de armazenamento, clique com o botão direito do rato para abrir a lista de regras.
5. Configurar a regra de acesso ao dispositivo de armazenamento:

   a. No bloco **Direitos dos utilizadores**, clique no botão **Adicionar**.

   Abre-se uma janela para adicionar uma nova regra de acesso aos dispositivos de armazenamento.

   b. No campo **Prioridade**, defina a prioridade de *gravação da regra*. Uma regra inclui os seguintes atributos: conta de utilizador, agendamento, permissões (leitura/gravação) e prioridade.

   Uma regra tem uma prioridade específica. Se um utilizador tiver sido adicionado a vários grupos, o Kaspersky Endpoint Security regula o acesso a dispositivos com base na regra com a prioridade mais alta. O Kaspersky Endpoint Security permite-lhe atribuir prioridade de 0 a 10 000. Quanto maior for o valor, maior será a prioridade. Por outras palavras, uma entrada com o valor 0 tem a prioridade mais baixa.

   Por exemplo, pode conceder permissões apenas de leitura ao grupo Todos e conceder permissões de leitura/gravação ao grupo de administradores. Para tal, atribua uma prioridade de 1 ao grupo de administradores e atribua uma prioridade de 0 ao grupo Todos.

   A prioridade de uma regra de bloqueio é superior à prioridade de uma regra de permissão. Por outras palavras, se um utilizador tiver sido adicionado a vários grupos e a prioridade de todas as regras for a mesma, o Kaspersky Endpoint Security regula o acesso a dispositivos com base em qualquer regra de bloqueio existente.

   c. Sob **Utilizadores**, selecione utilizadores ou grupos de utilizadores. Pode selecionar utilizadores no Active Directory ou introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

   d. Clique em **Ok**.
6. Sob **Agendamento de acesso aos dispositivos**, configure um agendamento de acesso a dispositivos de armazenamento para os utilizadores.

   Por exemplo, pode permitir que os utilizadores utilizem dispositivos de armazenamento apenas durante o horário de trabalho.
7. Configure as permissões de acesso dos utilizadores a dispositivos de armazenamento no gestor de ficheiros (**Ler** / **Escrever**).
8. Guarde as suas alterações.

Diferenciação de direitos de acesso do utilizador a dispositivos fiáveis

Dispositivos fiáveis são dispositivos aos quais os utilizadores especificados nas definições de dispositivo fiável têm acesso total, em qualquer altura. Para trabalhar com dispositivos fiáveis, pode conceder acesso a um utilizador individual, a um grupo de utilizadores ou a todos os utilizadores da organização. Pode configurar direitos de acesso do utilizador nas propriedades do dispositivo fiável.

Gerir o acesso a dispositivos móveis

O Kaspersky Endpoint Security permite controlar o acesso aos dados em dispositivos móveis com Android e iOS. Os dispositivos móveis pertencem à categoria de dispositivos portáteis (MTP). Portanto, para configurar o acesso aos dados em dispositivos móveis, precisa de editar as definições de acesso a dispositivos portáteis (MTP).

Quando um dispositivo móvel está ligado ao computador, o sistema operativo determina o tipo de dispositivo. Se o Android Debug Bridge (ADB), o iTunes ou aplicações equivalentes estiverem instalados no computador, o sistema operativo identifica os dispositivos móveis como dispositivos ADB ou iTunes. Em todos os outros casos, o sistema operativo pode identificar o tipo de dispositivo móvel como um dispositivo portátil (MTP) para transferência de ficheiros, um dispositivo PTP (câmara) para transferência de imagens ou outro dispositivo. O tipo de dispositivo depende do modelo do dispositivo móvel e do modo de ligação USB selecionado. O Kaspersky Endpoint Security permite configurar permissões de acesso individuais para dados em dispositivos móveis em aplicações ADB, iTunes ou o gestor de ficheiros. Em todos os outros casos, o Controlo 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 definições para eles são as mesmas. Pode selecionar um dos seguintes modos de acesso a dispositivos móveis:

- **Permitir**. O Kaspersky Endpoint Security permite o acesso completo a dispositivos móveis. Pode abrir, criar, modificar, copiar ou eliminar ficheiros em dispositivos móveis através do gestor de ficheiros ou de aplicações ADB e iTunes. Também pode carregar a bateria do dispositivo ao ligar o dispositivo móvel a uma porta USB do computador.

- **Bloquear**. O Kaspersky Endpoint Security restringe o acesso a dispositivos móveis no gestor de ficheiros e nas aplicações ADB e iTunes. A aplicação permite o acesso apenas a dispositivos móveis fiáveis. Também pode carregar a bateria do dispositivo ao ligar o dispositivo móvel a uma porta USB do computador.

- **Depende do barramento de ligação**. O Kaspersky Endpoint Security permite ligar-se a dispositivos móveis de acordo com o estado da ligação USB (**Permitir** ou **Bloquear**).

- **Por regras**. O Kaspersky Endpoint Security restringe o acesso a dispositivos móveis de acordo com as regras. Nas regras, pode configurar direitos de acesso (leitura/escrita), selecionar utilizadores ou um grupo de utilizadores que podem ter acesso a dispositivos móveis e configurar um agendamento de acesso para dispositivos móveis. Também pode restringir o acesso a dados em dispositivos móveis através das aplicações ADB e iTunes.

Configurar as regras de acesso a dispositivos móveis

As regras de acesso para dispositivos portáteis (MTP), dispositivos ADB e dispositivos iTunes são configuradas de forma diferente. Para dispositivos portáteis (MTP) e dispositivos ADB, pode configurar regras para utilizadores individuais ou grupos de utilizadores e criar uma programação para quando as regras serão aplicadas. Para dispositivos iTunes, não pode fazer isso. Apenas pode permitir ou negar o acesso aos dados através da aplicação do iTunes para todos os utilizadores.

Como configurar regras de acesso a dispositivos móveis na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança** → **Controlo de Dispositivos**.
4. Sob **Definições do Controlo de Dispositivos**, selecione a aba **Tipos de dispositivos**.

   A tabela lista as regras de acesso para todos os dispositivos que estão presentes na classificação do componente Controlo de Dispositivos.
5. No menu de contexto do tipo de dispositivo **Dispositivos portáteis (MTP)**, configure o modo de acesso aos dispositivos móveis: **Permitir**, **Bloquear** ou **Depende do barramento de ligação**.
6. Para configurar regras de acesso a dispositivos móveis, clique duas vezes para abrir a lista de regras.
7. Configure a regra de acesso ao dispositivo móvel:

   a. No bloco **Regras de acesso**, clique no botão **Adicionar**.

      Abre-se uma janela para adicionar uma nova regra de acesso aos dispositivos móveis.

   b. No campo **Prioridade**, defina a prioridade de gravação da regra. Uma regra inclui os seguintes atributos: conta de utilizador, agendamento, permissões (leitura/escrita/acesso ADB) e prioridade.

      Uma regra tem uma prioridade específica. Se um utilizador tiver sido adicionado a vários grupos, o Kaspersky Endpoint Security regula o acesso a dispositivos com base na regra com a prioridade mais alta. O Kaspersky Endpoint Security permite-lhe atribuir prioridade de 0 a 10 000. Quanto maior for o valor, maior será a prioridade. Por outras palavras, uma entrada com o valor 0 tem a prioridade mais baixa.

      Por exemplo, pode conceder permissões apenas de leitura ao grupo Todos e conceder permissões de leitura/gravação ao grupo de administradores. Para tal, atribua uma prioridade de 1 ao grupo de administradores e atribua uma prioridade de 0 ao grupo Todos.

      A prioridade de uma regra de bloqueio é superior à prioridade de uma regra de permissão. Por outras palavras, se um utilizador tiver sido adicionado a vários grupos e a prioridade de todas as regras for a mesma, o Kaspersky Endpoint Security regula o acesso a dispositivos com base em qualquer regra de bloqueio existente.

   c. Sob **Regra para utilizadores e grupos**, selecione utilizadores ou grupos de utilizadores. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

   d. Clique em **Ok**.

8. Sob **Agendas para a regra de acesso selecionada**, configure um agendamento de acesso a dispositivos móveis para os utilizadores.

   Não é possível configurar um agendamento de acesso separado para dispositivos ADB. Pode configurar um agendamento de acesso comum para dispositivos ADB e dispositivos portáteis (MTP).

9. Configure as permissões de acesso dos utilizadores a dispositivos móveis no gestor de ficheiros (**Ler** / **Escrever**).

10. Configure o acesso aos dados num dispositivo móvel através da aplicação ADB ao selecionar a caixa de verificação **Aceder via ADB**.

    Se a caixa de seleção estiver desmarcada, quando o dispositivo móvel estiver ligado, a aplicação ADB será impedida de detetar o dispositivo.

11. Em **Aceder via iTunes**, configure o acesso aos dados no dispositivo móvel através da aplicação do iTunes.

    O Kaspersky Endpoint Security aplica as definições para acesso de dispositivos móveis através da aplicação do iTunes para todos os utilizadores. Não é possível configurar um agendamento de acesso separado para dispositivos iTunes.

12. Guarde as suas alterações.

Como configurar as regras de acesso a dispositivos móveis na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Security Controls** → **Device Control**.

5. No bloco **Device access rules**, clique na ligação **Devices and Wi-Fi networks**.

   A tabela lista as regras de acesso para todos os dispositivos que estão presentes na classificação do componente Controlo de Dispositivos.

6. Selecione o tipo de dispositivo **Portable devices (MTP)**.

   Esta ação abre os direitos de acesso a dispositivos portáteis (MTP).

7. Configure o modo de acesso a dispositivos móveis: **Allow**, **Block**, **Depends on bus** ou **Custom**.

8. Com o botão **Access via iTunes for all users ENABLED**, configure o acesso aos dados no dispositivo móvel através da aplicação do iTunes.

   O Kaspersky Endpoint Security aplica as definições para acesso de dispositivos móveis através da aplicação do iTunes para todos os utilizadores. Não é possível configurar um agendamento de acesso separado para dispositivos iTunes.

9. Se selecionar o modo **Custom**, tem de adicionar regras de acesso a dispositivos. Para tal, sob **Users and their rights**, clique no botão **Add** e configure a regra de acesso do dispositivo móvel:

    a. No campo **Priority**, defina a prioridade de gravação da regra. Uma regra inclui os seguintes atributos: conta de utilizador, agendamento, permissões (leitura/escrita/acesso ADB) e prioridade.

    Uma regra tem uma prioridade específica. Se um utilizador tiver sido adicionado a vários grupos, o Kaspersky Endpoint Security regula o acesso a dispositivos com base na regra com a prioridade mais alta. O Kaspersky Endpoint Security permite-lhe atribuir prioridade de 0 a 10 000. Quanto maior for o valor, maior será a prioridade. Por outras palavras, uma entrada com o valor 0 tem a prioridade mais baixa.

    Por exemplo, pode conceder permissões apenas de leitura ao grupo Todos e conceder permissões de leitura/gravação ao grupo de administradores. Para tal, atribua uma prioridade de 1 ao grupo de administradores e atribua uma prioridade de 0 ao grupo Todos.

    A prioridade de uma regra de bloqueio é superior à prioridade de uma regra de permissão. Por outras palavras, se um utilizador tiver sido adicionado a vários grupos e a prioridade de todas as regras for a mesma, o Kaspersky Endpoint Security regula o acesso a dispositivos com base em qualquer regra de bloqueio existente.

    b. Sob **User or group**, selecione utilizadores ou grupos de utilizadores para aceder a dispositivos móveis. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

    c. Sob **Access schedule**, configure um agendamento de acesso a dispositivos móveis para os utilizadores.

    > Não é possível configurar um agendamento de acesso separado para dispositivos ADB. Pode configurar um agendamento de acesso comum para dispositivos ADB e dispositivos portáteis (MTP).

    d. Configure as permissões de acesso dos utilizadores a dispositivos móveis no gestor de ficheiros (**Read** / **Write**).

    e. Configure o acesso aos dados num dispositivo móvel através da aplicação ADB ao selecionar a caixa de verificação **Access via ADB**.

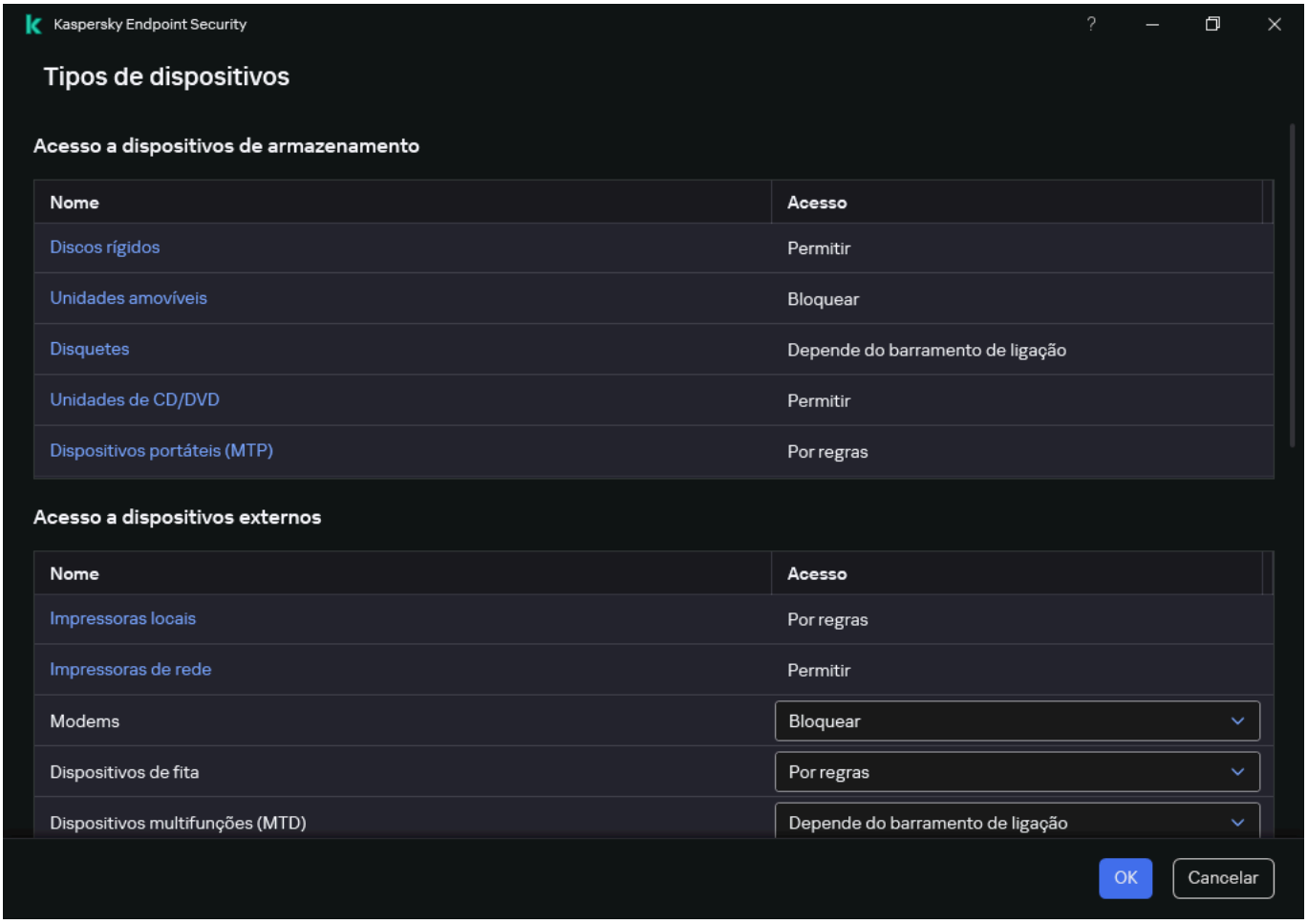
    Se a caixa de seleção estiver desmarcada, quando o dispositivo móvel estiver ligado, a aplicação ADB será impedida de detetar o dispositivo.

10. Guarde as suas alterações.

Como configurar regras de acesso a dispositivos móveis na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Dispositivos**.
3. No bloco **Definições de acesso**, clique no botão **Dispositivos e redes Wi-Fi**.

A janela aberta mostra as regras de acesso para todos os dispositivos incluídos na classificação de componentes do Controlo de Dispositivos.



Tipos de dispositivos no componente Controlo de Dispositivos

4. No bloco **Acesso a dispositivos de armazenamento**, clique na ligação **Dispositivos portáteis (MTP)**.

   Esta ação abre uma janela que contém as regras de acesso aos dispositivos portáteis (MTP).

5. Sob **Acesso**, configure o modo de acesso a dispositivos móveis: **Permitir**, **Bloquear**, **Depende do barramento de ligação** ou **Por regras**.

6. Se selecionar o modo **Por regras**, tem de adicionar regras de acesso a dispositivos:

   a. No bloco **Direitos dos utilizadores**, clique no botão **Adicionar**.

      Abre-se uma janela para adicionar uma nova regra de acesso aos dispositivos móveis.

   b. No campo **Prioridade**, defina a prioridade de gravação da regra. Uma regra inclui os seguintes atributos: conta de utilizador, agendamento, permissões (leitura/escrita/acesso ADB) e prioridade.

      Uma regra tem uma prioridade específica. Se um utilizador tiver sido adicionado a vários grupos, o Kaspersky Endpoint Security regula o acesso a dispositivos com base na regra com a prioridade mais alta. O Kaspersky Endpoint Security permite-lhe atribuir prioridade de 0 a 10 000. Quanto maior for o valor, maior será a prioridade. Por outras palavras, uma entrada com o valor 0 tem a prioridade mais baixa.

      Por exemplo, pode conceder permissões apenas de leitura ao grupo Todos e conceder permissões de leitura/gravação ao grupo de administradores. Para tal, atribua uma prioridade de 1 ao grupo de administradores e atribua uma prioridade de 0 ao grupo Todos.

      A prioridade de uma regra de bloqueio é superior à prioridade de uma regra de permissão. Por outras palavras, se um utilizador tiver sido adicionado a vários grupos e a prioridade de todas as regras for a mesma, o Kaspersky Endpoint Security regula o acesso a dispositivos com base em qualquer regra de bloqueio existente.

c. Sob **Condição**, ative a regra de acesso do dispositivo móvel.

d. Sob **Regras de acesso**, configure as permissões de acesso a dispositivos móveis para os utilizadores.

- Configure as permissões de acesso dos utilizadores a dispositivos móveis no gestor de ficheiros (**Ler** / **Escrever**).
- Configure o acesso aos dados num dispositivo móvel através da aplicação ADB ao selecionar a caixa de verificação **Aceder via ADB**.

  Se a caixa de seleção estiver desmarcada, quando o dispositivo móvel estiver ligado, a aplicação ADB será impedida de detetar o dispositivo.

e. Sob **Utilizadores**, selecione utilizadores ou grupos de utilizadores para aceder a dispositivos móveis. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

f. Sob **Agendamento de acesso aos dispositivos**, configure um agendamento de acesso a dispositivos para os utilizadores.

> Não é possível configurar um agendamento de acesso separado para dispositivos ADB. Pode configurar um agendamento de acesso comum para dispositivos ADB e dispositivos portáteis (MTP).

g. Em **Aceder via iTunes**, configure o acesso aos dados no dispositivo móvel através da aplicação do iTunes.

> O Kaspersky Endpoint Security aplica as definições para acesso de dispositivos móveis através da aplicação do iTunes para todos os utilizadores. Não é possível configurar um agendamento de acesso separado para dispositivos iTunes.

7. Guarde as suas alterações.

Como resultado, o acesso do utilizador a dispositivos móveis é restrito de acordo com as regras. Se proibiu o acesso a dispositivos móveis nas aplicações ADB e iTunes, ao ligar um dispositivo móvel, as aplicações ADB e iTunes são impedidas de detetar o dispositivo móvel.

Dispositivos móveis fiáveis

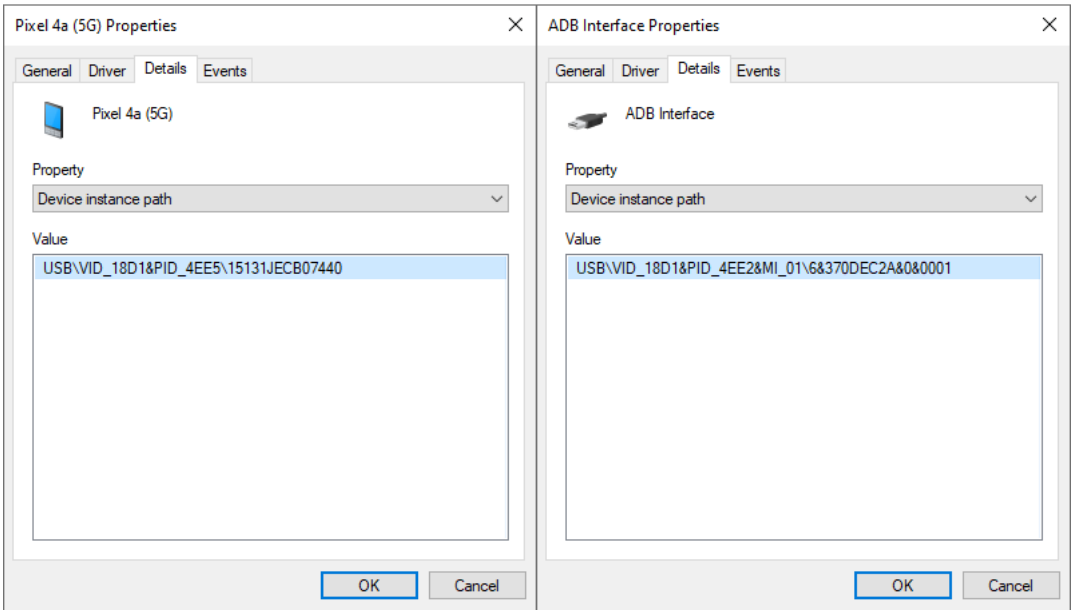
Dispositivos fiáveis são dispositivos aos quais os utilizadores especificados nas definições de dispositivo fiável têm acesso total, em qualquer altura.

O procedimento para adicionar um dispositivo móvel fiável é exatamente o mesmo que para outros tipos de dispositivos fiáveis. Pode adicionar um dispositivo móvel por ID ou modelo do dispositivo.

Para adicionar um dispositivo móvel fiável por ID, irá precisar de um ID exclusivo (Hardware ID – HWID). Pode encontrar o ID nas propriedades do dispositivo através das ferramentas do sistema operativo (veja a figura abaixo). A ferramenta Gestor de Dispositivos permite fazer isso. ID de dispositivos portáteis (MTP) e dispositivos ADB, iTunes são diferentes, inclusive para o mesmo dispositivo móvel. O ID de um dispositivo portátil (MTP) pode ter um formato idêntico a este: `15131JECB07440`. O ID de um dispositivo ADB pode ter um formato idêntico a este: `6&370DEC2A&0&0001`. Se desejar adicionar vários dispositivos específicos, é conveniente adicionar dispositivos por ID. Também pode utilizar máscaras.

Se instalou as aplicações ADB ou iTunes após ligar um dispositivo ao computador, o ID exclusivo do dispositivo poderá ser reposto. Isso significa que o Kaspersky Endpoint Security identificará esse dispositivo como um novo dispositivo. Se um dispositivo for fiável, adicione-o à lista fiável novamente.

Para adicionar um dispositivo móvel fiável por modelo de dispositivo, irá precisar do Vendor ID (VID) e Product ID (PID). Pode encontrar os ID nas propriedades do dispositivo através das ferramentas do sistema operativo (veja a figura abaixo). Modelo para inserir o VID e o PID: `VID_18D1&PID_4EE5`. Se usar dispositivos de um determinado modelo na sua organização, é conveniente adicionar dispositivos por modelo. Deste modo, pode adicionar todos os dispositivos deste modelo.



ID do Dispositivo no Gestor de Dispositivos

Gerir o acesso a dispositivos Bluetooth

O Kaspersky Endpoint Security permite gerir o acesso a dispositivos Bluetooth. Os dispositivos Bluetooth incluem teclados sem fio, ratos, auscultadores, impressoras, etc. Pode também utilizar o Bluetooth para comunicação, por exemplo. com um dispositivo móvel.

Quando os dispositivos Bluetooth são ligados ou desligados, a aplicação pode criar vários eventos sobre o dispositivo. O motivo para isso é que o sistema operativo pode detetar um dispositivo Bluetooth como vários dispositivos de tipos diferentes. O Kaspersky Endpoint Security também faz a gestão do adaptador Bluetooth ao qual o dispositivo está ligado como um dispositivo separado. É por isso que a aplicação cria um evento para cada um dos dispositivos detetados.

Pode selecionar um dos seguintes modos de acesso a dispositivos Bluetooth:

- **Permitir e não registar** . O Kaspersky Endpoint Security permite ligar qualquer dispositivo Bluetooth e não guarda informações sobre a ligação no registo de eventos. Pode ligar dispositivos Bluetooth de entrada (teclados, ratos, etc.), enviar dados por Bluetooth, gerir outros dispositivos Bluetooth (auscultadores, auriculares, etc.).

- **Permitir** . O Kaspersky Endpoint Security permite ligar quaisquer dispositivos Bluetooth. Pode ligar dispositivos Bluetooth de entrada (teclados, ratos, etc.), enviar dados por Bluetooth, gerir outros dispositivos Bluetooth (auscultadores, auriculares, etc.).

- **Bloquear** O Kaspersky Endpoint Security restringe o acesso a dispositivos Bluetooth. Pode permitir a ligação apenas de dispositivos de entrada Bluetooth (a classe Human Interface Devices). Estes dispositivos incluem teclados, ratos, joysticks, etc.

Não é possível criar uma lista de dispositivos Bluetooth fiáveis. Se restringiu o acesso a dispositivos com Bluetooth, apenas poderá conectar dispositivos de entrada Bluetooth.

Como configurar regras de acesso a dispositivos Bluetooth na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.

2. Na árvore da consola, selecione **Policies**.

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

4. Na janela de política, selecione **Controlos de segurança** → **Controlo de Dispositivos**.

5. Sob **Definições do Controlo de Dispositivos**, selecione a aba **Tipos de dispositivos**.

   A tabela lista as regras de acesso para todos os dispositivos que estão presentes na classificação do componente Controlo de Dispositivos.

6. No menu de contexto do tipo de dispositivo **Bluetooth**, configure o modo de acesso aos dispositivos Bluetooth: **Permitir** , **Bloquear** , **Permitir e não registar** .

7. Se selecionar o modo **Bloquear**, pode permitir a ligação apenas de dispositivos Bluetooth de entrada (teclados, ratos, etc.). Para fazer isso, em **Exclusões**, selecione a caixa de seleção **Dispositivos de entrada (ratos e teclados)**.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como configurar as regras de acesso a dispositivos Bluetooth na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Security Controls** → **Device Control**.

5. No bloco **Device access rules**, clique na ligação **Devices and Wi-Fi networks**.

   A tabela lista as regras de acesso para todos os dispositivos que estão presentes na classificação do componente Controlo de Dispositivos.

6. Selecione o tipo de dispositivo **Bluetooth devices**.

   Isso abre as definições de acesso ao dispositivo Bluetooth.

7. Configure o modo de acesso do dispositivo Bluetooth: **Allow**, **Block**, **Allow and do not log**.

8. Se selecionar o modo **Block**, pode permitir a ligação apenas de dispositivos Bluetooth de entrada (teclados, ratos, etc.). Para fazer isso, em **Exclusions**, selecione a caixa de seleção **Input devices (mice and keyboards)**.

9. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

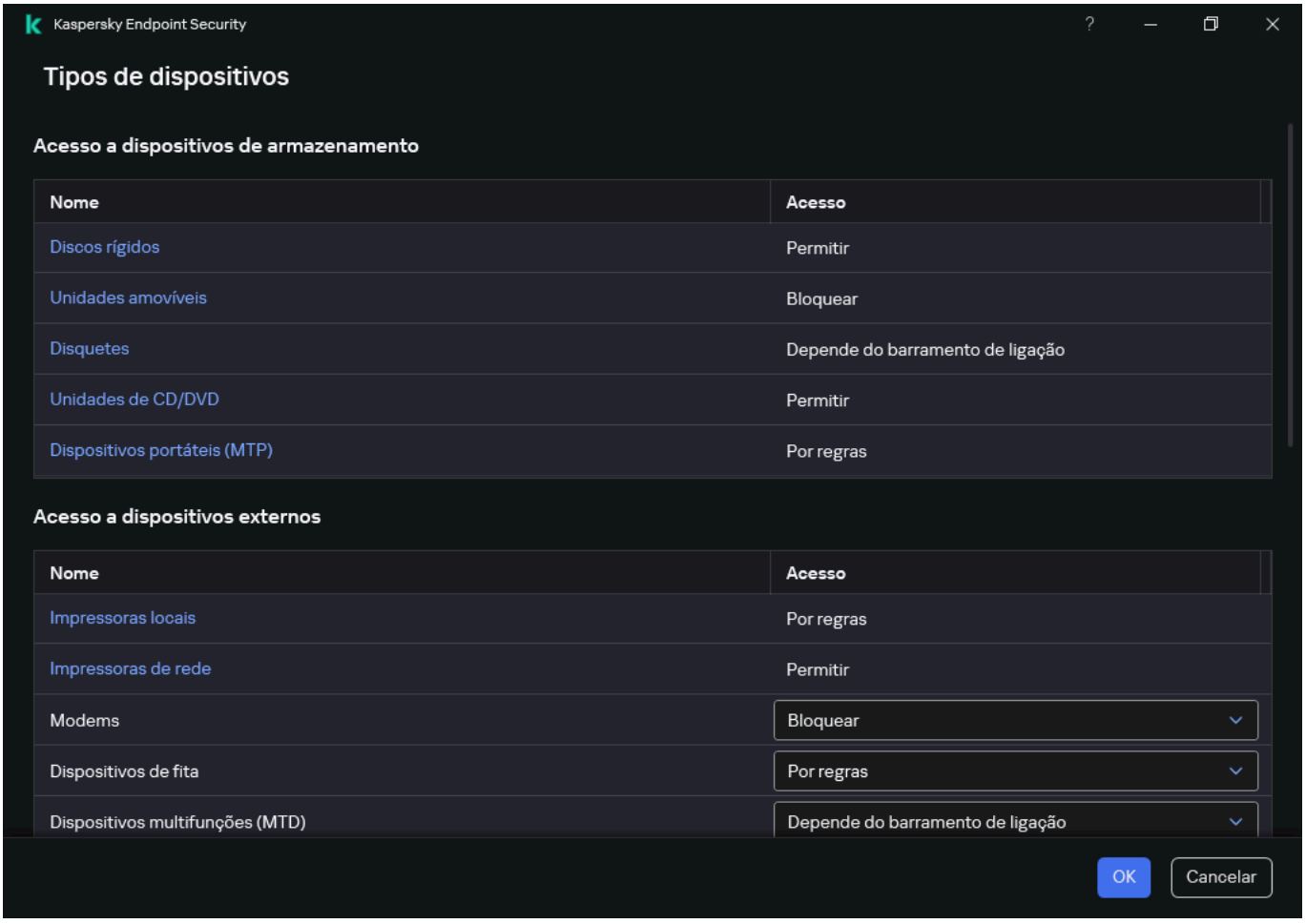
Como configurar regras de acesso a dispositivos com Bluetooth na interface da aplicação

1. Na janela principal da aplicação, clique no botão .

2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Dispositivos**.

3. No bloco **Definições de acesso**, clique no botão **Dispositivos e redes Wi-Fi**.

   A janela aberta mostra as regras de acesso para todos os dispositivos incluídos na classificação de componentes do Controlo de Dispositivos.



Tipos de dispositivos no componente Controlo de Dispositivos

4. No bloco **Acesso a dispositivos externos**, clique na ligação **Bluetooth**.

   Isso abre as definições de acesso ao dispositivo Bluetooth.

5. Em **Acesso**, configure o modo de acesso a dispositivos Bluetooth: **Permitir**, **Bloquear**, **Permitir e não registar**.

6. Se selecionar o modo **Bloquear**, pode permitir a ligação apenas de dispositivos Bluetooth de entrada (teclados, ratos, etc.). Para fazer isso, em **Exclusões**, selecione a caixa de seleção **Dispositivos de entrada (ratos e teclados)**.

7. Guarde as suas alterações.

Controlo de impressão

O controlo de impressão não é suportado em computadores baseados em Arm.

Pode utilizar o Controlo de impressão para configurar o acesso do utilizador às impressoras locais e de rede.

Controlo da impressora local

O Kaspersky Endpoint Security permite configurar o acesso a impressoras locais em dois níveis: *a ligar* e *a imprimir*.

O Kaspersky Endpoint Security controla a ligação da impressora local nos seguintes barramentos: USB, Porta Série (COM), Porta Paralela (LPT).

O Kaspersky Endpoint Security controla a ligação de impressoras locais a portas COM e LPT apenas ao nível do barramento. Assim, para impedir ligações de impressoras através de portas COM e LPT, tem de selecionar o modo de acesso Depende do barramento de ligação para impressoras locais e proibir ligações aos barramentos COM e LPT.

Para impressoras ligadas a USB, a aplicação exerce controlo em dois níveis: tipo de dispositivo (impressoras locais) e barramento de ligação (USB).

Pode selecionar um dos seguintes modos de acesso a impressoras locais por USB:

- **Permitir**. O Kaspersky Endpoint Security concede acesso total às impressoras locais para todos os utilizadores. Os utilizadores podem ligar impressoras e imprimir documentos através dos meios fornecidos pelo sistema operativo.

- **Bloquear**. O Kaspersky Endpoint Security bloqueia a ligação de impressoras locais. A aplicação permite ligar apenas impressoras fiáveis.

- **Depende do barramento de ligação**. O Kaspersky Endpoint Security permite ligar-se a impressoras locais de acordo com o estado de ligação de barramento USB (**Permitir** ou **Bloquear**).

- **Por regras**. Para controlar a impressão, tem de adicionar *regras de impressão*. Nas regras, pode selecionar utilizadores ou um grupo de utilizadores para os quais deseja permitir ou bloquear o acesso à impressão de documentos em impressoras locais.

Controlo das impressoras de rede

O Kaspersky Endpoint Security permite configurar o acesso à impressão em impressoras de rede. Pode selecionar um dos seguintes modos de acesso a impressoras de rede:

- **Permitir e não registar** . O Kaspersky Endpoint Security não controla a impressão em impressoras de rede. A aplicação concede acesso à impressão a todos os utilizadores e não guarda informações sobre a impressão no registo de eventos.
- **Permitir** . O Kaspersky Endpoint Security concede acesso à impressão em impressoras de rede a todos os utilizadores.
- **Bloquear** . O Kaspersky Endpoint Security restringe o acesso a impressoras de rede para todos os utilizadores. A aplicação permite o acesso apenas a impressoras fiáveis.
- **Por regras** . O Kaspersky Endpoint Security concede acesso à impressão de acordo com as regras de impressão. Nas regras, pode selecionar utilizadores ou um grupo de utilizadores que terão, ou não, permissão para imprimir documentos na impressora de rede.

Adicionar regras de impressão para impressoras

Como adicionar regras de impressão na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança** → **Controlo de Dispositivos**.
4. Sob **Definições do Controlo de Dispositivos**, selecione a aba **Tipos de dispositivos**.

   A tabela lista as regras de acesso para todos os dispositivos que estão presentes na classificação do componente Controlo de Dispositivos.
5. No menu de contexto dos tipos de dispositivos **Impressoras locais** e **Impressoras de rede**, configure o modo de acesso para as impressoras relevantes: **Permitir** , **Bloquear** , **Permitir e não registar** (apenas para impressoras de rede) ou **Depende do barramento de ligação** (apenas para impressoras locais).
6. Para configurar 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 utilizadores ou os grupos de utilizadores para os quais pretende aplicar a regra de impressão.

   a. Clique em **Adicionar**.

   Abre-se uma janela 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 utilizador, ação (permitir/bloquear) e prioridade.

Uma regra tem uma prioridade específica. Se um utilizador tiver sido adicionado a vários grupos, o Kaspersky Endpoint Security regula o acesso a dispositivos com base na regra com a prioridade mais alta. O Kaspersky Endpoint Security permite-lhe atribuir prioridade de 0 a 10 000. Quanto maior for o valor, maior será a prioridade. Por outras palavras, uma entrada com o valor 0 tem a prioridade mais baixa.

Por exemplo, pode conceder permissões apenas de leitura ao grupo Todos e conceder permissões de leitura/gravação ao grupo de administradores. Para tal, atribua uma prioridade de 1 ao grupo de administradores e atribua uma prioridade de 0 ao grupo Todos.

A prioridade de uma regra de bloqueio é superior à prioridade de uma regra de permissão. Por outras palavras, se um utilizador tiver sido adicionado a vários grupos e a prioridade de todas as regras for a mesma, o Kaspersky Endpoint Security regula o acesso a dispositivos com base em qualquer regra de bloqueio existente.

c. Sob **Ação**, configure o acesso do utilizador para imprimir na impressora.

d. Clique em **Utilizadores e grupos** e selecione utilizadores ou grupos de utilizadores para aceder à impressão. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

e. Clique em **Ok**.

9. Guarde as suas alterações.

Como adicionar regras de impressão na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Security Controls** → **Device Control**.

5. No bloco **Device access rules**, clique na ligação **Devices and Wi-Fi networks**.

   A tabela lista as regras de acesso para todos os dispositivos que estão presentes na classificação do componente Controlo de Dispositivos.

6. Selecione o tipo de dispositivo **Local printers** ou **Network printers**.

   Esta ação abre as regras de acesso à impressora.

7. Configure o modo de acesso para as impressoras relevantes: **Allow**, **Block**, **Allow and do not log** (apenas para impressoras de rede), **Depends on bus** (apenas para impressoras locais) ou **Custom**.

8. Se selecionar o modo **Custom**, tem de adicionar regras de impressão para impressoras locais ou de rede. Para tal, clique no botão **Add** na tabela de regras de impressão.

   Esta ação abre as definições da nova regra de impressão.

9. Atribua uma prioridade à entrada da regra. Uma entrada de regra inclui os seguintes atributos: conta de utilizador, ação (permitir/bloquear) e prioridade.

   Uma regra tem uma prioridade específica. Se um utilizador tiver sido adicionado a vários grupos, o Kaspersky Endpoint Security regula o acesso a dispositivos com base na regra com a prioridade mais alta. O Kaspersky Endpoint Security permite-lhe atribuir prioridade de 0 a 10 000. Quanto maior for o valor, maior será a prioridade. Por outras palavras, uma entrada com o valor 0 tem a prioridade mais baixa.

Por exemplo, pode conceder permissões apenas de leitura ao grupo Todos e conceder permissões de leitura/gravação ao grupo de administradores. Para tal, atribua uma prioridade de 1 ao grupo de administradores e atribua uma prioridade de 0 ao grupo Todos.

A prioridade de uma regra de bloqueio é superior à prioridade de uma regra de permissão. Por outras palavras, se um utilizador tiver sido adicionado a vários grupos e a prioridade de todas as regras for a mesma, o Kaspersky Endpoint Security regula o acesso a dispositivos com base em qualquer regra de bloqueio existente.

10. Sob **Action**, configure o acesso do utilizador para imprimir na impressora.

11. Sob **User or group**, selecione utilizadores ou grupos de utilizadores para aceder à impressão. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

12. Guarde as suas alterações.

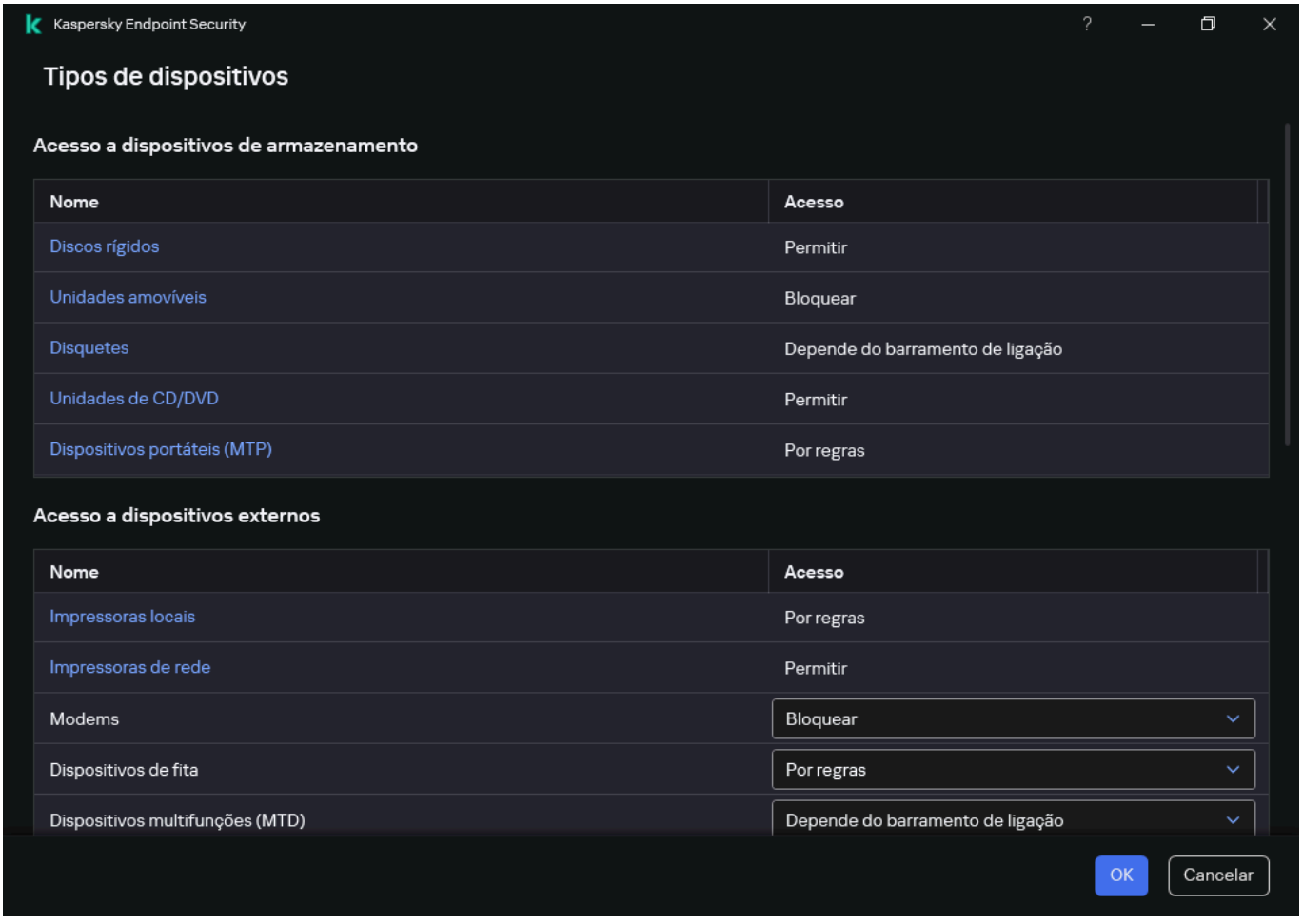
Como adicionar regras de impressão na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Dispositivos**.

3. No bloco **Definições de acesso**, clique no botão **Dispositivos e redes Wi-Fi**.

   A janela aberta mostra as regras de acesso para todos os dispositivos incluídos na classificação de componentes do Controlo de Dispositivos.



Tipos de dispositivos no componente Controlo de Dispositivos

4. Sob **Acesso a dispositivos externos**, clique em **Impressoras locais** ou **Impressoras de rede**.

   Esta ação abre uma janela com regras de acesso à impressora.

5. Em **Acesso a impressoras locais** ou **Acesso a impressoras da rede**, configure o modo de acesso para as impressoras: **Permitir**, **Bloquear**, **Permitir e não registar** (apenas para impressoras de rede), **Depende do barramento de ligação** (apenas para impressoras locais) ou **Por regras**.

6. Se selecionar o modo **Por regras**, tem de adicionar regras de impressão para impressoras. Selecione os utilizadores ou os grupos de utilizadores para os quais pretende aplicar a regra de impressão.

   a. Clique em **Adicionar**.

      Abre-se uma janela 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 utilizador, permissões (permitir/bloquear) e prioridade.

      Uma regra tem uma prioridade específica. Se um utilizador tiver sido adicionado a vários grupos, o Kaspersky Endpoint Security regula o acesso a dispositivos com base na regra com a prioridade mais alta. O Kaspersky Endpoint Security permite-lhe atribuir prioridade de 0 a 10 000. Quanto maior for o valor, maior será a prioridade. Por outras palavras, uma entrada com o valor 0 tem a prioridade mais baixa.

      Por exemplo, pode conceder permissões apenas de leitura ao grupo Todos e conceder permissões de leitura/gravação ao grupo de administradores. Para tal, atribua uma prioridade de 1 ao grupo de administradores e atribua uma prioridade de 0 ao grupo Todos.

      A prioridade de uma regra de bloqueio é superior à prioridade de uma regra de permissão. Por outras palavras, se um utilizador tiver sido adicionado a vários grupos e a prioridade de todas as regras for a mesma, o Kaspersky Endpoint Security regula o acesso a dispositivos com base em qualquer regra de bloqueio existente.

   c. Sob **Ação**, configure as permissões do utilizador para acesso à impressão.

   d. Sob **Utilizadores e grupos**, selecione utilizadores ou grupos de utilizadores para aceder à impressão. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

7. Guarde as suas alterações.

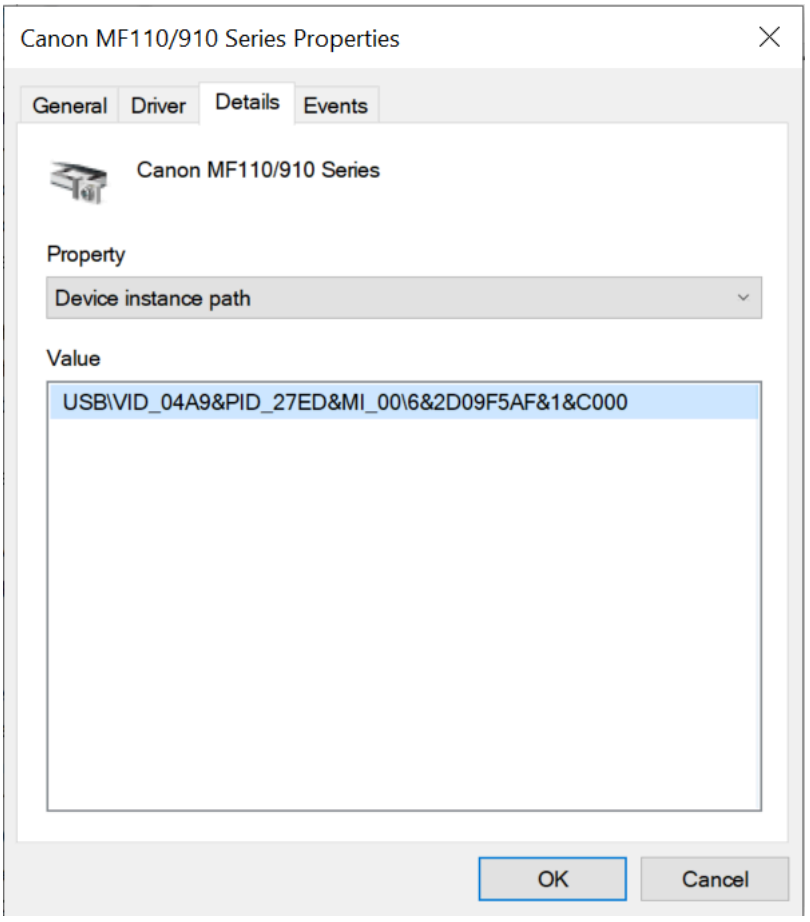
Impressoras fiáveis

Dispositivos fiáveis são dispositivos aos quais os utilizadores especificados nas definições de dispositivo fiável têm acesso total, em qualquer altura.

O procedimento para adicionar impressoras fiáveis é exatamente o mesmo que para outros tipos de dispositivos fiáveis. Pode adicionar impressoras locais por ID ou modelo do dispositivo. Só pode adicionar impressoras de rede por ID de dispositivo.

Para adicionar uma impressora local fiável por ID, irá precisar de um ID exclusivo (Hardware ID – HWID). Pode encontrar o ID nas propriedades do dispositivo através das ferramentas do sistema operativo (veja a figura abaixo). A ferramenta Device Manager permite fazer isso. O ID de uma impressora local tem um formato idêntico a este: `6&2D09F5AF&1&C000`. Se desejar adicionar vários dispositivos específicos, é conveniente adicionar dispositivos por ID. Também pode utilizar máscaras.

Para adicionar uma impressora local fiável por modelo de dispositivo, irá precisar do Vendor ID (VID) e Product ID (PID). Pode encontrar os ID nas propriedades do dispositivo através das ferramentas do sistema operativo (veja a figura abaixo). Modelo para inserir o VID e o PID: `VID_04A9&PID_27FD`. Se usar dispositivos de um determinado modelo na sua organização, é conveniente adicionar dispositivos por modelo. Deste modo, pode adicionar todos os dispositivos deste modelo.



ID do Dispositivo no Gestor de Dispositivos

Para adicionar uma impressora de rede fiável, irá precisar do ID do dispositivo. Para impressoras de rede, o ID do dispositivo pode ser o nome da rede da impressora (nome da impressora partilhada), o endereço IP da impressora ou o URL da impressora.

Controlo de ligações Wi-Fi

O Controlo de Dispositivos permite gerir a ligação Wi-Fi do computador portátil. As redes Wi-Fi públicas podem ser inseguras e o uso dessas redes pode resultar na perda de dados. O Controlo de Dispositivos permite bloquear a ligação de um utilizador ao Wi-Fi ou permitir a ligação apenas a redes fiáveis. Por exemplo, pode permitir a ligação apenas à rede Wi-Fi corporativa suficientemente segura. O Controlo de dispositivos irá bloquear o acesso a todas as redes Wi-Fi exceto às especificadas na lista fiável.

Nos computadores com o Windows 11, tem de ativar os serviços de localização para controlar as ligações Wi-Fi. Para o fazer, tem de ativar a opção dos **Serviços de localização** nas definições do sistema operativo (**Definições** → **Privacidade e segurança** → **Localização**). Se os Serviços de localização estiverem desativados, o Kaspersky Endpoint Security não controla as ligações a redes Wi-Fi.

Como restringir ligações Wi-Fi na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança** → **Controlo de Dispositivos**.
4. Sob **Definições do Controlo de Dispositivos**, selecione a aba **Tipos de dispositivos**.

   A tabela lista as regras de acesso para todos os dispositivos que estão presentes na classificação do componente Controlo de Dispositivos.
5. No menu de contexto do tipo de dispositivo **Wi-Fi**, selecione a ação Controlo de Dispositivos que é executada ao ligar-se ao Wi-Fi: **Permitir** (), **Bloquear** () ou **Bloquear com exceções** ().
6. Se selecionou a opção **Bloquear com exceções**, crie uma lista de redes Wi-Fi fiáveis:

   a. Clique duas vezes para abrir a lista de redes Wi-Fi fiáveis.

   b. No bloco **Redes Wi-Fi fiáveis**, clique no botão **Adicionar**.

   c. Esta ação abre uma janela; nessa janela, configure a rede Wi-Fi fiável (veja a figura abaixo):

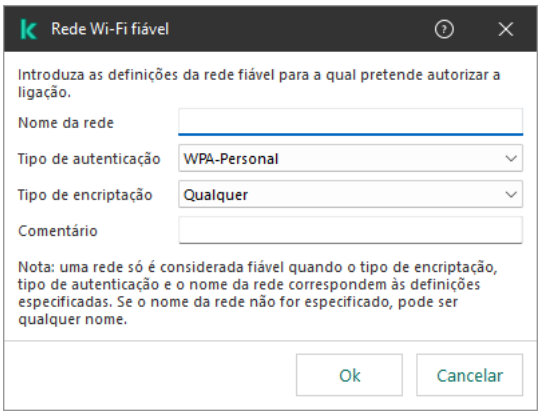
   - **Nome da rede**. Nome ou SSID (Service Set Identifier) da rede Wi-Fi.
   - **Tipo de autenticação**. Tipo de autenticação utilizada ao ligar-se à rede Wi-Fi.

     A partir do Kaspersky Endpoint Security for Windows versão 12.0, foi adicionado o suporte ao protocolo WPA3. Se uma política do Kaspersky Endpoint Security versão 12.2 for aplicada a um computador, o protocolo WPA2 será selecionado nos computadores com o Kaspersky Endpoint Security versão 11.11.0 e anterior; WPA2/WPA3 é selecionado para as versões 12.0 a 12.1; WPA3 é selecionado para versões 12.2 e posteriores.
   - **Tipo de encriptação**. Tipo de encriptação utilizada para proteger o tráfego Wi-Fi.
   - **Comentário**. Mais informações sobre a rede Wi-Fi adicionada.

   Pode ver as definições da rede Wi-Fi fiável nas definições do router.

   Uma rede Wi-Fi considera-se fiável se as suas definições corresponderem a todas as definições especificadas na regra.

7. Guarde as suas alterações.



Definições de rede Wi-Fi fiável

Como restringir ligações Wi-Fi na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Security Controls** → **Device Control**.
5. Sob **Device access rules**, selecione a aba **Devices and Wi-Fi networks**.

   A tabela lista as regras de acesso para todos os dispositivos que estão presentes na classificação do componente Controlo de Dispositivos.
6. No bloco **Wi-Fi networks**, clique na ligação **Wi-Fi**.
7. Na janela que se abre, selecione a ação Controlo de Dispositivos realizada ao ligar-se ao Wi-Fi: **Allow**, **Block** ou **Block with exclusions**.
8. Se selecionou a opção **Block with exclusions**, crie uma lista de redes Wi-Fi fiáveis:

   a. Clique duas vezes para abrir a lista de redes Wi-Fi fiáveis.

   b. No bloco **Trusted Wi-Fi networks**, clique no botão **Add**.

   c. Esta ação abre uma janela; nessa janela, configure a rede Wi-Fi fiável (veja a figura abaixo):

   - **Name**. Nome ou SSID (Service Set Identifier) da rede Wi-Fi.
   - **Authentication type**. Tipo de autenticação utilizada ao ligar-se à rede Wi-Fi.

   A partir do Kaspersky Endpoint Security for Windows versão 12.0, foi adicionado o suporte ao protocolo WPA3. Se uma política do Kaspersky Endpoint Security versão 12.2 for aplicada a um computador, o protocolo WPA2 será selecionado nos computadores com o Kaspersky Endpoint Security versão 11.11.0 e anterior; WPA2/WPA3 é selecionado para as versões 12.0 a 12.1; WPA3 é selecionado para versões 12.2 e posteriores.

- **Encryption type**. Tipo de encriptação utilizada para proteger o tráfego Wi-Fi.
- **Comment**. Mais informações sobre a rede Wi-Fi adicionada.

Pode ver as definições da rede Wi-Fi fiável nas definições do router.

> Uma rede Wi-Fi considera-se fiável se as suas definições corresponderem a todas as definições especificadas na regra.

9. Guarde as suas alterações.

Como restringir ligações Wi-Fi na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Dispositivos**.
3. No bloco **Definições de acesso**, clique no botão **Dispositivos e redes Wi-Fi**.

   A janela aberta mostra as regras de acesso para todos os dispositivos incluídos na classificação de componentes do Controlo de Dispositivos.
4. No bloco **Acesso a redes Wi-Fi**, clique na ligação **Wi-Fi**.

   A janela aberta mostra as regras de acesso à rede Wi-Fi.



Definições de acesso ao Wi-Fi

5. Sob **Acesso**, selecione a ação Controlo de Dispositivos realizada ao ligar-se ao Wi-Fi: **Permitir**, **Bloquear** ou **Bloquear com exceções**.

6. Se selecionou a opção **Bloquear com exceções**, crie uma lista de redes Wi-Fi fiáveis:

   a. No bloco **Redes Wi-Fi fiáveis**, clique no botão **Adicionar**.

   b. Esta ação abre uma janela; nessa janela, configure a rede Wi-Fi fiável (veja a figura abaixo):

   - **Nome da rede**. Nome ou SSID (Service Set Identifier) da rede Wi-Fi.
   - **Tipo de autenticação**. Tipo de autenticação utilizada ao ligar-se à rede Wi-Fi.

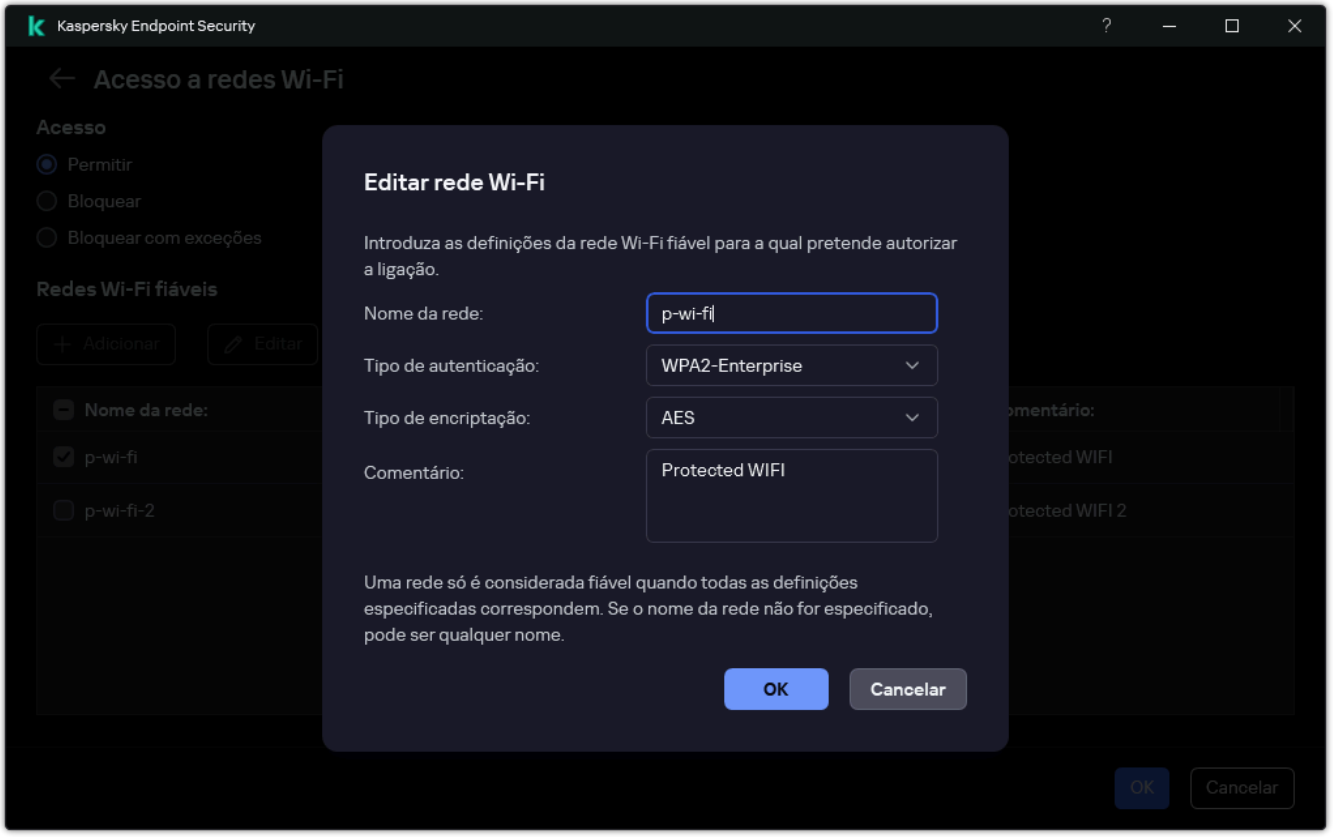
     A partir do Kaspersky Endpoint Security for Windows versão 12.0, foi adicionado o suporte ao protocolo WPA3. Se uma política do Kaspersky Endpoint Security versão 12.2 for aplicada a um computador, o protocolo WPA2 será selecionado nos computadores com o Kaspersky Endpoint Security versão 11.11.0 e anterior; WPA2/WPA3 é selecionado para as versões 12.0 a 12.1; WPA3 é selecionado para versões 12.2 e posteriores.

   - **Tipo de encriptação**. Tipo de encriptação utilizada para proteger o tráfego Wi-Fi.
   - **Comentário**. Mais informações sobre a rede Wi-Fi adicionada.

   Pode ver as definições da rede Wi-Fi fiável nas definições do router.

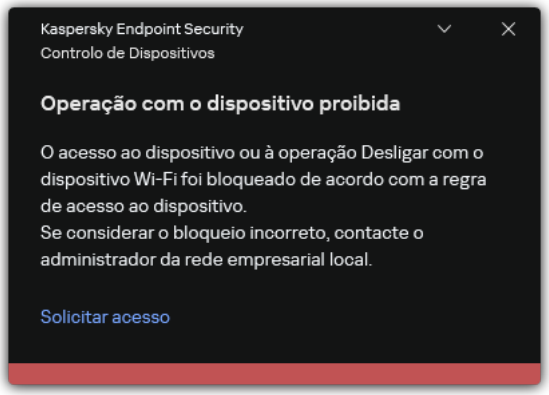
   Uma rede Wi-Fi considera-se fiável se as suas definições corresponderem a todas as definições especificadas na regra.

7. Guarde as suas alterações.



Definições de rede Wi-Fi fiável

Como resultado, quando um utilizador tenta ligar-se a uma rede Wi-Fi que não está listada como fiável, a aplicação bloqueia a ligação e exibe uma notificação (veja a figura abaixo).



Notificação de Controlo de Dispositivos

Monitorizar o uso de unidades amovíveis

Monitorizar o uso de unidades amovíveis inclui:

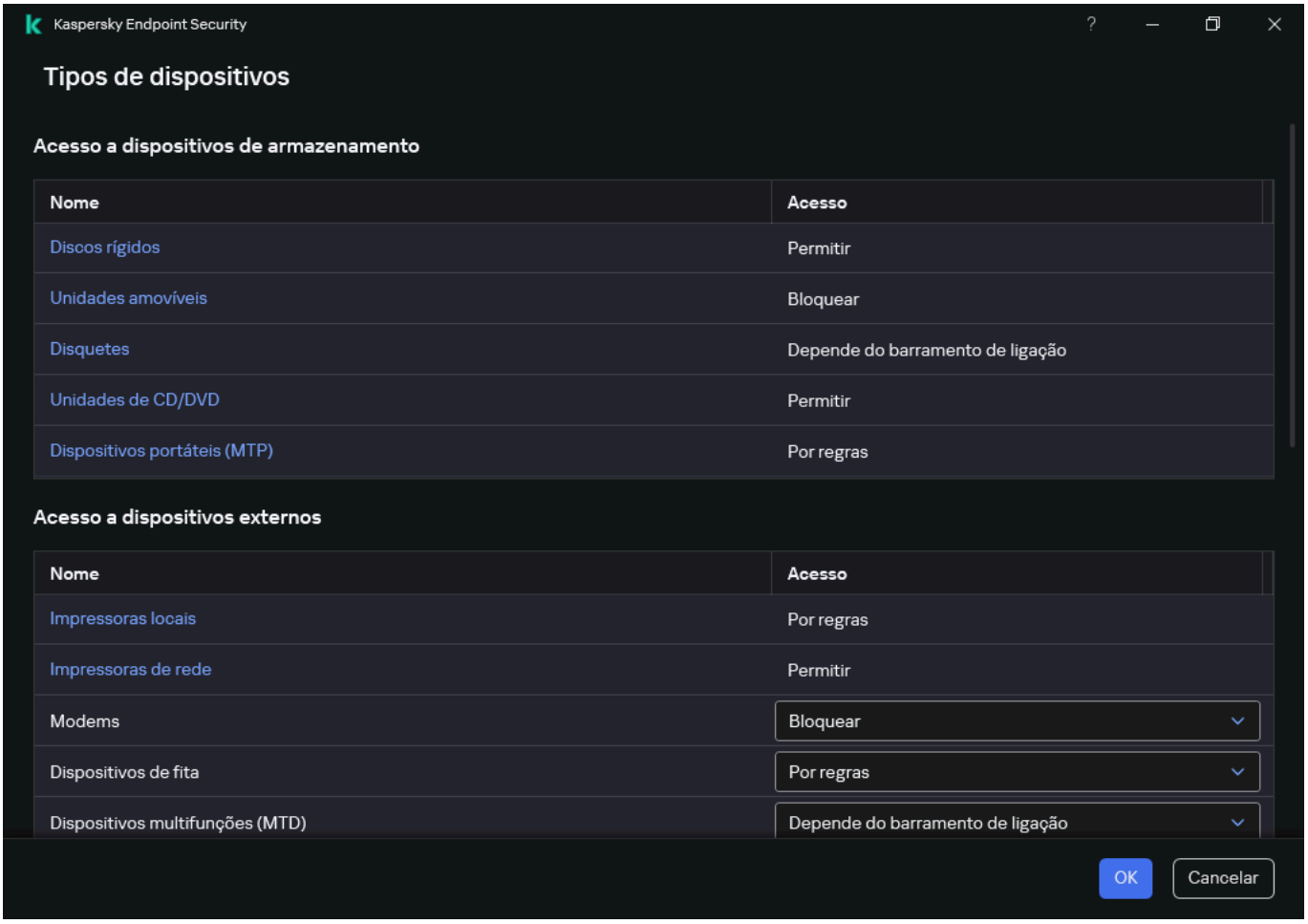
- Monitorizar operações em ficheiros em unidades amovíveis.
- Monitorizar a conexão e desconexão de unidades amovíveis fiáveis.

  O Kaspersky Endpoint Security permite monitorizar a conexão e a desconexão de todos os dispositivos fiáveis e não apenas das unidades amovíveis. É possível ativar o registo de eventos nas definições de notificação para o componente Controlo de Dispositivos. Os eventos têm o nível de gravidade *Mensagem informativa*.

Para ativar o monitorização do uso de uma unidade amovível:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança** → **Controlo de Dispositivos**.
3. No bloco **Definições de acesso**, clique no botão **Dispositivos e redes Wi-Fi**.

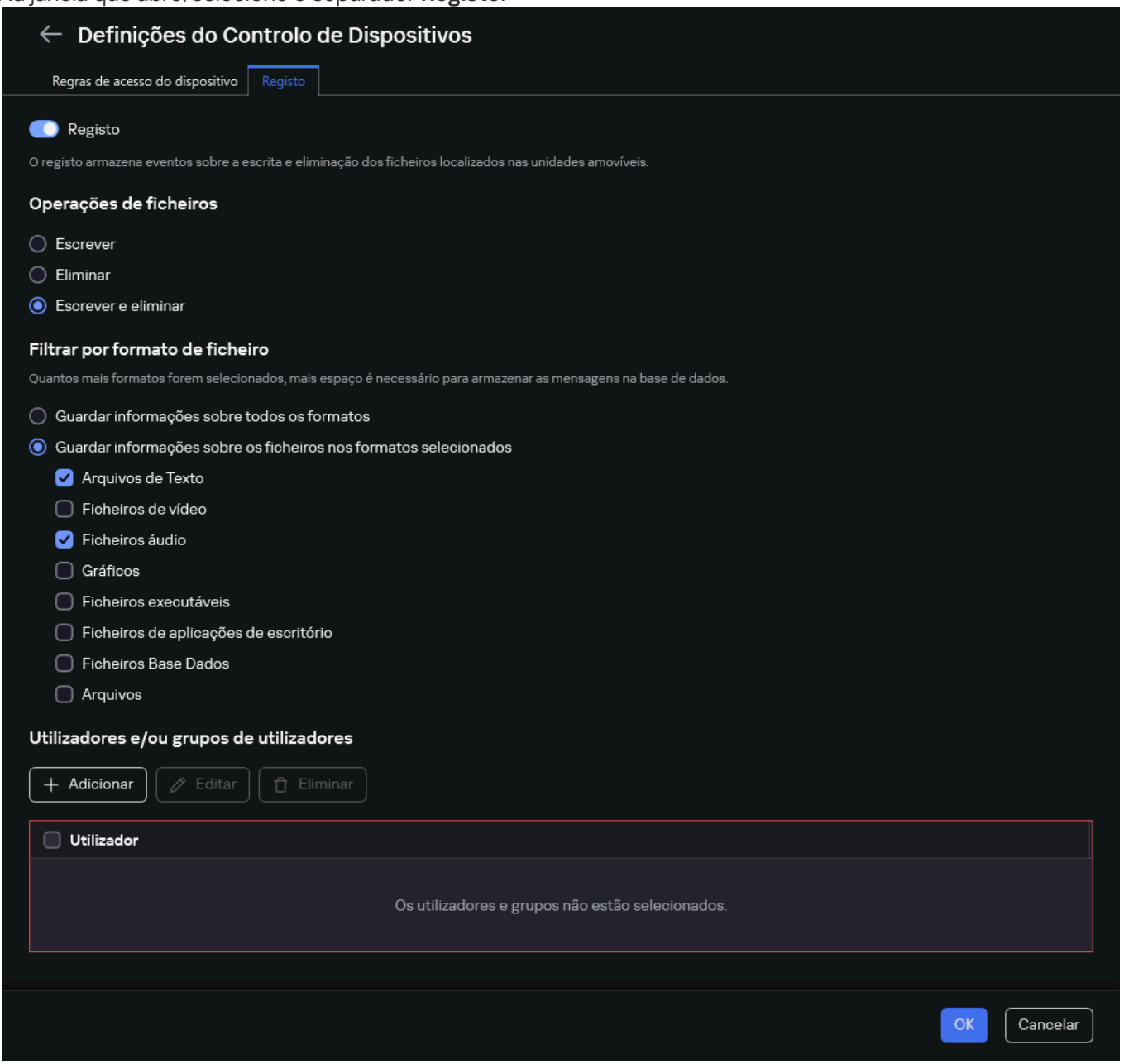
A janela aberta mostra as regras de acesso para todos os dispositivos incluídos na classificação de componentes do Controlo de Dispositivos.



Tipos de dispositivos no componente Controlo de Dispositivos

4. No bloco **Acesso a dispositivos de armazenamento**, selecione **Unidades amovíveis**.

5. Na janela que abre, selecione o separador **Registo**.



As definições de monitorização de utilização de unidade removível

6. Ative o botão de alternar **Registo**.

7. No bloco **Operações de ficheiros**, selecione as operações que pretende monitorizar: **Escrever**, **Eliminar**.

8. No bloco **Filtrar por formato de ficheiro**, selecione os formatos de ficheiros cujas operações associadas devem ser registadas pelo Controlo de Dispositivos.

9. Selecione os utilizadores ou o grupo de utilizadores cujo uso de unidades amovíveis pretende monitorizar.

10. Guarde as suas alterações.

Como resultado, quando os utilizadores gravam informações em ficheiros localizados em unidades amovíveis ou eliminam ficheiros de unidades amovíveis, o Kaspersky Endpoint Security guarda informações relativas a essas operações no registo de eventos e envia os eventos para o Kaspersky Security Center. Pode ver os eventos associados a ficheiros em unidades amovíveis na Consola de Administração do Kaspersky Security Center na área de trabalho do nó **Administration Server** no separador **Events**. Para que os eventos sejam apresentados no registo de eventos do Kaspersky Endpoint Security local, deve selecionar a caixa de verificação **Operação de ficheiro realizada** nas definições de notificação do componente Controlo de Dispositivos.

Alterar a duração da cache

O componente Controlo de Dispositivos regista eventos relacionados com os dispositivos monitorizados, como a ligação e o desligamento de um dispositivo, leitura de um ficheiro a partir de um dispositivo, gravação de um ficheiro num dispositivo e outros eventos. O Controlo de Dispositivos permite ou bloqueia a ação de acordo com as definições do Kaspersky Endpoint Security.

O Controlo de Dispositivos guarda as informações sobre eventos por um período específico de tempo denominado *período de armazenamento na cache*. Se as informações sobre um evento forem armazenadas na cache e este evento se repetir, não há necessidade de notificar o Kaspersky Endpoint Security de tal ou de mostrar outro pedido para conceder acesso à ação correspondente, como, por exemplo, ligar um dispositivo. Isto torna mais cómodo trabalhar com um dispositivo.

Um evento considera-se um evento duplicado se todas as definições do evento que se seguem corresponderem ao registo na cache:

- ID do dispositivo
- SID da conta do utilizador que tenta aceder
- Categoria do dispositivo
- Ação realizada com o dispositivo
- Permissão da aplicação para esta ação: permitida ou recusada
- Caminho para o processo utilizado para realizar a ação
- Ficheiro que está a ser acedido

Antes de alterar o período de armazenamento na cache, desative a Autodefesa do Kaspersky Endpoint Security. Depois de alterar o período de armazenamento na cache, ative a Autodefesa.

Para alterar o período de armazenamento na cache:

1. Abra o editor de registo no computador.
2. No editor de registo, vá para a seguinte secção:
   - Para sistemas operativos de 64 bits:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES.14.2\environment]`
   - Para sistemas operativos de 32 bits:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\environment]`
3. Abra `DeviceControlEventsCachePeriod` para edição.
4. Defina o número de minutos durante o qual o Controlo de Dispositivos deve guardar informações sobre um evento antes de essas informações serem eliminadas.

Ações com dispositivos fiáveis

Dispositivos fiáveis são dispositivos aos quais os utilizadores especificados nas definições de dispositivo fiável têm acesso total, em qualquer altura.

Para trabalhar com dispositivos fiáveis, pode conceder acesso a um utilizador individual, a um grupo de utilizadores ou a todos os utilizadores da organização.

Por exemplo, se a sua organização não permitir a utilização de unidades amovíveis, mas os administradores usarem unidades amovíveis no seu trabalho, pode permitir unidades amovíveis apenas para um grupo de administradores. Para tal, adicione unidades amovíveis à lista fiável e configure as permissões de acesso do utilizador.

Não é recomendado adicionar mais de 5000 dispositivos fiáveis, uma vez que tal pode provocar instabilidade do sistema.

O Kaspersky Endpoint Security permite adicionar um dispositivo à lista fiável das seguintes maneiras:

- Se o Kaspersky Security Center não estiver implementado na sua organização, pode ligar o dispositivo ao computador e adicioná-lo à lista fiável nas definições da aplicação. Para distribuir a lista de dispositivos fiáveis a todos os computadores da sua organização, pode ativar a união das listas dos dispositivos fiáveis numa política ou procedimento de exportação/importação.

- Se o Kaspersky Security Center estiver implementado na sua organização, pode detetar todos os dispositivos ligados remotamente e criar uma lista de dispositivos fiáveis na política. A lista de dispositivos fiáveis estará disponível em todos os computadores aos quais é aplicada a política.

O Kaspersky Endpoint Security permite controlar a utilização de dispositivos fiáveis (conexão e desconexão). É possível ativar o registo de eventos nas definições de notificação para o componente Controlo de Dispositivos. Os eventos têm o nível de gravidade *Informational messages*.

Adicionar um dispositivo à lista fiável

O Kaspersky Security Center recebe informações sobre os dispositivos se o Kaspersky Endpoint Security estiver instalado nos computadores, o Controlo de Dispositivos estiver ativado e a transmissão de dados do dispositivo estiver ativada. Só é possível adicionar um dispositivo à lista fiável se as informações sobre esse dispositivo estiverem disponíveis no Kaspersky Security Center.

Por predefinição, quando um dispositivo é adicionado à lista de dispositivos fiáveis, o acesso ao dispositivo é permitido a todos os utilizadores (no grupo de utilizadores Todos).

Pode adicionar um dispositivo à lista fiável de acordo com os seguintes dados:

- **Dispositivos por ID**. Cada dispositivo possui um identificador exclusivo (Hardware ID ou HWID). Pode ver a ID nas propriedades de dispositivo utilizando ferramentas do sistema operativo. Exemplo de um ID do dispositivo: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Se desejar adicionar vários dispositivos específicos, é conveniente adicionar dispositivos por ID.

- **Dispositivos por modelo**. Cada dispositivo possui um Vendor ID (VID) e um Product ID (PID). Pode examinar os IDs nas propriedades do dispositivo utilizando ferramentas do sistema operativo. Modelo para inserir o VID e o PID: `VID_1234&PID_5678`. Se usar dispositivos de um determinado modelo na sua organização, é conveniente adicionar dispositivos por modelo. Deste modo, pode adicionar todos os dispositivos deste modelo.

- **Dispositivos por máscara de ID**. Se estiver a utilizar vários dispositivos com IDs semelhantes, pode utilizar máscaras para adicionar dispositivos à lista fiável. O caráter `*` substitui qualquer conjunto de carateres. O Kaspersky Endpoint Security não suporta o caráter `?` ao introduzir uma máscara. Por exemplo, `WDC_C*`.

- **Dispositivos por máscara de modelo**. Se estiver a utilizar vários dispositivos com VIDs ou PIDs semelhantes (por exemplo, dispositivos do mesmo fabricante), pode utilizar máscaras para adicionar dispositivos à lista fiável. O caráter `*` substitui qualquer conjunto de carateres. O Kaspersky Endpoint Security não suporta o caráter `?` ao introduzir uma máscara. Por exemplo, `VID_05AC&PID_*`.

Como adicionar um dispositivo à lista fiável na Administration Console (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.

2. Na árvore da consola, selecione **Policies**.

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

4. Na janela de política, selecione **Controlos de segurança** → **Controlo de Dispositivos**.

5. Na parte direita da janela, selecione o separador **Dispositivos fiáveis**.

6. Selecione a caixa de verificação **Unir valores ao herdar** se desejar criar uma lista consolidada de dispositivos fiáveis para todos os computadores da empresa.

   As listas de dispositivos fiáveis nas políticas principais e secundárias serão unidas. As listas serão unidas, desde que a união de valores ao herdar esteja ativada. Os dispositivos fiáveis da política principal são apresentados nas políticas secundárias numa visualização apenas de leitura. Não é possível alterar ou eliminar dispositivos fiáveis da política principal.

7. Clique no botão **Adicionar** e selecione um método para adicionar um dispositivo à lista fiável.

8. Para filtrar dispositivos, selecione um tipo de dispositivo na lista pendente **Tipo de dispositivo** (por exemplo, **Unidades amovíveis**).

   O Kaspersky Endpoint Security não suporta a adição de dispositivos do tipo **Disquetes** à lista fiável.

9. No campo **Nome / modelo**, introduza a ID do dispositivo, o modelo (VID e PID) ou máscara, consoante o método de adição selecionado.

   A adição de dispositivos por máscara de modelo (VID e PID) funciona da seguinte forma: se introduzir uma máscara de modelo que não corresponda a nenhum modelo, o Kaspersky Endpoint Security verifica se a 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 de modelo corresponder a esta parte do ID do dispositivo, os dispositivos que correspondem à máscara serão adicionados à lista de dispositivos fiáveis no computador. Simultaneamente, a lista de dispositivos no Kaspersky Security Center fica vazia quando clica no botão **Upgrade**. Para apresentar a lista de dispositivos corretamente, pode adicionar dispositivos por máscara de ID do dispositivo.

10. Para filtrar dispositivos, no campo **Computador**, insira o nome do computador ou de uma máscara para o nome do computador ao qual o dispositivo está conectado.

    O caráter `*` substitui qualquer conjunto de carateres. O caráter `?` substitui qualquer caráter individual.

11. Clique em **Upgrade**.

    A tabela apresenta uma lista de dispositivos que cumprem os critérios de filtragem definidos.

12. Selecione as caixas de verificação junto aos nomes dos dispositivos que pretende adicionar à lista fiável.

13. No campo **Comentário**, insira uma descrição do motivo da adição de dispositivos à lista fiável.

14. Clique no botão **Select** à direita do campo **Permitir a utilizadores e/ou grupos de utilizadores**.

    Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

    Por predefinição, o acesso a dispositivos fiáveis é permitido para o grupo Todos.

15. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como adicionar um dispositivo à lista fiável na Web Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda à secção **Trusted Zone**.

5. Na janela que abre, clique na ligação **Devices**.

   Abre-se uma janela que contém uma lista de dispositivos fiáveis.

6. Na parte direita da janela, selecione o separador **Dispositivos fiáveis**.

7. Selecione a caixa de verificação **Merge values when inheriting** se desejar criar uma lista consolidada de dispositivos fiáveis para todos os computadores da empresa.

   As listas de dispositivos fiáveis nas políticas principais e secundárias serão unidas. As listas serão unidas, desde que a união de valores ao herdar esteja ativada. Os dispositivos fiáveis da política principal são apresentados nas políticas secundárias numa visualização apenas de leitura. Não é possível alterar ou eliminar dispositivos fiáveis da política principal.

8. Clique em **Add**.

   Abre-se o formulário para adicionar um dispositivo fiável.

9. Em **User or group**, selecione os utilizadores aos quais pretende permitir o acesso a dispositivos fiáveis.

   Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

   Por predefinição, o acesso a dispositivos fiáveis é permitido para o grupo Todos.

10. Para filtrar dispositivos, selecione um tipo de dispositivo na lista pendente **Device type** (por exemplo, **Removable drives**).

    O Kaspersky Endpoint Security não suporta a adição de dispositivos do tipo **Floppy disks** à lista fiável.

11. Se não souber o ID exato ou o modelo do dispositivo, selecione a caixa de seleção **Use mask**.

12. Selecione como pretende adicionar o dispositivo: por ID do dispositivo ou por modelo (VID e PID).

    A adição de dispositivos por máscara de modelo (VID e PID) funciona da seguinte forma: se introduzir uma máscara de modelo que não corresponda a nenhum modelo, o Kaspersky Endpoint Security verifica se a 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 de modelo corresponder a esta parte do ID do dispositivo, os dispositivos que correspondem à máscara serão adicionados à lista de dispositivos fiáveis no computador. Ao mesmo tempo, será apresentada no Kaspersky Security Center uma lista de dispositivos vazia. Para apresentar a lista de dispositivos corretamente, pode adicionar dispositivos por máscara de ID do dispositivo.

13. Para filtrar dispositivos, no campo **Search for trusted devices**, insira o nome do computador ou de uma máscara para o nome do computador ao qual o dispositivo está conectado.

    O caráter `*` substitui qualquer conjunto de carateres. O caráter `?` substitui qualquer caráter individual.

    A tabela apresenta uma lista de dispositivos que cumprem os critérios de filtragem definidos.

14. Selecione as caixas de verificação junto aos nomes dos dispositivos que pretende adicionar à lista fiável.

15. No campo **Comment**, insira uma descrição do motivo da adição de dispositivos à lista fiável.

16. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como adicionar um dispositivo à lista fiável na interface da aplicação

1. Na janela principal da aplicação, clique no botão .

2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Dispositivos**.

3. No bloco **Definições de acesso**, clique no botão **Dispositivos fiáveis**.

   Abre-se a lista de dispositivos fiáveis.

4. Clique em **Selecionar**.

   Abre-se a lista de dispositivos ligados. A lista de dispositivos depende do valor selecionado na lista pendente **Mostrar dispositivos ligados**.

5. Na lista de dispositivos, selecione o dispositivo que pretende adicionar à lista fiável.

   O Kaspersky Endpoint Security não suporta a adição de dispositivos do tipo **Disquetes** à lista fiável.

6. No campo **Comentário**, pode fornecer quaisquer informações relevantes sobre o dispositivo fiável.

7. Selecione os utilizadores ou grupos de utilizadores para os quais pretende permitir o acesso a dispositivos fiáveis.

   Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

8. Guarde as suas alterações.

Quando um dispositivo está ligado, o Kaspersky Endpoint Security verifica a lista de dispositivos fiáveis para um utilizador autorizado. Se o dispositivo for fiável, o Kaspersky Endpoint Security permite o acesso ao dispositivo com todas as permissões, mesmo se o acesso ao tipo de dispositivo ou ao barramento de ligação for negado. Se o dispositivo não for fiável e o acesso for negado, pode solicitar acesso ao dispositivo bloqueado.

Exportar e importar a lista de dispositivos fiáveis

Para distribuir a lista de dispositivos fiáveis a todos os computadores da sua organização, pode utilizar o procedimento de exportação/importação.

Por exemplo, se precisar de distribuir uma lista de unidades amovíveis fiáveis, deve fazer o seguinte:

1. Conecte sequencialmente unidades amovíveis ao seu computador.

2. Nas definições do Kaspersky Endpoint Security, adicione as unidades amovíveis à lista fiável. Se necessário, configure as permissões de acesso do utilizador. Por exemplo, autorize administradores apenas a acederem a unidades amovíveis.

3. Exporte a lista de dispositivos fiáveis nas definições do Kaspersky Endpoint Security (consulte as instruções abaixo).

4. Distribua o ficheiro da lista de dispositivos fiáveis para outros computadores na sua organização. Por exemplo, coloque o ficheiro numa pasta partilhada.

5. Importe a lista de dispositivos fiáveis nas definições do Kaspersky Endpoint Security para outros computadores da organização (consulte as instruções abaixo).

Para importar ou exportar a lista de dispositivos fiáveis:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Dispositivos**.
3. No bloco **Definições de acesso**, clique no botão **Dispositivos fiáveis**.

   Abre-se a lista de dispositivos fiáveis.
4. Para exportar a lista de dispositivos fiáveis:
   a. Selecione os dispositivos fiáveis que pretende exportar.
   b. Clique em **Exportar**.
   c. Na janela que surgir, especifique o nome do ficheiro XML para o qual pretende exportar a lista de dispositivos fiáveis, e selecione a pasta onde pretende guardar este ficheiro e clique no botão Guardar.
   d. Guardar o ficheiro.

      O Kaspersky Endpoint Security exporta toda a lista de dispositivos fiáveis para o ficheiro XML.
5. Para importar a lista de dispositivos fiáveis:
   a. Na lista pendente **Importar**, selecione a ação relevante: **Importar e adicionar a existente** ou **Importar e substituir existente**.
   b. Na janela que surgir, selecione o ficheiro XML do qual deseja importar a lista de dispositivos fiáveis.
   c. Abrir o ficheiro.
6. Guarde as suas alterações.

Quando um dispositivo está ligado, o Kaspersky Endpoint Security verifica a lista de dispositivos fiáveis para um utilizador autorizado. Se o dispositivo for fiável, o Kaspersky Endpoint Security permite o acesso ao dispositivo com todas as permissões, mesmo se o acesso ao tipo de dispositivo ou ao barramento de ligação for negado.

Obter acesso a um dispositivo bloqueado

Ao configurar o Controlo de Dispositivos, pode bloquear acidentalmente o acesso a um dispositivo necessário para o trabalho.

Se o Kaspersky Security Center não estiver implementado na sua organização, pode fornecer acesso a um dispositivo nas configurações do Kaspersky Endpoint Security. Por exemplo, pode adicionar o dispositivo à lista fiável ou desativar temporariamente o Controlo de Dispositivos.

Se o Kaspersky Security Center estiver implementado na sua organização e uma política tiver sido aplicada aos computadores, pode fornecer acesso a um dispositivo na Consola de Administração.

Modo online para conceder acesso

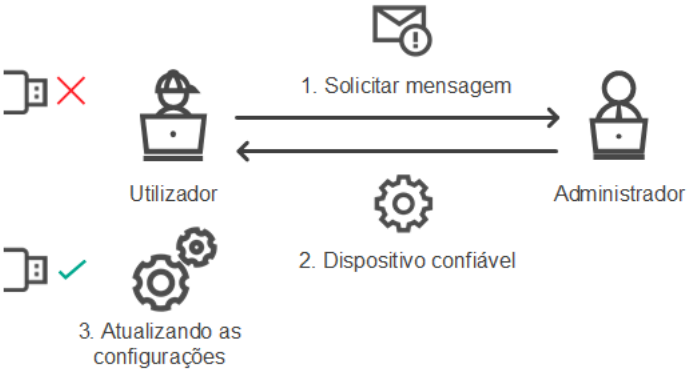
Pode conceder acesso a um dispositivo bloqueado no modo online apenas se o Kaspersky Security Center estiver implementado na organização e uma política tiver sido aplicada ao computador. O computador deve ter a capacidade de estabelecer uma ligação ao Servidor de Administração.

A concessão de acesso no modo online consiste nos seguintes passos:

1. O utilizador envia ao administrador uma mensagem com um pedido de acesso.
2. O administrador recebe uma mensagem com a solicitação na consola do Kaspersky Security Center.

   A consola do Kaspersky Security Center tem uma seleção de eventos predefinida *User requests* para fácil rastreamento de mensagens de utilizadores.
3. O administrador adiciona o dispositivo à lista fiável.

   Pode adicionar um dispositivo fiável numa política para o grupo de administração ou nas definições da aplicação local para um computador individual.
4. O administrador atualiza as definições do Kaspersky Endpoint Security no computador do utilizador.



Esquema para conceder acesso a um dispositivo no modo online

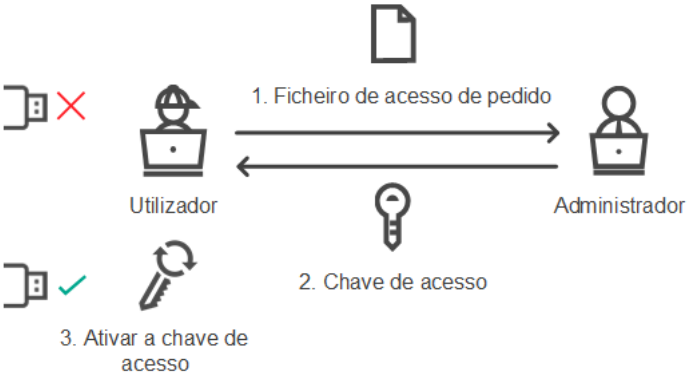
Modo offline para conceder acesso

Pode conceder acesso a um dispositivo bloqueado no modo offline apenas se o Kaspersky Security Center estiver implementado na organização e uma política tiver sido aplicada ao computador. Nas definições da política, na secção **Controlo de Dispositivos**, a caixa de verificação **Permitir pedidos de acesso temporário** deve ser selecionada.

Se precisar de conceder acesso temporário a um dispositivo bloqueado, mas não puder adicionar o dispositivo à lista fiável, pode conceder acesso ao dispositivo no modo offline. Desta maneira, pode conceder acesso a um dispositivo bloqueado, mesmo se o computador não tiver acesso à rede ou se o computador estiver fora da rede empresarial.

A concessão de acesso no modo offline consiste nos seguintes passos:

1. O utilizador cria um ficheiro de pedido de acesso e envia-o ao administrador.
2. O administrador cria uma chave de acesso a partir do ficheiro de pedido de acesso e envia-o ao utilizador.
3. O utilizador ativa a chave de acesso.



Esquema para conceder acesso a um dispositivo no modo offline

Modo online para conceder acesso

Pode conceder acesso a um dispositivo bloqueado no modo online apenas se o Kaspersky Security Center estiver implementado na organização e uma política tiver sido aplicada ao computador. O computador deve ter a capacidade de estabelecer uma ligação ao Servidor de Administração.

Um utilizador solicita acesso a um dispositivo bloqueado da seguinte maneira:

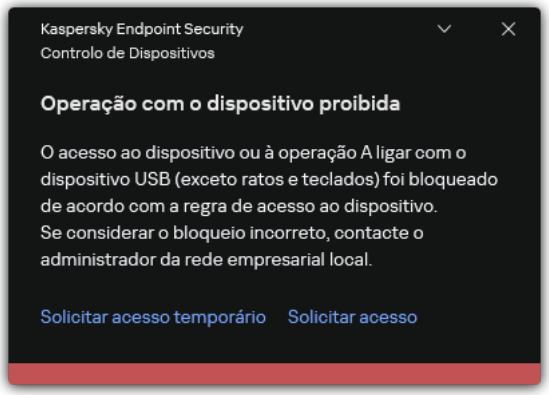
1. Ligue o dispositivo ao computador.

   O Kaspersky Endpoint Security irá apresentar uma notificação a indicar que o acesso ao dispositivo está bloqueado (ver a figura abaixo).

2. Clique na hiperligação **Solicitar acesso**.

   Esta ação abre uma janela com uma mensagem para o administrador. Esta mensagem contém informações sobre o dispositivo bloqueado.

3. Clique em **Enviar**.



Notificação de Controlo de Dispositivos

A seguir, o administrador na consola do Kaspersky Security Center recebe o evento *Mensagem de bloqueio do acesso ao dispositivo para o administrador*. O evento inclui o nome do utilizador, nome do computador, dados do dispositivo para o qual o utilizador está a tentar obter acesso e outras informações. É possível configurar a forma como o administrador é notificado sobre esses eventos e, por exemplo, selecionar notificações por e-mail. A consola do Kaspersky Security Center tem uma seleção de eventos predefinida *User requests* para fácil rastreamento de mensagens de utilizadores.

Para permitir o acesso, tem de adicionar o dispositivo à lista fiável. Após atualizar as definições do Kaspersky Endpoint Security no computador, o utilizador pode obter acesso ao dispositivo.

Modo offline para conceder acesso

Pode conceder acesso a um dispositivo bloqueado no modo offline apenas se o Kaspersky Security Center estiver implementado na organização e uma política tiver sido aplicada ao computador. Nas definições da política, na secção **Controlo de Dispositivos**, a caixa de verificação **Permitir pedidos de acesso temporário** deve ser selecionada.

Um utilizador solicita acesso a um dispositivo bloqueado da seguinte maneira:

1. Ligue o dispositivo ao computador.

   O Kaspersky Endpoint Security irá apresentar uma notificação a indicar que o acesso ao dispositivo está bloqueado (ver a figura abaixo).

2. Clique na hiperligação **Solicitar acesso temporário**.

   Abre-se uma janela que contém uma lista dos dispositivos ligados.

3. Na lista de dispositivos ligados, selecione o dispositivo ao qual pretende obter acesso.

4. Clique em **Gerar ficheiro de acesso de pedido**.

5. No campo **Duração do acesso**, especifique o período de tempo durante o qual pretende ter acesso ao dispositivo.

6. Guarde o ficheiro na memória do computador.

Como resultado, um ficheiro de pedido de acesso com a extensão * .akey será transferido para a memória do computador. Use qualquer método disponível para enviar o ficheiro de pedido de acesso ao dispositivo ao administrador da LAN empresarial.



Notificação de Controlo de Dispositivos

Como é que o administrador pode criar uma chave de acesso para o dispositivo bloqueado na Administration Console (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Managed devices** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração ao qual o computador cliente em questão pertence.
3. Na área de trabalho, selecione o separador **Devices**.
4. Na lista de computadores clientes, selecione o computador cujo utilizador necessita de acesso temporário a um dispositivo bloqueado.
5. No menu de contexto do computador, selecione **Conceder acesso em modo offline**.
6. Esta ação abre uma janela; nessa janela, selecione o separador **Controlo de Dispositivos**.
7. Clique no botão **Procurar** e transfira o ficheiro de pedido de acesso recebido do utilizador.

   Irá ver informações sobre o dispositivo bloqueado ao qual o utilizador solicitou acesso.
8. Se necessário, altere o valor da definição **Duração do acesso**.

   Por predefinição, a definição **Duração do acesso** aceita o valor indicado pelo utilizador ao criar o ficheiro de pedido de acesso.
9. Especifique o valor da definição **Ativar por**.

   Esta configuração define o período de tempo durante o qual o utilizador pode ativar o acesso ao dispositivo bloqueado utilizando a chave de acesso fornecida.
10. Guarde o ficheiro da chave de acesso na memória do computador.

Como é que o administrador pode criar uma chave de acesso para o dispositivo bloqueado na Web Console e Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Assets (Devices)**.
2. Na lista de computadores clientes, selecione o computador cujo utilizador necessita de acesso temporário a um dispositivo bloqueado.
3. Clique no botão de reticências (...) acima da lista de computadores e, em seguida, clique no botão **Grant access to the device in offline mode**.
4. Na janela que surgir, selecione a secção **Device Control**.
5. Clique no botão **Overview** e transfira o ficheiro de pedido de acesso recebido do utilizador.

   Irá ver informações sobre o dispositivo bloqueado ao qual o utilizador solicitou acesso.
6. Se necessário, altere o valor da definição **Access duration (hours)**.

   Por predefinição, a definição **Access duration (hours)** aceita o valor indicado pelo utilizador ao criar o ficheiro de pedido de acesso.

7. Especifique o período durante o qual a chave de acesso pode ser ativada no dispositivo.

   Esta configuração define o período de tempo durante o qual o utilizador pode ativar o acesso ao dispositivo bloqueado utilizando a chave de acesso fornecida.

8. Guarde o ficheiro da chave de acesso na memória do computador.

Como resultado, a chave de acesso ao dispositivo bloqueado será transferida para a memória do computador. Um ficheiro da chave de acesso possui a extensão * .acode. Use qualquer método disponível para enviar a chave de acesso ao dispositivo bloqueado ao utilizador.

O utilizador ativa a chave de acesso da seguinte maneira:

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Controlos de segurança** → **Controlo de Dispositivos**.

3. No bloco **Pedido de acesso**, clique no botão **Solicitar acesso ao dispositivo**.

4. Na janela que abre, clique no botão **Ativar chave de acesso**.

5. Na janela que abre, selecione o ficheiro com a chave de acesso ao dispositivo que recebeu do administrador da rede empresarial.

   Isto abre uma janela contendo informações sobre a disposição do acesso.

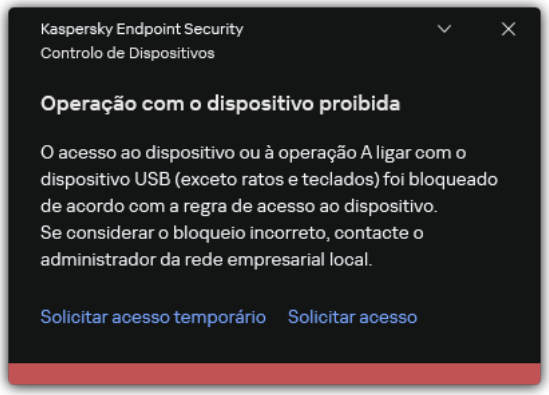
6. Clique em **OK**.

Como resultado, o utilizador recebe acesso ao dispositivo durante o período de tempo definido pelo administrador. O utilizador recebe o conjunto completo de direitos para aceder ao dispositivo (leitura e escrita). O acesso ao dispositivo será bloqueado quando a chave expirar. Se o utilizador exigir acesso permanente ao dispositivo, adicione-o à lista fiável.

Editar modelos de mensagens de Controlo de Dispositivos

Quando o utilizador tenta aceder a um dispositivo bloqueado, o Kaspersky Endpoint Security apresenta uma mensagem a declarar que o acesso ao dispositivo está bloqueado ou que uma operação com os conteúdos do dispositivo é proibida. Os especialistas da Kaspersky fornecem um modelo de uma mensagem ao utilizador a descrever as razões pelas quais o acesso ao dispositivo foi bloqueado (consulte a figura abaixo).

São fornecidas variáveis especiais para gerir os modelos da mensagem (por exemplo, %USER_NAME%). As variáveis permitem que um único modelo de mensagem seja usado para diferentes computadores. Ao gerar uma mensagem, o Kaspersky Endpoint Security recupera o valor da variável das definições do sistema operativo e insere-o na mensagem correspondente ao computador, utilizador e evento específicos.



Notificação de Controlo de Dispositivos

Se o utilizador considerar que o acesso ao dispositivo foi bloqueado incorretamente ou que uma operação com os conteúdos do dispositivo foi proibida por engano, o utilizador pode enviar uma mensagem ao administrador local da rede da empresa clicando na ligação na mensagem apresentada relativa à ação bloqueada. Para o fazer, o utilizador tem de clicar nos botões **Solicitar acesso** ou **Solicitar acesso temporário** e enviar uma mensagem ao administrador a descrever a situação. Também pode preparar um modelo da mensagem para o administrador, acrescentando-lhe dados que possam informar a sua decisão de permitir ou bloquear o acesso ao dispositivo. Depois de o utilizador solicitar acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio do acesso ao dispositivo para o administrador**. A descrição do evento contém uma mensagem para o administrador com variáveis substituídas. Pode visualizar estes eventos na consola do Kaspersky Security Center utilizando a seleção de eventos predefinida **User requests**. Se a sua organização não tiver o Kaspersky Security Center implementado ou não houver uma ligação ao Servidor de Administração, a aplicação irá enviar uma mensagem ao administrador para o endereço de e-mail especificado.

Como alterar os modelos de mensagem do Controlo de Dispositivos na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança** → **Controlo de Dispositivos**.
4. No bloco **Definições dos modelos de mensagem**, clique no botão **Modelos**.
5. Irá abrir-se uma janela; nessa janela, configure os modelos do Controlo das Aplicações:

   - **Mensagem sobre o bloqueio**. Modelo da mensagem que surge quando um utilizador tenta aceder a um dispositivo bloqueado. Esta mensagem surge também quando um utilizador tenta executar uma operação no conteúdo do dispositivo que foi bloqueado para este utilizador.
   - **Mensagem para o administrador**. Um modelo da mensagem que é enviada para o administrador da rede local quando o utilizador considera que o acesso ao dispositivo foi bloqueado por erro ou que uma operação com conteúdo do dispositivo foi proibida por erro.

   Para adicionar uma variável ao texto do modelo, coloque o cursor na posição desejada, clique em **Variável** e selecione a variável necessária na lista de opções disponíveis.

Também pode restaurar o texto do modelo padrão.

6. Guarde as suas alterações.

Como alterar os modelos de mensagem do Controlo de Dispositivos na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Security Controls** → **Device Control**.
5. No bloco **Message templates**, configure os modelos para mensagens de Controlo das Aplicações:

   - **Message to user**. Modelo da mensagem que surge quando um utilizador tenta aceder a um dispositivo bloqueado. Esta mensagem surge também quando um utilizador tenta executar uma operação no conteúdo do dispositivo que foi bloqueado para este utilizador.
   - **Message to administrator**. Um modelo da mensagem que é enviada para o administrador da rede local quando o utilizador considera que o acesso ao dispositivo foi bloqueado por erro ou que uma operação com conteúdo do dispositivo foi proibida por erro.

   Para adicionar uma variável ao texto do modelo, coloque o cursor na posição desejada, clique em **Add variable** e selecione a variável necessária na lista de opções disponíveis.

   Também pode restaurar o texto do modelo padrão.
6. Guarde as suas alterações.

Como alterar os modelos de mensagem do Controlo de Dispositivo na interface de aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança** → **Controlo das aplicações**.
3. No bloco **Modelos de mensagem**, configure os modelos para mensagens de Controlo das Aplicações:

   - **Mensagem sobre o bloqueio**. Modelo da mensagem que surge quando um utilizador tenta aceder a um dispositivo bloqueado. Esta mensagem surge também quando um utilizador tenta executar uma operação no conteúdo do dispositivo que foi bloqueado para este utilizador.
   - **Mensagem para o administrador**. Um modelo da mensagem que é enviada para o administrador da rede local quando o utilizador considera que o acesso ao dispositivo foi bloqueado por erro ou que uma operação com conteúdo do dispositivo foi proibida por erro.

   Para adicionar uma variável ao texto do modelo, coloque o cursor na posição desejada, clique em **Adicionar variável** e selecione a variável necessária na lista de opções disponíveis.

   Também pode restaurar o texto do modelo padrão.
4. Guarde as suas alterações.

Anti-Bridging

O Anti-Bridging inibe a criação de pontes de rede ao impedir o estabelecimento simultâneo de várias ligações de rede a um computador. Isto permite-lhe proteger uma rede empresarial contra ataques através de redes não protegidas e não autorizadas.

O Anti-Bridging regula o estabelecimento de ligações de rede utilizando as *regras de ligação*.

As regras de ligação foram criadas para os seguintes tipos predefinidos de dispositivos:

- Adaptadores de rede;
- Adaptadores de Wi-Fi;
- Modems.

Se uma regra de ligação for ativada, o Kaspersky Endpoint Security:

- Bloqueia a ligação ativa ao estabelecer uma nova ligação, se o tipo de dispositivo especificado na regra for usado para ambas as ligações;
- Bloqueia as ligações estabelecidas utilizando os tipos de dispositivos para os quais as regras de prioridade inferior são utilizadas.

Ativar Anti-Bridging

O Anti-Bridging encontra-se desativado por predefinição.

Para ativar Anti-Bridging:

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Dispositivos**.
3. No bloco **Definições de acesso**, clique no botão **Anti-Bridging**.
4. Use o botão de alternar **Ativar Anti-Bridging** para ativar ou desativar esta funcionalidade.
5. Guarde as suas alterações.

Após a ativação de Anti-Bridging, o Kaspersky Endpoint Security bloqueia ligações já estabelecidas, de acordo com as regras de ligação.

Alterar o estado de uma regra de ligação

Para alterar o estado de uma regra de ligação:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Dispositivos**.
3. No bloco **Definições de acesso**, clique no botão **Anti-Bridging**.
4. No bloco **Regras para os dispositivos**, selecione a regra cujo estado pretende alterar.
5. Use os botões de alternar na coluna **Controlo** para ativar ou desativar a regra.
6. Guarde as suas alterações.

Alterar a prioridade de uma regra de ligação

Para alterar a prioridade de uma regra de ligação:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Dispositivos**.
3. No bloco **Definições de acesso**, clique no botão **Anti-Bridging**.
4. No bloco **Regras para os dispositivos**, selecione a regra cuja prioridade pretende alterar.
5. Use os botões **Para cima**/**Para baixo** para definir a prioridade da regra de ligação.

   Quanto mais alta for a posição de uma regra na lista de regras, mais alta será a sua prioridade. O Anti-Bridging bloqueia todas as ligações, exceto uma ligação estabelecida utilizando o tipo de dispositivo para o qual a regra de prioridade mais elevada é utilizada.
6. Guarde as suas alterações.

Controlo de Anomalias Adaptativo

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para estações de trabalho. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para servidores.

O componente Controlo de Anomalias Adaptativo monitoriza e bloqueia ações que não são típicas dos computadores na rede de uma empresa. O Controlo de Anomalias Adaptativo usa um conjunto de regras para rastrear comportamento invulgar (por exemplo, a regra *Início da Microsoft PowerShell da aplicação de ambiente de trabalho*). As regras são criadas pelos especialistas da Kaspersky com base em cenários típicos de atividade maliciosa. Pode configurar o modo como o Controlo de Anomalias Adaptativo manuseia cada regra e, por exemplo, permitir a execução de scripts do PowerShell que automatizam determinadas tarefas do fluxo de trabalho. O Kaspersky Endpoint Security atualiza o conjunto de regras a par das bases de dados da aplicação. As atualizações dos conjuntos de regras devem ser confirmadas manualmente.

Definições do Controlo de Anomalias Adaptativo

A configuração do Controlo de Anomalias Adaptativo consiste nas seguintes etapas:

1. Formação do Controlo de Anomalias Adaptativo.

   Depois de ativar o Controlo de Anomalias Adaptativo, as suas regras funcionam no *modo de formação*. Durante a formação, o Controlo de Anomalias Adaptativo monitoriza o acionamento de regras e envia os eventos de acionamento para o Kaspersky Security Center. Cada regra tem sua própria duração do modo de formação. A duração do modo de formação é estabelecida por peritos da Kaspersky. Normalmente, o modo de formação fica ativo durante duas semanas.

   Se uma regra não for acionada de todo durante a formação, o Controlo de Anomalias Adaptativo irá considerar as ações associadas a esta regra como não típicas. O Kaspersky Endpoint Security irá bloquear todas as ações associadas a essa regra.

   Se uma regra for acionada durante a formação, o Kaspersky Endpoint Security regista os eventos no relatório de acionamento da regra e no repositório **Rule triggers in Smart Training state**.

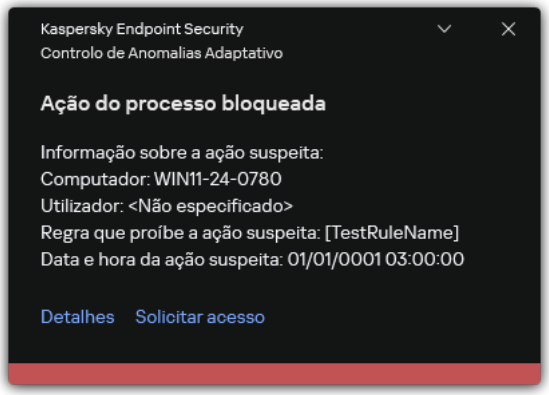
2. A analisar o relatório de acionamento de regras.

   O administrador analisa o relatório de acionamento de regras ou o conteúdo do repositório do **Rule triggers in Smart Training state**. O administrador pode então selecionar o comportamento do Controlo de Anomalias Adaptativo quando a regra é acionada: bloquear ou permitir. O administrador pode também continuar a monitorizar o funcionamento da regra e prolongar a duração do modo de formação. Se o administrador não realizar nenhuma ação, a aplicação continuará também a funcionar no modo de formação. O prazo do modo de formação é reiniciado.

O Controlo de Anomalias Adaptativo é configurado em tempo real através dos seguintes canais:

- O Controlo de Anomalias Adaptativo começa automaticamente a bloquear as ações associadas às regras que nunca foram acionadas no modo de formação.
- O Kaspersky Endpoint Security adiciona novas regras ou remove as obsoletas.
- O administrador configura a operação do Controlo de Anomalias Adaptativo depois de rever o relatório do acionamento de regras e o conteúdo do repositório de **Rule triggers in Smart Training state**. Recomendamos que verifique o relatório sobre o acionamento das regras e os conteúdos do armazenamento **Rule triggers in Smart Training state**.

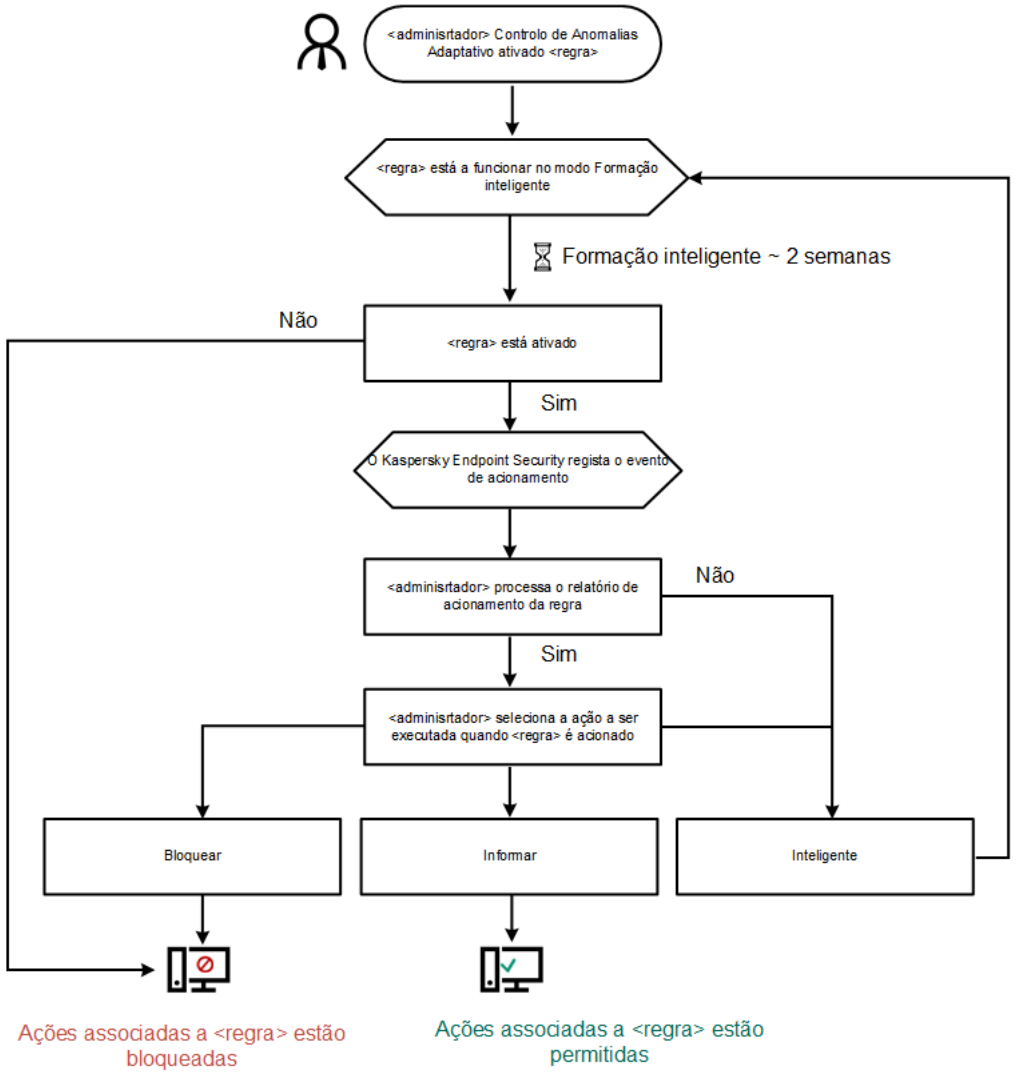
Quando uma aplicação maliciosa tentar realizar uma ação, o Kaspersky Endpoint Security irá bloquear a ação e exibir uma notificação (ver figura abaixo).



Notificação do Controlo de Anomalias Adaptativo

Algoritmo operacional do Controlo de Anomalias Adaptativo

O Kaspersky Endpoint Security decide se permite ou bloqueia uma ação associada a uma regra com base no seguinte algoritmo (ver figura abaixo).



Algoritmo operacional do Controlo de Anomalias Adaptativo

Formação do Controlo de Anomalias Adaptativo

O Controlo de Anomalias Adaptativo inclui um conjunto de regras (padrões de comportamento). Depois de ativar o Controlo de Anomalias Adaptativo, as suas regras funcionam no *modo de formação*. Durante a formação, o Controlo de Anomalias Adaptativo monitoriza o acionamento de regras e envia os eventos de acionamento para o Kaspersky Security Center. O Controlo de Anomalias Adaptativo não bloqueia a atividade da aplicação no computador, mas apenas informa o administrador. Também pode selecionar manualmente a ação que é efetuada quando uma regra de Controlo de Anomalias Adaptativo é acionada.

Como ver a lista de regras de Controlo de Anomalias Adaptativo na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Security Controls** → **Adaptive Anomaly Control**.
5. Selecione a caixa de verificação **Controlo de Anomalias Adaptativo**.
6. Em **Definições da regra do Controlo de Anomalias Adaptativo**, veja a lista de regras.

   Por padrão, todas as regras funcionam no modo **Inteligente**.
7. Se for necessário, confirme a atualização da regra do Controlo de Anomalias Adaptativo.
8. Se for necessário, selecione uma ação quando uma regra de Controlo de Anomalias Adaptativo é acionada:

   - **Bloquear**. Se esta ação estiver selecionada, quando uma regra do Controlo de Anomalias Adaptativo é acionada, o Kaspersky Endpoint Security bloqueia a atividade abrangida pela regra e regista uma entrada que contém informação sobre a atividade.
   - **Informar**. Se esta ação estiver selecionada, quando uma regra do Controlo de Anomalias Adaptativo é acionada, o Kaspersky Endpoint Security permite a atividade abrangida pela regra e regista uma entrada que contém informação sobre a atividade.
9. Se for necessário, desative as regras que não pretende utilizar.
10. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ver as regras do Controlo de Anomalias Adaptativo na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Security Controls** → **Adaptive Anomaly Control**.
5. Ative o botão de alternar **Adaptive Anomaly Control ENABLED**.

6. Em **Rules**, veja a lista de regras.

   Por padrão, todas as regras funcionam no modo **Smart**.

7. Se for necessário, confirme a atualização da regra do Controlo de Anomalias Adaptativo.

8. Se for necessário, selecione uma ação quando uma regra de Controlo de Anomalias Adaptativo é acionada:

   - **Block**. Se esta ação estiver selecionada, quando uma regra do Controlo de Anomalias Adaptativo é acionada, o Kaspersky Endpoint Security bloqueia a atividade abrangida pela regra e regista uma entrada que contém informação sobre a atividade.

   - **Inform**. Se esta ação estiver selecionada, quando uma regra do Controlo de Anomalias Adaptativo é acionada, o Kaspersky Endpoint Security permite a atividade abrangida pela regra e regista uma entrada que contém informação sobre a atividade.

9. Se for necessário, desative as regras que não pretende utilizar.

10. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ver as regras do Controlo de Anomalias Adaptativo na interface da aplicação

1. Na janela principal da aplicação, clique no botão .

2. Na janela Application settings, selecione **Security Controls** → **Adaptive Anomaly Control**.

3. Ative o botão de alternar **Controlo de Anomalias Adaptativo**.

4. No bloco **Regras**, clique na ligação **Editar regras**.

   Abre-se a lista de regras do Controlo de anomalias adaptativo. Por padrão, todas as regras funcionam no modo **Inteligente**.

5. Se for necessário, confirme a atualização da regra do Controlo de Anomalias Adaptativo.

6. Se for necessário, selecione uma ação quando uma regra de Controlo de Anomalias Adaptativo é acionada:

   - **Bloquear**. Se esta ação estiver selecionada, quando uma regra do Controlo de Anomalias Adaptativo é acionada, o Kaspersky Endpoint Security bloqueia a atividade abrangida pela regra e regista uma entrada que contém informação sobre a atividade.

   - **Informar**. Se esta ação estiver selecionada, quando uma regra do Controlo de Anomalias Adaptativo é acionada, o Kaspersky Endpoint Security permite a atividade abrangida pela regra e regista uma entrada que contém informação sobre a atividade.

7. Se for necessário, desative as regras que não pretende utilizar.

8. Guarde as suas alterações.

Cada regra tem sua própria duração do modo de formação. A duração do modo de formação é estabelecida por peritos da Kaspersky. Normalmente, o modo de formação fica ativo durante duas semanas.

Se, durante a formação, uma regra nunca for acionada, o Controlo de Anomalias Adaptativo considera esse comportamento atípico e altera o estado da regra para **Bloqueio inteligente**. Posteriormente, a aplicação bloqueia qualquer atividade que corresponda a essa regra.

Se uma regra for acionada durante a formação, tem de configurar manualmente a ação que a aplicação aplica à atividade detetada que corresponde a esta regra. Se não selecionar a ação quando a regra é acionada, o Controlo de Anomalias Adaptativo continua no modo de formação.

Ativar e desativar uma regra de Controlo de Anomalias Adaptativo

Para ativar ou desativar a regra de Controlo de Anomalias Adaptativo:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança** → **Controlo de Anomalias Adaptativo**.
3. No bloco **Regras**, clique no botão **Editar regras**.

   Abre-se a lista de regras do Controlo de anomalias adaptativo.
4. Na tabela, selecione um conjunto de regras (por exemplo, *Atividade das aplicações do Office*) e expanda o conjunto.
5. Selecione uma regra (por exemplo, *Início da Microsoft PowerShell da aplicação de ambiente de trabalho*).
6. Use o botão de alternar na coluna **Condição** para ativar ou desativar a regra do Controlo de Anomalias Adaptativo.
7. Guarde as suas alterações.

Modificar a ação efetuada quando uma regra de Controlo de Anomalias Adaptativo é acionada

Para editar a ação efetuada quando uma regra de Controlo de Anomalias Adaptativo é acionada:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança** → **Controlo de Anomalias Adaptativo**.
3. No bloco **Regras**, clique no botão **Editar regras**.

   Abre-se a lista de regras do Controlo de anomalias adaptativo.
4. Selecione uma regra na tabela.
5. Clique em **Editar**.

   Abre-se a janela de propriedades das regras do Controlo de anomalias adaptativo.

6. No bloco **Ação**, selecione uma das seguintes opções:

   - **Inteligente**. Se esta opção estiver selecionada, a regra de Controlo de Anomalias Adaptativo funciona no estado de treino Inteligente durante um período do tempo definido por especialistas da Kaspersky. Neste modo, quando uma regra de Controlo de Anomalias Adaptativo é acionada, o Kaspersky Endpoint Security permite a atividade abrangida pela regra e regista uma entrada no armazenamento do **Rule triggers in Smart Training state** do Kaspersky Security Center Administration Server. Quando o período de tempo definido para trabalhar no estado de Treino Inteligente termina, o Kaspersky Endpoint Security bloqueia a atividade abrangida por uma regra do Controlo de Anomalias Adaptativo e regista uma entrada contendo informação sobre a atividade.

   - **Bloquear**. Se esta ação estiver selecionada, quando uma regra do Controlo de Anomalias Adaptativo é acionada, o Kaspersky Endpoint Security bloqueia a atividade abrangida pela regra e regista uma entrada que contém informação sobre a atividade.

   - **Informar**. Se esta ação estiver selecionada, quando uma regra do Controlo de Anomalias Adaptativo é acionada, o Kaspersky Endpoint Security permite a atividade abrangida pela regra e regista uma entrada que contém informação sobre a atividade.

7. Guarde as suas alterações.

Criar uma exclusão para uma regra do Controlo de Anomalias Adaptativo

Pode criar até 1000 exclusões das regras do Controlo de Anomalias Adaptativo. Não recomendamos a criação de mais de 200 exclusões. Para reduzir o número de exclusões utilizadas, recomendamos a utilização de máscaras nas definições de exclusões.

Uma exclusão para uma regra de Controlo Adaptativo de Anormalidades inclui uma descrição dos objetos original e alvo. O *objeto original* é o objeto que realiza as ações. O *objeto alvo* é o objeto onde as ações estão a ser realizadas. Por exemplo, abriu um ficheiros de nome `file.xlsx`. Como tal, um ficheiro de biblioteca com a extensão DLL é carregado na memória do computador. Esta biblioteca é usada por um navegador (o ficheiro executável denominou `browser.exe`). Neste exemplo, `file.xlsx` é o objeto original, o Excel é o processo original, `browser.exe` é o objeto alvo e o navegador é o processo alvo.

Para criar uma exclusão para uma regra do Controlo de Anomalias Adaptativo:

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Anomalias Adaptativo**.

3. No bloco **Regras**, clique no botão **Editar regras**.

   Abre-se a lista de regras do Controlo de anomalias adaptativo.

4. Selecione uma regra na tabela.

5. Clique em **Editar**.

   Abre-se a janela de propriedades das regras do Controlo de anomalias adaptativo.

6. No bloco **Exclusões**, clique no botão **Adicionar**.

   Abre-se a janela de propriedades da exclusão.

7. Selecione o utilizador para o qual pretende configurar uma exclusão.

   Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

   O Controlo de Anomalias Adaptativo não suporta exclusões para grupos de utilizadores. Se selecionar um grupo de utilizadores, o Kaspersky Endpoint Security não aplica a exclusão.

8. No campo **Descrição**, introduza uma descrição da exclusão.

9. Define as definições do objeto original ou processo original iniciado pelo objeto:

   - **Processo original**. Caminho ou a máscara do caminho do ficheiro ou pasta contendo ficheiro (por exemplo, `C:\Dir\File.exe` ou `Dir\*.exe`).
   - **Hash do processo original**. Hash SHA256 do ficheiro.
   - **Objeto de origem**. Caminho ou a máscara do caminho do ficheiro ou pasta contendo ficheiro (por exemplo, `C:\Dir\File.exe` ou `Dir\*.exe`). Por exemplo, o caminho do ficheiro `document.docm`, que usa um script ou macro para iniciar os processos alvo.

     Também pode especificar outros objetos a excluir, tais como endereços Web, macro, comandos na command line, caminhos de registo ou outros. Especifique o objeto de acordo com o modelo seguinte: `object://<object>` onde `<object>` refere-se ao nome do objeto, por exemplo, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. Pode também usar máscaras, por exemplo, `object://*C:\Windows\temp\*`.
   - **Hash do ficheiro original**. Hash SHA256 do ficheiro.

   A regra de Controlo de Anomalias Adaptativo não é aplicada a ações realizadas pelo objeto ou para processos iniciados pelo objeto.

10. Especifique as definições do objeto alvo ou processos alvo iniciados no objeto.

    - **Processo de destino**. Caminho ou a máscara do caminho do ficheiro ou pasta contendo ficheiro (por exemplo, `C:\Dir\File.exe` ou `Dir\*.exe`).
    - **Hash do processo destino**. Hash SHA256 do ficheiro.
    - **Objeto de destino**. O comando para iniciar o processo alvo. Especifique o comando usando o seguinte padrão `object://<command>`, por exemplo, `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`. Pode também usar máscaras, por exemplo, `object://*C:\Windows\temp\*`.
    - **Hash do objeto de destino**. Hash SHA256 do ficheiro.

    A regra de Controlo de Anomalias Adaptativo não é aplicada a ações realizadas no objeto ou para processos iniciados no objeto.

11. Guarde as suas alterações.

Exportar e importar exclusões para regras do Controlo de Anomalias Adaptativo

Para exportar ou importar a lista de exclusões para regras selecionadas:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança** → **Controlo de Anomalias Adaptativo**.
3. No bloco **Regras**, clique no botão **Editar regras**.

   Abre-se a lista de regras do Controlo de anomalias adaptativo.
4. Para exportar a lista de regras:
   a. Selecione as regras cujas exceções pretende exportar.
   b. Clique em **Exportar**.
   c. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de exclusões e selecione a pasta onde pretende guardar este ficheiro.
   d. Confirme que quer exportar apenas as exclusões selecionadas ou exportar toda a lista de exclusões.
   e. Guardar o ficheiro.
5. Para importar a lista de exclusões:
   a. Clique em **Importar**.
   b. Na janela que se abre, selecione o ficheiro XML do qual deseja importar a lista de exclusões.
   c. Abrir o ficheiro.

      Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security irá solicitar-lhe a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro XML.
6. Guarde as suas alterações.

Aplicar atualizações para regras de Controlo de Anomalias Adaptativo

As regras do Controlo de Anomalias Adaptativo podem ser adicionadas à tabela de regras e as regras existentes do Controlo de Anomalias Adaptativo podem ser eliminadas da tabela de regras quando as bases de dados de antivírus são atualizadas. O Kaspersky Endpoint Security distingue as regras do Controlo de Anomalias Adaptativo que devem ser eliminadas ou adicionadas à tabela, se uma atualização dessas regras não tiver sido aplicada.

Até à atualização da aplicação, o Kaspersky Endpoint Security apresenta as regras do Controlo de Anomalias Adaptativo definidas para eliminação pela atualização na tabela de regras e atribui-lhes o estado *Desativado*. Não é possível alterar as definições destas regras.

Para aplicar atualizações para regras de Controlo de Anomalias Adaptativo:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança** → **Controlo de Anomalias Adaptativo**.
3. No bloco **Regras**, clique no botão **Editar regras**.

   Abre-se a lista de regras do Controlo de anomalias adaptativo.
4. Na janela que abre, clique no botão **Aprovar atualizações**.

   O botão **Aprovar atualizações** está disponível se uma atualização das regras de Controlo de Anomalia Adaptável estiver disponível.
5. Guarde as suas alterações.

Editar modelos de mensagem do Controlo de Anomalias Adaptativo

Quando um utilizador tenta executar uma ação, bloqueada pelas regras do Controlo de Anomalias Adaptativo, o Kaspersky Endpoint Security apresenta uma mensagem a informar que ações potencialmente perigosas são bloqueadas. Se o utilizador considerar que o arranque de uma ação foi bloqueada incorretamente, o utilizador pode utilizar a ligação no texto da mensagem para enviar uma mensagem ao administrador local da rede da empresa.

Estão disponíveis modelos especiais para mensagens ao administrador sobre o bloqueio de ações potencialmente prejudiciais. São fornecidas variáveis especiais para gerir os modelos da mensagem (por exemplo, `%USER_NAME%`). As variáveis permitem que um único modelo de mensagem seja usado para diferentes computadores. Ao gerar uma mensagem, o Kaspersky Endpoint Security recupera o valor da variável das definições do sistema operativo e insere-o na mensagem correspondente ao computador, utilizador e evento específicos.

Para editar um modelo de mensagem:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança → Controlo de Anomalias Adaptativo**.
3. No bloco **Modelos**, configure os modelos para mensagens de Controlo de Anomalias Adaptativo:
   - **Mensagem sobre o bloqueio**. Modelo da mensagem apresentada a um utilizador quando uma regra do Controlo de Anomalias Adaptativo que bloqueia uma ação não típica é acionada.
   - **Mensagem para o administrador**. Modelo da mensagem que um utilizador pode enviar para o administrador da rede empresarial local se considerar que o bloqueio foi um erro. Depois de o utilizador solicitar acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio da atividade da aplicação para o administrador**. A descrição do evento contém uma mensagem para o administrador com variáveis substituídas. Pode visualizar estes eventos na consola do Kaspersky Security Center utilizando a seleção de eventos predefinida **User requests**. Se a sua organização não tiver o Kaspersky Security Center implementado ou não houver uma ligação ao Servidor de Administração, a aplicação irá enviar uma mensagem ao administrador para o endereço de e-mail especificado.

   Para adicionar uma variável ao texto do modelo, coloque o cursor na posição desejada, clique em **Adicionar variável** e selecione a variável necessária na lista de opções disponíveis.

   Também pode restaurar o texto do modelo padrão ao clicar em **Repor**.
4. Guarde as suas alterações.

Monitorização de operações de Controlo de Anomalias Adaptativo

O Controlo de Anomalias Adaptativo inclui diversas ferramentas de monitorização. O objetivo principal da monitorização do Controlo de Anomalias Adaptativo é configurar o componente durante o treino.

Relatórios de Controlo de Anomalias Adaptativo

O Controlo de Anomalias Adaptativo utiliza os seguintes relatórios:

- **Reportar o estado das regras do Controlo de Anomalias Adaptativo**. O relatório contém informações sobre o estado das regras do Controlo de Anomalias Adaptativo (*Off*, *Smart Training*, *Smart Block*, *Notify*, *Block*). Este relatório permite analisar o nível de treino do Controlo de Anomalias Adaptativo e avaliar o número de regras que mudaram do modo *Smart Training* para o modo de operação normal (por exemplo, *Smart Block*).
- **Reportar as regras acionadas do Controlo de Anomalias Adaptativo**. O relatório contém informações sobre acionamentos de regras. O relatório também mostra o modo de acionamento da regra: *Block* (incluindo *Smart Block*) ou *Notify*. Este relatório permite avaliar a atividade do Controlo de Anomalias Adaptativo nos computadores dos utilizadores.

Como ver relatórios de Controlo de Anomalias Adaptativo na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança → Controlo de Anomalias Adaptativo**.
4. Execute uma das ações seguintes:
   - Se quiser ver o relatório sobre o estado das regras de Controlo de anomalias adaptativo, clique em **Reportar o estado das regras do Controlo de Anomalias Adaptativo**.
   - Se quiser ver o relatório sobre as regras acionadas do Controlo de anomalias adaptativo, clique em **Reportar as regras acionadas do Controlo de Anomalias Adaptativo**.
5. O processo de criação do relatório é iniciado.

O relatório é apresentado numa nova janela.

Como ver relatórios de Controlo de Anomalias Adaptativo na Consola Web

1. Na janela principal da Consola Web, selecione o separador **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Security Controls → Adaptive Anomaly Control**.
5. No bloco **Rules**, execute uma das seguintes ações:
   - Se quiser visualizar o relatório sobre as regras de Controlo de Anomalias Adaptativo, selecione **View report → Rules state**.
   - Se quiser visualizar o relatório sobre as regras do Controlo de Anomalias Adaptativo, clique em **View report → Detections**.
6. O processo de criação do relatório é iniciado.

O relatório é apresentado numa nova janela.

Para gerar relatórios na consola do Kaspersky Security Center, deve ativar a transferência de dados para o Servidor de administração. A transferência de dados é ativada por defeito.

Como ativar a transferência de dados para o Controlo de Anomalias Adaptativo na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais → Relatórios e armazenamento**.
4. No bloco **Transferência de dados para o Servidor de administração**, clique no botão **Definições**.

5. Marque as seguintes caixas:
   - **Reportar o estado das regras do Controlo de Anomalias Adaptativo**.
   - **Reportar as regras acionadas do Controlo de Anomalias Adaptativo**.
6. Guarde as suas alterações.

Como ativar a transferência de dados para o Controlo de Anomalias Adaptativo na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **KSC Integration**.
5. Sob **Data transfer to Administration Server**, selecione as seguintes caixas de seleção:
   - **Report on Adaptive Anomaly Control rules state**.
   - **Report on triggered Adaptive Anomaly Control rules**.
6. Guarde as suas alterações.

Armazenamento Rule triggers in Smart Training state

No modo de treino, o Controlo de Anomalias Adaptativo envia informações sobre regras acionadas para um armazenamento separado, **Rule triggers in Smart Training state**. Informações sobre regras acionadas são representadas no armazenamento como uma lista de eventos. Para ajustar o Controlo de Anomalias Adaptativo, pode confirmar o comportamento atípico no computador ou adicionar uma exclusão da regra.

Eventos do Controlo de Anomalias Adaptativo

Os registos de Controlo de Anomalias Adaptativo acionam eventos de regras nos modos *Block* (incluindo *Smart Block*) e *Notify*. Os seguintes eventos são previstos para este fim:

Process action blocked

Process action skipped

Os eventos contêm informações sobre a atividade suspeita, incluindo somas de verificação de ficheiros, os utilizadores envolvidos, a hora de ativação da regra e o nome do computador. Depois de analisar o evento, pode adicionar imediatamente exclusões da regra se achar que a atividade é legítima.

Controlo das Aplicações

O Controlo das Aplicações gere a inicialização de aplicações nos computadores dos utilizadores. Isso permite-lhe implementar uma política de segurança empresarial ao usar aplicações. O Controlo das Aplicações reduz também o risco de infeção do computador, restringindo o acesso às aplicações.

A configuração do Controlo das Aplicações consiste nas seguintes etapas:

1. Criar categorias de aplicações.

   O administrador cria categorias de aplicações que o administrador deseja gerir. As categorias de aplicações destinam-se a todos os computadores da rede empresarial, independentemente dos grupos de administração. Para criar uma categoria, pode utilizar os seguintes critérios: categoria KL (por exemplo, *Navegadores*), hash do ficheiro, fornecedor da aplicação e outros critérios.

2. Criar Regras de Controlo das Aplicações.

   O administrador cria regras do Controlo das aplicações na política para o grupo de administração. A regra inclui as categorias de aplicações e o estado de inicialização das aplicações destas categorias: bloqueados ou permitidos. O administrador pode criar muitas regras. Uma aplicação pode corresponder aos critérios de várias regras. A prioridade de uma regra de bloqueio é superior à prioridade de uma regra de permissão. O Kaspersky Endpoint Security verifica se uma aplicação corresponde a uma regra sempre que é iniciado. O Kaspersky Endpoint Security compara sequencialmente a aplicação com todas as regras do Controlo de aplicações.

3. Selecionar o modo de Controlo das Aplicações.

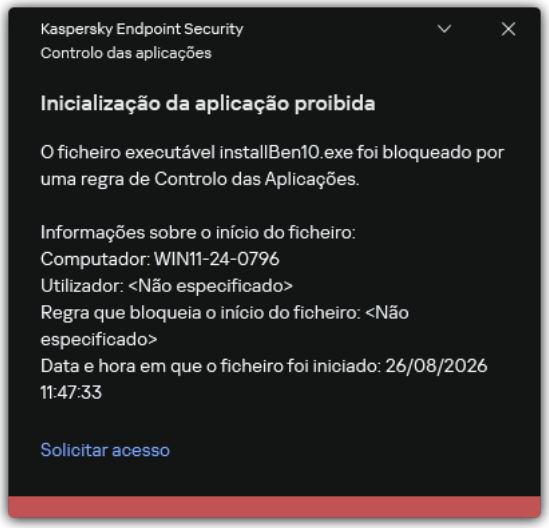
   O administrador escolhe o modo para trabalhar com aplicações que não estão incluídas em nenhuma das regras (lista de bloqueio e lista de permissão de aplicações).

Quando um utilizador tenta iniciar uma aplicação proibida, o Kaspersky Endpoint Security impede o início da aplicação e exibe uma notificação (ver a figura abaixo).

Um *modo de teste* é fornecido para verificar a configuração do Controlo das Aplicações. Neste modo, o Kaspersky Endpoint Security faz o seguinte:

- Permite a inicialização de aplicações, incluindo as proibidas.
- Mostra uma notificação sobre a inicialização de uma aplicação proibida e adiciona informações ao relatório no computador do utilizador.

- Envia dados sobre a inicialização de aplicações proibidas ao Kaspersky Security Center.



Notificação do Controlo das Aplicações

Modos de funcionamento do Controlo das Aplicações

O componente Controlo das Aplicações funciona em dois modos:

- **Lista de bloqueio**. Neste modo, o Controlo das Aplicações permite que todos os utilizadores iniciem todas as aplicações, exceto as aplicações proibidas nas regras do Controlo das Aplicações.

  Este modo do Controlo das Aplicações está ativado, por predefinição.

- **Lista de permissão**. Neste modo, o Controlo das Aplicações bloqueia o início de todas as aplicações por parte de todos os utilizadores, exceto as aplicações permitidas e não proibidas nas regras do Controlo das Aplicações.

  Se as regras de permissão do Controlo das Aplicações estiverem configuradas na íntegra, o componente bloqueia o arranque de todas as novas aplicações que não tenham sido verificadas pelo administrador da rede local e permite o funcionamento do sistema operativo e das aplicações fiáveis das quais os utilizadores dependem para realizarem as suas tarefas.

  Pode ler as recomendações sobre a configuração das Regras de Controlo das Aplicações no modo de lista de permissão.

O Controlo das Aplicações pode ser configurado para funcionar nestes modos com a interface local do Kaspersky Endpoint Security e utilizando o Kaspersky Security Center.

Contudo, o Kaspersky Security Center fornece ferramentas que não estão disponíveis na interface local do Kaspersky Endpoint Security, como por exemplo, as ferramentas necessárias para as tarefas seguintes:

- Criar categorias de aplicações.

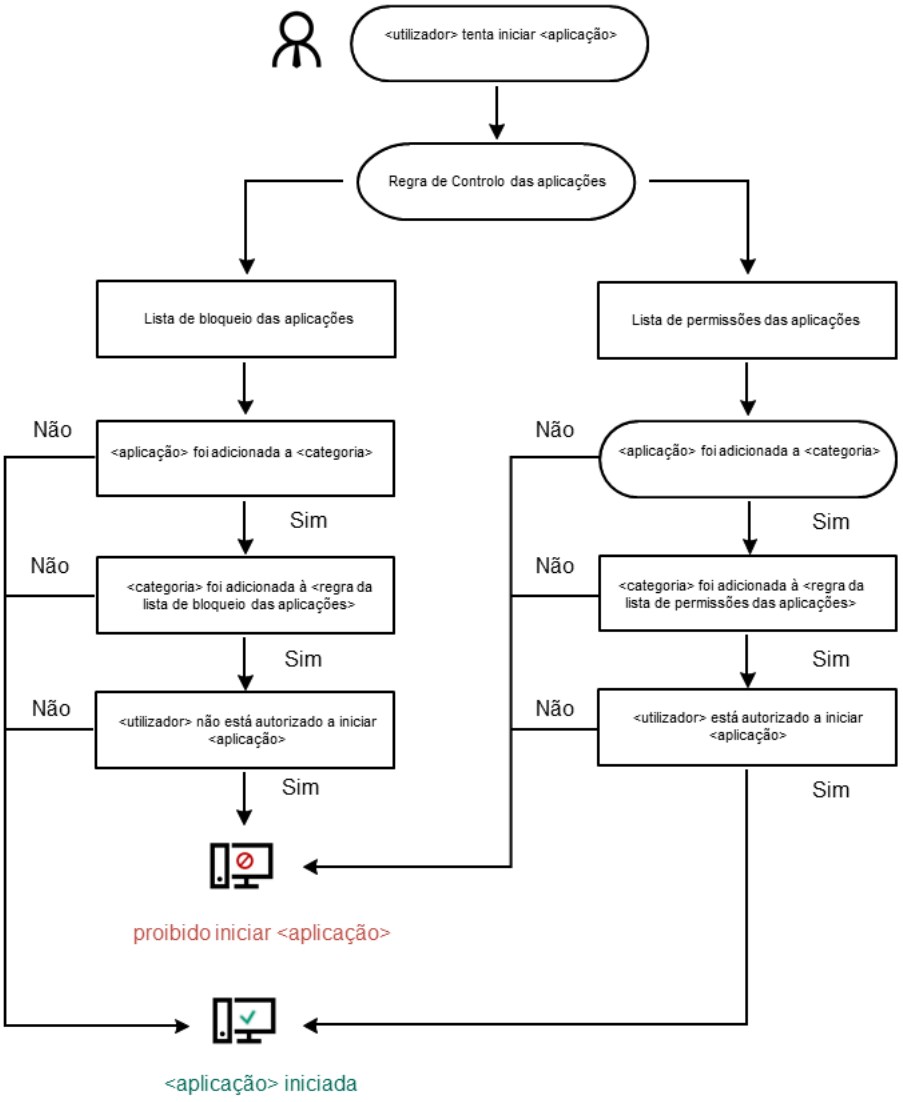
  As Regras de Controlo das aplicações criadas na Consola de Administração do Kaspersky Security Center baseiam-se nas suas categorias de aplicações personalizadas e não nas condições de inclusão ou de exclusão, como na interface local do Kaspersky Endpoint Security.

- Recolher informações sobre as aplicações instaladas nos computadores da rede local empresarial.

Por este motivo, recomenda-se a utilização do Kaspersky Security Center para configurar o funcionamento do componente Controlo das Aplicações.

Algoritmo operacional do Controlo das Aplicações

O Kaspersky Endpoint Security usa um algoritmo para tomar uma decisão sobre o início de uma aplicação (ver a figura abaixo).



Algoritmo operacional do Controlo das Aplicações

Limitações da funcionalidade de Controlo das Aplicações

O funcionamento do componente Controlo das Aplicações está limitado nos seguintes casos:

- Quando a versão da aplicação é atualizada, não é suportada a importação das definições do componente Controlo das Aplicações.
- Se não existir ligação aos servidores da KSN, o Kaspersky Endpoint Security recebe informação relativa à reputação das aplicações e respetivos módulos apenas a partir de bases de dados locais.

  A lista de aplicações destacadas pelo Kaspersky Endpoint Security para a categoria KL **Outro software\Aplicações e software confiável de acordo com a reputação no KSN** pode diferir em função da disponibilidade ou indisponibilidade de uma ligação aos servidores da KSN.

- Na base de dados do Kaspersky Security Center, é possível armazenar informações de 150 000 ficheiros processados. Assim que este número de registos tenha sido alcançado, os novos ficheiros não serão processados. Para retomar operações de inventário, deve eliminar os ficheiros que foram anteriormente inventariados na base de dados do Kaspersky Security Center a partir do computador no qual o Kaspersky Endpoint Security está instalado.
- O componente não controla o arranque de scripts a menos que o script seja enviado ao interpretador através da command line.

  Se o arranque de um interpretador for autorizado pelas Regras de Controlo das Aplicações, o componente não irá bloquear um script iniciado a partir deste interpretador.

  Se pelo menos um dos scripts especificados na linha de comando interpretadora for bloqueado desde o início pelas Regras de Controlo das Aplicações, o componente bloqueia todos os scripts, especificados na linha de comando interpretadora.

- O componente não controla o arranque de scripts de interpretadores que não são suportados pelo Kaspersky Endpoint Security.

  O Kaspersky Endpoint Security suporta os seguintes interpretadores:

  - Java
  - PowerShell

  São suportados os seguintes tipos de interpretadores:

  - %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 as aplicações instaladas

Para criar Regras de Controlo das Aplicações otimizadas, é recomendado que primeiro tenha uma perspetiva das aplicações que são utilizadas nos computadores na rede local empresarial. Para tal, pode obter a seguinte informação:

- Fornecedores, versões e localizações de aplicações utilizadas na rede local empresarial.
- Frequência de atualizações da aplicação.
- Políticas de utilização de aplicações na empresa (podem ser políticas de segurança ou políticas administrativas).
- Localização de armazenamento de pacotes de distribuição de aplicações.

Ver informações sobre a aplicação

As informações sobre as aplicações instaladas são fornecidas pelo Agente de Rede do Kaspersky Security Center. As informações sobre as aplicações instaladas estão disponíveis na consola do Kaspersky Security Center, na pasta **Applications registry**. O Agente de Rede atualiza as informações a cada sincronização com o Kaspersky Security Center. Para conhecer os detalhes sobre as informações enviadas pelo Agente de Rede, consulte a Ajuda do Kaspersky Security Center.

Para abrir as propriedades da aplicação na pasta Registo das aplicações:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da Consola de Administração, selecione **Advanced** → **Application management** → **Applications registry**.
3. Selecionar uma aplicação.
4. No menu de contexto da aplicação, selecione **Properties**.

Visualizar informações sobre ficheiros executáveis

Pode reduzir a carga na base de dados ao consultar informações sobre ficheiros executáveis. Para o conseguir, recomendamos que execute a tarefa *Inventário* em vários computadores de referência que tenham o seu conjunto padrão de software instalado.

As informações sobre os ficheiros executáveis são fornecidas pelo Kaspersky Endpoint Security. Para receber informações de hardware, tem de aplicar uma política ativa que permita a transmissão de informações sobre as aplicações instaladas (esta transmissão está ativada por predefinição).

Como ativar o envio de informações da aplicação na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais** → **Relatórios e armazenamento**.
4. No bloco **Transferência de dados para o Servidor de administração**, clique no botão **Definições**.
5. Selecione a caixa de verificação **Aplicações iniciadas**.
6. Guarde as suas alterações.

Como ativar o envio das informações da aplicação na Consola Web e Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **General Settings** → **KSC Integration**.

5. No bloco **Data transfer to Administration Server**, clique no botão **Advanced settings**.

6. Na janela que abre, selecione a caixa de verificação **About started applications**.

7. Guarde as suas alterações.

Pode obter uma lista dos ficheiros executáveis através da tarefa *Inventário* do Kaspersky Endpoint Security. Pode ver a lista de ficheiros executáveis na consola do Kaspersky Security Center, na pasta **Executable files**.

Antes de executar a tarefa *Inventário*, certifique-se de que a base de dados cumpre as recomendações do Kaspersky Security Center. Para obter informações sobre as limitações da base de dados, consulte a Ajuda do Kaspersky Security Center.

Como executar a tarefa Inventário na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

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

Passo 2. Âmbito de inventário

Crie uma lista de pastas nas quais deseja que o Kaspersky Endpoint Security procure ficheiros executáveis. Configure as definições do inventário (consulte a tabela abaixo).

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

Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 4. Selecionar a conta para executar a tarefa

Selecione uma conta para executar a tarefa *Inventário*. Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de utilizador local. Se o âmbito do inventário incluir unidades de rede ou outros objetos com acesso restrito, selecione uma conta de utilizador com os direitos de acesso suficientes.

Passo 5. Configurar um agendamento de início de uma tarefa

Configure o agendamento de tarefas, por exemplo, manualmente.

Passo 6. Definir o nome da tarefa

Digite um nome para a tarefa, por exemplo, *Inventário de linha de base*.

Passo 7. Completar a criação da tarefa

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa. Como resultado, é realizada uma pesquisa de ficheiros executáveis nos computadores dos utilizadores de acordo com o calendário configurado.

Como executar uma tarefa de Inventário na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

    a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

    b. Na lista pendente **Task type**, selecione **Inventory**.

    c. No campo **Task name**, introduza uma breve descrição, por exemplo, *Inventário de linha de base*.

    d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Avance para o passo seguinte.

5. Selecione uma conta para executar a tarefa. Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de utilizador local.

6. Conclua o assistente.

    Será apresentada uma nova tarefa na lista de tarefas.

7. Para configurar a tarefa, aceda às propriedades da tarefa (consulte a tabela abaixo).

8. Selecione a caixa de verificação junto à tarefa.

9. Clique em **Start**.

    Pode controlar o estado da tarefa e o número de dispositivos nos quais a tarefa foi concluída com êxito ou concluída com um erro. Na sequência disto, os ficheiros executáveis serão pesquisados nos computadores do utilizador de acordo com o calendário especificado.

Para abrir a janela de propriedades de um ficheiro executável na pasta Executable files:

1. Abra a Consola de Administração do Kaspersky Security Center.

2. Na árvore da Consola de Administração, selecione **Advanced** → **Application management** → **Executable files**.

3. Selecione um ficheiro executável.

4. No menu de contexto do ficheiro executável, selecione **Properties**.

Para ver informações gerais sobre a aplicação e os respetivos ficheiros executáveis, e para aceder à lista de computadores nos quais uma aplicação está instalada, abra a janela de propriedades da aplicação selecionada na pasta Applications registry ou na pasta **Executable files**.

Atualizar as informações sobre as aplicações instaladas e os ficheiros executáveis

O funcionamento do componente Controlo das Aplicações com a base de dados de ficheiros executáveis foi otimizado no Kaspersky Endpoint Security. O Kaspersky Endpoint Security atualiza automaticamente a base de dados depois de o ficheiro ser eliminado do computador. Isto permite manter a base de dados atualizada e poupar recursos do Kaspersky Security Center. Para manter atualizada a base de dados das aplicações instaladas, o envio de informações da aplicação para o Servidor de Administração deve estar ativado (ativado por predefinição).

Parâmetro	Descrição
Inventory scopes	Lista de objetos que irão formar o âmbito do inventário.
DLL modules inventory	O Kaspersky Endpoint Security procura módulos DLL no âmbito do inventário e envia informações ao Kaspersky Security Center. Ativar o inventário de módulos DLL aumenta significativamente o tempo necessário para concluir a tarefa do Inventário e o tamanho da base de dados.
Script files inventory	O Kaspersky Endpoint Security procura scripts no âmbito do inventário e envia as informações para o Kaspersky Security Center. Ativar o inventário de ficheiros script aumenta significativamente o tempo necessário para concluir a tarefa do Inventário e o tamanho da base de dados.
Run only when the computer is idle	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 ecrã estiver ativada. Se interrompeu a execução da tarefa (por exemplo, ao desbloquear o computador), o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que foi interrompido. Esta opção de agendamento permite-lhe conservar os recursos do computador quando o computador está a ser utilizado.
Scan only new and modified files	Verifica apenas os ficheiros novos e os que foram modificados desde a última vez em que foram verificados. Isto ajuda a reduzir a duração de uma verificação. Este modo aplica-se a ficheiros simples e compostos.
Skip file that is scanned for longer than (sec) N seg	Limitar o tempo de execução da tarefa. Após o período especificado, o Kaspersky Endpoint Security interrompe a tarefa. A tarefa não está assinalada como concluída. Quando o Kaspersky Endpoint Security voltar a executar a tarefa, esta será executada desde o início e de acordo com o agendamento.
Scan archives	A verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros arquivos. A aplicação verifica arquivos não só pela extensão, mas também pelo formato. Ao verificar os arquivos, a aplicação efetua uma descompactação recursiva. Isto permite a deteção de ameaças dentro de arquivos multinível (um arquivo dentro de um arquivo).
Scan distribution packages	Verificar pacotes de distribuição de aplicações de terceiros.
Do not unpack large compound files	Se esta caixa de verificação estiver selecionada, a aplicação não verifica ficheiros compostos se o tamanho destes exceder o valor especificado. Se esta caixa de verificação for desmarcada, a aplicação verifica ficheiros compostos de todos os tamanhos. A aplicação verifica ficheiros grandes extraídos de arquivos, independentemente de a caixa de seleção estar selecionada ou não.

Como ativar o modo de Aplicações bloqueadas

No modo *Aplicações bloqueadas* é o modo, quando o Controlo das Aplicações permite que todos os utilizadores iniciem todas as aplicações, exceto as aplicações proibidas nas regras do Controlo das Aplicações. Ou seja, se não existir nenhuma regra de negação, o Controlo de Aplicações permite iniciar a aplicação. Este modo do Controlo das Aplicações está ativado, por predefinição.

Antes de ativar o modo *Aplicações bloqueadas*, recomendamos que teste as suas regras do Controlo das Aplicações. Para este efeito, pode ativar o modo de teste.

Como ativar o modo de Aplicações bloqueadas na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.

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

4. Na janela de política, selecione **Controlos de segurança → Controlo das Aplicações**.

5. Selecione a caixa de verificação **Controlo das aplicações**.

6. No bloco **Definições do Controlo das Aplicações**, utilize a lista pendente **Modo de controlo** para selecionar **Lista de bloqueio**.

7. Na lista pendente **Ação**, selecione a ação para o Controlo das Aplicações:

   - **Testar regras**. O Controlo das Aplicações não bloqueia as aplicações que são impedidas de serem executadas pelas regras, mas gera eventos sobre a execução de aplicações que, de outra forma, seriam bloqueadas.

   - **Aplicar regras**. O Controlo das Aplicações bloqueia as aplicações bloqueadas e gera os eventos correspondentes.

8. Selecione o estado para as regras de Controlo das Aplicações:

   - **Ativado**. Este estado significa que a regra é utilizada quando o componente Controlo das Aplicações está em execução.

   - **Desativado**. Este estado significa que a regra é ignorada quando o componente Controlo das Aplicações está em execução.

   - **Teste**. Este estado significa que o Kaspersky Endpoint Security permite sempre o arranque da aplicação à qual é aplicável a regra, mas regista informações sobre o arranque de tais aplicações no relatório.

   Se for necessário, adicione novas regras de Controlo das Aplicações.

9. Configure as definições avançadas do Controlo das Aplicações:

   - **Monitorizar a carga dos módulos DLL (aumenta significativamente a carga no sistema)**. Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security controla o carregamento dos módulos DLL quando os utilizadores tentam iniciar as aplicações. A informação sobre o módulo DLL e a aplicação que carregou este módulo DLL está registada no relatório.

     Ao ativar o controlo sobre o carregamento dos módulos DLL e controladores, certifique-se de que uma das regras seguintes está ativada nas definições de Controlo das Aplicações: a regra predefinida **Golden Image** ou outra regra que contenha a categoria KL **Golden Image\Certificados confiáveis**", e certifique-se de que os módulos DLL e os controladores fiáveis são carregados antes de iniciar o Kaspersky Endpoint Security. Permitir o controlo do carregamento de módulos DLL e controladores quando a regra **Golden Image** está desativada pode provocar instabilidade no sistema operativo.

     O Kaspersky Endpoint Security só monitoriza os módulos DLL e os controladores carregados desde a seleção da caixa de verificação. Depois de selecionar a caixa de verificação, é aconselhável reiniciar o computador para garantir que a aplicação monitoriza todos os módulos DLL e controladores, incluindo os carregados antes de o Kaspersky Endpoint Security iniciar.

- **Utilizar verificação estrita da assinatura digital**. Pode selecionar um certificado como condição de ativação para uma regra de Controlo das Aplicações. Se esta caixa de verificação estiver selecionada, o Kaspersky Endpoint Security aplica regras a aplicações assinadas com certificados apenas do arquivo de certificados do sistema fiável. As aplicações assinadas com esse certificado também são consideradas fiáveis pelos componentes de proteção, por exemplo, a tarefa *Verificação de software malicioso*. No entanto, se especificar um certificado de um armazenamento diferente numa regra de Controlo das Aplicações, o Kaspersky Endpoint Security não aplica essa regra.

  Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security aplica regras a aplicações assinadas por um certificado do Windows Trusted Root Certificate Store. Estas aplicações não fazem parte da zona fiável. Os componentes de proteção monitorizam a atividade dessas aplicações.

- **Mensagem sobre o bloqueio**. Modelo da mensagem que é apresentada quando é acionada uma regra de Controlo das Aplicações que bloqueia o início de uma aplicação.

- **Mensagem para o administrador**. Modelo da mensagem que um utilizador pode enviar ao administrador da LAN empresarial se o utilizador acreditar que uma aplicação foi bloqueada por engano.

10. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar o modo de Aplicações bloqueadas na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Security Controls** → **App Control**.

5. Ative o botão de alternar **Application Control ENABLED**.

6. No bloco **Operating mode**, selecione **Block all except the rules list**.

7. No bloco **Action**, selecione a ação para o Controlo das Aplicações:

   - **Inform**. O Controlo das Aplicações não bloqueia as aplicações que são impedidas de serem executadas pelas regras, mas gera eventos sobre a execução de aplicações que, de outra forma, seriam bloqueadas.

   - **Apply rules**. O Controlo das Aplicações bloqueia as aplicações bloqueadas e gera os eventos correspondentes.

8. Selecione o estado para as regras de Controlo das Aplicações:

   - **Enabled**. Este estado significa que a regra é utilizada quando o componente Controlo das Aplicações está em execução.

   - **Disabled**. Este estado significa que a regra é ignorada quando o componente Controlo das Aplicações está em execução.

   - **Test mode**. Este estado significa que o Kaspersky Endpoint Security permite sempre o arranque da aplicação à qual é aplicável a regra, mas regista informações sobre o arranque de tais aplicações no relatório.

   Se for necessário, adicione novas regras de Controlo das Aplicações.

9. Configure as definições avançadas do Controlo das Aplicações:

   - **Monitor loading of DLL modules**. Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security controla o carregamento dos módulos DLL quando os utilizadores tentam iniciar as aplicações. A informação sobre o módulo DLL e a aplicação que carregou este módulo DLL está registada no relatório.

     Ao ativar o controlo sobre o carregamento dos módulos DLL e controladores, certifique-se de que uma das regras seguintes está ativada nas definições de Controlo das Aplicações: a regra predefinida **Golden Image** ou outra regra que contenha a categoria KL **Golden Image\Certificados confiáveis**", e certifique-se de que os módulos DLL e os controladores fiáveis são carregados antes de iniciar o Kaspersky Endpoint Security. Permitir o controlo do carregamento de módulos DLL e controladores quando a regra **Golden Image** está desativada pode provocar instabilidade no sistema operativo.

     O Kaspersky Endpoint Security só monitoriza os módulos DLL e os controladores carregados desde a seleção da caixa de verificação. Depois de selecionar a caixa de verificação, é aconselhável reiniciar o computador para garantir que a aplicação monitoriza todos os módulos DLL e controladores, incluindo os carregados antes de o Kaspersky Endpoint Security iniciar.

   - **Use strict digital signature verification**. Pode selecionar um certificado como condição de ativação para uma regra de Controlo das Aplicações. Se esta caixa de verificação estiver selecionada, o Kaspersky Endpoint Security aplica regras a aplicações assinadas com certificados apenas do arquivo de certificados do sistema fiável. As aplicações assinadas com esse certificado também são consideradas fiáveis pelos componentes de proteção, por exemplo, a tarefa *Verificação de software malicioso*. No entanto, se especificar um certificado de um armazenamento diferente numa regra de Controlo das Aplicações, o Kaspersky Endpoint Security não aplica essa regra.

     Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security aplica regras a aplicações assinadas por um certificado do Windows Trusted Root Certificate Store. Estas aplicações não fazem parte da zona fiável. Os componentes de proteção monitorizam a atividade dessas aplicações.

   - **Message to user**. Modelo da mensagem que é apresentada quando é acionada uma regra de Controlo das Aplicações que bloqueia o início de uma aplicação.

   - **Message to administrator**. Modelo da mensagem que um utilizador pode enviar ao administrador da LAN empresarial se o utilizador acreditar que uma aplicação foi bloqueada por engano.

10. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar o modo de Aplicações bloqueadas na interface da aplicação

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Controlos de segurança → Controlo das aplicações**.
3. Ative o botão de alternar **Controlo das Aplicações**.
4. No bloco **Modo de controlo do arranque da aplicação**, selecione **Lista de bloqueio. São permitidas todas as aplicações, exceto as que estejam indicadas na lista de regras**.

5. No bloco **Ação no arranque das aplicações bloqueadas por regras**, selecione a ação para o Controlo das Aplicações:

   - **Informar (Modo de teste) e registar eventos em relatório**. O Controlo das Aplicações não bloqueia as aplicações que são impedidas de serem executadas pelas regras, mas gera eventos sobre a execução de aplicações que, de outra forma, seriam bloqueadas.

   - **Bloquear**. O Controlo das Aplicações bloqueia as aplicações bloqueadas e gera os eventos correspondentes.

6. Selecione o estado para as regras de Controlo das Aplicações:

   - **Ativada**. Este estado significa que a regra é utilizada quando o componente Controlo das Aplicações está em execução.

   - **Desativada**. Este estado significa que a regra é ignorada quando o componente Controlo das Aplicações está em execução.

   - **Modo de teste**. Este estado significa que o Kaspersky Endpoint Security permite sempre o arranque da aplicação à qual é aplicável a regra, mas regista informações sobre o arranque de tais aplicações no relatório.

   Se for necessário, adicione novas regras de Controlo das Aplicações.

7. Configure as definições avançadas do Controlo das Aplicações:

   - **Monitorizar o carregamento de módulos DLL**. Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security controla o carregamento dos módulos DLL quando os utilizadores tentam iniciar as aplicações. A informação sobre o módulo DLL e a aplicação que carregou este módulo DLL está registada no relatório.

     Ao ativar o controlo sobre o carregamento dos módulos DLL e controladores, certifique-se de que uma das regras seguintes está ativada nas definições de Controlo das Aplicações: a regra predefinida **Golden Image** ou outra regra que contenha a categoria KL **Golden Image\Certificados confiáveis**", e certifique-se de que os módulos DLL e os controladores fiáveis são carregados antes de iniciar o Kaspersky Endpoint Security. Permitir o controlo do carregamento de módulos DLL e controladores quando a regra **Golden Image** está desativada pode provocar instabilidade no sistema operativo.

     O Kaspersky Endpoint Security só monitoriza os módulos DLL e os controladores carregados desde a seleção da caixa de verificação. Depois de selecionar a caixa de verificação, é aconselhável reiniciar o computador para garantir que a aplicação monitoriza todos os módulos DLL e controladores, incluindo os carregados antes de o Kaspersky Endpoint Security iniciar.

   - **Utilizar verificação estrita da assinatura digital**. Pode selecionar um certificado como condição de ativação para uma regra de Controlo das Aplicações. Se esta caixa de verificação estiver selecionada, o Kaspersky Endpoint Security aplica regras a aplicações assinadas com certificados apenas do arquivo de certificados do sistema fiável. As aplicações assinadas com esse certificado também são consideradas fiáveis pelos componentes de proteção, por exemplo, a tarefa *Verificação de software malicioso*. No entanto, se especificar um certificado de um armazenamento diferente numa regra de Controlo das Aplicações, o Kaspersky Endpoint Security não aplica essa regra.

     Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security aplica regras a aplicações assinadas por um certificado do Windows Trusted Root Certificate Store. Estas aplicações não fazem parte da zona fiável. Os componentes de proteção monitorizam a atividade dessas aplicações.

- **Modelos de mensagens sobre bloqueio de aplicações**. Modelo da mensagem que é apresentada quando é acionada uma regra de Controlo das Aplicações que bloqueia o início de uma aplicação.

- **Texto da mensagem modelo apresentado quando o início de uma aplicação é bloqueado**. Modelo da mensagem que um utilizador pode enviar ao administrador da LAN empresarial se o utilizador acreditar que uma aplicação foi bloqueada por engano.

8. Guarde as suas alterações.

Como resultado, o Controlo das Aplicações bloqueia as aplicações bloqueadas. O Kaspersky Endpoint Security também gera eventos *Inicialização da aplicação proibida*. Pode utilizar estes eventos para gerar o relatório *Report on prohibited applications* na consola do Kaspersky Security Center. No resumo do relatório, pode ver a lista de aplicações e computadores em que a regra do Controlo das Aplicações foi acionada.

Controlo das Aplicações com base num computador de linha de base

Pode utilizar um computador de linha de base para criar uma imagem com um conjunto de aplicações de que necessita. Pode então utilizar esta imagem para implementar o sistema operativo e as aplicações noutros computadores. Nem sempre é possível manter a imagem atualizada. O Controlo das Aplicações permite-lhe manter uma lista de aplicações permitidas com base num computador de linha de base. O Controlo das Aplicações determina automaticamente as aplicações que estão instaladas no computador de linha de base e atualiza a categoria. Desta forma, os computadores obtêm uma lista atualizada das aplicações permitidas.

A configuração do Controlo das Aplicações com base num computador de linha de base envolve os seguintes passos:

1. Crie uma categoria de atualização automática. Ao criar a nova categoria, selecione a categoria **Category that includes executable files from a specific folder** e selecione o seu computador de linha de base.

   Como criar uma categoria de atualização automática na Consola de Administração (MMC)

   1. Abra a Consola de Administração do Kaspersky Security Center.

   2. Na árvore da Consola de Administração, selecione **Advanced** → **Application management** → **Application categories**.

   3. Clique no botão **New category** na área de trabalho.

      Esta ação inicia o assistente de criação de categoria da aplicação.

   4. Siga as instruções apresentadas no assistente de criação de categorias da aplicação.

   Passo 1. Selecionar o tipo de categoria

   Selecione **Category that includes executable files from selected devices** como o tipo de categoria.

Passo 2. Introduzir o nome de uma categoria de utilizador

Neste passo, especifique um nome para a categoria da aplicação.

Passo 3. Definições

> Este passo fica disponível se tiver selecionado o tipo de **Category that includes executable files from selected devices**.

Neste passo, clique no botão **Add** e especifique os computadores cujos ficheiros executáveis serão adicionados à categoria da aplicação pelo Kaspersky Security Center. Todos os ficheiros executáveis dos computadores especificados apresentados na pasta **Executable files** serão adicionados à categoria da aplicação pelo Kaspersky Security Center.

Neste passo, também pode configurar as seguintes definições:

- Algoritmo para cálculo da função hash. Para selecionar um algoritmo, tem de selecionar, pelo menos, uma das seguintes caixas de verificação:
  - **Calculate SHA256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions)**.
  - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.
- A caixa de verificação **Synchronize data with Administration Server repository**. Selecione esta caixa de verificação, se pretender que o Kaspersky Security Center limpe periodicamente a categoria de aplicações e que lhe adicione todos os ficheiros executáveis de computadores especificados apresentados na pasta **Executable files**.

  Se a caixa de verificação **Synchronize data with Administration Server repository** estiver desmarcada, o Kaspersky Security Center não efetuará quaisquer modificações a uma categoria de aplicação após a sua criação.

Passo 4. Filtrar

Neste passo, configure um filtro para os ficheiros.

Pode especificar o tipo de ficheiro que se pretende utilizar para criar a categoria de aplicação.

- **All files**. A categoria irá corresponder a todos os ficheiros. Esta opção está selecionada por predefinição.
- **Only files outside the application categories**. A categoria irá corresponder apenas a ficheiros fora das categorias da aplicação.

Pode especificar pastas de computadores selecionados que contêm ficheiros que pretende utilizar para criar a categoria da aplicação.

- **All folders**. A categoria irá corresponder a todas as pastas. Esta opção está selecionada por predefinição.
- **Specified folder**. A categoria irá corresponder apenas à pasta especificada. Se selecionar esta opção, tem de especificar um caminho para a pasta.

Passo 5. Criar uma categoria personalizada

Conclua o assistente.

Como criar uma categoria com conteúdo adicionado automaticamente na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Operations** → **Third-party applications** → **Application categories**.

   Abre-se a lista de categorias de aplicações.

2. Clique em **Add**.

   Esta ação inicia o assistente de criação de categoria da aplicação.

3. Configure as definições gerais da categoria da aplicação:

   - Nome da categoria.
   - Método de criação da categoria. Selecione **Category that includes executable files from selected devices** como o tipo de categoria.

   Avance para o passo seguinte.

4. Configure as definições avançadas da categoria da aplicação:

   - Especifique os computadores a partir dos quais o Kaspersky Security Center irá adicionar ficheiros executáveis à categoria da aplicação. Todos os ficheiros executáveis dos computadores especificados apresentados na pasta **Executable files** serão adicionados à categoria da aplicação pelo Kaspersky Security Center.
   - Selecione um algoritmo para cálculo da função hash.
   - Configure um intervalo para sincronizar os dados com o armazenamento do Servidor de Administração.
   - Configure um filtro para os ficheiros.

5. Conclua o assistente.

Ao criar uma categoria atualizada automaticamente, pode ser conveniente subdividir os ficheiros em várias categorias. Por exemplo, os ficheiros do sistema operativo e os ficheiros da pasta Program Files. Para tal, pode utilizar um filtro nas definições da categoria e selecionar pastas individuais.

2. Selecionar o modo de Controlo das Aplicações. Tem de impedir a execução de todas as aplicações que não sejam explicitamente permitidas. Para tal, selecione o modo *Aplicações bloqueadas*.

3. Crie uma regras de Controlo das Aplicações. Nas definições de regras, selecione a categoria a que pertencem os ficheiros executáveis do computador da linha de base.

Como configurar o Controlo das Aplicações com base num computador de linha de base na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Controlos de segurança → Controlo das Aplicações**.
5. Selecione a caixa de verificação **Controlo das aplicações**.
6. No bloco **Definições do Controlo das Aplicações**, utilize a lista pendente **Modo de controlo** para selecionar **Lista de bloqueio**.
7. Na lista pendente **Ação**, selecione a ação para o Controlo das Aplicações:
   - **Testar regras**. O Controlo das Aplicações não bloqueia as aplicações que são impedidas de serem executadas pelas regras, mas gera eventos sobre a execução de aplicações que, de outra forma, seriam bloqueadas.
   - **Aplicar regras**. O Controlo das Aplicações bloqueia as aplicações bloqueadas e gera os eventos correspondentes.
8. Na lista das regras do Controlo das Aplicações, clique no botão **Adicionar**.

   É iniciado o assistente para adicionar uma regra de Controlo das Aplicações.
9. Na lista pendente **Categoria**, selecione uma categoria atualizada automaticamente com base no computador de linha de base.
10. Selecione os utilizadores ou os grupos de utilizadores para os quais pretende aplicar a regra de Controlo das Aplicações.
11. Configure as definições avançadas da regra de Controlo das Aplicações:
    - **Recusar para outros utilizadores**. A aplicação impede o lançamento de aplicações que pertençam à categoria selecionada para todos os utilizadores que não estejam na lista.
    - **Atualizadores fiáveis**. O Kaspersky Endpoint Security considera as aplicações incluídas na categoria selecionada enquanto atualizadores fiáveis com permissão para criar outros ficheiros executáveis que terão permissão para serem subsequentemente executados.
12. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como configurar o Controlo das Aplicações com base num computador de linha de base na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione o separador **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Security Controls** → **App Control**.

5. Ative o botão de alternar **Application Control ENABLED**.

6. No bloco **Operating mode**, selecione **Block all except the rules list**.

7. No bloco **Action**, selecione a ação para o Controlo das Aplicações:

   - **Inform**. O Controlo das Aplicações não bloqueia as aplicações que são impedidas de serem executadas pelas regras, mas gera eventos sobre a execução de aplicações que, de outra forma, seriam bloqueadas.

   - **Apply rules**. O Controlo das Aplicações bloqueia as aplicações bloqueadas e gera os eventos correspondentes.

8. Na lista das regras do Controlo das Aplicações, clique no botão **Add**.

   É iniciado o assistente para adicionar uma regra de Controlo das Aplicações.

9. Em **Categories/Applications**, selecione uma categoria atualizada automaticamente com base no computador de linha de base.

10. Selecione os utilizadores ou os grupos de utilizadores para os quais pretende aplicar a regra de Controlo das Aplicações.

11. Configure as definições avançadas da regra de Controlo das Aplicações:

    - **Users**. A aplicação impede o lançamento de aplicações que pertençam à categoria selecionada para todos os utilizadores que não estejam na lista.

    - **Trusted Updaters**. O Kaspersky Endpoint Security considera as aplicações incluídas na categoria selecionada enquanto atualizadores fiáveis com permissão para criar outros ficheiros executáveis que terão permissão para serem subsequentemente executados.

12. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como configurar o Controlo das Aplicações com base num computador de linha de base na interface de aplicações

1. Na janela principal da aplicação, clique no botão .

2. Na janela Application settings, selecione **Controlos de segurança** → **Controlo das Aplicações**.

3. Ative o botão de alternar **Controlo das Aplicações**.

4. No bloco **Modo de controlo do arranque da aplicação**, selecione **Lista de bloqueio. São permitidas todas as aplicações, exceto as que estejam indicadas na lista de regras**.

5. No bloco **Ação no arranque das aplicações bloqueadas por regras**, selecione a ação para o Controlo das Aplicações:

   - **Informar (Modo de teste) e registar eventos em relatório**. O Controlo das Aplicações não bloqueia as aplicações que são impedidas de serem executadas pelas regras, mas gera eventos sobre a execução de aplicações que, de outra forma, seriam bloqueadas.

   - **Bloquear**. O Controlo das Aplicações bloqueia as aplicações bloqueadas e gera os eventos correspondentes.

6. Na lista das regras do Controlo das Aplicações, clique no botão **Adicionar**.

   É iniciado o assistente para adicionar uma regra de Controlo das Aplicações.

7. Em **Categoria**, selecione uma categoria atualizada automaticamente com base no computador de linha de base.

8. Selecione os utilizadores ou os grupos de utilizadores para os quais pretende aplicar a regra de Controlo das Aplicações.

9. Configure as definições avançadas da regra de Controlo das Aplicações:

   - **Recusar para outros utilizadores**. A aplicação impede o lançamento de aplicações que pertençam à categoria selecionada para todos os utilizadores que não estejam na lista.

   - **Atualizadores fiáveis**. O Kaspersky Endpoint Security considera as aplicações incluídas na categoria selecionada enquanto atualizadores fiáveis com permissão para criar outros ficheiros executáveis que terão permissão para serem subsequentemente executados.

10. Guarde as suas alterações.

Gerir as regras de Controlo das aplicações

O Kaspersky Endpoint Security controla o arranque das aplicações por utilizadores por meio de regras. Uma Regra de Controlo das aplicações especifica as condições de ativação e ações executadas pelo Controlo das Aplicações quando a regra é ativada (permitindo ou bloqueando o arranque da aplicação pelos utilizadores).

Condições de ativação de regras

Uma condição de acionamento de regra tem a seguinte correlação: «tipo de condição — critério da condição — valor da condição». Com base nas condições de ativação de regras, o Kaspersky Endpoint Security aplica (ou não aplica) uma regra a uma aplicação.

Nas regras usam-se os seguintes tipos de condições:

- *Condições de inclusão*. O Kaspersky Endpoint Security aplica a regra à aplicação se a aplicação combinar com, pelo menos, uma das condições de inclusão.

- *Condições de exclusão*. O Kaspersky Endpoint Security não aplica a regra à aplicação se a aplicação combinar com, pelo menos, uma das condições de exclusão e não combinar com nenhuma das condições de inclusão.

As condições de ativação de regras são criadas utilizando critérios. Os seguintes critérios são utilizados para criar regras no Kaspersky Endpoint Security:

- Caminho para a pasta com o ficheiro executável da aplicação ou o caminho para o ficheiro executável da aplicação.
- Metadados: nome do ficheiro executável da aplicação, versão do ficheiro executável da aplicação, nome da aplicação, versão da aplicação, fornecedor da aplicação.
- Hash do ficheiro executável da aplicação.
- Certificado: emissor, assunto, thumbprint.
- Inclusão da aplicação numa categoria KL.
- Localização do ficheiro executável da aplicação numa unidade amovível.

O valor do critério tem de ser especificado para cada critério utilizado na condição. Se os parâmetros da aplicação que está a ser iniciada coincidirem com os valores dos critérios especificados na condição de inclusão, a regra é ativada. Neste caso, o Controlo das Aplicações executa a ação prevista na regra. Se os parâmetros da aplicação corresponderem aos valores dos critérios especificados na condição de exclusão, o Controlo das Aplicações não controla o arranque da aplicação.

Se selecionou um certificado como uma condição de acionamento de regras, tem de garantir que este certificado é adicionado ao armazenamento de sistema fidedigno no computador e verificar as definições de utilização do armazenamento de sistema fidedigno na aplicação.

Decisões tomadas pelo componente Controlo das Aplicações quando uma regra é ativada

Quando uma regra é ativada, o Controlo das Aplicações permite aos utilizadores (ou grupos de utilizadores) iniciar aplicações ou bloquear o arranque de acordo com a regra. Pode selecionar utilizadores individuais ou grupos de utilizadores autorizados ou não autorizados a iniciar aplicações que ativam uma regra.

Se uma regra não especificar os utilizadores autorizados a iniciar aplicações que cumpram a regra, esta é denominada uma regra de *bloqueio*.

Uma regra que não especifica quaisquer utilizadores não autorizados a iniciar aplicações que correspondem à regra é denominada regra de *permissão*.

A prioridade de uma regra de bloqueio é superior à prioridade de uma regra de permissão. Por exemplo, se uma regra de permissão de Controlo das Aplicações foi atribuída para um grupo de utilizadores e uma regra de bloqueio de Controlo das Aplicações foi atribuída para um utilizador do grupo, esse utilizador estará impedido de iniciar a aplicação.

Estado operacional de uma regra

As regras de controlo das aplicações podem ter um dos seguintes estados de funcionamento:

- **Ativada**. Este estado significa que a regra é utilizada quando o componente Controlo das Aplicações está em execução.
- **Desativada**. Este estado significa que a regra é ignorada quando o componente Controlo das Aplicações está em execução.
- **Modo de teste**. Este estado significa que o Kaspersky Endpoint Security permite o arranque das aplicações às quais são aplicáveis as regras, mas regista informações sobre o arranque de tais aplicações no relatório.

Adicionar uma condição de ativação para a Regra de Controlo das aplicações

Para uma maior conveniência ao criar Regras de Controlo das Aplicações, pode criar categorias da aplicação.

É recomendado criar uma categoria de "Aplicações de trabalho" que inclua o grupo de aplicações padrão utilizadas na empresa. Se diferentes grupos de utilizadores utilizarem conjuntos de aplicações diferentes no desempenho das suas tarefas, pode ser criada uma categoria de aplicações separada para cada grupo de utilizadores.

Para criar uma categoria de aplicações na Consola de Administração:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da Consola de Administração, selecione **Advanced** → **Application management** → **Application categories**.
3. Clique no botão **New category** na área de trabalho.

   O assistente de criação de categorias de utilizador é iniciado.
4. Siga as instruções apresentadas no assistente de criação de uma nova categoria.

Passo 1. Selecionar o tipo de categoria

Neste passo, selecione um dos seguintes tipos de categorias da aplicação:

- Category with content added manually. Data of executable files is manually added to the category Se tiver selecionado este tipo de categoria, no passo *Configuring conditions for inclusion of applications in categories* e no passo *Configuring conditions for exclusion of applications from categories*, poderá definir os critérios pelos quais os ficheiros executáveis serão incluídos na categoria.

- Category that includes executable files from selected devices. These executable files are processed automatically and their metrics are added to the category Se tiver selecionado este tipo de categoria, no passo *Settings* poderá especificar um computador cujos ficheiros executáveis serão automaticamente incluídos na categoria.

- Category that includes executable files from a specific folder. Executable files of applications copied to the specified folder are automatically processed and their metrics are added to the category Se tiver selecionado este tipo de categoria, no passo *Repository folder* poderá especificar uma pasta a partir da qual os ficheiros executáveis serão automaticamente incluídos na categoria.

Ao criar uma categoria com conteúdo adicionado automaticamente, o Kaspersky Security Center realiza inventário em ficheiros com os seguintes formatos: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX e SCR.

Passo 2. Introduzir o nome de uma categoria de utilizador

Neste passo, especifique um nome para a categoria da aplicação.

Passo 3. Configurar as condições para a inclusão de aplicações numa categoria

Ao adicionar um grande número de condições às regras de Controlo das Aplicações (por exemplo, hashes de ficheiros), o consumo de recursos do computador aumenta. Quando o número total de condições atingir 50.000, podem ocorrer problemas de desempenho. Para otimizar o desempenho, recomenda-se rever e reduzir o número de condições.

Este passo fica disponível se tiver selecionado o tipo de **Category with content added manually**.

Neste passo, na lista pendente **Add**, selecione as condições para incluir aplicações na categoria:

- **From the list of executable files**. Adicione aplicações da lista de ficheiros executáveis no dispositivo do cliente à categoria personalizada.

- **From file properties**. Especifique dados detalhados dos ficheiros executáveis como condição para adicionar aplicações à categoria personalizada.

- **Metadata from files in folder**. Selecione uma pasta no dispositivo do cliente que contenha ficheiros executáveis. O Kaspersky Security Center indica os metadados destes ficheiros executáveis como condição para adicionar aplicações à categoria personalizada.

- **Checksums of the files in the folder**. Selecione uma pasta no dispositivo do cliente que contenha ficheiros executáveis. O Kaspersky Security Center indica os hashes destes ficheiros executáveis como condição para adicionar aplicações à categoria personalizada.

- **Certificates for the files from the folder**. Selecione uma pasta no dispositivo do cliente que contenha ficheiros executáveis assinados com certificados. O Kaspersky Security Center indica os certificados destes ficheiros executáveis como condição para adicionar aplicações à categoria personalizada.

  É recomendado utilizar condições cujas propriedades não tenham o parâmetro **Certificate fingerprint** especificado.

- **MSI installer files metadata**. Selecione o pacote MSI. O Kaspersky Security Center indica os metadados de ficheiros executáveis incluídos neste pacote MSI como condição para adicionar aplicações à categoria personalizada.

- **Checksums of the files from the MSI installer of the application**. Selecione o pacote MSI. O Kaspersky Security Center indica os hashes de ficheiros executáveis incluídos neste pacote MSI como condição para adicionar aplicações à categoria personalizada.

- **From KL category**. Especifique uma categoria KL como condição para adicionar aplicações à categoria personalizada. Uma *categoria KL* é uma lista de aplicações com atributos de tema partilhados. A lista é mantida por peritos da Kaspersky. Por exemplo, a categoria KL conhecida como *Office Applications* inclui as aplicações do conjunto de programas do Microsoft Office, Adobe Acrobat e outros.

  Pode selecionar categorias KL para gerar uma lista ampliada de aplicações fiáveis.

- **Specify path to application (masks supported)**. Selecione uma pasta no dispositivo do cliente. O Kaspersky Security Center adiciona ficheiros executáveis desta pasta à categoria personalizada.

- **Select certificate from repository**. Selecione os certificados que foram utilizados para assinar ficheiros executáveis como uma condição para adicionar aplicações à categoria personalizada.

  É recomendado utilizar condições cujas propriedades não tenham o parâmetro **Certificate fingerprint** especificado.

  Pode escolher o armazenamento de certificados. Por defeito, o Controlo das Aplicações aplica regras apenas a aplicações assinadas com um certificado do arquivo de certificados do sistema fiável. Isto é ativado pela caixa de verificação **Utilizar verificação estrita da assinatura digital**.

- **Drive type**. Especifique um tipo de dispositivo de armazenamento (todos os discos rígidos e unidades amovíveis, ou apenas unidades amovíveis) como condição para adicionar aplicações à categoria personalizada.

Passo 4. Configurar as condições para a exclusão de aplicações de uma categoria

Este passo fica disponível se tiver selecionado o tipo de **Category with content added manually**.

As aplicações especificadas neste passo são excluídas da categoria, mesmo se tais aplicações tiverem sido especificadas no passo "Configurar as condições para a inclusão de aplicações numa categoria".

Neste passo, na lista pendente **Add**, selecione as condições para a exclusão de aplicações da categoria:

- **From the list of executable files**. Adicione aplicações da lista de ficheiros executáveis no dispositivo do cliente à categoria personalizada.
- **From file properties**. Especifique dados detalhados dos ficheiros executáveis como condição para adicionar aplicações à categoria personalizada.
- **Metadata from files in folder**. Selecione uma pasta no dispositivo do cliente que contenha ficheiros executáveis. O Kaspersky Security Center indica os metadados destes ficheiros executáveis como condição para adicionar aplicações à categoria personalizada.
- **Checksums of the files in the folder**. Selecione uma pasta no dispositivo do cliente que contenha ficheiros executáveis. O Kaspersky Security Center indica os hashes destes ficheiros executáveis como condição para adicionar aplicações à categoria personalizada.
- **Certificates for the files from the folder**. Selecione uma pasta no dispositivo do cliente que contenha ficheiros executáveis assinados com certificados. O Kaspersky Security Center indica os certificados destes ficheiros executáveis como condição para adicionar aplicações à categoria personalizada.
- **MSI installer files metadata**. Selecione o pacote MSI. O Kaspersky Security Center indica os metadados de ficheiros executáveis incluídos neste pacote MSI como condição para adicionar aplicações à categoria personalizada.
- **Checksums of the files from the MSI installer of the application**. Selecione o pacote MSI. O Kaspersky Security Center indica os hashes de ficheiros executáveis incluídos neste pacote MSI como condição para adicionar aplicações à categoria personalizada.
- **From KL category**. Especifique uma categoria KL como condição para adicionar aplicações à categoria personalizada. Uma *categoria KL* é uma lista de aplicações com atributos de tema partilhados. A lista é mantida por peritos da Kaspersky. Por exemplo, a categoria KL conhecida como *Office Applications* inclui as aplicações do conjunto de programas do Microsoft Office, Adobe Acrobat e outros.

  Pode selecionar categorias KL para gerar uma lista ampliada de aplicações fiáveis.
- **Specify path to application (masks supported)**. Selecione uma pasta no dispositivo do cliente. O Kaspersky Security Center adiciona ficheiros executáveis desta pasta à categoria personalizada.
- **Select certificate from repository**. Selecione os certificados que foram utilizados para assinar ficheiros executáveis como uma condição para adicionar aplicações à categoria personalizada.
- **Drive type**. Especifique um tipo de dispositivo de armazenamento (todos os discos rígidos e unidades amovíveis, ou apenas unidades amovíveis) como condição para adicionar aplicações à categoria personalizada.

Passo 5. Definições

Este passo fica disponível se tiver selecionado o tipo de **Category that includes executable files from selected devices**.

Neste passo, clique no botão **Add** e especifique os computadores cujos ficheiros executáveis serão adicionados à categoria da aplicação pelo Kaspersky Security Center. Todos os ficheiros executáveis dos computadores especificados apresentados na pasta **Executable files** serão adicionados à categoria da aplicação pelo Kaspersky Security Center.

Neste passo, também pode configurar as seguintes definições:

- Algoritmo para cálculo da função hash. Para selecionar um algoritmo, tem de selecionar, pelo menos, uma das seguintes caixas de verificação:
  - **Calculate SHA256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions)**.
  - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.
- A caixa de verificação **Synchronize data with Administration Server repository**. Selecione esta caixa de verificação, se pretender que o Kaspersky Security Center limpe periodicamente a categoria de aplicações e que lhe adicione todos os ficheiros executáveis de computadores especificados apresentados na pasta **Executable files**.

  Se a caixa de verificação **Synchronize data with Administration Server repository** estiver desmarcada, o Kaspersky Security Center não efetuará quaisquer modificações a uma categoria de aplicação após a sua criação.

Passo 6. Pasta do repositório

Este passo fica disponível se tiver selecionado o tipo de **Category that includes executable files from a specific folder**.

Neste passo, especifique a pasta em que o Kaspersky Security Center deve procurar ficheiros executáveis para adicionar automaticamente aplicações à categoria de aplicações.

Neste passo, também pode configurar as seguintes definições:

- A caixa de verificação **Include dynamic-link libraries (DLL) in this category**. Selecione esta caixa de verificação se pretender incluir as bibliotecas de ligações dinâmicas (DLL) na categoria da aplicação.

  A inclusão de ficheiros DLL na categoria da aplicação pode reduzir o desempenho do Kaspersky Security Center.

- A caixa de verificação **Include script data in this category**. Selecione esta caixa de verificação se pretender incluir scripts na categoria da aplicação.

  A inclusão de scripts na categoria da aplicação pode reduzir o desempenho do Kaspersky Security Center.

- Algoritmo para cálculo da função hash. Para selecionar um algoritmo, tem de selecionar, pelo menos, uma das seguintes caixas de verificação:

  - **Calculate SHA256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions)**.
  - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

- A caixa de verificação **Force folder scan for changes**. Selecione esta caixa de verificação se pretender que o Kaspersky Security Center procure, periodicamente, ficheiros executáveis na pasta utilizada para acréscimo automático à categoria da aplicação.

  Se a caixa de verificação **Force folder scan for changes** for desmarcada, o Kaspersky Security Center apenas procura ficheiros executáveis na pasta utilizada para o acréscimo automático à categoria de aplicações, se tiverem sido realizadas alterações na pasta e se tiverem sido adicionados ou eliminados ficheiros da pasta.

- O campo **Scan interval (1–168 hours)**. Neste campo, pode especificar o intervalo de tempo (em horas) após o qual o Kaspersky Security Center procura ficheiro executáveis na pasta utilizada para o acréscimo automático à categoria de aplicações.

  O campo fica disponível se a caixa de verificação **Force folder scan for changes** for selecionada.

Passo 7. Criar uma categoria personalizada

Conclua o assistente.

Para adicionar uma nova condição de ativação para uma Regra de Controlo das aplicações na interface da aplicação:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança** → **Controlo das aplicações**.
3. Clique no botão **Aplicações bloqueadas** ou **Aplicações permitidas**.

   Abre-se a lista de Regras de Controlo das Aplicações.
4. Selecione um computada regra para a qual pretende configurar uma condição de acionamento.

   Abre-se a janela de propriedades da regra de Controlo das Aplicações.
5. Selecione o separador **Condições: N** ou **Exclusões: N** e clique no botão **Adicionar**.

6. Selecione as condições de acionamento para uma Regra de Controlo das aplicações:

   - **Condições das propriedades das aplicações iniciadas**. Na lista de aplicações em execução, pode selecionar as aplicações às quais será aplicada a regra de controlo de aplicações. O Kaspersky Endpoint Security também lista as aplicações que estavam em execução anteriormente no computador. Precisa de selecionar o critério que pretende usar para criar uma ou várias condições de acionamento de regras: **Hash do ficheiro**, **Certificado**, **Categoria KL**, **Metadados** ou **Caminho para o ficheiro ou pasta**.

   - **Condições "Categoria KL"**. Uma *categoria KL* é uma lista de aplicações com atributos de tema partilhados. A lista é mantida por peritos da Kaspersky. Por exemplo, a categoria KL conhecida como "aplicações do Office" inclui as aplicações do conjunto de programas do Microsoft Office, Adobe® Acrobat® e outros.

   - **Condição personalizada**. Pode selecionar o ficheiro da aplicação e selecionar uma das condições de acionamento da regra: **Hash do ficheiro**, **Certificado**, **Metadados** ou **Caminho para o ficheiro ou pasta**.

   - **Condição por unidade de ficheiros (unidade amovível)**. A regra de Controlo das Aplicações é aplicada apenas a ficheiros executados numa unidade amovível.

   - **Condições das propriedades dos ficheiros na pasta especificada**. A regra de Controlo das Aplicações é aplicada apenas a ficheiros na pasta especificada. Também pode incluir ou excluir ficheiros de subpastas. Precisa de selecionar o critério que pretende usar para criar uma ou várias condições de acionamento de regras: **Hash do ficheiro**, **Certificado**, **Categoria KL**, **Metadados** ou **Caminho para o ficheiro ou pasta**.

7. Guarde as suas alterações.

Ao adicionar condições, tenha em conta as seguintes considerações especiais para o Controlo das Aplicações:

- O Kaspersky Endpoint Security suporta os caracteres `*` e `?` para introduzir uma máscara nos metadados: **File name**, **Application name**, **Vendor**.

- O Kaspersky Endpoint Security não suporta um hash do ficheiro MD5 e não controla a inicialização das aplicações com base num hash MD5. Um hash de SHA256 é utilizado como uma condição de ativação de regras.

- Não é recomendado que se utilize apenas os critérios **Emissor** e **Requerente do certificado** como condições de ativação de regras. A utilização destes critérios não é segura.

- Se estiver a utilizar uma ligação simbólica no campo **Caminho para o ficheiro ou pasta**, aconselhamo-lo a resolver a ligação simbólica para o funcionamento correto da regra de Controlo das Aplicações. Para tal, clique no botão **Resolver ligação simbólica**.

Adicionar ficheiros executáveis da pasta de Ficheiros executáveis à categoria de aplicações

Na pasta **Executable files** é apresentada a lista de ficheiros executáveis detetados no computador. O Kaspersky Endpoint Security gera uma lista de ficheiros executáveis depois de executar a tarefa de Inventário.

Adicionar ficheiros executáveis da pasta Executable files à categoria de aplicações:

1. Abra a Consola de Administração do Kaspersky Security Center.

2. Na árvore da Consola de Administração, selecione **Advanced** → **Application management** → **Executable files**.

3. Na área de trabalho, selecione os ficheiros executáveis que quer adicionar à categoria de aplicações.

4. Clique com o botão direito para abrir o menu de contexto dos ficheiros executáveis e selecione **Add to category**.

5. Na janela que surgir, faça o seguinte:

   - Na parte superior direita da janela, escolha uma das seguintes opções:

     - **Add to a new application category**. Escolha esta opção se quiser criar uma nova categoria de aplicações e adicionar-lhe ficheiros executáveis.

     - **Add to an existing application category**. Escolha esta opção se quiser selecionar uma categoria de aplicações existente e adicionar-lhe ficheiros executáveis.

   - No bloco **Rule type**, selecione uma das seguintes opções:

     - **Rules for adding to inclusions**. Selecione esta opção se quiser criar uma condição que adiciona ficheiros executáveis à categoria de aplicações.

     - **Rules for adding to exclusions**. Selecione esta opção se quiser criar uma condição que exclui ficheiros executáveis da categoria de aplicações.

   - No bloco **Parameter used as a condition**, selecione uma das seguintes opções:

     - **Certificate details (or SHA256 hashes for files without a certificate)**.

     - **Certificate details (files without a certificate will be skipped)**.

     - **Only SHA256 (files without a hash will be skipped)**.

     - **Only MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1 version)**.

6. Guarde as suas alterações.

Adicionar ficheiros executáveis relacionados a eventos à categoria de aplicações

Para adicionar ficheiros executáveis relacionados com os eventos do Controlo das Aplicações à categoria de aplicações:

1. Abra a Consola de Administração do Kaspersky Security Center.

2. No nó **Administration Server** da árvore da Consola de Administração, selecione o separador **Events**.

3. Escolha uma seleção de eventos relacionados à operação do componente de Controlo das Aplicações (Ver eventos que resultam da operação do componente de Controlo das Aplicações, Ver eventos que resultam da operação de teste do componente de Controlo das Aplicações) na lista pendente **Event selections**.

4. Selecione o botão **Run selection**.

5. Selecione os eventos cujos ficheiros executáveis associados que quer adicionar à categoria de aplicações.

6. Clique com o botão direito para abrir o menu de contexto dos eventos selecionados e selecione **Add to category**.

7. Na janela que abre, configure as definições da categoria de aplicações:

   - Na parte superior direita da janela, escolha uma das seguintes opções:

     - **Add to a new application category**. Escolha esta opção se quiser criar uma nova categoria de aplicações e adicionar-lhe ficheiros executáveis.

     - **Add to an existing application category**. Escolha esta opção se quiser selecionar uma categoria de aplicações existente e adicionar-lhe ficheiros executáveis.

   - No bloco **Rule type**, selecione uma das seguintes opções:

     - **Rules for adding to inclusions**. Selecione esta opção se quiser criar uma condição que adiciona ficheiros executáveis à categoria de aplicações.

     - **Rules for adding to exclusions**. Selecione esta opção se quiser criar uma condição que exclui ficheiros executáveis da categoria de aplicações.

   - No bloco **Parameter used as a condition**, selecione uma das seguintes opções:

     - **Certificate details (or SHA-256 hashes for files without a certificate)**.

     - **Certificate details (files without a certificate will be skipped)**.

     - **Only SHA-256 (files without a hash will be skipped)**.

     - **Only MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1 version)**.

8. Guarde as suas alterações.

Adicionar uma Regra de Controlo das Aplicações

Para adicionar uma regra de Controlo das Aplicações utilizando o Kaspersky Security Center:

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Controlos de segurança → Controlo das Aplicações**.

   Na parte direita da janela, são apresentadas as definições do componente Controlo das Aplicações.

4. Clique em **Adicionar**.

   Abre-se a janela **Regra de Controlo das Aplicações**.

5. Execute uma das ações seguintes:

   - Se pretende criar uma nova categoria:

     a. Clique em **Criar categoria**.

        O assistente de criação de categorias de utilizador é iniciado.

b. Siga as instruções apresentadas no assistente de criação de uma nova categoria.

c. Na lista pendente **Categoria**, selecione a categoria da aplicação criada.

- Se pretende editar uma categoria existente:

a. Na lista pendente **Categoria**, selecione a categoria de aplicação criada com base que pretende editar.

b. Clique em **Propriedades**.

c. Modificar as definições da categoria da aplicação selecionada.

d. Guarde as suas alterações.

e. Na lista pendente **Categoria**, selecione a categoria de aplicação criada com base na qual pretende criar uma regra.

6. Na tabela **Utilizadores e os seus direitos**, clique no botão **Adicionar**.

   Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

7. Na tabela **Utilizadores e os seus direitos**, faça o seguinte:

   - Se pretender permitir que os utilizadores e/ou os grupos de utilizadores iniciem aplicações que pertencem à categoria selecionada, selecione a caixa de verificação **Permitir** nas linhas relevantes.

   - Se pretender bloquear esses utilizadores e/ou os grupos de utilizadores de iniciar aplicações que pertencem à categoria selecionada, selecione a caixa de verificação **Bloquear** nas linhas relevantes.

8. Selecione a caixa de verificação **Recusar para outros utilizadores** se pretender que todos os utilizadores que não são apresentados na coluna **Utilizador ou grupo** e que não façam parte do grupo de utilizadores especificado na coluna **Utilizador ou grupo** sejam impedidos de iniciar aplicações que pertençam à categoria selecionada.

9. Se pretender que o Kaspersky Endpoint Security considere as aplicações incluídas na categoria de aplicações selecionada enquanto atualizadores fiáveis com permissão para criar outros ficheiros executáveis que terão permissão para serem subsequentemente executados, selecione a caixa de verificação **Atualizadores fiáveis**.

   Quando as definições de Kaspersky Endpoint Security são migradas, a lista de ficheiros executáveis criados por atualizadores fiáveis também é migrada.

10. Guarde as suas alterações.

Para adicionar uma Regra de Controlo das Aplicações:

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Controlos de segurança** → **Controlo das aplicações**.

3. Clique no botão **Aplicações bloqueadas** ou **Aplicações permitidas**.

   Abre-se a lista de Regras de Controlo das Aplicações.

4. Clique em **Adicionar**.

   Esta ação abre a janela de definições de regra Controlo das Aplicações.

5. No separador **Definições gerais**, defina as definições principais da regra:

   a. No campo **Nome da regra**, introduza o nome da regra.

   b. No campo **Descrição**, introduza uma descrição da regra.

   c. Na tabela **Utilizadores e os seus direitos**, clique no botão **Adicionar**.

      Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

      A regra é aplicável a todos os utilizadores por predefinição.

      > Se não existir utilizador especificado na tabela, a regra não pode ser guardada.

   d. Na tabela **Utilizadores e os seus direitos**, use o botão de alternar para definir o direito de os utilizadores iniciarem aplicações.

   e. Selecione a caixa de verificação **Recusar para outros utilizadores** se quiser que a aplicação impeça a execução de aplicações que satisfaçam as condições de ativação de regras para todos os utilizadores que não estejam listados na tabela **Utilizadores e os seus direitos** e não sejam membros de grupos de utilizadores listados na tabela **Utilizadores e os seus direitos**.

      > Se a caixa de verificação **Recusar para outros utilizadores** estiver desmarcada, o Kaspersky Endpoint Security não controla o arranque de aplicações por utilizadores que não são apresentados na tabela **Utilizadores e os seus direitos** e que não pertencem aos grupos de utilizadores especificados na tabela **Utilizadores e os seus direitos**.

   f. Selecione a caixa de seleção **Atualizadores fiáveis**, se desejar que o Kaspersky Endpoint Security considere as aplicações que correspondem às condições de acionamento de regras como atualizadores fiáveis. *Atualizadores fiáveis* são aplicações que têm permissão para criar outros ficheiros executáveis que poderão ser executados posteriormente.

      Se uma aplicação acionar várias regras, o Kaspersky Endpoint Security define o sinalizador *Atualizadores fiáveis* se as seguintes condições forem cumpridas:

      - Todas as regras permitem que a aplicação seja executada.
      - Pelo menos uma regra tem a caixa de verificação **Atualizadores fiáveis** selecionada.

6. No separador **Condições: N**, crie ou edite a lista de condições de inclusão para ativar a regra.

7. No separador **Exclusões: N**, crie ou edite a lista de condições de exclusão para ativar a regra.

   Quando as definições de Kaspersky Endpoint Security são migradas, a lista de ficheiros executáveis criados por atualizadores fiáveis também é migrada.

8. Guarde as suas alterações.

Alterar o estado de uma Regra de Controlo das aplicações utilizando o Kaspersky Security Center

Para alterar o estado de uma Regra de Controlo das aplicações na Consola de Administração:

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança → Controlo das Aplicações**.

   Na parte direita da janela, são apresentadas as definições do componente Controlo das Aplicações.
4. Na coluna **Estado**, clique com o botão esquerdo para apresentar o menu de contexto e selecionar uma das seguintes opções:

   - **Ativado**. Este estado significa que a regra é utilizada quando o componente Controlo das Aplicações está em execução.
   - **Desativado**. Este estado significa que a regra é ignorada quando o componente Controlo das Aplicações está em execução.
   - **Teste**. Este estado significa que o Kaspersky Endpoint Security permite sempre o arranque da aplicação à qual é aplicável a regra, mas regista informações sobre o arranque de tais aplicações no relatório.
5. Guarde as suas alterações.

Para alterar o estado de uma Regra de Controlo das aplicações na interface da aplicação:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança → Controlo das aplicações**.
3. Clique no botão **Aplicações bloqueadas** ou **Aplicações permitidas**.

   Abre-se a lista de Regras de Controlo das Aplicações.
4. Na coluna **Estado**, abra o menu de contexto e selecione uma das seguintes opções:

   - **Ativada**. Este estado significa que a regra é utilizada quando o componente Controlo das Aplicações está em execução.
   - **Desativada**. Este estado significa que a regra é ignorada quando o componente Controlo das Aplicações está em execução.
   - **Modo de teste**. Este estado significa que o Kaspersky Endpoint Security permite sempre o arranque da aplicação à qual é aplicável esta regra, mas regista informações sobre o arranque de tais aplicações no relatório.
5. Guarde as suas alterações.

Exportar e importar Regras de Controlo das Aplicações

Pode exportar a lista de Regras de Controlo das Aplicações para um ficheiro XML. Pode utilizar a função de exportação/importação para fazer uma cópia de segurança da lista de Regras de Controlo das Aplicações ou para migrar a lista para um servidor diferente.

Ao importar e exportar regras de Controlo das Aplicações, lembre-se de ter em conta o seguinte:

- O Kaspersky Endpoint Security exporta a lista de regras apenas para o modo de Controlo das Aplicações ativo. Por outras palavras, se o Controlo das Aplicações estiver a funcionar no modo de lista de bloqueio, o Kaspersky Endpoint Security exporta as regras apenas para esse modo. Para exportar a lista de regras para o modo de lista de permissão, precisará de mudar o modo e voltar a executar a operação de exportação.
- O Kaspersky Endpoint Security utiliza categorias da aplicação para que as Regras de Controlo das Aplicações funcionem. Ao migrar a lista de Regras de Controlo das Aplicações para um servidor diferente, também precisará de migrar a lista de categorias da aplicação. Para obter mais detalhes sobre a exportação ou a importação de categorias da aplicação, consulte a Ajuda do Kaspersky Security Center.

Como exportar e importar uma lista de regras de Controlo das Aplicações na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança → Controlo das Aplicações**.
4. Para exportar a lista de regras de Controlo das Aplicações:
   a. Selecione as regras que pretende exportar. Para selecionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.
      Se não tiver selecionado nenhuma regra, o Kaspersky Endpoint Security exportará todas as regras.
   b. Clique na hiperligação **Exportar**.
   c. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de regras e selecione a pasta onde pretende guardar este ficheiro.
   d. Guardar o ficheiro.
      O Kaspersky Endpoint Security exporta a lista de regras para o ficheiro XML.
5. Para importar uma lista das regras de Controlo das Aplicações:
   a. Clique na hiperligação **Importar**.
      Na janela que se abre, selecione o ficheiro XML a partir do qual pretende importar a lista de regras.
   b. Abrir o ficheiro.
      Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro XML.
6. Guarde as suas alterações.

Como exportar e importar uma lista de regras de Controlo das Aplicações na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Security Controls** → **App Control**.
5. Sob **Operating mode**, selecione uma lista de regras: lista de bloqueio ou de permissão de aplicações.
6. Para exportar a lista de regras:
   a. Selecione as regras que pretende exportar.
   b. Selecione o botão → **Export**.
      O Kaspersky Endpoint Security exporta a lista de regras para um ficheiro JSON na pasta de transferências predefinida.
7. Para importar a lista de regras:
   a. Selecione o botão → **Import**.
      Na janela que se abre, selecione o ficheiro JSON a partir do qual pretende importar a lista de regras.
   b. Abrir o ficheiro.
      Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro JSON.
8. Guarde as suas alterações.

Ver eventos que resultam da operação do componente de Controlo das Aplicações

Para ver eventos que resultam da operação do componente de Controlo das Aplicações recebido pelo Kaspersky Security Center:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. No nó **Administration Server** da árvore da Consola de Administração, selecione o separador **Events**.
3. Selecione o botão **Create a selection**.
4. Na janela que surgir, aceda à secção **Events**.
5. Selecione o botão **Clear all**.
6. Na tabela **Events**, selecione a caixa de verificação **Inicialização da aplicação proibida**.
7. Guarde as suas alterações.

8. Na lista pendente **Event selections**, escolha a seleção criada.

9. Selecione o botão **Run selection**.

Ver um relatório sobre aplicações bloqueadas

Para ver o relatório sobre as aplicações bloqueadas:

1. Abra a Consola de Administração do Kaspersky Security Center.

2. No nó **Administration Server** da árvore da Consola de Administração, selecione o separador **Reports**.

3. Clique em **New report template**.

   O novo Assistente de Modelos de Relatório é iniciado.

4. Siga as instruções do Assistente de Modelos de Relatório. No passo **Selecting the report template type**, selecione **Other → Report on prohibited applications**.

   Depois de concluir o Novo Assistente de Modelos de Relatório, o novo modelo de relatório é apresentado na tabela no separador **Reports**.

5. Abra o relatório fazendo duplo clique.

O processo de criação do relatório é iniciado. O relatório é apresentado numa nova janela.

Testar Regras de Controlo das Aplicações

Para assegurar que as Regras de Controlo das Aplicações não bloqueia aplicações necessárias para o trabalho, recomenda-se que o teste seja ativado para as Regras de Controlo das Aplicações e que o seu funcionamento seja analisado depois de as regras serem criadas. Quando o teste está ativado, o Kaspersky Endpoint Security não bloqueará as aplicações cuja inicialização esteja proibida pelo Controlo das Aplicações, mas enviará notificações sobre o sua inicialização para o Servidor de Administração.

Uma análise do funcionamento das Regras de Controlo das Aplicações requer uma revisão dos eventos do Controlo das Aplicações resultantes reportados ao Kaspersky Security Center. Se o modo de teste não resultar em nenhum evento de inicialização bloqueado para todas as aplicações necessárias para o trabalho do utilizador de computador, isto significa que as regras corretas foram criadas. Caso contrário, é aconselhável atualizar as configurações que criou ou eliminar as regras existentes.

Por predefinição, o Kaspersky Endpoint Security permite a inicialização de todas as aplicações, exceto as aplicações proibidas pelas regras.

Ativar e desativar teste de regras do Controlo das Aplicações

Para ativar ou desativar os testes das Regras de Controlo das Aplicações no Kaspersky Security Center:

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Controlos de segurança → Controlo das Aplicações**.

   Na parte direita da janela, são apresentadas as definições do componente Controlo das Aplicações.

4. Na lista pendente **Modo de controlo**, selecione um dos seguintes itens:

   - **Lista de bloqueio**. Se esta opção estiver selecionada, o Controlo das Aplicações permite que todos os utilizadores iniciem qualquer tipo de aplicação, exceto nos casos em que as aplicações satisfazem as condições das regras de bloqueio do Controlo das Aplicações.

   - **Lista de permissão**. Se esta opção estiver selecionada, o Controlo das Aplicações bloqueia todos os utilizadores de iniciarem qualquer tipo de aplicação, exceto nos casos em que satisfazem as condições das regras de permissão do Controlo das Aplicações.

5. Execute uma das ações seguintes:

   - Para ativar os testes das Regras de Controlo das Aplicações, selecione a opção **Testar regras** na lista pendente **Ação**.

   - Se pretender ativar o Controlo das Aplicações para gerir o arranque de aplicações nos computadores dos utilizadores, na lista pendente, selecione **Aplicar regras**.

6. Guarde as suas alterações.

Para ativar o modo de teste das Regras de Controlo das Aplicações ou selecionar uma ação de bloqueio do Controlo das aplicações:

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Controlos de segurança → Controlo das aplicações**.

3. Clique no botão **Aplicações bloqueadas** ou **Aplicações permitidas**.

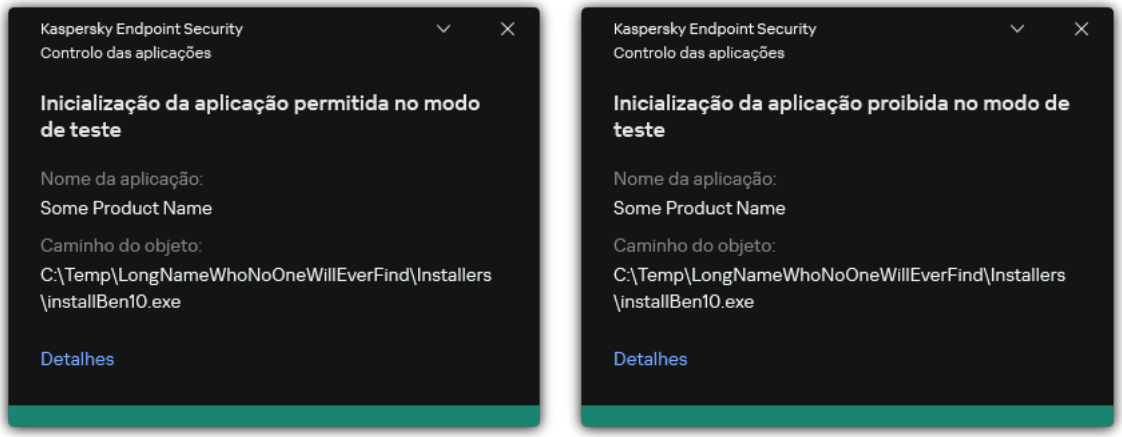
   Abre-se a lista de Regras de Controlo das Aplicações.

4. Na coluna **Estado**, selecione **Modo de teste**.

   Este estado significa que o Kaspersky Endpoint Security permite sempre o arranque da aplicação à qual é aplicável esta regra, mas regista informações sobre o arranque de tais aplicações no relatório.

5. Guarde as suas alterações.

O Kaspersky Endpoint Security não bloqueará as aplicações cuja inicialização esteja proibida pelas Regras de Controlo das aplicações, mas enviará notificações sobre a sua inicialização para o Servidor de Administração. Também pode configurar a exibição de notificações sobre o teste de regras no computador do utilizador (veja a figura abaixo).



Notificações do Controlo das Aplicações no modo de teste

Ver um relatório sobre as aplicações bloqueadas no modo de teste

Para ver o relatório sobre as aplicações bloqueadas no modo de teste:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. No nó **Administration Server** da árvore da Consola de Administração, selecione o separador **Reports**.
3. Clique em **New report template**.

   O novo Assistente de Modelos de Relatório é iniciado.
4. Siga as instruções do Assistente de Modelos de Relatório. No passo **Selecting the report template type**, selecione **Other → Report on prohibited applications in test mode**.

   Depois de concluir o Novo Assistente de Modelos de Relatório, o novo modelo de relatório é apresentado na tabela no separador **Reports**.
5. Abra o relatório fazendo duplo clique.

O processo de criação do relatório é iniciado. O relatório é apresentado numa nova janela.

Ver eventos que resultam de operação de teste do componente de Controlo das Aplicações

Para ver eventos dos testes do Controlo das Aplicações recebidos pelo Kaspersky Security Center:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. No nó **Administration Server** da árvore da Consola de Administração, selecione o separador **Events**.
3. Selecione o botão **Create a selection**.
4. Na janela que surgir, aceda à secção **Events**.
5. Selecione o botão **Clear all**.

6. Na tabela **Events**, selecione as caixas de verificação **Inicialização da aplicação proibida no modo de teste** e **Inicialização da aplicação permitida no modo de teste**.

7. Guarde as suas alterações.

8. Na lista pendente **Event selections**, escolha a seleção criada.

9. Selecione o botão **Run selection**.

Monitor de atividade das aplicações

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para estações de trabalho. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para servidores.

O *Monitor de Atividade das Aplicações* é uma ferramenta concebida para visualizar informações sobre a atividade das aplicações no computador de um utilizador em tempo real.

O uso do Monitor de Atividade das Aplicações exige a instalação dos componentes Controlo das Aplicações e Prevenção contra invasões. Se estes componentes não estiverem instalados, a secção Monitor de Atividade das Aplicações na janela principal da aplicação está oculta.

Para iniciar o Monitor de Atividade das Aplicações:

Na janela principal da aplicação, na secção **Monitorização**, clique em **Monitor de Atividade das Aplicações**.

Nesta janela, as informações sobre a atividade das aplicações no computador de um utilizador são apresentadas em três separadores:

- O separador **Todas as aplicações** apresenta informações acerca de todas as aplicações instaladas no computador.
- O separador **Em execução** apresenta informações acerca do consumo de recursos do computador por cada aplicação em tempo real. A partir desse separador, também é possível proceder à configuração de permissões pata uma aplicação individual.
- O separador **Executar no arranque** apresenta a lista das aplicações que se iniciam quando o sistema operativo é iniciado.

Se deseja ocultar as informações de atividade da aplicação no computador do utilizador, pode restringir o acesso do utilizador à ferramenta Monitor de atividade das aplicações.

Como ocultar o Monitor de atividade das aplicações na interface da aplicação utilizando a Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Definições gerais → Interface**.

4. Utilize a caixa de vericação **Secção Ocultar Monitor de Atividade das Aplicações** para conceder ou revogar o acesso à ferramenta.

5. Guarde as suas alterações.

Como ocultar o Monitor de atividade das aplicações na interface da aplicação utilizando a Consola Web e a Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **General Settings** → **User Interaction**.

5. Utilize a caixa de vericação **Hide Application Activity Monitor section** para conceder ou revogar o acesso à ferramenta.

6. Guarde as suas alterações.

Regras para criar máscaras de nome para ficheiros ou pastas

Uma *máscara de um ficheiro ou nome de pasta* é uma representação do nome de uma pasta ou nome e extensão de um ficheiro utilizando carateres comuns.

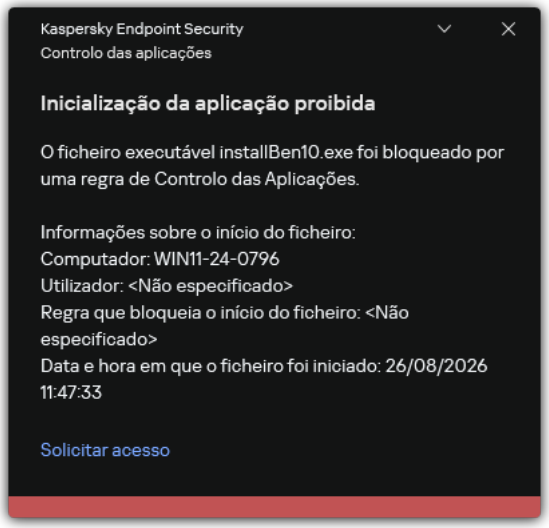
Pode utilizar os seguintes carateres comuns para criar uma máscara de nome de ficheiro ou pasta:

- O carácter `*` (asterisco), que ocupa o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio). Por exemplo, a máscara `C:\*.txt` incluirá todos os caminhos para ficheiros com a extensão `txt` encontrados em pastas e subpastas na unidade (C:).

- O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.

Editar modelos de mensagens do Controlo das Aplicações

Quando um utilizador tenta iniciar uma aplicação bloqueada por uma Regra de Controlo das aplicações, o Kaspersky Endpoint Security apresenta uma mensagem a avisar que o arranque da aplicação está bloqueado. Os especialistas da Kaspersky fornecem um modelo de uma mensagem ao utilizador a descrever as razões pelas quais a aplicação foi bloqueada (consulte a figura abaixo). São fornecidas variáveis especiais para gerir os modelos da mensagem (por exemplo, `%USER_NAME%`). As variáveis permitem que um único modelo de mensagem seja usado para diferentes computadores. Ao gerar uma mensagem, o Kaspersky Endpoint Security recupera o valor da variável das definições do sistema operativo e insere-o na mensagem correspondente ao computador, utilizador e evento específicos.



Notificação do Controlo das Aplicações

Se o utilizador considerar que o arranque de uma aplicação foi bloqueado incorretamente, o utilizador pode utilizar a ligação no texto da mensagem para enviar uma mensagem ao administrador local da rede da empresa. Para o fazer, o utilizador tem de clicar no botão **Solicitar acesso** e enviar uma mensagem ao administrador a descrever a situação. Também pode preparar um modelo da mensagem para o administrador, acrescentando-lhe dados que possam informar a sua decisão de permitir ou bloquear o acesso à aplicação. Depois de o utilizador solicitar acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio da inicialização da aplicação para o administrador**. A descrição do evento contém uma mensagem para o administrador com variáveis substituídas. Pode visualizar estes eventos na consola do Kaspersky Security Center utilizando a seleção de eventos predefinida **User requests**. Se a sua organização não tiver o Kaspersky Security Center implementado ou não houver uma ligação ao Servidor de Administração, a aplicação irá enviar uma mensagem ao administrador para o endereço de e-mail especificado.

Como editar o modelo de mensagem do Controlo das Aplicações na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança** → **Controlo das Aplicações**.
4. No bloco **Definições dos modelos de mensagem**, clique no botão **Modelos**.

5. Irá abrir-se uma janela; nessa janela, configure os modelos do Controlo das Aplicações:

   - **Mensagem sobre o bloqueio**. Modelo da mensagem que é apresentada quando é acionada uma regra de Controlo das Aplicações que bloqueia o início de uma aplicação.

     Não pode configurar modelos de mensagem para o Controlo das Aplicações no modo de teste. O Controlo das Aplicações no modo de teste apresenta notificações predefinidas.

   - **Mensagem para o administrador**. Modelo da mensagem que um utilizador pode enviar ao administrador da LAN empresarial se o utilizador acreditar que uma aplicação foi bloqueada por engano.

   Para adicionar uma variável ao texto do modelo, coloque o cursor na posição desejada, clique em **Variável** e selecione a variável necessária na lista de opções disponíveis.

   Também pode restaurar o texto do modelo padrão ao clicar em **Por defeito**.

6. Guarde as suas alterações.

Como editar o modelo de mensagem do Controlo das Aplicações na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Security Controls** → **App Control**.
5. No bloco **Message templates**, clique na ligação **Messages about application startup block** e configure modelos para mensagens do Controlo das Aplicações:

   - **Message to user**. Modelo da mensagem que é apresentada quando é acionada uma regra de Controlo das Aplicações que bloqueia o início de uma aplicação.

     Não pode configurar modelos de mensagem para o Controlo das Aplicações no modo de teste. O Controlo das Aplicações no modo de teste apresenta notificações predefinidas.

   - **Message to administrator**. Modelo da mensagem que um utilizador pode enviar ao administrador da LAN empresarial se o utilizador acreditar que uma aplicação foi bloqueada por engano.

   Para adicionar uma variável ao texto do modelo, coloque o cursor na posição desejada, clique em **Add variable** e selecione a variável necessária na lista de opções disponíveis.

   Também pode restaurar o texto do modelo padrão ao clicar em **Reset to default**.

6. Guarde as suas alterações.

Como editar o modelo de mensagem do Controlo das Aplicações na interface de aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Controlos de segurança** → **Controlo das aplicações**.

3. No bloco **Modelos de mensagens sobre bloqueio de aplicações**, configure os modelos para mensagens de Controlo das Aplicações:

   - **Mensagem sobre o bloqueio**. Modelo da mensagem que é apresentada quando é acionada uma regra de Controlo das Aplicações que bloqueia o início de uma aplicação.

     Não pode configurar modelos de mensagem para o Controlo das Aplicações no modo de teste. O Controlo das Aplicações no modo de teste apresenta notificações predefinidas.

   - **Mensagem para o administrador**. Modelo da mensagem que um utilizador pode enviar ao administrador da LAN empresarial se o utilizador acreditar que uma aplicação foi bloqueada por engano.

   Para adicionar uma variável ao texto do modelo, coloque o cursor na posição desejada, clique em **Adicionar variável** e selecione a variável necessária na lista de opções disponíveis.

   Também pode restaurar o texto do modelo padrão ao clicar em **Repor**.

4. Guarde as suas alterações.

Variáveis em modelos de mensagens do Controlo das aplicações

Pode utilizar as seguintes variáveis nos modelos de mensagens do utilizador ou nos modelos de mensagens do administrador:

- **O nome da regra que foi acionada** – `%RULE%`.

  Nome da regra que bloqueou a execução de um ficheiro.

- **Data atual** – `%DATE%`.

  Data em que a execução do ficheiro foi bloqueada, no formato DD.MM.AAAA.

- **Hora atual** – `%TIME%`.

  Horário em que a execução do ficheiro foi bloqueada, no formato HH:MM.

- **Nome de utilizador** – `%USER_NAME%`.

  Nome da conta de utilizador atual no computador em que a execução do ficheiro 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 ficheiro foi bloqueada.

- **Nome do ficheiro executável** – `%FILE_NAME%`.

  Nome do ficheiro executável da aplicação bloqueada.

- **Categoria KL do ficheiro executável** – `%KL_CAT%`.

  Categoria KL à qual pertence a aplicação bloqueada (por exemplo, *Navegadores* ou outra categoria).

- **Caminho para o ficheiro executável** – `%FILE_PATH%`.

  Caminho completo para o ficheiro executável da aplicação bloqueada.

- **Versão do ficheiro executável** – `%FILE_VERSION%`.

  Versão do ficheiro executável da aplicação bloqueada.

- **Nome original do ficheiro executável** – `%ORIGINAL_FILE_NAME%`.

  Nome original do ficheiro executável da aplicação bloqueada. O nome do ficheiro é especificado nas propriedades do ficheiro executável da aplicação.

- **Fornecedor** – `%FILE_PUBLISHER%`.

  Fornecedor da aplicação bloqueada.

- **Nome da aplicação** – `%FILE_PRODUCT_NAME%`.

  Nome da aplicação bloqueada.

- **Versão da aplicação** – `%PRODUCT_VERSION%`.

  Versão da aplicação bloqueada.

- **Hash do ficheiro executável** – `%FILE_HASH%`.

  Hash do ficheiro executável da aplicação bloqueada.

- **Emissor do certificado** – `%CERT_ISSUER%`.

  Emissor do certificado com o qual o ficheiro executável está assinado.

- **Requerente do certificado** – `%CERT_SUBJECT%`.

  Assunto do certificado com o qual o ficheiro executável está assinado.

- **Thumbprint do certificado** – `%CERT_THUMBPRINT%`.

  Impressão digital do certificado com o qual o ficheiro executável está assinado.

Melhores práticas para efetuar um inventário de ficheiros executáveis

A tarefa *Inventory* obtém informações sobre ficheiros executáveis (por exemplo, EXE, BAT e CMD), módulos DLL e scripts (PowerShell, JS, entre outros). Estas informações são necessárias para configurar as categorias do Controlo das Aplicações e as permissões de aplicações do componente Prevenção contra invasões. A tarefa *Inventory* deve ser executada periodicamente para manter as informações atualizadas. A tarefa *Inventory*, tal como a tarefa *Malware Scan*, utiliza muitos recursos. Por conseguinte, recomendamos que configure a execução da tarefa durante a noite ou aos fins de semana.

Etapas do inventário de ficheiros executáveis

1. Selecione o grupo de computadores de referência nos quais está instalado o conjunto de software típico da sua organização. Recomendamos que reduza ao mínimo o número de computadores utilizados para o procedimento de inventário de ficheiros executáveis. Quanto menos tarefas *Inventory* forem executadas, menor será a carga no Kaspersky Security Center Administration Server.

2. Mova os computadores de referência para um grupo de administração separado na consola do Kaspersky Security Center. Pode atribuir um nome ao grupo, por exemplo, *Computadores de referência*.

3. Crie uma tarefa *Inventory* para o grupo de administração *Computadores de referência*. Recomendamos que mantenha as predefinições da tarefa.

Exemplo de um inventário de ficheiros executáveis numa organização

Por exemplo, a sua organização tem 100 computadores com o Windows 11 25H2. Todos os computadores têm a mesma versão e localização do sistema operativo. O conjunto de atualizações instaladas nos computadores também é o mesmo.

Numa organização deste tipo, não é necessário executar a tarefa *Inventory* em todos os computadores. A maioria dos ficheiros executáveis nestes computadores é idêntica. É suficiente criar uma tarefa para um computador de referência. Pode criar tarefas *Inventory* adicionais para computadores com uma configuração diferente da configuração de referência.

Melhores práticas para implementar uma lista de aplicações permitidas

Ao planear a implementação de uma lista de aplicações permitidas, é aconselhável realizar as seguintes ações:

1. Forme os seguintes tipos de grupos:

   - Grupos de utilizadores. Os grupos de utilizadores para os quais precisa de permitir a utilização de vários conjuntos de aplicações.

   - Grupos de administração. Um ou vários grupos de computadores para os quais o Kaspersky Security Center irá aplicar a lista de aplicações permitidas. É necessário criar vários grupos de computadores se forem utilizadas diferentes definições de lista de permissão para esses grupos.

2. Crie uma lista de aplicações cujo início tem de ser permitido.

   Antes de criar uma lista, é aconselhável fazer o seguinte:

   a. Execute a tarefa de inventário.

      A informação sobre a criação, reconfiguração e arranque de uma tarefa de inventário encontra-se disponível na secção Gestão de tarefas.

   b. Ver a lista de ficheiros executáveis.

Configurar o modo de lista de permissão para aplicações

Ao configurar o modo de lista de permissão, é aconselhável realizar as seguintes ações:

1. Crie categorias da aplicação com as aplicações cujo início tem de ser permitido.

Pode selecionar um dos seguintes métodos para criar categorias da aplicação:

- **Category with content added manually**. Pode adicionar manualmente a esta categoria utilizando as seguintes condições:
  - Metadados do ficheiro. O Kaspersky Security Center adiciona todos os ficheiros executáveis com os metadados especificados à categoria de aplicações.
  - Código de hash do ficheiro. O Kaspersky Security Center adiciona todos os ficheiros executáveis com o hash especificado à categoria da aplicação.

    A utilização desta condição exclui a capacidade de instalar automaticamente atualizações, pois versões diferentes dos ficheiros terão um hash diferente.

  - Certificado do ficheiro. O Kaspersky Security Center adiciona todos os ficheiros executáveis assinados com o certificado especificado à categoria da aplicação.
  - Categoria KL. O Kaspersky Security Center adiciona todas as aplicações na categoria KL especificada à categoria da aplicação.
  - Pasta da aplicação. O Kaspersky Security Center adiciona todos os ficheiros executáveis desta pasta à categoria personalizada.

    A utilização da **Application folder** poderá não ser segura, pois qualquer aplicação da pasta especificada estará autorizada a ser inicializada. Recomenda-se aplicar regras que usam as categorias da aplicação com a condição da **Application folder** só àqueles utilizadores para quem a instalação automática de atualizações deve ser permitida.

- **Category that includes executable files from a specific folder**. Pode especificar a pasta a partir da qual os ficheiros executáveis serão automaticamente atribuídos à categoria da aplicação criada.
- **Categoria que inclui ficheiros executáveis de dispositivos selecionados**. Pode especificar um computador a partir do qual todos os ficheiros executáveis serão automaticamente atribuídos à categoria da aplicação criada.

  Quando utilizar este tipo de categorias da aplicação, o Kaspersky Security Center recebe informações sobre aplicações no computador a partir da pasta **Executable files**.

2. Selecione o modo de lista de permissão para o componente Controlo das Aplicações.
3. Crie Regras de Controlo das aplicações utilizando as categorias da aplicação criadas.

A regra de **Golden Image** e a regra de **Atualizadores fiáveis** são inicialmente definidas para o modo de Lista de Permissão. Estas Regras de Controlo das Aplicações correspondem às categorias KL. A categoria KL *Golden Image* inclui programas que garantem o funcionamento normal do sistema operativo. A categoria KL *Atualizadores fiáveis* inclui atualizadores para os fornecedores de software de maior renome. Não é possível eliminar estas regras. As definições destas regras não podem ser editadas. Por predefinição, a regra **Golden Image** está ativada e a regra **Atualizadores fiáveis** está desativada. Todos os utilizadores podem iniciar aplicações que cumpram as condições de ativação destas regras.

4. Determine as aplicações para as quais a instalação automática de atualizações deve ser permitida.

   Pode permitir a instalação automática de atualizações de uma das seguintes formas:

   - Especifique uma lista completa de aplicações permitidas, permitindo a inicialização de todas as aplicações que pertencem a qualquer categoria KL.
   - Especifique uma lista completa de aplicações permitidas, permitindo a inicialização de todas as aplicações assinadas com certificados.

     Para permitir o arranque de todas as aplicações assinadas com certificados, pode criar uma categoria com uma condição baseada em certificado que utilize apenas o parâmetro **Subject** com o valor `*`.
   - Para as Regras de Controlo das aplicações, selecione o parâmetro **Atualizadores fiáveis**. Se esta caixa de verificação estiver selecionada, o Kaspersky Endpoint Security considera as aplicações incluídas na regra como Atualizadores fiáveis. O Kaspersky Endpoint Security permite o arranque de aplicações que foram instaladas ou atualizadas por aplicações especificadas na regra, se nenhuma regra de bloqueio for aplicável a essas aplicações.

     Quando as definições de Kaspersky Endpoint Security são migradas, a lista de ficheiros executáveis criados por atualizadores fiáveis também é migrada.
   - Crie uma pasta e coloque nela os ficheiros executáveis das aplicações para os quais pretende permitir a instalação automática de atualizações. Em seguida, crie uma categoria de aplicação com a condição **Application folder** e especifique o caminho para a pasta. Em seguida, crie uma regra de permissão e selecione esta categoria.

     A utilização da **Application folder** poderá não ser segura, pois qualquer aplicação da pasta especificada estará autorizada a ser inicializada. Recomenda-se aplicar regras que usam as categorias da aplicação com a condição da **Application folder** só àqueles utilizadores para quem a instalação automática de atualizações deve ser permitida.

Testar o modo de lista de permissão

Para assegurar que as Regras de Controlo das Aplicações não bloqueia aplicações necessárias para o trabalho, recomenda-se que o teste seja ativado para as Regras de Controlo das Aplicações e que o seu funcionamento seja analisado depois de as regras serem criadas. Quando o teste está ativado, o Kaspersky Endpoint Security não bloqueará as aplicações cuja inicialização esteja proibida pelas Regras de Controlo das Aplicações, mas enviará notificações sobre o sua inicialização para o Servidor de Administração.

Ao testar o modo de lista de permissão, é aconselhável realizar as seguintes ações:

1. Determine o período de teste (desde vários dias a dois meses).
2. Ative o teste para as Regras de Controlo das Aplicações.
3. Examine os eventos que resultam do teste de funcionamento do Controlo das Aplicações e relatórios sobre aplicações bloqueadas no modo de teste para analisar os resultados do teste.
4. Com base nos resultados da análise, faça alterações às definições do modo de lista de permissão.

   Em particular, com base nos resultados do teste, pode adicionar ficheiros executáveis relacionados a eventos a uma categoria da aplicação.

Suporte para o modo de lista de permissão

Depois de selecionar uma ação de bloqueio para o Controlo das Aplicações, recomenda-se que continue a suportar o modo de lista de permissão realizando as seguintes ações:

- Examine os eventos que resultam da operação de Controlo das Aplicações e relatórios sobre execuções bloqueadas para analisar a eficácia do Controlo das Aplicações.
- Analise pedidos de utilizadores para aceder a aplicações.
- Analise ficheiros executáveis desconhecidos verificando sua reputação na Kaspersky Security Network.
- Antes da instalação de atualizações do sistema operativo ou do software, instale as atualizações num grupo de computadores de teste para verificar como serão processados pelas Regras de Controlo das Aplicações.
- Adicione as aplicações necessárias às categorias usadas em Regras de Controlo das Aplicações.

Monitorização de portas de rede

Durante a operação do Kaspersky Endpoint Security, os componentes Controlo de Internet, Proteção contra ameaças de correio, Proteção contra ameaças da Web, Deteção de comportamento e Prevenção de explorações monitorizam os fluxos de dados transmitidos através de protocolos específicos e que passam por determinadas portas TCP e UDP abertas no computador do utilizador. Por exemplo, o componente Proteção contra ameaças de correio analisa a informação transmitida através de SMTP, enquanto que o componente Proteção contra ameaças da Web analisa a informação transmitida através de HTTP e FTP.

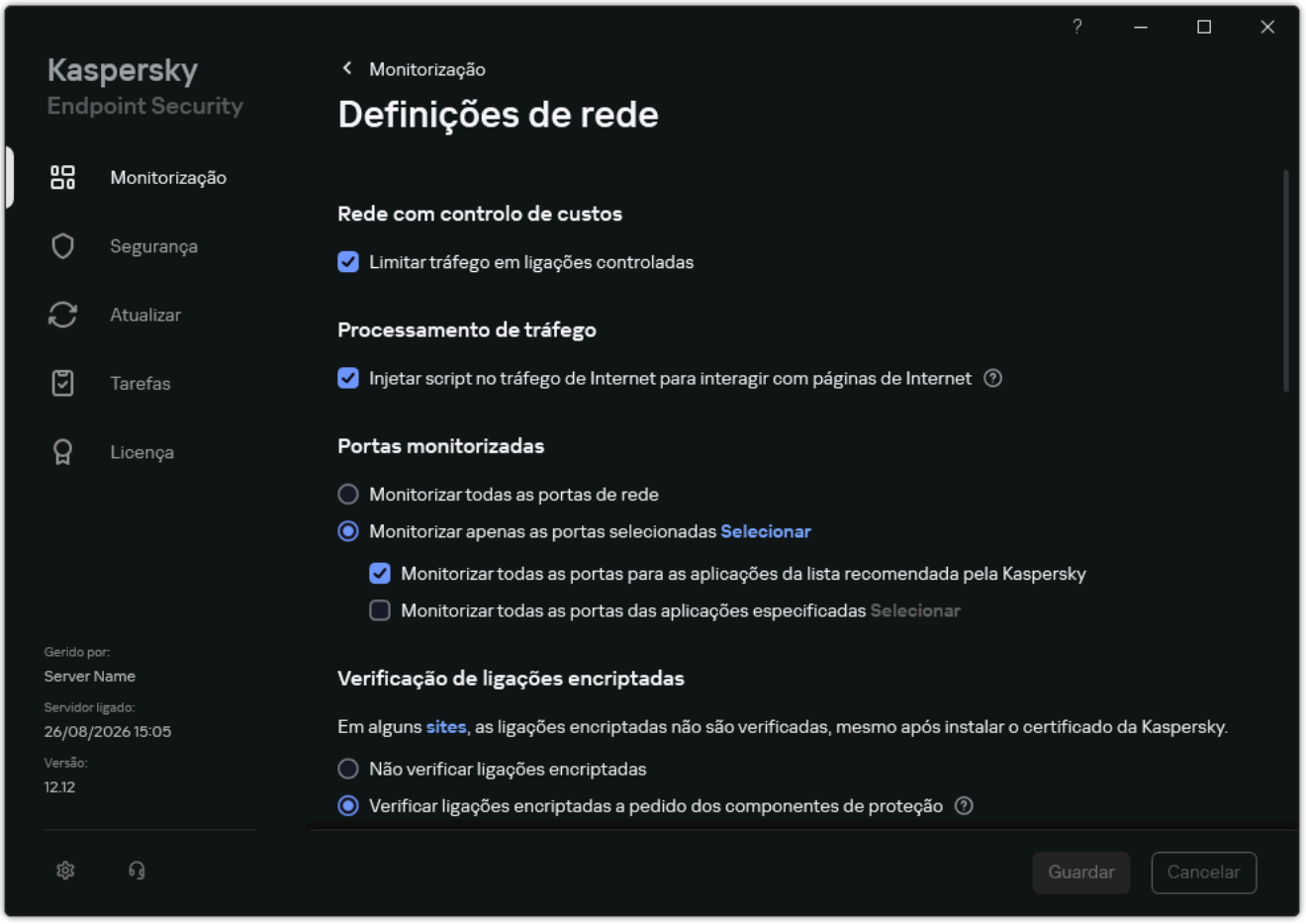
O Kaspersky Endpoint Security divide as portas TCP e UDP do computador do utilizador em vários grupos, conforme a probabilidade de a sua segurança vir a ser comprometida. Algumas portas de rede estão reservadas para serviços vulneráveis. Recomenda-se uma monitorização mais atenta destas portas, visto que elas têm uma maior probabilidade de serem alvo de um ataque à rede. Se utilizar serviços diferentes dos normais que confiem em portas de rede diferentes das normais, estas portas de rede poderão também ser alvo de um ataque por outro computador. Pode especificar uma lista de portas de rede e uma lista de aplicações que solicitam acesso à rede. Estas portas e aplicações são alvo de atenção especial dos componentes Proteção contra ameaças de correio e Proteção contra ameaças da Web durante a monitorização do tráfego de rede.

Para ajudar a garantir a segurança do computador, os componentes Deteção de comportamento e Prevenção de exploração também monitorizam os fluxos de dados que passam pelas portas de rede. Os componentes monitorizam continuamente o tráfego de rede em busca de processos individuais que podem ser ameaçadores.

Ativar a monitorização de todas as portas de rede

Para ativar a monitorização de todas as portas de rede:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Definições de rede**.



Definições de monitorização de portas de rede

3. No bloco **Portas monitorizadas**, selecione **Monitorizar todas as portas de rede**.
4. Guarde as suas alterações.

Criar uma lista de portas de rede monitorizadas

Para criar uma lista de portas de rede monitorizadas:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Definições de rede**.
3. No bloco **Portas monitorizadas**, selecione **Monitorizar apenas as portas selecionadas**.

4. Clique em **Selecionar**.

   Abre-se uma lista das portas de rede utilizadas normalmente para transmissão de e-mail e de tráfego de rede. A lista de portas de rede está incluída no pacote do Kaspersky Endpoint Security.

5. Use o botão de alternar na coluna **Estado** para ativar ou desativar a monitorização das portas de rede.

6. Se uma porta de rede não for apresentada na lista de portas de rede, adicione a mesma do seguinte modo:

   a. Clique em **Adicionar**.

   b. Na janela que se abre, introduza o número da porta de rede e uma breve descrição.

   c. Defina o estado **Ativo** ou **Inativo** para a monitorização das portas de rede.

7. Guarde as suas alterações.

Quando o protocolo de FTP é executado em modo passivo, a ligação pode ser estabelecida através de uma porta de rede aleatória que não é adicionada à lista de portas de rede monitorizadas. Para proteger essas ligações, ative a monitorização de todas as portas de rede ou configure o controlo das portas de rede para aplicações que estabelecem ligações FTP.

Criar uma lista das aplicações para as quais todas as portas de rede são monitorizadas

Pode criar uma lista de aplicações para a qual o Kaspersky Endpoint Security monitoriza todas as portas de rede.

É recomendado incluir as aplicações que recebem ou transmitem dados através do protocolo de FTP na lista de aplicações para as quais o Kaspersky Endpoint Security monitoriza todas as portas de rede.

Para criar uma lista das aplicações para as quais todas as portas de rede são monitorizadas:

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Definições gerais** → **Definições de rede**.

3. No bloco **Portas monitorizadas**, selecione **Monitorizar apenas as portas selecionadas**.

4. Selecione a caixa de verificação **Monitorizar todas as portas para as aplicações da lista recomendada pela Kaspersky**.

   Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security monitoriza todas as portas para as seguintes aplicações:

   - 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. Selecione a caixa de verificação **Monitorizar todas as portas das aplicações especificadas**.
6. Clique em **Selecionar**.
   Abre-se uma lista de aplicações para as quais o Kaspersky Endpoint Security monitoriza as portas de rede.
7. Use o botão de alternar na coluna **Estado** para ativar ou desativar a monitorização das portas de rede.
8. Se uma aplicação não estiver incluída na lista de aplicações, adicione-a da seguinte forma:
   a. Clique em **Adicionar**.
   b. Na janela que se abre, introduza o caminho para o ficheiro executável da aplicação e uma breve descrição.
   c. Defina o estado **Ativo** ou **Inativo** para a monitorização das portas de rede.
9. Guarde as suas alterações.

Exportar e importar listas de portas monitorizadas

O Kaspersky Endpoint Security utiliza as seguintes listas para monitorizar as portas de rede: lista de portas de rede e lista de aplicações cujas portas são monitorizadas pelo Kaspersky Endpoint Security. Pode exportar listas de portas monitorizadas para um ficheiro XML. Em seguida, pode modificar o ficheiro para, por exemplo, adicionar um grande número de portas com a mesma descrição. Também pode usar a função de exportação/importação para fazer uma cópia de segurança das listas de portas monitorizadas ou para migrar as listas para um servidor diferente.

Como exportar e importar listas de portas monitorizadas na Consola de Administração (MMC)

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.

4. Aceda a **General Settings** → **Network Settings**.

5. Para exportar a lista de portas de rede:

   a. No bloco **Monitored ports**, selecione **Monitor selected network ports only**.

   b. Cliqueno link das **selected N ports**.

      Abre-se a janela **Network ports**. A janela **Network ports** apresenta uma lista das portas de rede utilizadas normalmente para transmissão de e-mail e de tráfego de rede. A lista de portas de rede está incluída no pacote do Kaspersky Endpoint Security.

   c. Na lista de portas de rede, selecione as portas que pretende exportar.

   d. Clique em **Export**.

   e. Na janela que surgir, introduza o nome do ficheiro XML para o qual pretende exportar a lista de portas de rede, e selecione a pasta onde pretende guardar este ficheiro e clique no botão Guardar.

   f. Guardar o ficheiro.

      O Kaspersky Endpoint Security exporta toda a lista de portas de rede para o ficheiro XML.

6. Para exportar a lista de aplicações cujas portas são monitorizadas pelo Kaspersky Endpoint Security:

   a. No bloco **Monitored ports**, selecione a caixa de verificação **Monitor all ports for specified applications**.

   b. Cliqueno link das **selected N applications**.

   c. Na lista de aplicações, selecione as aplicações que pretende exportar.

   d. Clique em **Export**.

   e. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de aplicações e selecione a pasta onde pretende guardar este ficheiro.

   f. Guardar o ficheiro.

      O Kaspersky Endpoint Security exporta toda a lista de aplicações para o ficheiro XML.

7. Para importar a lista de portas de rede:

   a. Na lista de portas de rede, clique no botão **Import**.

      Na janela que se abre, selecione o ficheiro XML a partir do qual pretende importar a lista de portas de rede.

   b. Abrir o ficheiro.

      Se o computador já tiver uma lista de portas de rede, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas a esta lista a partir do ficheiro XML.

8. Para importar uma lista de aplicações cujas portas são monitorizadas pelo Kaspersky Endpoint Security:

   a. Na lista de aplicações, clique no botão **Import**.

      Na janela que se abre, selecione o ficheiro XML a partir do qual pretende importar a lista de aplicações.

b. Abrir o ficheiro.

Se o computador já tiver uma lista de aplicações, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas a esta lista a partir do ficheiro XML.

9. Guarde as suas alterações.

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Definições gerais → Definições de Rede**.

4. No bloco **Portas monitorizadas**, selecione **Monitorizar apenas as portas selecionadas**.

5. Clique em **Definições**.

Abre-se a janela **Portas de rede**. A janela **Portas de rede** apresenta uma lista das portas de rede utilizadas normalmente para transmissão de e-mail e de tráfego de rede. A 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 pretende exportar. Para selecionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.

Se não tiver selecionado nenhuma porta, o Kaspersky Endpoint Security exportará todas as portas.

b. Clique em **Exportar**.

c. Na janela que surgir, introduza o nome do ficheiro XML para o qual pretende exportar a lista de portas de rede, e selecione a pasta onde pretende guardar este ficheiro e clique no botão Guardar.

d. Guardar o ficheiro.

O Kaspersky Endpoint Security exporta toda a lista de portas de rede para o ficheiro XML.

7. Para exportar a lista de aplicações cujas portas são monitorizadas pelo Kaspersky Endpoint Security:

a. Selecione a caixa de verificação **Monitorizar todas as portas das aplicações especificadas**.

b. Na lista de aplicações, selecione as aplicações que pretende exportar. Para selecionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.

Se não tiver selecionado nenhuma aplicação, o Kaspersky Endpoint Security exportará todas as aplicações.

c. Clique em **Exportar**.

d. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de aplicações e selecione a pasta onde pretende guardar este ficheiro.

e. Guardar o ficheiro.

O Kaspersky Endpoint Security exporta toda a lista de aplicações para o ficheiro XML.

8. Para importar a lista de portas de rede:

a. Na lista de portas de rede, clique no botão **Importar**.

Na janela que se abre, selecione o ficheiro XML a partir do qual pretende importar a lista de portas de rede.

b. Abrir o ficheiro.

Se o computador já tiver uma lista de portas de rede, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas a esta lista a partir do ficheiro XML.

9. Para importar uma lista de aplicações cujas portas são monitorizadas pelo Kaspersky Endpoint Security:

a. Na lista de aplicações, clique no botão **Importar**.

Na janela que se abre, selecione o ficheiro XML a partir do qual pretende importar a lista de aplicações.

b. Abrir o ficheiro.

Se o computador já tiver uma lista de aplicações, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas a esta lista a partir do ficheiro XML.

10. Guarde as suas alterações.

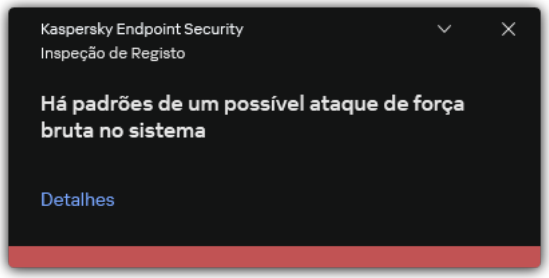
Inspeção do Registo

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para servidores. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para estações de trabalho.

A Inspeção de Registo monitoriza a integridade do ambiente protegido com base na análise do registo de eventos do Windows. Quando a aplicação deteta sinais de comportamento atípico no sistema, ela informa o administrador, visto que este comportamento pode indicar uma tentativa de ciberataque.

O Kaspersky Endpoint Security analisa os registos de eventos do Windows e deteta violações de acordo com as regras. O componente inclui regras predefinidas. As regras predefinidas são alimentadas por análise heurística. Também pode adicionar as suas próprias regras (regras personalizadas). Quando uma regra é acionada, a aplicação cria um evento com o estado *Critical* (veja a figura abaixo).

Se quiser utilizar a Inspeção de Registo, certifique-se de que as definições de segurança da política de auditoria estão configuradas e que o sistema está a registar os eventos relevantes (para obter detalhes, consulte o site de suporte técnico da Microsoft.).



Notificação da Inspeção de Registo

Configurar regras predefinidas

As regras predefinidas incluem modelos de atividade anormal no computador protegido. Atividade anormal pode significar uma tentativa de ataque. As regras predefinidas são alimentadas por análise heurística. Estão disponíveis sete regras predefinidas para a Inspeção de Registo. Pode ativar ou desativar qualquer uma das regras. As regras predefinidas não podem ser eliminadas.

Pode configurar os critérios de acionamento para as regras que monitorizam eventos para as seguintes operações:

- Deteção de força bruta de password
- Deteção de início de sessão de rede

Como configurar regras predefinidas na Administration Console (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança** → **Inspeção de Registo**.
4. Certifique-se de que a caixa de verificação **Inspeção de Registo** está assinalada.
5. No bloco **Regras predefinidas**, clique no botão **Definições**.
6. Assinale ou desmarque as caixas de verificação para configurar as regras predefinidas:
   - **Há padrões de um possível ataque de força bruta no sistema**.
   - **Foi detetada uma atividade atípica durante um início de sessão da rede**.
   - **Há padrões de um possível abuso do Registo de Eventos do Windows**.
   - **Ações atípicas detetadas em nome de um novo serviço instalado**.
   - **Início de sessão atípico que utiliza credenciais explícitas detetadas**.
   - **Existem padrões de um possível ataque ao PAC forjado do Kerberos (MS14-068) no sistema**.
   - **Alterações suspeitas detetadas no grupo de Administradores integrado privilegiado**.
7. Se necessário, configure a regra **Há padrões de um possível ataque de força bruta no sistema**:
   a. Clique no botão **Definições** abaixo da regra.
   b. Na janela que se abre, especifique o número de tentativas e um período de tempo dentro do qual as tentativas de introduzir uma password têm de ser realizadas para que a regra seja acionada.
   c. Clique em **OK**.

8. Se selecionou a regra **Foi detetada uma atividade atípica durante um início de sessão da rede**, tem de configurar as respetivas definições:

    a. Clique no botão **Definições** abaixo da regra.

    b. No bloco **Deteção de início de sessão de rede**, especifique o início e o fim do intervalo de tempo.

    O Kaspersky Endpoint Security considera as tentativas de início de sessão realizadas durante o intervalo definido como atividade anormal.

    Por predefinição, o intervalo não está definido e a aplicação não monitoriza as tentativas de início de sessão. Para que a aplicação monitorize continuamente as tentativas de início de sessão, defina o intervalo para 00:00 – 23:59. O início e o fim do intervalo não devem coincidir. Se forem o mesmo, a aplicação não monitoriza as tentativas de início de sessão.

    c. Crie a lista de utilizadores fiáveis e endereços IP fiáveis (IPv4 e IPv6).

    Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio. O Kaspersky Endpoint Security não monitoriza as tentativas de início de sessão destes utilizadores e computadores.

    d. Clique em **OK**.

9. Guarde as suas alterações.

Como configurar as regras predefinidas na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

    É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Security Controls** → **Log Inspection**.
5. Certifique-se de que o botão de alternar **Log Inspection ENABLED** está ativado.
6. No bloco **Predefined rules**, ative ou desative as regras predefinidas utilizando os botões de alternar:

    - **There are patterns of a possible brute-force attack in the system**.
    - **There is an atypical activity detected during a network logon session**.
    - **There are patterns of a possible Windows Event Log abuse**.
    - **Atypical actions detected on behalf of a new service installed**.
    - **Atypical logon that uses explicit credentials detected**.
    - **There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system**.

    a. **Suspicious changes detected in the privileged built-in Administrators group**.

7. Se necessário, configure a regra **There are patterns of a possible brute-force attack in the system**:

    a. Clique em **Settings** sob a regra.

    b. Na janela que se abre, especifique o número de tentativas e um período de tempo dentro do qual as tentativas de introduzir uma password têm de ser realizadas para que a regra seja acionada.

    c. Clique em **OK**.

8. Se selecionou a regra **There is an atypical activity detected during a network logon session**, tem de configurar as respetivas definições:

    a. Clique em **Settings** sob a regra.

    b. No bloco **Network logon detection**, especifique o início e o fim do intervalo de tempo.

    O Kaspersky Endpoint Security considera as tentativas de início de sessão realizadas durante o intervalo definido como atividade anormal.

    Por predefinição, o intervalo não está definido e a aplicação não monitoriza as tentativas de início de sessão. Para que a aplicação monitorize continuamente as tentativas de início de sessão, defina o intervalo para 00:00 – 23:59. O início e o fim do intervalo não devem coincidir. Se forem o mesmo, a aplicação não monitoriza as tentativas de início de sessão.

    c. No bloco **Exclusions**, adicione utilizadores fiáveis e endereços IP fiáveis (IPv4 e IPv6).

    Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio. O Kaspersky Endpoint Security não monitoriza as tentativas de início de sessão destes utilizadores e computadores.

    d. Clique em **OK**.

9. Guarde as suas alterações.

Como configurar as regras predefinidas na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Controlos de segurança → Inspeção de Registo**.

3. Certifique-se de que o botão de alternar **Inspeção de Registo** está ativado.

4. No bloco **Regras predefinidas**, clique no botão **Configurar**.

5. Assinale ou desmarque as caixas de verificação para configurar as regras predefinidas:

    - **Há padrões de um possível ataque de força bruta no sistema**.
    - **Foi detetada uma atividade atípica durante um início de sessão da rede**.
    - **Há padrões de um possível abuso do Registo de Eventos do Windows**.
    - **Ações atípicas detetadas em nome de um novo serviço instalado**.

- **Início de sessão atípico que utiliza credenciais explícitas detetadas**.
- **Existem padrões de um possível ataque ao PAC forjado do Kerberos (MS14-068) no sistema**.

a. **Alterações suspeitas detetadas no grupo de Administradores integrado privilegiado**.

6. Se necessário, configure a regra **Há padrões de um possível ataque de força bruta no sistema**:

   a. Clique em **Definições** sob a regra.

   b. Na janela que se abre, especifique o número de tentativas e um período de tempo dentro do qual as tentativas de introduzir uma password têm de ser realizadas para que a regra seja acionada.

7. Se selecionou a regra **Foi detetada uma atividade atípica durante um início de sessão da rede**, tem de configurar as respetivas definições:

   a. Clique em **Definições** sob a regra.

   b. No bloco **Deteção de início de sessão de rede**, especifique o início e o fim do intervalo de tempo.

   O Kaspersky Endpoint Security considera as tentativas de início de sessão realizadas durante o intervalo definido como atividade anormal.

   Por predefinição, o intervalo não está definido e a aplicação não monitoriza as tentativas de início de sessão. Para que a aplicação monitorize continuamente as tentativas de início de sessão, defina o intervalo para 00:00 – 23:59. O início e o fim do intervalo não devem coincidir. Se forem o mesmo, a aplicação não monitoriza as tentativas de início de sessão.

   c. No bloco **Exclusões**, adicione utilizadores fiáveis e endereços IP fiáveis (IPv4 e IPv6).

   Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio. O Kaspersky Endpoint Security não monitoriza as tentativas de início de sessão destes utilizadores e computadores.

8. Guarde as suas alterações.

Como resultado, quando a regra é acionada, o Kaspersky Endpoint Security cria um *Evento crítico*.

Adicionar regras personalizadas

Pode definir os seus próprios critérios de acionamento da regra da Inspeção de Registo. Para o fazer, tem de inserir um ID do evento e selecionar uma fonte do evento. Pode procurar o ID do evento no site de suporte técnico da Microsoft. Pode selecionar uma fonte do evento entre os registos padrão: *Application*, *Security* ou *System*. Também pode especificar o registo de uma aplicação de terceiros. Pode descobrir o nome do registo da aplicação de terceiros utilizando a ferramenta Visualizador de eventos. Os registos de aplicações de terceiros são mantidos na pasta Registos de Aplicações e de Serviços (por exemplo, o registo do *Windows PowerShell*).

A aplicação não verifica se o registo especificado está realmente presente no registo de eventos do Windows. Se houver um erro no nome do registo, a aplicação não monitoriza os eventos desse registo.

A lista de regras personalizadas já inclui três regras criadas por especialistas da Kaspersky.

Como adicionar uma regra personalizada na Administration Console (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança → Inspeção de Registo**.
4. Certifique-se de que a caixa de verificação **Inspeção de Registo** está assinalada.
5. No bloco **Regras personalizadas**, clique no botão **Definições**.
6. Na janela que se abre, selecione as caixas de verificação correspondentes às regras personalizadas que deseja ativar.
7. Se for necessário, clique em **Adicionar** para criar as suas próprias regras personalizadas.
8. Irá abrir-se uma janela; nessa janela, configure a regra personalizada:
   - **Nome da regra**.
   - **Nome do registo**. Registos de Eventos do Windows. Estão disponíveis os seguintes registos: *Application*, *Security*, *System*.
   - **Origem**. Registos de aplicações de terceiros. Pode descobrir o nome do registo da aplicação de terceiros utilizando a ferramenta Visualizador de eventos. Os registos de aplicações de terceiros são mantidos na pasta Registos de Aplicações e de Serviços (por exemplo, o registo do *Windows PowerShell*).
   - **Identificadores de eventos**. ID de eventos no Registo de Eventos do Windows. Pode procurar o ID do evento na Documentação técnica da Microsoft.
9. Guarde as suas alterações.

Como adicionar uma regra personalizada na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Security Controls → Log Inspection**.
5. Certifique-se de que o botão de alternar **Log Inspection ENABLED** está ativado.
6. No bloco **Custom rules**, selecione as regras personalizadas que pretende ativar.
7. Se for necessário, clique em **Add** para criar as suas próprias regras personalizadas.
8. Irá abrir-se uma janela; nessa janela, configure a regra personalizada:
   - **Rule name**.
   - **Custom log name**. Registos de Eventos do Windows. Estão disponíveis os seguintes registos: *Application*, *Security*, *System*.

- **Origin**. Registos de aplicações de terceiros. Pode descobrir o nome do registo da aplicação de terceiros utilizando a ferramenta Visualizador de eventos. Os registos de aplicações de terceiros são mantidos na pasta Registos de Aplicações e de Serviços (por exemplo, o registo do *Windows PowerShell*).

- **Event Identifiers**. ID de eventos no Registo de Eventos do Windows. Pode procurar o ID do evento na Documentação técnica da Microsoft.

9. Guarde as suas alterações.

Como adicionar uma regra personalizada na interface da aplicação

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Controlos de segurança** → **Inspeção de Registo**.
3. Certifique-se de que o botão de alternar **Inspeção de Registo** está ativado.
4. No bloco **Regras personalizadas**, clique no botão **Configurar**.
5. Na janela que se abre, selecione as caixas de verificação correspondentes às regras personalizadas que deseja ativar.
6. Se for necessário, clique em **Adicionar** para criar as suas próprias regras personalizadas.
7. Irá abrir-se uma janela; nessa janela, configure a regra personalizada:

   - **Nome da regra**.

   - **Nome do registo**. Registos de Eventos do Windows. Estão disponíveis os seguintes registos: *Application*, *Security*, *System*.

   - **Origem**. Registos de aplicações de terceiros. Pode descobrir o nome do registo da aplicação de terceiros utilizando a ferramenta Visualizador de eventos. Os registos de aplicações de terceiros são mantidos na pasta Registos de Aplicações e de Serviços (por exemplo, o registo do *Windows PowerShell*).

   - **Identificador de eventos**. ID de eventos no Registo de Eventos do Windows. Pode procurar o ID do evento na Documentação técnica da Microsoft.

8. Guarde as suas alterações.

Como resultado, quando a regra é acionada, o Kaspersky Endpoint Security cria um evento *Critical*.

Monitorização da integridade do sistema

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para servidores. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para estações de trabalho.

A partir da versão 12.6, o Kaspersky Endpoint Security for Windows inclui o componente Monitorização da integridade do sistema, em vez do componente Monitor de integridade do ficheiro. O componente Monitorização da integridade do sistema inclui todas as funcionalidades do Monitor de integridade do ficheiro e, adicionalmente, permite monitorizar alterações de registo e conexão de dispositivos externos.

O componente Monitorização da integridade do sistema monitoriza as alterações no sistema operativo que podem indicar violações da segurança informática. Quando essas alterações são detetadas, o Kaspersky Endpoint Security gera eventos correspondentes e alerta o administrador. A Monitorização da integridade do sistema pode operar em tempo real e também realizar verificações de integridade do sistema mediante pedido.

Monitorização da integridade do sistema em tempo real

No modo de tempo real, a Monitorização da integridade do sistema rastreia alterações em objetos incluídos no âmbito do componente (o *âmbito de monitorização*). A Monitorização da integridade do sistema também permite bloquear o acesso não autorizado a esses objetos em tempo real.

Verificação de integridade do sistema mediante pedido

A Verificação de integridade do sistema mediante pedido é uma tarefa que pode realizar manualmente ou de forma programada. Para realizar a tarefa *Verificação de integridade do sistema*, tem de configurar o âmbito do componente (o *âmbito de monitorização*) e criar uma linha de base. A *linha de base* é um estado registado de objetos no sistema, que a aplicação usa como referência ao comparar com o estado atual.

Migrar as definições do Monitor de integridade do ficheiro

Ao atualizar o Kaspersky Endpoint Security para a versão 12.6, as definições do Monitor de integridade do ficheiro são migradas automaticamente. Como parte da migração, a aplicação move as regras de monitorização para a Monitorização da integridade do sistema. As regras do Monitor de integridade do ficheiro também são migradas para a Monitorização da integridade do sistema ao migrar do KSWS para o KES.

Para assegurar o correto funcionamento da Monitorização da integridade do sistema, a aplicação Kaspersky Endpoint Security e o plug-in de gestão devem ser atualizados para a versão 12.6. Se tiver uma versão anterior do plug-in de gestão instalada, não pode configurar a Monitorização da integridade do sistema porque o plug-in de gestão não tem a secção **Monitorização da integridade do sistema**.

Sobre as regras da Monitorização da integridade do sistema

Para que a Monitorização da integridade do sistema funcione, tem de adicionar, pelo menos, uma regra. A *regra de Monitorização da integridade do sistema* é um conjunto de critérios que definem o acesso dos utilizadores aos ficheiros e ao registo. A Monitorização da integridade do sistema deteta alterações nos ficheiros e no registo dentro do *âmbito especificado da monitorização*. O âmbito da monitorização é um dos critérios de uma regra da Monitorização da integridade do sistema.

A Monitorização da integridade do sistema permite monitorizar os seguintes objetos:

- Ficheiros
- Registo
- Dispositivos externos

Considerações especiais envolvidas na monitorização de ficheiros

A Monitorização da integridade do sistema monitoriza alterações em ficheiros e pastas, bem como ficheiros que são adicionados ao âmbito de monitorização ou removidos dele. Estas alterações podem indicar uma violação de segurança do computador. Recomendamos que adicione objetos raramente modificados ou objetos aos quais apenas o administrador tem acesso. O que irá reduzir o número de eventos da Monitorização da integridade do sistema.

A Monitorização da integridade do sistema não monitoriza as alterações aos ficheiros nas pastas partilhadas do servidor. A Monitorização da integridade do sistema só pode ser utilizada localmente.

O Kaspersky Endpoint Security monitoriza as alterações de ficheiros e pastas apenas nos discos que estavam ligados quando a Monitorização da integridade do sistema em tempo real começou a funcionar. Se um disco não estiver ligado quando a Monitorização da integridade do sistema em tempo real começou a funcionar, a aplicação não irá monitorizar as alterações de ficheiros e pastas nesse disco, mesmo que os ficheiros e pastas sejam adicionados ao âmbito de monitorização.

Considerações especiais envolvidas na monitorização de registos

A Monitorização da integridade do sistema monitoriza o registo. Estas alterações podem indicar uma violação de segurança do computador.

A Monitorização da integridade do sistema monitoriza as seguintes chaves raiz do registo:

- `HKCR`
- `HKLM`
- `HKU`
- `HKCC`
- `HKEY_CLASSES_ROOT`
- `HKEY_LOCAL_MACHINE`
- `HKEY_USERS`
- `HKEY_CURRENT_CONFIG` (disponível apenas na Monitorização da integridade do sistema em tempo real)

- `HKEY_CURRENT_USER` (disponível apenas na Monitorização da integridade do sistema em tempo real)

  A tarefa *Verificação de integridade do sistema* não suporta a chave `HKEY_CURRENT_USER`. Pode especificar uma chave em `HKEY_USERS` como `HKEY_USERS\<user profile ID>\<key>`.

Considerações especiais envolvidas na monitorização de dispositivos externos

A Monitorização da integridade do sistema monitoriza a ligação e desativação de dispositivos externos. Isto é necessário para proteger o computador contra ameaças à segurança que podem resultar da troca de ficheiros com esses dispositivos. A Monitorização da integridade do sistema não monitoriza o acesso a dispositivos externos e não bloqueia a troca de ficheiros. Pode configurar o acesso aos dispositivos através de um componente de aplicação diferente, Controlo de Dispositivos.

Ao executar a tarefa *Monitorização da integridade do sistema de linha de base*, a aplicação ignora a nova ligação de dispositivos externos se os dispositivos tiverem a mesma letra de unidade no sistema operativo. Para serem registados, os dispositivos novamente ligados têm de ter letras de unidade diferentes.

A Monitorização da integridade do sistema monitoriza a ligação dos seguintes tipos de dispositivos externos:

- Unidade amovível (incluindo unidades flash USB)
- Disco rígido
- Adaptador de rede externo
- Unidade de CD/DVD/Blu-ray
- Scanner/câmara

Monitorização da integridade do sistema em tempo real

A Monitorização da integridade do sistema permite rastrear alterações no sistema operativo em tempo real. Pode rastrear alterações que podem indicar violações de segurança no computador. O componente permite bloquear estas alterações ou simplesmente registar eventos de alteração.

Para que a Monitorização da integridade do sistema funcione, tem de adicionar, pelo menos, uma regra. A *regra de Monitorização da integridade do sistema* é um conjunto de critérios que definem o acesso dos utilizadores aos ficheiros e ao registo. A Monitorização da integridade do sistema deteta alterações nos ficheiros e no registo dentro do *âmbito especificado da monitorização*. O âmbito da monitorização é um dos critérios de uma regra da Monitorização da integridade do sistema.

Modos de Monitorização da integridade do sistema em tempo real

Para garantir que as regras da Monitorização da integridade do sistema não bloqueiem nenhuma ação com recursos críticos para o funcionamento do sistema operativo ou de outros serviços, recomendamos que ative o modo de Teste e analise como o componente afeta o sistema. Com o modo de Teste ativado, o Kaspersky Endpoint Security não bloqueia atividades do utilizador proibidas pelas regras, gerando eventos *Aviso* ⚠.

O componente Monitorização da integridade do sistema em tempo real possui dois modos:

- Bloquear

  Neste modo, a Monitorização da integridade do sistema rastreia alterações no sistema e executa uma ação de acordo com as regras: **Permitir** ou **Bloquear**. A Monitorização da integridade do sistema também gera um evento correspondente e altera o estado do dispositivo na consola do Kaspersky Security Center.

- Informar

  Neste modo, a Monitorização da integridade do sistema permite ações com ficheiros e chaves de registo do âmbito de monitorização. Se a ação com ficheiros ou o registo for proibido, a aplicação gera um evento: *A operação proibida foi permitida no modo de teste*. Para analisar como as regras afetam o sistema, pode consultar os relatórios.

Ativar a Monitorização da integridade do sistema em tempo real

Como ativar a Monitorização da integridade do sistema em tempo real na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança** → **Monitorização da integridade do sistema**.
4. Selecione a caixa de verificação **Monitorização da integridade do sistema**.
5. Em **Modo operativo das regras de bloqueio**, selecione um modo para a Monitorização da integridade do sistema em tempo real:
   - **Bloquear**. Neste modo, a Monitorização da integridade do sistema bloqueia ações com ficheiros e chaves de registo do âmbito de monitorização e gera um evento correspondente.
   - **Informar**. Neste modo, a Monitorização da integridade do sistema permite ações com ficheiros e chaves de registo do âmbito de monitorização e gera um evento correspondente.
6. No bloco **Monitorização da integridade do sistema em tempo real**, selecione a caixa de verificação **Monitorização da integridade do sistema em tempo real**.
7. Configure a monitorização de dispositivos externos:
   a. Selecione a caixa de verificação **Monitorizar dispositivos**.
   b. Na lista suspensa **Nível de gravidade do evento**, selecione o nível de importância dos eventos de monitorização de dispositivos externos: *Informativo* ⓘ, *Aviso* ⚠, *Crítico* ⓘ.

A Monitorização da integridade do sistema regista a ligação atual de dispositivos externos. A aplicação começa a monitorizar a ligação e desativação de dispositivos externos após o componente ser ativado nas definições da aplicação. Posteriormente, quando um dispositivo externo é ligado ou desativado, a aplicação gera um evento correspondente.

8. Configure a monitorização de ficheiros e registos:

   a. Selecione a caixa de verificação **Monitorizar ficheiros e o registo**.

   b. Clique em **Definições**.

   Esta ação abre a lista de regras de Monitorização da integridade do sistema.

   c. Clique em **Adicionar**.

   Também pode importar regras de outra fonte.

   d. Configure a regra de Monitorização da integridade do sistema (consulte a tabela abaixo).

9. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar a Monitorização da integridade do sistema em tempo real na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Security Controls** → **System Integrity Monitoring**.

5. Ative o botão de alternar **System Integrity Monitoring ENABLED**.

6. Selecione o separador **Windows**.

7. Em **Real-Time System Integrity Monitoring**, selecione um modo para a Monitorização da integridade do sistema em tempo real:

   - **Apply rules**. Neste modo, a Monitorização da integridade do sistema bloqueia ações com ficheiros e chaves de registo do âmbito de monitorização e gera um evento correspondente.

   - **Test rules (Inform)**. Neste modo, a Monitorização da integridade do sistema permite ações com ficheiros e chaves de registo do âmbito de monitorização e gera um evento correspondente.

8. Configure a monitorização de ficheiros e registos:

   a. Selecione a caixa de verificação **Monitor files and the registry**.

   b. Clique em **Rules**.

   Esta ação abre a lista de regras de Monitorização da integridade do sistema.

   c. Clique em **Add**.

   Também pode importar regras de outra fonte.

   d. Configure a regra de Monitorização da integridade do sistema (consulte a tabela abaixo).

9. Configure a monitorização de dispositivos externos:

    a. Selecione a caixa de verificação **Monitor devices**.

    b. Na lista suspensa **Event severity level**, selecione o nível de importância dos eventos de monitorização de dispositivos externos: *Informational*, *Warning*, *Critical*.

    A Monitorização da integridade do sistema regista a ligação atual de dispositivos externos. A aplicação começa a monitorizar a ligação e desativação de dispositivos externos após o componente ser ativado nas definições da aplicação. Posteriormente, quando um dispositivo externo é ligado ou desativado, a aplicação gera um evento correspondente.

10. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar a Monitorização da integridade do sistema em tempo real na interface da aplicação

1. Na janela principal da aplicação, clique no botão .

2. Na janela Application settings, selecione **Controlos de segurança → Monitorização da integridade do sistema**.

3. Ative o botão de alternar **Monitorização da integridade do sistema**.

4. Em **Modo operativo das regras de bloqueio**, selecione um modo para a Monitorização da integridade do sistema em tempo real:

    - **Bloquear**. Neste modo, a Monitorização da integridade do sistema bloqueia ações com ficheiros e chaves de registo do âmbito de monitorização e gera um evento correspondente.

    - **Informar**. Neste modo, a Monitorização da integridade do sistema permite ações com ficheiros e chaves de registo do âmbito de monitorização e gera um evento correspondente.

5. No bloco **Monitorização da integridade do sistema em tempo real**, selecione a caixa de verificação **Monitorização da integridade do sistema em tempo real**.

6. Configure a monitorização de dispositivos externos:

    a. Selecione a caixa de verificação **Monitorizar dispositivos**.

    b. Na lista suspensa **Nível de gravidade do evento**, selecione o nível de importância dos eventos de monitorização de dispositivos externos: *Informativo*, *Aviso*, *Crítico*.

    A Monitorização da integridade do sistema regista a ligação atual de dispositivos externos. A aplicação começa a monitorizar a ligação e desativação de dispositivos externos após o componente ser ativado nas definições da aplicação. Posteriormente, quando um dispositivo externo é ligado ou desativado, a aplicação gera um evento correspondente.

7. Configure a monitorização de ficheiros e registos:

    a. Selecione a caixa de verificação **Monitorizar ficheiros e o registo**.

    b. Clique em **Configurar**.

    Esta ação abre a lista de regras de Monitorização da integridade do sistema.

    c. Clique em **Adicionar**.

    Também pode importar regras de outra fonte.

8. Configure a regra de Monitorização da integridade do sistema (consulte a tabela abaixo).

9. Guarde as suas alterações.

Definições da regra de Monitorização da integridade do sistema em tempo real

Parâmetro	Descrição
Nome da regra	Nome da regra de Monitorização da integridade do sistema em tempo real
Operações com ficheiros e registo	• **Permitir**. A Monitorização da integridade do sistema permite ações com ficheiros e chaves de registo do âmbito de monitorização. • **Bloquear**. O comportamento da Monitorização da integridade do sistema depende do modo selecionado. Se selecionou o *Modo de proteção do sistema*, a Monitorização da integridade do sistema bloqueia ações com ficheiros e chaves de registo do âmbito de monitorização, gera um evento correspondente e altera o estado do dispositivo na consola do Kaspersky Security Center. Se selecionou o *Modo de teste*, a Monitorização da integridade do sistema permite ações com ficheiros e chaves de registo do âmbito de monitorização.
Nível de gravidade do evento	O Kaspersky Endpoint Security regista eventos de modificação de ficheiro sempre que um ficheiro ou chave de registo no âmbito de monitorização é modificado. Os seguintes níveis de gravidade do evento estão disponíveis: *Informativo*, *Aviso*, *Crítico*.

Âmbito da monitorização	• **Ficheiro**. Lista de ficheiros e pastas monitorizadas pelo componente. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.
	Usar máscaras:
	  • O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.
	  • Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.
	  • O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.
	• **Registo**. Lista de chaves de registo e valores monitorizados pelo componente. O Kaspersky Endpoint Security suporta os caracteres `*` e `?` ao introduzir uma máscara.

Exclusões	• **Ficheiro**. Lista de exclusões do âmbito de monitorização. O Kaspersky Endpoint Security suporta variáveis de ambiente e os 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 do âmbito de monitorização.
	Usar máscaras:
	  • O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.
	  • Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.
	  • O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.
	• **Registo**. Lista de exclusões do âmbito de monitorização. O Kaspersky Endpoint Security suporta os caracteres `*` e `?` ao introduzir uma máscara. As entradas de exclusão têm uma prioridade mais alta do que as entradas do âmbito de monitorização.

Utilizadores e/ou grupos de utilizadores fiáveis	Um *utilizador fiável* é um utilizador que tem permissão para realizar ações com ficheiros e chaves de registo no âmbito de monitorização. Se o Kaspersky Endpoint Security detetar uma ação realizada por um utilizador fiável, a Monitorização da integridade do sistema gera um evento *Informativo*. Pode selecionar utilizadores no Active Directory, na lista de contas do Kaspersky Security Center ou ao introduzir manualmente um nome de utilizador local. A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio.

Parâmetro	Descrição
Marcadores de operações de ficheiros/Operações monitorizadas	Marcadores que caracterizam a ação com ficheiros ou chaves de registo que a aplicação irá monitorizar.
Hashing	Calcular um hash de ficheiro na modificação. O Kaspersky Endpoint Security adiciona informações sobre o hash do ficheiro quando um evento é gerado.

Verificação de integridade do sistema mediante pedido

A Verificação de integridade do sistema mediante pedido é uma tarefa que pode realizar manualmente ou de forma programada. Ao executar a tarefa *Verificação de integridade do sistema*, a aplicação compara o estado atual dos objetos incluídos no âmbito de monitorização com o seu estado *linha de base*. Em contraste com a Monitorização da 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 operativo.

Para que a Monitorização da integridade do sistema funcione, tem de adicionar, pelo menos, uma regra. A *regra de Monitorização da integridade do sistema* é um conjunto de critérios que definem o acesso dos utilizadores aos ficheiros e ao registo. A Monitorização da integridade do sistema deteta alterações nos ficheiros e no registo dentro do *âmbito especificado da monitorização*. O âmbito da monitorização é um dos critérios de uma regra da Monitorização da integridade do sistema. Pode configurar as regras a serem partilhadas pela Monitorização da integridade do sistema em tempo real e pela 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 âmbito da monitorização da tarefa *Verificação de integridade do sistema* para a tarefa *Atualização da linha de base*.

Criar e atualizar 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 registado de objetos no sistema, que a aplicação usa como referência ao comparar com o estado atual. Se o estado atual do sistema for diferente do estado do sistema registado na linha de base, o Kaspersky Endpoint Security gera o evento correspondente. Pode criar ou atualizar uma linha de base com a tarefa *Atualização da linha de base*.

Pode atualizar a linha de base nos seguintes modos:

- Atualização completa.

  A aplicação atualiza todos os objetos no âmbito de monitorização.

- Atualização incremental.

  A aplicação deteta e atualiza apenas objetos novos ou modificados.

Como criar ou atualizar uma linha de vase na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Atualização da linha de base**.

Passo 2. Selecionar o modo de atualização da linha de base

Selecione um modo de atualização da linha de base:

- **Atualização completa**. A aplicação atualiza todos os objetos no âmbito de monitorização.
- **Atualização incremental**. A aplicação deteta e atualiza apenas objetos novos ou modificados.

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

Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 4. Definir o nome da tarefa

Introduza o nome da tarefa, por exemplo *Linha de Base 2024*.

Passo 5. Completar a criação da tarefa

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa.

Como criar ou atualizar uma linha de base na Consola Web

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **Baseline update**.

   c. No campo **Task name**, introduza uma breve descrição, por exemplo, *Linha de Base 2024*.

   d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Avance para o passo seguinte.

5. Selecione uma conta para executar a tarefa. Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de utilizador local.

6. Conclua o assistente.

   Será apresentada uma nova tarefa na lista de tarefas.

7. Clique em nova tarefa.

   É apresentada a janela de propriedades da tarefa.

8. Selecione o separador **Application settings**.

9. Selecione um modo de atualização da linha de base:

   - **Full update**. A aplicação atualiza todos os objetos no âmbito de monitorização.
   - **Incremental update**. A aplicação deteta e atualiza apenas objetos novos ou modificados.

10. Guarde as suas alterações.

11. Selecione a caixa de verificação junto à tarefa.

12. Clique em **Start**.

Configurar o âmbito de monitorização para a tarefa Verificação de integridade do sistema

Por padrão, o âmbito de monitorização da tarefa *Verificação de integridade do sistema* é igual ao âmbito de monitorização da Monitorização da integridade do sistema em tempo real. Pode configurar um âmbito de monitorização diferente para a tarefa.

A Monitorização da Integridade do Sistema não suporta a importação das chaves `HKEY_CURRENT_USER` e `HKEY_CURRENT_CONFIG` para a tarefa *Verificação de integridade do sistema*. Se o âmbito da monitorização da tarefa tiver estas chaves, a aplicação gera o evento *O âmbito da monitorização inclui objetos incorretos*.

Como configurar um âmbito de monitorização diferente para a tarefa Verificação de integridade do sistema na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança → Monitorização da integridade do sistema**.
4. Selecione a caixa de verificação **Monitorização da integridade do sistema**.
5. Em **Verificação de integridade do sistema**, selecione o modo de configuração da tarefa: **Definições personalizadas**.
6. Configure a monitorização de dispositivos externos:
   a. Selecione a caixa de verificação **Monitorizar dispositivos**.
   b. Na lista suspensa **Nível de gravidade do evento**, selecione o nível de importância dos eventos de monitorização de dispositivos externos: *Informativo*, *Aviso*, *Crítico*.

   A Monitorização da integridade do sistema regista informações sobre dispositivos externos ligados no momento em que a linha de base é criada. Posteriormente, quando um dispositivo externo é ligado, a aplicação gera um evento correspondente. Ao executar a tarefa *Verificação de integridade do sistema*, a aplicação não monitoriza a desativação de dispositivos externos.
7. Configure a monitorização de ficheiros e registos:
   a. Selecione a caixa de verificação **Monitorizar ficheiros e o registo**.
   b. Clique em **Definições**.
      Esta ação abre a lista de regras de Monitorização da integridade do sistema.
   c. Clique em **Adicionar**.
      Também pode importar regras de outra fonte.
   d. Configure a regra de Monitorização da integridade do sistema (consulte a tabela abaixo).
8. Guarde as suas alterações.

Como configurar um âmbito de monitorização diferente para a tarefa System Integrity Check na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Security Controls → System Integrity Monitoring**.
5. Selecione o separador **Windows**.
6. Ative o botão de alternar **System Integrity Monitoring ENABLED**.

7. Em **System Integrity Check**, selecione o modo de configuração da tarefa: **Custom settings**.

8. Configure a monitorização de dispositivos externos:

   a. Selecione a caixa de verificação **Monitor devices**.

   b. Na lista suspensa **Event severity level**, selecione o nível de importância dos eventos de monitorização de dispositivos externos: *Informational* ⓘ, *Warning* ⚠, *Critical* ⓘ.

   A Monitorização da integridade do sistema regista informações sobre dispositivos externos ligados no momento em que a linha de base é criada. Posteriormente, quando um dispositivo externo é ligado, a aplicação gera um evento correspondente. Ao executar a tarefa *Verificação de integridade do sistema*, a aplicação não monitoriza a desativação de dispositivos externos.

9. Configure a monitorização de ficheiros e registos:

   a. Selecione a caixa de verificação **Monitor files and the registry**.

   b. Clique em **Rules**.

      Esta ação abre a lista de regras de Monitorização da integridade do sistema.

   c. Clique em **Add**.

      Também pode importar regras de outra fonte.

   d. Configure a regra de Monitorização da integridade do sistema (consulte a tabela abaixo).

10. Guarde as suas alterações.

Como configurar um âmbito de monitorização diferente para a tarefa Verificação de integridade do sistema na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Controlos de segurança → Monitorização da integridade do sistema**.

3. Ative o botão de alternar **Monitorização da integridade do sistema**.

4. Em **Verificação de integridade do sistema**, selecione o modo de configuração da tarefa: **Definições personalizadas**.

5. Configure a monitorização de dispositivos externos:

   a. Selecione a caixa de verificação **Monitorizar dispositivos**.

   b. Na lista suspensa **Nível de gravidade do evento**, selecione o nível de importância dos eventos de monitorização de dispositivos externos: *Informativo* ⓘ, *Aviso* ⚠, *Crítico* ⓘ.

   A Monitorização da integridade do sistema regista informações sobre dispositivos externos ligados no momento em que a linha de base é criada. Posteriormente, quando um dispositivo externo é ligado, a aplicação gera um evento correspondente. Ao executar a tarefa *Verificação de integridade do sistema*, a aplicação não monitoriza a desativação de dispositivos externos.

6. Configure a monitorização de ficheiros e registos:

   a. Selecione a caixa de verificação **Monitorizar ficheiros e o registo**.

   b. Clique em **Configurar**.

   Esta ação abre a lista de regras de Monitorização da integridade do sistema.

   c. Clique em **Adicionar**.

   Também pode importar regras de outra fonte.

   d. Configure a regra de Monitorização da integridade do sistema (consulte a tabela abaixo).

7. Guarde as suas alterações.

Definições 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 regista eventos de modificação de ficheiro sempre que um ficheiro ou chave de registo no âmbito de monitorização é modificado. Os seguintes níveis de gravidade do evento estão disponíveis: *Informativo*, *Aviso*, *Crítico*.

Âmbito da monitorização	• **Ficheiro**. Lista de ficheiros e pastas monitorizadas pelo componente. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.
	Usar máscaras:
	  • O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.
	  • Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.
	  • O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.
	• **Registo**. Lista de chaves de registo e valores monitorizados pelo componente. O Kaspersky Endpoint Security suporta os caracteres `*` e `?` ao introduzir uma máscara.

Exclusões	• **Ficheiro**. Lista de exclusões do âmbito de monitorização. O Kaspersky Endpoint Security suporta variáveis de ambiente e os 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 do âmbito de monitorização.
	Usar máscaras:
	  • O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.
	  • Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.
	  • O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.
	• **Registo**. Lista de exclusões do âmbito de monitorização. O Kaspersky Endpoint Security suporta os caracteres `*` e `?` ao introduzir uma máscara. As entradas de exclusão têm uma prioridade mais alta do que as entradas do âmbito de monitorização.

Executar a tarefa Verificação de integridade do sistema

A tarefa *Verificação de integridade do sistema* permite verificar se há alterações em ficheiros ou chaves de registo e também verificar a ligação de dispositivos externos. Para verificar se há alterações nos ficheiros, pode executar a tarefa *Verificação de integridade do sistema* nos seguintes modos:

- Verificação rápida.

  Ao verificar se há alterações nos ficheiros, as aplicações verificam apenas os atributos do ficheiro. A aplicação não verifica o conteúdo dos ficheiros.

- Verificação completa.

  Ao verificar se há alterações nos ficheiros, as aplicações verificam todos os atributos e o conteúdo dos ficheiros.

O modo em que a tarefa é executada não afeta a verificação do registo ou dos dispositivos externos.

Como executar a tarefa Verificação de integridade do sistema na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Tasks**.

   A lista de tarefas é aberta.
3. Clique em **New task**.

   O Assistente de Tarefas é iniciado. Siga as instruções do Assistente.
4. Selecione o **Kaspersky Endpoint Security → Monitorização da integridade do sistema de linha de base**. Selecione um modo de Monitorização de integridade do sistema:

   - **Verificação completa**. Neste modo, a aplicação verifica todos os atributos e hashes dos ficheiros.
   - **Verificação Rápida**. Neste modo, a aplicação verifica apenas atributos de ficheiros.
5. Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

   - Selecione os computadores detetados pelo Servidor de administração na rede: unassigned devices. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
   - Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.
   - Especifique a seleção de dispositivos para os quais deseja executar a tarefa.
   - Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
6. Selecione uma conta para executar a tarefa. Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de utilizador local.
7. Configure um agendamento para iniciar uma tarefa, por exemplo, manualmente ou num dia específico da semana.

8. Insira um nome para a tarefa.

9. Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa.

Como executar uma tarefa de System Integrity Check na Consola Web

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **System Integrity Check**.

   c. No campo **Task name**, introduza uma breve descrição, por exemplo, *Verificação semanal da integridade do sistema*.

   d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Avance para o passo seguinte.

5. Selecione uma conta para executar a tarefa. Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de utilizador local.

6. Conclua o assistente.

   Será apresentada uma nova tarefa na lista de tarefas.

7. Clique em nova tarefa.

   É apresentada a janela de propriedades da tarefa.

8. Selecione o separador **Application settings**.

9. Selecione um modo de Verificação de integridade do sistema:

   - **Quick Scan**. A aplicação verifica apenas atributos de ficheiro. A aplicação não verifica o conteúdo dos ficheiros.

   - **Full Scan**. A aplicação verifica todos os atributos dos ficheiros, bem como o seu conteúdo.

10. Guarde as suas alterações.

11. Selecione a caixa de verificação junto à tarefa.

12. Clique em **Start**.

Para que a tarefa *Verificação de integridade do sistema* seja concluída com sucesso, o âmbito de monitorização da tarefa *Verificação de integridade do sistema* tem de corresponder completamente à linha de base. Se o âmbito de monitorização for diferente, a tarefa irá terminar com um erro. Para sincronizar âmbitos de monitorização, execute a tarefa *Atualização da linha de base* com um novo âmbito de monitorização.

Exportar e importar as regras da Monitorização da integridade do sistema

Pode exportar a lista de regras de Monitorização da integridade do sistema para um ficheiro XML. Em seguida, pode modificar o ficheiro para, por exemplo, adicionar um grande número de registos do mesmo tipo. Pode utilizar a função de exportação/importação para fazer uma cópia de segurança da lista de regras de Monitorização da integridade do sistema ou para migrar a lista para um servidor diferente.

A Monitorização da Integridade do Sistema não suporta a importação das chaves `HKEY_CURRENT_USER` e `HKEY_CURRENT_CONFIG` para a tarefa *Verificação de integridade do sistema*. Se o âmbito da monitorização da tarefa tiver estas chaves, a aplicação gera o evento *O âmbito da monitorização inclui objetos incorretos*.

Como exportar e importar uma lista de regras da Monitorização da integridade do sistema na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Controlos de segurança → Monitorização da integridade do sistema**.
4. Para exportar ou importar as regras da *Monitorização da integridade do sistema em tempo real*:
   a. No bloco **Monitorização da integridade do sistema em tempo real**, clique no botão **Definições**.
   b. Para exportar uma lista de regras da Monitorização da integridade do sistema em tempo real:
      1. Selecione as regras que pretende exportar. Para selecionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.
         Se não tiver selecionado nenhuma regra, o Kaspersky Endpoint Security exportará todas as regras.
      2. Clique na hiperligação **Exportar**.
      3. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de regras e selecione a pasta onde pretende guardar este ficheiro.
      4. Guardar o ficheiro.
         O Kaspersky Endpoint Security exporta a lista de regras para o ficheiro XML.
   c. Para importar uma lista de regras da Monitorização da integridade do sistema em tempo real:
      1. Clique na hiperligação **Importar**.
         Na janela que se abre, selecione o ficheiro XML a partir do qual pretende importar a lista de regras.
      2. Abrir o ficheiro.
         Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro XML.

5. Para exportar ou importar regras da *Verificação de integridade do sistema*:

   a. No bloco **Verificação de integridade do sistema**, selecione **Definições personalizadas**.

   b. Clique em **Definições**.

   c. Para exportar a lista de regras da Verificação de integridade do sistema:

      1. Selecione as regras que pretende exportar. Para selecionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.

         Se não tiver selecionado nenhuma regra, o Kaspersky Endpoint Security exportará todas as regras.

      2. Clique na hiperligação **Exportar**.

      3. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de regras e selecione a pasta onde pretende guardar este ficheiro.

      4. Guardar o ficheiro.

      O Kaspersky Endpoint Security exporta a lista de regras para o ficheiro XML.

   d. Para importar uma lista de regras da Verificação de integridade do sistema:

      1. Clique na hiperligação **Importar**.

         Na janela que se abre, selecione o ficheiro XML a partir do qual pretende importar a lista de regras.

      2. Abrir o ficheiro.

      Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro XML.

6. Guarde as suas alterações.

Como exportar e importar uma lista de regras da Monitorização da integridade do sistema na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Security Controls → System Integrity Monitoring**.

5. Selecione o separador **Windows**.

6. Para exportar ou importar as regras da *Monitorização da integridade do sistema em tempo real*:

   a. No bloco **Real-Time System Integrity Monitoring**, clique na ligação **Rules**.

   b. Para exportar uma lista de regras da Monitorização da integridade do sistema em tempo real:

      1. Selecione as regras que pretende exportar.

      2. Selecione o botão → **Export**.

         O Kaspersky Endpoint Security exporta a lista de regras para um ficheiro JSON na pasta de transferências predefinida.

   c. Para importar uma lista de regras da Monitorização da integridade do sistema em tempo real:

      1. Selecione o botão → **Import**.

         Na janela que se abre, selecione o ficheiro JSON a partir do qual pretende importar a lista de URL fiáveis.

      2. Abrir o ficheiro.

         Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro JSON.

7. Para exportar ou importar regras da *Verificação de integridade do sistema*:

   a. No bloco **On-Demand System Integrity Check**, selecione **Custom settings**.

   b. Clique na hiperligação **Rules**.

   c. Para exportar a lista de regras da Verificação de integridade do sistema:

      1. Selecione as regras que pretende exportar.

      2. Selecione o botão → **Export**.

         O Kaspersky Endpoint Security exporta a lista de regras para um ficheiro JSON na pasta de transferências predefinida.

   d. Para importar uma lista de regras da Verificação de integridade do sistema:

      1. Selecione o botão → **Import**.

         Na janela que se abre, selecione o ficheiro JSON a partir do qual pretende importar a lista de URL fiáveis.

      2. Abrir o ficheiro.

         Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro JSON.

8. Guarde as suas alterações.

Visualizar os relatórios da Monitorização da integridade do sistema

Para analisar o desempenho das regras de Monitorização da integridade do sistema, pode consultar os relatórios e eventos gerados pela aplicação. O Kaspersky Endpoint Security gera os seguintes relatórios sobre o componente:

- Na interface da aplicação:
  - O relatório de Monitorização da integridade do sistema
  - O relatório de Verificação de integridade do sistema
  - O relatório de Atualização da linha de base

  Os relatórios contêm eventos da Monitorização da integridade do sistema.
- Na Consola do Kaspersky Security Center:
  - Relatório sobre computadores nos quais as regras de monitorização foram acionadas o maior número de vezes
  - Relatório sobre regras de monitorização acionadas com mais frequência

  Por padrão, um relatório é criado para os 30 dias anteriores, incluindo a data em que o relatório foi criado.

  Como visualizar relatórios de Monitorização da integridade do sistema na Consola de Administração (MMC)

  1. Abra a Consola de Administração do Kaspersky Security Center.
  2. No nó **Administration Server** da árvore da Consola de Administração, selecione o separador **Reports**.
  3. Clique em **New report template**.

     O novo Assistente de Modelos de Relatório é iniciado.
  4. Siga as instruções do Assistente de Modelos de Relatório. No passo **Selecting the report template type**, selecione um relatório de Monitorização da integridade do sistema (a secção **Other**):
     - **Top 10 devices with File Integrity Monitor / System Integrity Monitoring rules most frequently triggered**.
     - **Top 10 rules of File Integrity Monitor / System Integrity Monitoring that were triggered on devices most frequently**.

     Depois de concluir o Novo Assistente de Modelos de Relatório, o novo modelo de relatório é apresentado na tabela no separador **Reports**.
  5. Abra o relatório fazendo duplo clique.

  O processo de criação do relatório é iniciado. O relatório é apresentado numa nova janela.

Como visualizar relatórios de Monitorização da integridade do sistema na Consola Web

1. Na janela principal da Consola Web, selecione **Monitoring → Reports**.
2. Clique em **Add**.

   O novo Assistente de Modelos de Relatório é iniciado.
3. Em **Template type**, na secção **Other**, selecione um relatório de Monitorização da integridade do sistema:

   - **Top 10 devices with File Integrity Monitor / System Integrity monitoring rules most frequently triggered**.
   - **Top 10 rules of File Integrity Monitor / System Integrity Monitoring that were triggered on devices most frequently**.

   Depois de concluir o Novo Assistente de Modelos de Relatório, o novo modelo de relatório é apresentado na tabela.
4. Selecione e execute o relatório.

O processo de criação do relatório é iniciado. O relatório é apresentado numa nova janela.

Para visualizar eventos gerados pela aplicação, também pode usar seleções de eventos na consola do Kaspersky Security Center.

Redefinição do estado de integridade do sistema

Os computadores na consola do Kaspersky Security Center têm um dos seguintes estados: *OK*, *Warning* ou *Critical*. Se a Monitorização da integridade do sistema detetar modificação de ficheiros ou chaves de registo no âmbito de monitorização, o estado do computador irá mudar para *Warning* ou *Critical*. O estado atribuído pela Monitorização da integridade do sistema é chamado de *estado da integridade do sistema*. Pode redefinir o estado da integridade do sistema, por exemplo, se a análise o convenceu de que a modificação detetada de objetos não afeta a segurança do computador.

Como repor o estado de integridade do sistema na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Tasks**.

   A lista de tarefas é aberta.
2. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

Selecione **Kaspersky Endpoint Security for Windows (14.2) → Reposição do estado de integridade do sistema**.

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

Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 3. Configurar um agendamento de início de uma tarefa

Configure o agendamento de tarefas, por exemplo, manualmente.

Passo 4. Definir o nome da tarefa

Insira o nome da tarefa, por exemplo, *Redefinir o estado após modificar o âmbito de monitorização*.

Passo 5. Completar a criação da tarefa

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa.

Como redefinir o estado de integridade do sistema na Consola Web

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **System integrity status reset**.

   c. No campo **Task name**, insira uma breve descrição, por exemplo, *Redefinir o estado após modificar o âmbito de monitorização*.

   d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Avance para o passo seguinte.

5. Selecione uma conta para executar a tarefa. Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com os direitos de uma conta de utilizador local.

6. Conclua o assistente.

   Será apresentada uma nova tarefa na lista de tarefas.

7. Selecione a caixa de verificação junto à tarefa.

8. Clique em **Start**.

Como resultado, se o estado do computador for alterado para *Warning* ou *Critical* devido a eventos de monitorização da integridade do sistema, o estado do computador é redefinido para *OK*. Se o estado do computador também tiver sido alterado devido a outros eventos, o estado do computador irá permanecer inalterado.

Cloud Discovery

O Cloud Discovery gere o acesso dos utilizadores 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, *File sharing*, *Messengers*, *Email*. Os especialistas da Kaspersky atualizam regularmente as categorias do Cloud Discovery e os serviços na nuvem classificados nas categorias. O Kaspersky Endpoint Security atualiza o conjunto de categorias e serviços na nuvem a par das bases de dados da aplicação. Isto significa que o Cloud Discovery não utiliza o Kaspersky Security Network para categorizar os serviços da nuvem.

O Cloud Discovery oferece as seguintes funcionalidades:

- Monitorização da utilização de serviços na nuvem
- Bloqueio do acesso dos utilizadores aos serviços na nuvem

Requisitos do sistema

O Cloud Discovery está disponível se as seguintes condições forem satisfeitas:

- A aplicação é instalada num computador com Windows para estações de trabalho.

  O componente não está disponível para servidores.

- Kaspersky Security Center versão 15.1 ou superior.

  O componente não está disponível na Consola de Administração (MMC). Pode configurar o Cloud Discovery na Consola Web do Kaspersky Security Center e na Cloud Console do Kaspersky Security Center.

- Próxima licença da Kaspersky.

Ative a funcionalidade da aplicação que o componente Cloud Discovery requer:

1. **Verificar ligações encriptadas**. Isto é necessário para a monitorização de tráfego HTTPS. Pode gerir esta funcionalidade na secção **Definições de Rede**.

2. **Injetar script no tráfego de Internet para interagir com páginas de Internet**. O script permite o registo de eventos do Cloud Discovery. O script também permite o bloqueio completo do acesso a serviços na nuvem. Sem o script, a aplicação bloqueia o acesso apenas por domínios de serviços na nuvem. Pode gerir esta funcionalidade na secção **Definições de Rede**.

Também pode ativar a funcionalidade **Registar a abertura de páginas permitidas**. A funcionalidade inclui o agrupamento de eventos quando um utilizador visita páginas Web que pertencem ao mesmo domínio. Desta forma, quando um utilizador utiliza um serviço na nuvem, o Cloud Discovery regista apenas um evento em vez de vários eventos para cada página de Internet. Pode gerir esta funcionalidade na secção **Controlo de Internet**.

Monitorização de serviços na nuvem

Quando um utilizador começa a usar um serviço na nuvem, o Kaspersky Endpoint Security regista esse evento e cria uma entrada no relatório. O Cloud Discovery controla a utilização de serviços na nuvem no navegador, bem como nas aplicações correspondentes. O Cloud Discovery controla a utilização de serviços na nuvem através de HTTP e HTTPS.

Como ativar a monitorização do serviço de nuvem n Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Communication & Web Protection** → **Cloud Discovery**.

5. Ative o botão de alternar **Cloud Discovery ENABLED**.

6. Guarde as suas alterações.

Como resultado, a aplicação encaminha informações sobre os serviços na nuvem que estão a ser utilizados para o Kaspersky Security Center. Pode ver as informações de utilização do serviço da nuvem nos relatórios. Se necessário, pode bloquear o acesso aos serviços da nuvem.

Bloqueio do acesso aos serviços na nuvem

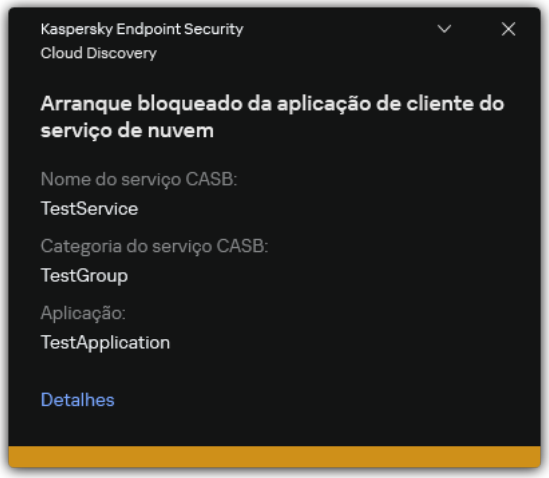
O bloqueio do acesso a serviços da nuvem está disponível apenas para a licença do Kaspersky Next EDR Optimum e XDR Expert. Esta funcionalidade não está disponível para a licença do Kaspersky Next EDR Foundations. Comparação da funcionalidade da aplicação dependendo do tipo de licença do Kaspersky Next, consulte em Ajuda do Kaspersky Next.

O administrador pode restringir o acesso do utilizador a categorias do Cloud Discovery ou aos serviços na nuvem individuais. Desta forma, o administrador pode permitir apenas serviços seguros na nuvem e evitar fugas de dados. *As informações sobre o nível de risco* são apresentadas para cada serviço da nuvem no Cloud Discovery. O nível de risco ajuda a detetar serviços que não satisfazem os requisitos de segurança da organização.

O nível de risco é uma estimativa e não implica quaisquer declarações sobre a qualidade do serviço de computação na nuvem ou do seu fornecedor. O nível de risco é simplesmente uma recomendação dos especialistas da Kaspersky.

Os níveis de risco dos serviços na nuvem são apresentados na secção **Cloud Discovery** da política na lista de todos os serviços de computação controlados na nuvem.

Outros componentes do Kaspersky Endpoint Security oferecem proteção contra ameaças e rastreio de atividade suspeita do utilizador ao usar serviços na nuvem.



Notificação do Cloud Discovery

O Cloud Discovery não bloqueia aplicações na nuvem que tenham sido iniciadas antes do Kaspersky Endpoint Security.

Como bloquear o acesso a serviços da nuvem na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Communication & Web Protection** → **Cloud Discovery**.
5. Ative o botão de alternar **Cloud Discovery ENABLED**.

   É apresentada uma lista de todos os serviços da nuvem. Os serviços em nuvem são agrupados em categorias, por exemplo, *File sharing*, *Messengers*, *Email*. Os especialistas da Kaspersky atualizam regularmente as categorias do Cloud Discovery e os serviços na nuvem classificados nas categorias. O Kaspersky Endpoint Security atualiza o conjunto de categorias e serviços na nuvem a par das bases de dados da aplicação.

6. Utilizar o botão de alternar na coluna **Access** para configurar o acesso aos serviços da nuvem.

7. Guarde as suas alterações.

Como resultado, a aplicação controla a utilização de serviços na nuvem no navegador, bem como nas aplicações correspondentes.

Zona fiável

Uma *zona fiável* consiste numa lista de objetos e aplicações, configurada pelo administrador do sistema, que o Kaspersky Endpoint Security não monitoriza quando está ativo.

O administrador cria a zona fiável de forma independente, tendo em consideração as características dos objetos processados e das aplicações instaladas no computador. Poderá ser necessário incluir objetos e aplicações na zona fiável quando o Kaspersky Endpoint Security bloqueia o acesso a um determinado objeto ou aplicação, caso o utilizador esteja seguro de que o objeto ou aplicação não constitui qualquer risco. Um administrador também pode permitir que um utilizador crie a sua própria zona fiável local para um computador específico. Desta forma, os utilizadores podem criar as suas próprias listas locais de exclusões e de aplicações fiáveis, além da zona fiável geral numa política.

A partir do Kaspersky Endpoint Security 12.5 for Windows, pode adicionar telemetria EDR à zona fiável. Isto permite otimizar os dados que a aplicação envia para o servidor de recolha de Telemetria para a solução do Kaspersky Anti Targeted Attack Platform (EDR).

A partir do Kaspersky Endpoint Security 12.6 para Windows, as exclusões de verificação e as aplicações fiáveis são adicionadas à zona fiável. Exclusões de verificação predefinidas e aplicações fiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e System Center Configuration Manager. Isto significa que não é necessário configurar manualmente uma zona fiável para a aplicação nos servidores.

A partir do Kaspersky Endpoint Security 12.8 para Windows, pode instalar aplicação no modo Light Agent para proteger ambientes virtuais. As exclusões de verificação predefinidas e as aplicações fiáveis podem ajudá-lo a configurar rapidamente o Kaspersky Endpoint Security em ambientes virtuais Citrix e VMware.

Criar uma exclusão de verificação

Uma *exclusão de verificação* consiste num conjunto de condições que devem ser cumpridas para que o Kaspersky Endpoint Security não verifique a existência de vírus e outras ameaças num objeto específico. As exclusões de verificação possibilitam a utilização segura de software legítimo que pode ser explorado por criminosos para danificar o computador ou os dados do utilizador. Estas aplicações não têm necessariamente uma finalidade maliciosa, mas podem ser exploradas por hackers. Para obter informações detalhadas sobre aplicações legítimas que os intrusos podem utilizar para comprometer o computador ou os dados do utilizador, visite o site da Enciclopédia da Kaspersky.

Essas aplicações podem ser bloqueadas pelo Kaspersky Endpoint Security. Para impedir que sejam bloqueadas, pode configurar exclusões de verificação para as aplicações em utilização. Para tal, adicione o nome ou a máscara do nome indicada na Kaspersky IT Encyclopedia à zona fiável. Por exemplo, utiliza frequentemente a aplicação Radmin para a administração remota dos computadores. O Kaspersky Endpoint Security considera esta atividade como suspeita e pode bloqueá-la. Para impedir o bloqueio da aplicação, crie uma regra de exclusão de verificação com o nome ou a máscara do nome indicada na Kaspersky IT Encyclopedia.

Se uma aplicação que recolhe informação e a envia para ser processada estiver instalada no seu computador, o Kaspersky Endpoint Security pode classificar esta aplicação como software malicioso. Para evitar esta situação, pode excluir a aplicação da verificação, configurando o Kaspersky Endpoint Security como descrito neste documento.

As exclusões de verificação podem ser utilizadas pelos seguintes componentes e tarefas da aplicação, que são configurados pelo administrador do sistema:

- Deteção de comportamento.
- Prevenção de explorações.
- Prevenção contra invasões.
- Proteção contra ameaças de ficheiros.
- Proteção contra ameaças da Web.
- Proteção contra ameaças de correio.
- Tarefa de *Verificação de software malicioso*

O Kaspersky Endpoint Security não verifica um objeto a unidade ou a pasta que contém este objeto estiverem incluídos no âmbito de verificação no início de uma das tarefas de verificação. No entanto, a exclusão de verificação não é aplicada quando é iniciada uma tarefa de verificação personalizada para este objeto específico.

Como criar uma exclusão de verificação na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Definições gerais** → **Exclusões e tipos de objetos**.
5. No bloco **Analisar exclusões e aplicações fiáveis** → **Exclusões de verificação**, clique no botão **Definições**.

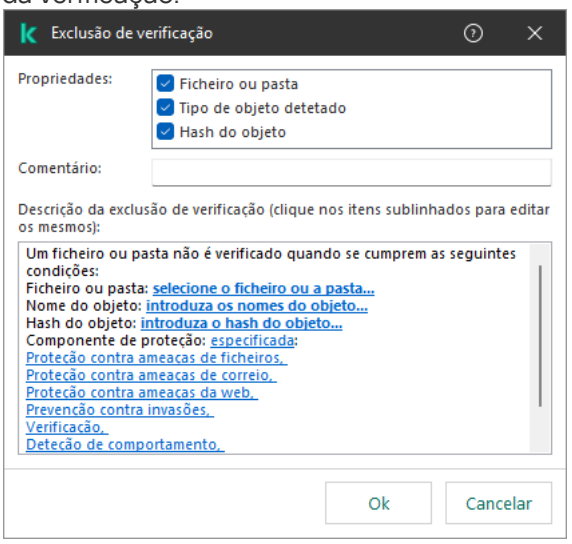
   Abre-se uma janela que contém uma lista de exclusões.
6. Selecione a caixa de verificação **Unir valores ao herdar** se quiser criar uma lista consolidada de exclusões para todos os computadores da empresa. As listas de exclusões nas políticas principal e subordinadas serão unidas. As listas serão unidas, desde que a união de valores ao herdar esteja ativada. As exclusões da política principal são apresentadas nas políticas subordinadas numa vista apenas de leitura. Não é possível alterar ou eliminar exclusões da política principal.
7. Selecione a caixa de verificação **Permitir a utilização de exclusões locais** se pretender permitir que o utilizador crie uma lista local de exclusões. Desta forma, um utilizador pode criar a sua própria lista local de exclusões, além da lista geral de exclusões gerada na política. Um administrador pode usar o Kaspersky Security Center para ver, adicionar, editar ou eliminar itens da lista nas propriedades do computador.

   Se a caixa de verificação estiver desmarcada, o utilizador só consegue aceder à lista geral de exclusões gerada na política. Além disso, se esta caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security oculta a lista consolidada de exclusões de verificação na interface de utilizador da aplicação.

8. Clique em **Adicionar** e selecione uma ação:

- **Categoria**. Pode agrupar exclusões de verificação em categorias separadas. Para criar uma nova categoria, insira o nome da categoria e adicione, pelo menos, uma exclusão de verificação à categoria.
- **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 em servidores SQL, servidores Microsoft Exchange e o System Center Configuration Manager, a aplicação inclui *exclusões de verificação predefinidas*. Também foram adicionadas exclusões de verificação predefinidas para suportar a configuração de aplicações em ambientes virtuais Citrix e VMware. Tem de selecionar exclusões de verificação predefinidas dependendo da finalidade do servidor protegido.
- **Nova exclusão da categoria selecionada**. Para adicionar uma nova exclusão de verificação a uma categoria específica, selecione uma categoria.

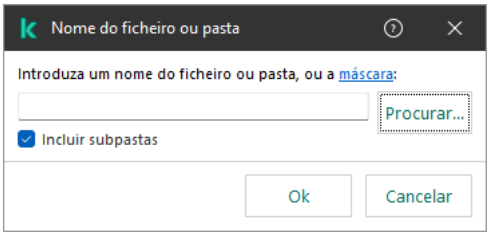
9. Para excluir um ficheiro ou pasta da verificação:



Definições de exclusão

a. No bloco **Propriedades**, selecione a caixa de verificação **Ficheiro ou pasta**.

b. Clique na ligação no bloco abaixo para abrir a janela **Nome do ficheiro ou pasta**.



Selecionar um ficheiro ou pasta

a. Introduza o nome do ficheiro ou da pasta ou a máscara do ficheiro ou nome da pasta, ou selecione o ficheiro ou pasta na árvore de pasta clicando em **Procurar**.

Usar máscaras:

- O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.

- Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

- O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.

Pode utilizar máscaras no início, no meio ou no final do caminho do ficheiro. Por exemplo, se quiser adicionar uma pasta para todos os utilizadores às exclusões, introduza a máscara `?:\Users\*\Folder\`.

O Kaspersky Endpoint Security suporta variáveis de ambiente

Pode excluir pastas de rede. Para o fazer, insira o caminho para a pasta de rede manualmente (por exemplo, `\\Network Share\*`).

> O Kaspersky Endpoint Security não suporta a variável do ambiente `%userprofile%` ao gerar uma lista de aplicações fiáveis na consola do Kaspersky Security Center. Para aplicar a entrada a todas as contas de utilizador, pode utilizar o caractere `*` (por exemplo, `C:\Users\*\Documents\File.exe`). Sempre que adiciona uma nova variável de ambiente, tem de reiniciar a aplicação.

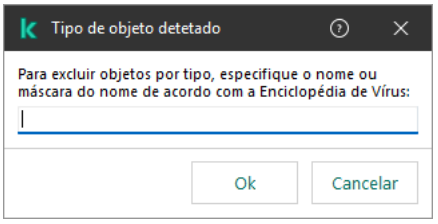
b. Se necessário, desative a funcionalidade **Incluir subpastas**. Se esta funcionalidade estiver ativada, a aplicação não verifica os ficheiros em todas as subpastas. Se esta funcionalidade estiver desativada, a aplicação exclui apenas a pasta selecionada do âmbito da verificação. Esta opção está ativada por predefinição.

c. Guarde as suas alterações.

10. Para excluir objetos com um nome específico da verificação:

    a. No bloco **Propriedades**, selecione a caixa de verificação **Tipo de objeto detetado**.

    b. Clique na ligação no bloco abaixo para abrir a janela **Tipo de objeto detetado**.



Selecionar objeto

    a. Introduza o nome do tipo de objeto de acordo com a classificação da Enciclopédia Kaspersky (por exemplo, `Email-Worm`, `Rootkit` ou `RemoteAdmin`).

    Pode usar máscaras com o caráter `?` (substitui qualquer caráter único) e o caráter `*` (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. Guarde as suas alterações.

11. Se quiser eliminar um ficheiro individual das verificações:

    a. No bloco **Propriedades**, selecione a caixa de verificação **Hash do objeto**.

    b. Clique na ligação no bloco abaixo para abrir a janela **Hash do objeto**.



Selecionar ficheiro

    a. Insira o hash do ficheiro ou selecione o ficheiro clicando no botão **Procurar**.

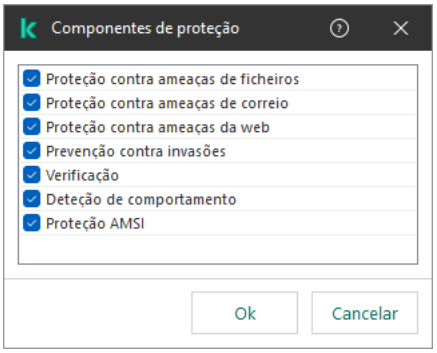
    Se o ficheiro for modificado, o hash do ficheiro também será modificado. Se isso acontecer, o ficheiro modificado não será adicionado às exclusões.

    b. Guarde as suas alterações.

12. Se necessário, no campo **Comentário**, introduza um breve comentário na exclusão de verificação que está a criar.

13. Especifique os componentes do Kaspersky Endpoint Security que devem utilizar a exclusão de verificação:

    a. Clique na ligação no bloco abaixo para abrir a janela **Componentes de proteção**.



Selecionar componentes de proteção

    a. Selecione as caixas de verificação à frente dos componentes aos quais a exclusão de verificação deve ser aplicada.

    Se os componentes estiverem especificados nas definições da exclusão de verificação, esta exclusão é aplicada apenas durante a verificação por estes componentes do Kaspersky Endpoint Security.

    Se os componentes não estiverem especificados nas definições da exclusão de verificação, esta exclusão é aplicada durante a verificação de todos os componentes do Kaspersky Endpoint Security.

14. Clique em **OK**.

    A nova exclusão será adicionada à lista. Pode desativar a exclusão em qualquer altura utilizando a caixa de verificação junto ao objeto.

15. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como criar uma exclusão de verificação na Kaspersky Security Center Web Console

1. Na janela principal da Consola Web, selecione o separador **Asset management → Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda à secção **Trusted Zone**.

5. Na janela que abre, clique na ligação **Malware Scan exclusions**.

6. Selecione a caixa de verificação **Merge values when inheriting** se quiser criar uma lista consolidada de exclusões para todos os computadores da empresa. As listas de exclusões nas políticas principal e subordinadas serão unidas. As listas serão unidas, desde que a união de valores ao herdar esteja ativada. As exclusões da política principal são apresentadas nas políticas subordinadas numa vista apenas de leitura. Não é possível alterar ou eliminar exclusões da política principal.

7. Selecione a caixa de verificação **Allow use of local exclusions** se pretender permitir que o utilizador crie uma lista local de exclusões. Desta forma, um utilizador pode criar a sua própria lista local de exclusões, além da lista geral de exclusões gerada na política. Um administrador pode usar o Kaspersky Security Center para ver, adicionar, editar ou eliminar itens da lista nas propriedades do computador.

   Se a caixa de verificação estiver desmarcada, o utilizador só consegue aceder à lista geral de exclusões gerada na política. Além disso, se esta caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security oculta a lista consolidada de exclusões de verificação na interface de utilizador da aplicação.

8. Clique em **Add** e selecione uma ação:

   - **Category**. Pode agrupar exclusões de verificação em categorias separadas. Para criar uma nova categoria, insira o nome da categoria e adicione, pelo menos, uma exclusão de verificação à categoria.
   - **New exclusion**. O Kaspersky Endpoint Security adiciona uma nova exclusão de verificação à raiz da lista.
   - **Select exclusion from list**. Para configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e o System Center Configuration Manager, a aplicação inclui *exclusões de verificação predefinidas*. Também foram adicionadas exclusões de verificação predefinidas para suportar a configuração de aplicações em ambientes virtuais Citrix e VMware. Tem de selecionar exclusões de verificação predefinidas dependendo da finalidade do servidor protegido.

   Para adicionar uma nova exclusão de verificação a uma categoria específica, selecione a caixa de verificação ao lado dessa categoria e selecione a opção **New exclusion**.

9. Selecione como pretende adicionar a exclusão: **Path to the file or folder**, **Object type** ou **Object hash**.

10. Para excluir um ficheiro ou pasta da verificação, insira o caminho manualmente. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara:

    - O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.
    - Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.
    - O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.

      Pode utilizar máscaras no início, no meio ou no final do caminho do ficheiro. Por exemplo, se quiser adicionar uma pasta para todos os utilizadores às exclusões, introduza a máscara `?:\Users\*\Folder\`.

      Pode excluir pastas de rede. Para o fazer, insira o caminho para a pasta de rede manualmente (por exemplo, `\\Network Share\*`).

11. Se quiser excluir um tipo específico de objeto das verificações, no campo **Object type**, introduza o nome do tipo de objeto de acordo com a classificação da Enciclopédia Kaspersky (por exemplo, `Email-Worm`, `Rootkit` ou `RemoteAdmin`).

    Pode usar máscaras com o caráter `?` (substitui qualquer caráter único) e o caráter `*` (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 quiser excluir um ficheiro individual das verificações, introduza o hash do ficheiro no campo **Object hash**.

    Se o ficheiro for modificado, o hash do ficheiro também será modificado. Se isso acontecer, o ficheiro modificado não será adicionado às exclusões.

13. No bloco **Apply exclusion to**, selecione os componentes aos quais pretende que a exclusão de verificação se aplique.

14. Se necessário, no campo **Comment**, introduza um breve comentário na exclusão de verificação que está a criar.

15. Clique em **OK**.

    A nova exclusão será adicionada à lista. Pode usar o botão de alternar para parar uma exclusão a qualquer momento.

16. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

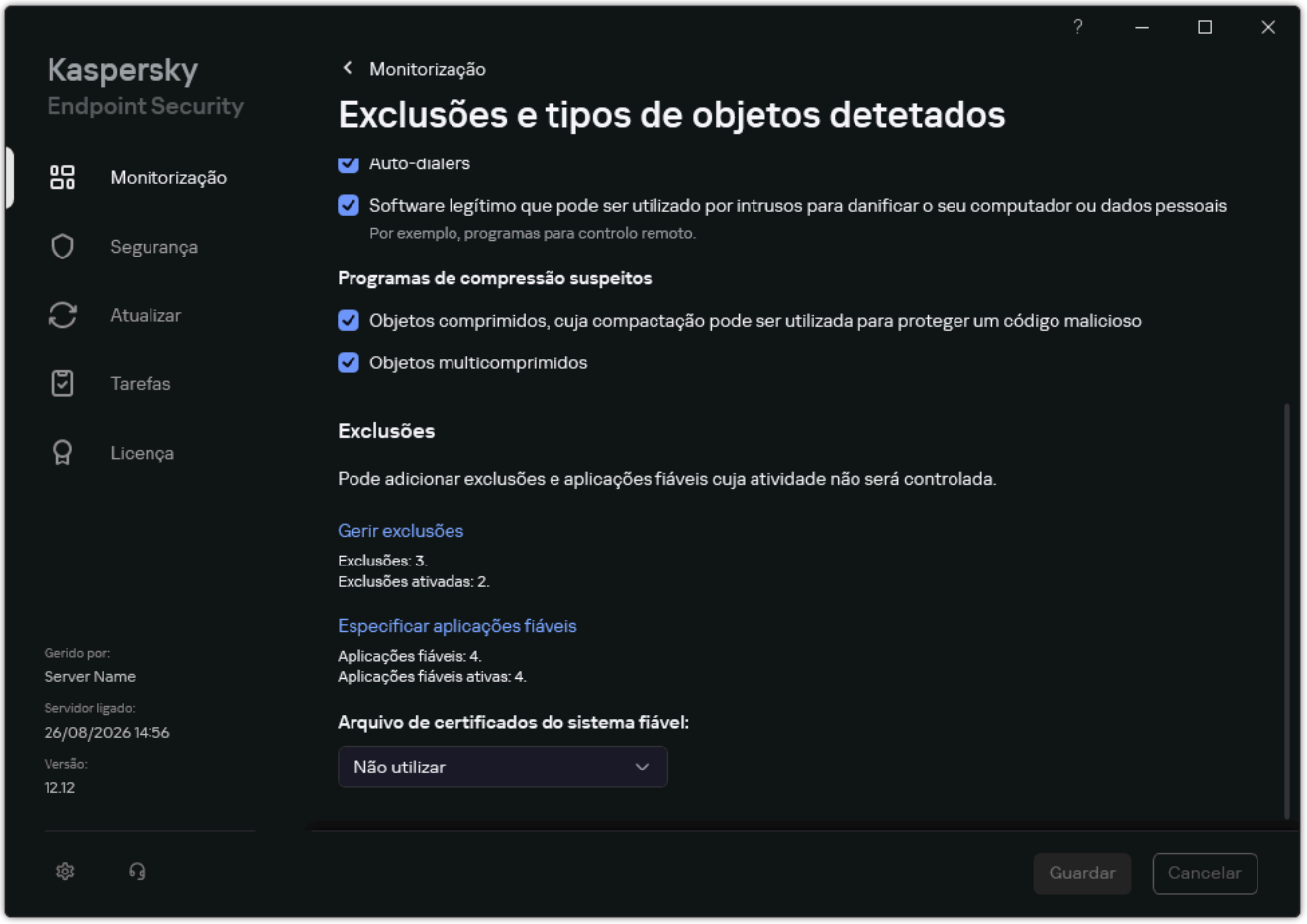
Como criar uma exclusão de verificação na interface da aplicação

1. Na janela principal da aplicação, clique no botão .

2. Na janela Application settings, selecione **Definições gerais → Exclusões e tipos de objetos detetados**.

3. No bloco **Exclusões**, clique na ligação **Gerir exclusões**.

> O Kaspersky Endpoint Security oculta a lista de exclusões de verificação na interface de utilizador da aplicação se a configuração de exclusões de verificação for bloqueada pelo administrador na consola (símbolo de "cadeado fechado") e se as exclusões de verificação locais forem proibidas (a caixa de verificação **Permitir a utilização de exclusões locais** está desmarcada).



Definições de exclusões

4. Clique em **Adicionar** e selecione uma ação:

   - **Categoria**. Pode agrupar exclusões de verificação em categorias separadas. Para criar uma nova categoria, insira o nome da categoria e adicione, pelo menos, uma exclusão de verificação à categoria.

   - **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 em servidores SQL, servidores Microsoft Exchange e o System Center Configuration Manager, a aplicação inclui *exclusões de verificação predefinidas*. Também foram adicionadas exclusões de verificação predefinidas para suportar a configuração de aplicações em ambientes virtuais Citrix e VMware. Tem de selecionar exclusões de verificação predefinidas dependendo da finalidade do servidor protegido.

   Para adicionar uma nova exclusão de verificação a uma categoria específica, selecione a caixa de verificação ao lado dessa categoria e selecione a opção **Nova exclusão**.

5. Se quiser excluir um ficheiro ou uma pasta das verificações, selecione o ficheiro ou a pasta clicando no botão **Procurar**.

   Também pode introduzir o caminho manualmente. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara:

   - O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.

   - Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

   - O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.

     Pode utilizar máscaras no início, no meio ou no final do caminho do ficheiro. Por exemplo, se quiser adicionar uma pasta para todos os utilizadores às exclusões, introduza a máscara `?:\Users\*\Folder\`.

     Pode excluir pastas de rede. Para o fazer, insira o caminho para a pasta de rede manualmente (por exemplo, `\\Network Share\*`).

6. Se quiser excluir um tipo específico de objeto das verificações, no campo **Tipo de objeto detetado**, introduza o nome do tipo de objeto de acordo com a classificação da Enciclopédia Kaspersky (por exemplo, `Email-Worm`, `Rootkit` ou `RemoteAdmin`).

   Pode usar máscaras com o caráter `?` (substitui qualquer caráter único) e o caráter `*` (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 quiser excluir um ficheiro individual das verificações, introduza o hash do ficheiro no campo **Hash do objeto**.

   Se o ficheiro for modificado, o hash do ficheiro também será modificado. Se isso acontecer, o ficheiro modificado não será adicionado às exclusões.

8. No bloco **Componentes de proteção**, selecione os componentes aos quais pretende que a exclusão de verificação se aplique.

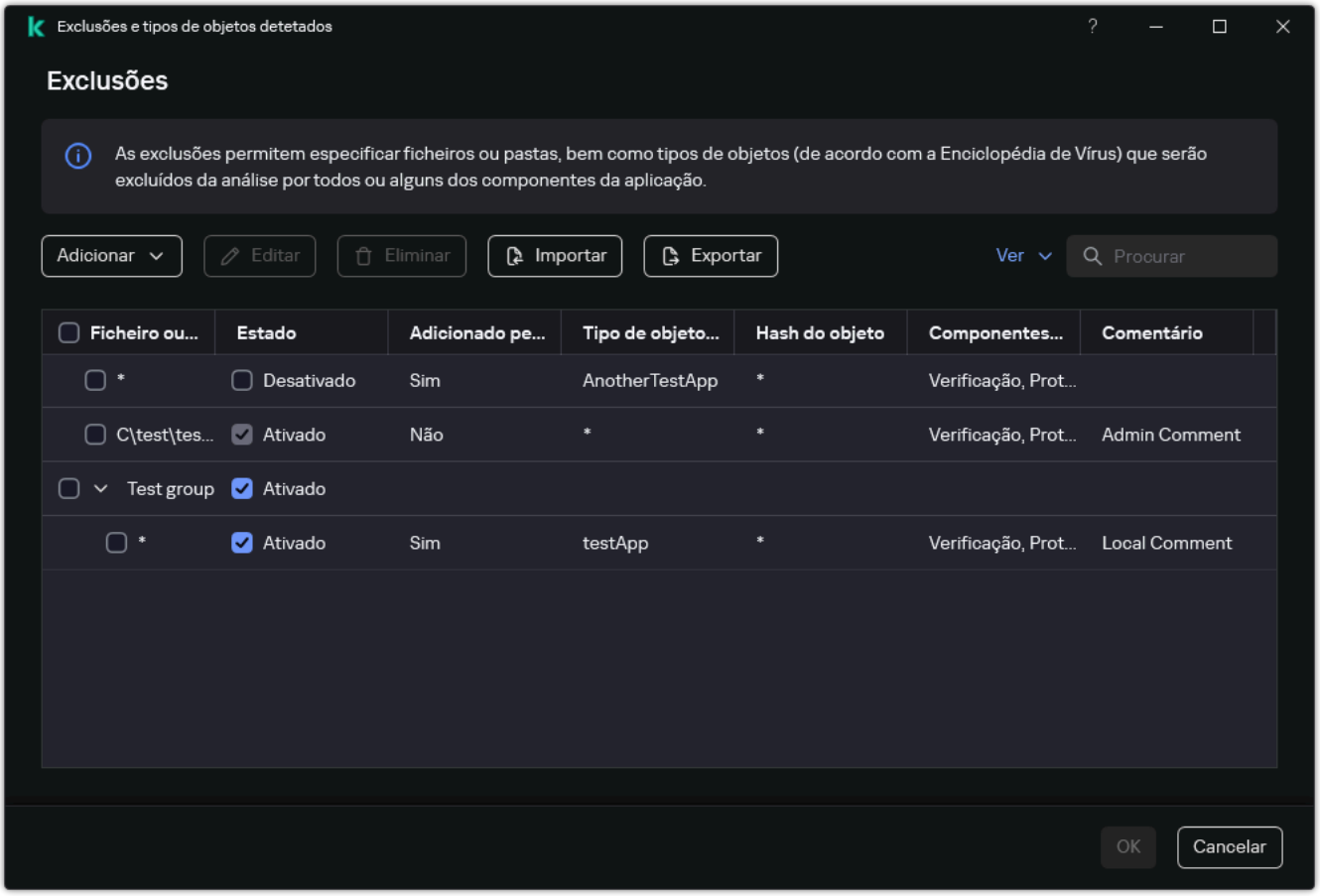
9. Se necessário, no campo **Comentário**, introduza um breve comentário na exclusão de verificação que está a criar.

10. Selecione o estado **Ativo** para a exclusão.

11. Clique em **Adicionar**.

    A nova exclusão será adicionada à lista. Pode desativar a exclusão em qualquer altura utilizando a caixa de verificação na coluna **Estado**.

12. Guarde as suas alterações.



Lista de exclusões

Exemplos de máscara de caminho:

Recomendamos especificar caminhos relativos, em vez de caminhos absolutos. Isto permite excluir não apenas objetos do sistema de ficheiros, mas também objetos sem ficheiros. Por exemplo, `*\Program Files (x86)\Folder\Subfolder`.

Caminhos para ficheiros localizados em qualquer pasta:

- A máscara `*.exe` inclui todos os caminhos para ficheiros com a extensão exe.
- O `example*` de máscara incluirá todos os caminhos para ficheiros com o nome EXAMPLE.

Caminhos para ficheiros localizados numa pasta especificada:

- A máscara `C:\dir\*.*` inclui todos os caminhos para ficheiros localizados na pasta `C:\dir\`, mas não nas subpastas de `C:\dir\`.
- A máscara `C:\dir\*` inclui todos os caminhos para ficheiros localizados na pasta `C:\dir\`, incluindo as subpastas.
- A máscara `C:\dir\` inclui todos os caminhos para ficheiros localizados na pasta `C:\dir\`, incluindo as subpastas.
- A máscara `C:\dir\*.exe` inclui todos os caminhos para ficheiros com a extensão EXE localizados na pasta `C:\dir\`, mas não nas subpastas de `C:\dir\`.
- A máscara `C:\dir\test` inclui todos os caminhos para ficheiros denominados "test" localizados na pasta `C:\dir\`, mas não nas subpastas de `C:\dir\`.
- A máscara `C:\dir\*\test` inclui todos os caminhos em ficheiros denominados "test" localizados na pasta `C:\dir\` e nas subpastas de `C:\dir\`.
- A máscara `C:\dir1\*\dir3\` inclui todos os caminhos para ficheiros nas subpastas dir3 um nível na pasta `C:\dir1\\`.
- A máscara `C:\dir1\**\dirN\` inclui todos os caminhos para ficheiros nas subpastas dirN na pasta `C:\dir1\` em qualquer nível.

Caminhos para ficheiros localizados em todas as pastas com um nome especificado:

- A máscara `dir\*.*` inclui todos os caminhos para ficheiros em pastas denominadas "dir", mas não nas subpastas dessas pastas.
- A máscara `dir\*` inclui todos os caminhos para ficheiros em pastas denominadas "dir", mas não nas subpastas dessas pastas.
- A máscara `dir\` inclui todos os caminhos para ficheiros em pastas denominadas "dir", mas não nas subpastas dessas pastas.
- A máscara `dir\*.exe` inclui todos os caminhos para ficheiros com a extensão EXE em pastas denominadas "dir", mas não nas subpastas dessas pastas.
- A máscara `dir\test` inclui todos os caminhos para ficheiros denominados "test" nas pastas denominadas "dir", mas não nas subpastas dessas pastas.

Criar uma exclusão por tipo de objetos detetados

O Kaspersky Endpoint Security classifica os objetos detetados da seguinte forma:

- **Vírus e worms**

  Subcategoria: vírus e worms (Viruses_and_Worms)

  Nível de perigo: elevado

  Os vírus e worms clássicos executam ações não autorizadas pelo utilizador. Estes podem criar cópias de si próprios que são capazes de se auto-multiplicar.

  Vírus clássico

Quando um vírus clássico se infiltra no computador, infeta um ficheiro, ativa-se, executa ações maliciosas e adiciona cópias de si próprio a outros ficheiros.

Um vírus clássico multiplica-se apenas em recursos locais do computador; não conseguindo, por si só, penetrar noutros computadores. Só pode ser transmitido a outro computador se adicionar uma cópia de si próprio a um ficheiro armazenado numa pasta partilhada ou CD inserido ou se o utilizador reencaminhar uma mensagem de e-mail com um ficheiro infetado anexado.

O código de um vírus clássico pode penetrar várias áreas dos computadores, sistemas operativos e aplicações. Dependendo do ambiente, os vírus dividem-se em *vírus de ficheiro*, *vírus de inicialização*, *vírus de script* e *vírus de macro*.

Os vírus podem infetar ficheiros através de diversas técnicas. Os vírus *Overwriting* substituem o código do ficheiro infetado pelo seu próprio código, apagando, deste modo, o conteúdo do ficheiro. O ficheiro infetado deixa de funcionar e não pode ser restaurado. Os vírus *Parasitic* modificam ficheiros, deixando-os total ou parcialmente funcionais. Os *Companion* não modificam ficheiros, mas criam duplicados. Quando um ficheiro infetado é aberto, é iniciado um duplicado deste ficheiro (que é, na verdade, um vírus). São também detetados os seguintes tipos de vírus: o vírus *Link*, *vírus OBJ*, *vírus LIB*, *vírus em código fonte* e muitos outros.

Worm

Tal como um vírus clássico, o código de um worm é ativado e executa ações maliciosas após infiltrar-se num computador. O nome "worm" (verme) deve-se à sua capacidade de "rastejar" de um computador para outro e de disseminar cópias através de inúmeros canais de dados, sem a autorização do utilizador.

A principal característica que permite diferenciar os vários tipos de worms é a forma como se disseminam. A tabela que se segue faculta uma descrição geral dos vários tipos de worms, que são classificados pela forma como se disseminam.

Formas de disseminação de worms

Tipo	Name	Descrição
Worm de e-mail	Worm de e-mail	Disseminam-se por e-mail. Uma mensagem infetada contém um ficheiro anexado com uma cópia de um worm ou uma ligação a um ficheiro que é carregado para um site, o qual pode ter sido pirateado ou criado exclusivamente para esse fim. Quando o utilizador abre o ficheiro anexado, o worm é ativado. Quando o utilizador clica na ligação, transfere e, depois, abre o ficheiro, o worm começa também a executar as respetivas ações maliciosas. Depois disso, o worm continua a disseminar cópias de si próprio, a procurar outros endereços de e-mail e a enviar mensagens infetadas a esses endereços.
IM-Worm	Worms de cliente de MI	Estes disseminam-se através de clientes de MI. Normalmente, estes worms enviam mensagens que contêm uma ligação a um ficheiro com uma cópia do worm num site, utilizando a lista de contactos do utilizador. Quando o utilizador transfere e abre o ficheiro, o worm é ativado.
IRC-Worm	Worms de salas de conversação	Estes disseminam-se através de Internet Relay Chats (IRC), sistemas de serviços que permitem comunicar com outras pessoas, em tempo real, através da Internet. Estes worms publicam um ficheiro com uma cópia de si próprios ou uma ligação ao ficheiro numa sala de conversação na Internet. Quando o utilizador transfere e abre o ficheiro, o worm é ativado.
Net-Worm	Worms de rede	Estes worms disseminam-se através de redes de computadores. Ao contrário dos outros tipos de worms, um worm de rede típico dissemina-se sem a participação do utilizador. Este procura na rede local os computadores que contêm programas com vulnerabilidades. Para tal, envia um pacote de rede especialmente criado (exploit) que contém o código do worm ou uma parte desse código. Se existir um computador "vulnerável" na rede, este receberá o pacote de rede. O worm é ativado quando tiver penetrado completamente no computador.

Tipo	Name	Descrição
P2P-Worm	Worms de rede de partilha de ficheiros	Disseminam-se em redes de partilha de ficheiros peer-to-peer. Para se infiltrar numa rede P2P, o worm copia-se a si próprio para uma pasta de partilha de ficheiros que, normalmente, está localizada no computador do utilizador. A rede P2P apresenta informação sobre este ficheiro, de forma a que o utilizador possa "encontrar" o ficheiro infetado na rede como qualquer outro ficheiro, transferi-lo e abri-lo. Os worms mais sofisticados imitam o protocolo de rede de uma rede P2P específica: devolvem respostas positivas a pedidos de pesquisa e disponibilizam cópias de si próprios para transferência.
Worm	Outros tipos de worms	Outros tipos de worms incluem: • Worms que disseminam cópias de si próprios através de recursos de rede. Utilizando as funções do sistema operativo, estes worms procuram pastas de rede disponíveis, estabelecem ligação a computadores na Internet e tentam obter acesso total às respetivas unidades de disco. Ao contrário dos tipos de worms descritos anteriormente, os outros tipos de worms não se ativam por si próprios, mas sim quando o utilizador abre um ficheiro que contém uma cópia do worm. • Os worms que não utilizam nenhum dos métodos descritos na tabela anterior para disseminar-se (por exemplo, aqueles que se disseminam por telemóveis).

- **Trojans (incluindo ransomware)**

  Subcategoria: Trojans

  Nível de perigo: elevado

  Ao contrário dos worms e dos vírus, os Trojans não se auto-multiplicam. Por exemplo, estes penetram num computador através do e-mail ou do navegador quando o utilizador visita uma página da Internet infetada. Os Trojans são iniciados com a participação do utilizador. Começam a efetuar as suas ações maliciosas assim que são executados.

  Diferentes Trojans têm comportamentos diferentes nos computadores infetados. As principais funções dos "Trojans" incluem bloquear, modificar ou destruir informações, e desativar os computadores ou redes. Os Trojans também podem receber ou enviar ficheiros, executá-los, apresentar mensagens no ecrã, solicitar páginas da Internet, transferir e instalar programas e reiniciar o computador.

  Muitas vezes, os hackers utilizam "conjuntos" de vários Trojans.

  Os tipos de comportamento dos Trojan estão descritos na tabela seguinte.

  Tipos de comportamento de Trojans num computador infetado

Tipo	Name	Descrição
Trojan-ArcBomb	Trojans – "arquivos bomba"	Uma vez descompactados, a dimensão destes arquivos aumenta de tal forma que o funcionamento do computador é afetado. Quando o utilizador tenta descompactar este arquivo, o computador pode começar a trabalhar de forma lenta ou bloquear e o disco pode ficar cheio de dados "vazios". Os "arquivos bomba" são especialmente perigosos para os servidores de ficheiros e de e-mails. Se o servidor utilizar um sistema automático para processar a informação recebida, um "arquivo bomba" pode parar o servidor.
Backdoor	Trojans para administração remota	São considerados o tipo de programa Trojan mais perigoso. Em termos de funções, são semelhantes às aplicações de administração remota instaladas nos computadores. Estes programas instalam-se no computador sem serem detetados pelo utilizador, permitindo ao intruso gerir remotamente o computador.
Trojan	Trojans	Estes incluem as seguintes aplicações maliciosas: • **Trojans clássicos**. Estes programas executam apenas as principais funções dos Trojans: bloquear, modificar ou destruir informações e desativar computadores ou redes. Não incluem quaisquer funções avançadas, ao contrário dos outros tipos de Trojans descritos na tabela. • **Trojans versáteis**. Estes programas têm as características avançadas típicas de vários tipos de Trojans.
Trojan-Ransom	Trojans de resgate	Estes "tomam como refém" a informação do utilizador, alterando-a ou bloqueando-a, ou perturbam o funcionamento do computador, de forma a que o utilizador não consiga utilizar a informação. O intruso exige um resgate ao utilizador, prometendo enviar uma aplicação que restaura o desempenho do computador e os dados que tinham sido armazenados na mesma.

Tipo	Name	Descrição
Trojan-Clicker	Trojans de comandos	Estes acedem à página da Internet a partir do computador do utilizador, enviando comandos para um navegador ou alterando os endereços da Internet especificados nos ficheiros do sistema operativo. Ao utilizar estes programas, os intrusos efetuam ataques de rede e aumentam as visitas dos sites, aumentando o número de apresentações das faixas de publicidade (banners).
Trojan-Downloader	Trojans de transferências	Estes acedem à página da Internet do intruso, transferem outras aplicações maliciosas nessa localização e instalam-nas no computador do utilizador. Podem conter o nome do ficheiro da aplicação maliciosa a transferir ou recebê-lo a partir da página da Internet acedida.
Trojan-Dropper	Trojans instaladores	Estes contêm outros Trojans que instalam no disco rígido. Os intrusos podem utilizar programas do tipo Trojan Dropper com os objetivos seguintes: • Instalar uma aplicação maliciosa sem tal ser detetado pelo utilizador: Os programas do tipo Trojan Dropper não apresentam qualquer mensagem nem mensagens falsas, por exemplo, para notificar sobre um erro num arquivo ou sobre uma versão incompatível do sistema operativo. • Impedir que outra aplicação maliciosa conhecida seja detetada: nem todo o software antivírus consegue detetar aplicações maliciosas com uma aplicação do tipo Trojan Dropper.
Trojan-Notifier	Trojans notificadores	Estes informam um intruso de que um computador infetado está acessível, enviando-lhe informação sobre o computador: Endereço IP, número de uma porta aberta ou endereço de e-mail. Estes estabelecem ligação ao intruso por e-mail, por FTP, acedendo à página da Internet do intruso, ou de outra forma. Os programas do tipo Trojan Notifier são muitas vezes utilizados em conjuntos constituídos por vários Trojans. Estes notificam o intruso de que existem outros Trojans instalados com êxito no computador do utilizador.
Trojan-Proxy	Trojans proxies	Permitem ao intruso aceder a páginas de Internet de forma anónima, utilizando o computador do utilizador e são muitas vezes utilizados para enviar spam.
Trojan-PSW	Software de roubo de passwords	O software de roubo de passwords é um tipo de Trojan que rouba contas de utilizadores, por exemplo, dados de registo de software. Estes Trojans localizam dados confidenciais nos ficheiros do sistema e no registo e enviam-nos para o seu "atacante" por e-mail, por FTP, acedendo à página de Internet do intruso, ou de outra forma. Alguns destes programas Trojan estão categorizados em tipos separados descritos nesta tabela. Estes Trojans roubam contas bancárias (Trojan-Banker), dados de utilizadores de clientes de MI (Trojan-IM), e informações de utilizadores de jogos online (Trojan-GameThief).
Trojan-Spy	Trojans espiões	Estes espiam o utilizador, recolhendo informações sobre as ações do utilizador enquanto trabalha no computador. Estes podem intercetar os dados inseridos pelo utilizador através do teclado, tiram fotografias do ecrã ou recolhem listas de aplicações ativas. Depois de receberem esta informação, transferem-na para o intruso por e-mail, por FTP, acedendo à página de Internet do intruso, ou de outra forma.
Trojan-DDoS	Trojans de ataques de rede	Estes enviam numerosos pedidos a partir do computador do utilizador para um servidor remoto. O servidor não terá recursos suficientes para processar todos os pedidos, de tal forma que irá parar de funcionar (Recusa de Serviço ou simplesmente DoS). Muitas vezes, os hackers infetam vários computadores com estes programas para utilizarem os computadores para atacar em simultâneo um único servidor. Os programas DoS efetuam um ataque a partir de um único computador com o conhecimento do utilizador. Os programas DDoS (DoS Distribuído) efetuam ataques distribuídos a partir de diversos computadores, sem serem detetados pelo utilizador do computador infetado.
Trojan-IM	Trojans que roubam informações dos utilizadores de clientes de MI	Roubam números de contas e passwords de utilizadores de clientes de MI. Estes transferem informação para o intruso por e-mail, por FTP, acedendo à página de Internet do intruso, ou de outra forma.
Rootkit	Processos ocultos (Rootkits)	Estes ocultam outras aplicações maliciosas e as suas atividades e, assim, prolongam a existência dessas aplicações no sistema operativo. Também podem ocultar ficheiros, processos na memória de um computador infetado ou chaves de registo que executam aplicações maliciosas. Os rootkits podem ocultar o intercâmbio de dados entre aplicações no computador do utilizador e outros computadores da rede.
Trojan-SMS	Trojans sob a forma de mensagens SMS	Estes infetam os telemóveis e enviam mensagens SMS para números de valor acrescentado.
Trojan-GameThief	Trojans que roubam informações de utilizadores de jogos online	Estes roubam credenciais dos utilizadores de jogos online e, em seguida, enviam os dados para o intruso por e-mail, por FTP, acedendo à página de Internet do intruso, ou de outra forma.

Tipo	Name	Descrição
Trojan-Banker	Trojans que roubam contas bancárias	Estes roubam dados de contas bancárias ou dados de sistemas de dinheiro eletrónico e enviam os dados para o intruso por e-mail, por FTP, acedendo à página de Internet do intruso, ou de outra forma.
Trojan-Mailfinder	Trojans que recolhem endereços de e-mail	Estes recolhem endereços de e-mail guardados num computador e transferem-nos para o intruso por e-mail, por FTP, acedendo à página de Internet do intruso, ou de outra forma. Os intrusos podem enviar spam para os endereços que recolheram.

- **Ferramentas maliciosas**

  Subcategoria: Ferramentas maliciosas

  Nível de perigo: médio

  Ao contrário de outros tipos de software malicioso, as ferramentas maliciosas não executam as suas ações assim que são iniciadas. Estas podem ser armazenadas e executadas em segurança no computador do utilizador. Os intrusos muitas vezes utilizam as funções destes programas para criarem vírus, worms e Trojans, organizarem ataques de rede em servidores remotos, para penetrarem em computadores ou efetuarem outras ações maliciosas.

  As diversas funções das ferramentas maliciosas estão agrupadas por tipo na tabela que se segue.

  Funções das ferramentas maliciosas

Tipo	Name	Descrição
Constructor	Construtores	Permitem criar novos vírus, worms e Trojans. Alguns construtores apresentam uma interface padrão baseada em janelas, na qual o utilizador pode selecionar o tipo de aplicação maliciosa a criar, o método para contornar os depuradores e outras características.
Dos	Ataques de rede	Estes enviam numerosos pedidos a partir do computador do utilizador para um servidor remoto. O servidor não terá recursos suficientes para processar todos os pedidos, de tal forma que irá parar de funcionar (Recusa de Serviço ou simplesmente DoS).
Exploit	Explorações de vulnerabilidades	A *exploração de vulnerabilidades (exploit)* é um conjunto de dados ou um código de programa, que utiliza as vulnerabilidades da aplicação, na qual é processado, para executar uma ação maliciosa num computador. Por exemplo, a exploração de vulnerabilidades pode escrever ou ler ficheiros ou solicitar páginas de Internet "infetadas". Os diferentes tipos de exploração utilizam as vulnerabilidades em diferentes aplicações ou serviços de rede. Disfarçado de um pacote de rede, a exploração é transferida através da rede para múltiplos computadores, procurando computadores com serviços de rede vulneráveis. Uma exploração de num ficheiro DOC utiliza as vulnerabilidades de um editor de texto. Quando o utilizador abre o ficheiro infetado, essa exploração de vulnerabilidades pode começar a executar ações pré-programadas por um hacker. Uma exploração de vulnerabilidades incorporada numa mensagem de e-mail procura vulnerabilidades em qualquer cliente de e-mail. Esta pode começar a executar uma ação maliciosa, assim que o utilizador abrir a mensagem infetada neste cliente de e-mail. Os worms de rede (Net-Worms) disseminam-se nas redes através da exploração de vulnerabilidades. O exploit Nuker é constituído por pacotes de rede que desativam os computadores.
FileCryptor	Encriptadores	Estes encriptam outras aplicações maliciosas, para os ocultarem das aplicações antivírus.
Flooder	Programas para "contaminar" redes	Estes enviam um elevado número de mensagens através de canais de rede. Este tipo de ferramentas inclui, por exemplo, programas que contaminam canais de salas de conversação (IRC). As ferramentas do tipo Flooder não incluem programas que "contaminam" os canais utilizados por clientes de e-mail, clientes de MI e sistemas de comunicação móvel. Estes programas são distinguidos como tipos separados, estando descritos na tabela (Email-Flooder, MI-Flooder e SMS-Flooder).
HackTool	Ferramentas de Hackers	Estes exploits permitem penetrar no computador onde estão instalados ou atacar outro computador (por exemplo, adicionando novas contas de sistema sem a autorização do utilizador, apagando os registos do sistema para ocultar quaisquer vestígios da sua presença no sistema operativo). Este tipo de ferramentas inclui alguns programas farejadores (sniffers), que possuem funções maliciosas, tais como a interceção de passwords. Os programas farejadores são programas que permitem visualizar o tráfego de rede.
Hoax	Programas de engodo (Hoaxes)	Estes surpreendem os utilizadores com mensagens semelhantes a vírus: podem "detetar um vírus" num ficheiro não infetado ou notificar o utilizador de que o disco foi formatado, embora, tal não tenha sucedido de facto.

Tipo	Name	Descrição
Spoofer	Ferramentas de falsificação	Estas enviam mensagens e pedidos de rede com um endereço falso de um remetente. Os intrusos utilizam ferramentas de falsificação para se fazerem passar por remetentes legítimos, por exemplo.
VirTool	Ferramentas que modificam aplicações maliciosas	Estas permitem modificar outros programas de software malicioso, ocultando os mesmos das aplicações antivírus.
Email-Flooder	Programas que "contaminam" endereços de e-mail	Estes enviam numerosas mensagens para diversos endereços de e-mail, "contaminando-os". O elevado volume de mensagens recebidas impede que os utilizadores vejam as mensagens úteis nas suas caixas de correio.
IM-Flooder	Programas que "contaminam" o tráfego de clientes de MI	Enviam grandes quantidades de mensagens aos utilizadores de clientes de MI. O elevado volume de mensagens impede que os utilizadores vejam as mensagens úteis recebidas.
SMS-Flooder	Programas que "contaminam" o tráfego com mensagens SMS	Estes enviam numerosos SMS para telemóveis.

- **Adware**

  Subcategoria: software de publicidade (Adware)

  Nível de perigo: médio

  O adware apresenta informações de publicidade ao utilizador. Os programas de Adware apresentam faixas de publicidade (banners) nas interfaces de outros programas, redirecionando os pedidos de pesquisa para páginas da Internet com publicidade. Alguns destes programas recolhem e enviam ao seu criador informações de marketing sobre o utilizador: esta informação pode incluir os nomes dos sites visitados pelo utilizador ou o conteúdo dos pedidos de pesquisa do utilizador. Ao contrário dos programas Trojan espiões, os programas de Adware enviam esta informação ao programador com a permissão do utilizador.

- **Auto-dialers**

  Subcategoria: Auto-dialers (Dialer).

  Nível de perigo: médio

  Os auto-dialers podem estabelecer sub-repticiamente ligações telefónicas utilizando um modem.

- **Software legítimo que pode ser utilizado por intrusos para danificar o seu computador ou dados pessoais**

  Subcategoria: software legal que pode ser utilizado por intrusos para danificar o computador ou os dados pessoais do utilizador.

  Nível de perigo: médio

  A maioria destas aplicações é útil, por isso muitos utilizadores executam-nas. Estas aplicações incluem clientes de IRC, auto-dialers, programas de transferências de ficheiros, monitores da atividade do sistema do computador, ferramentas de gestão de passwords, servidores de internet dos serviços FTP, HTTP, e Telnet.

  Contudo, se os intrusos obtiverem acesso a estes programas ou se os implantarem no computador do utilizador, algumas das suas funcionalidades podem ser utilizadas para violação da segurança.

Estas aplicações diferem em termos de funções; os respectivos tipos são descritos na tabela seguinte.

Tipo	Name	Descrição
Client-IRC	Clientes de conversação na Internet	Os utilizadores instalam estes programas para comunicarem com pessoas através de salas de conversação. Os intrusos utilizam-nos para espalharem software malicioso.
Downloader	Programas para transferências	Estes conseguem transferir ficheiros a partir de páginas de Internet, de forma oculta.
Monitor	Programas para monitorização	Estes permitem monitorizar as atividades no computador onde estão instalados (verificando quais as aplicações que estão ativas e como estas trocam dados com aplicações instaladas noutros computadores).
PSWTool	Programas de restauro de passwords	Estes permitem visualizar e restaurar as passwords esquecidas. Os intrusos implantam estes programas, de forma secreta, nos computadores dos utilizadores, com esse mesmo propósito.
RemoteAdmin	Programas de administração remota	Estes programas são muito utilizados por administradores de sistema. Estes programas permitem obter acesso à interface de um computador remoto para o monitorizar e gerir. Os intrusos implantam estes programas, de forma secreta, nos computadores dos utilizadores, com esse mesmo propósito: monitorizar e gerir computadores remotos. Os programas legítimos de administração remota são diferentes dos Trojans do tipo backdoor para administração remota. Os Trojans conseguem penetrar no sistema operativo de forma independente e instalam-se no computador; os programas legais não o conseguem fazer.
Server-FTP	Servidores de FTP	Estes funcionam como servidores FTP. Os intrusos implantam-nos no computador do utilizador para abrirem o acesso remoto ao mesmo, através do protocolo FTP.
Server-Proxy	Servidores proxy	Estes funcionam como servidores de proxy. Os intrusos implantam-nos no computador do utilizador para enviarem spam em nome do utilizador.
Server-Telnet	Servidores Telnet	Estes funcionam como servidores Telnet. Os intrusos implantam-nos no computador do utilizador para abrirem o acesso remoto ao mesmo, através do protocolo Telnet.
Server-Web	Servidores da Internet	Estes funcionam como servidores de Internet. Os intrusos implantam-nos no computador do utilizador para abrirem o acesso remoto ao mesmo, através do protocolo HTTP.
RiskTool	Ferramentas para trabalhar num computador local	Estas fornecem ao utilizador opções adicionais quando trabalha no seu computador. As ferramentas permitem ao utilizador ocultar ficheiros ou janelas de aplicações ativas e terminar processos ativos.
NetTool	Ferramentas de risco	Estas fornecem ao utilizador opções adicionais quando trabalha com outros computadores na rede. Estas ferramentas permitem reiniciar esses computadores, detetar portas abertas e executar aplicações instaladas nos computadores.
Client-P2P	Programas de rede P2P	Estes permitem trabalhar em redes Peer-to-Peer. Podem ser utilizados pelos intrusos para espalhar software malicioso.
Client-SMTP	Clientes SMTP	Enviam mensagens de e-mail sem conhecimento do utilizador. Os intrusos implantam-nos no computador do utilizador para enviarem spam em nome do utilizador.
WebToolbar	Barras de ferramenta da Internet	Estes programas adicionam barras de ferramentas às interfaces de outras aplicações para utilizar motores de pesquisa.
FraudTool	Pseudo-programas	Estes programas fazem-se passar por outros programas. Por exemplo, existem programas pseudo-antivírus que apresentam mensagens sobre a deteção de software malicioso. Contudo, na verdade, não detetam nem desinfetam qualquer ameaça.

- **Objetos comprimidos, cuja compactação pode ser utilizada para proteger um código malicioso**

  Subcategoria: ficheiros comprimidos que podem causar danos.

  Nível de perigo: médio.

  O ficheiro é comprimido utilizando um programa de compressão especial que é utilizado para comprimir software malicioso: vírus, worms, Trojans. O Kaspersky Endpoint Security verifica o módulo de descompressão com arquivos SFX (extração automática).

  Para esconder o software malicioso da deteção por um anti-vírus, os hackers comprimem-no utilizando programas de compressão especiais. Os especialistas da Kaspersky identificaram os programas de compressão mais populares entre os hackers.

- **Objetos multicomprimidos**

  Subcategoria: ficheiros multi-comprimidos.

  Nível de perigo: médio.

  O ficheiro é comprimido com um ou mais programas de compressão três ou mais vezes.

  Para esconder o software malicioso da deteção por um antivírus, os hackers podem comprimir um ficheiro várias vezes. O Kaspersky Endpoint Security verifica os ficheiros comprimidos.

Por padrão, o Kaspersky Endpoint Security deteta todos os tipos de objetos. Recomendamos manter a deteção de todos os tipos de objetos ativada para melhorar a segurança do computador. Se estiver a utilizar utilitários internos que a aplicação deteta como maliciosos, adicione esses utilitários a uma lista de exclusões, mas não desative a deteção de todo o tipo de objetos.

Como selecionar tipos de objetos detetáveis na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Definições gerais** → **Exclusões e tipos de objetos**.
5. No bloco **Tipos de objetos detetados**, clique no botão **Definições**.
6. Na janela que se abre, selecione as caixas de verificação em frente aos tipos de objetos que pretende que o Kaspersky Endpoint Security detete.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como selecionar tipos de objetos detetáveis na Consola Web e na Console Cloud

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

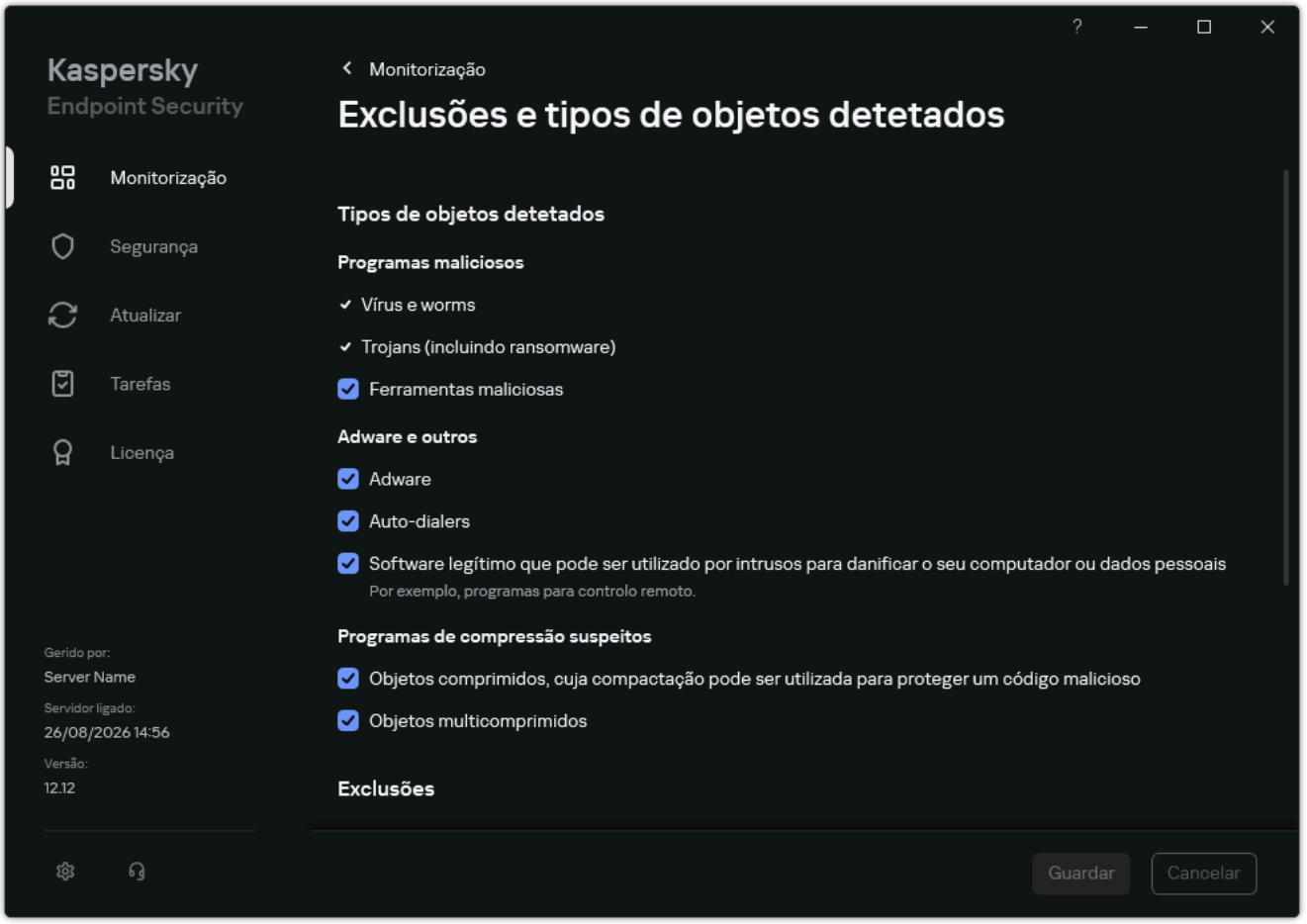
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **Detection Settings**.
5. No bloco **Detection of other types of objects**, selecione as caixas de verificação em frente aos tipos de objetos que pretende que o Kaspersky Endpoint Security detete.
6. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como selecionar tipos de objetos detetáveis na interface da aplicação

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Definições gerais** → **Exclusões e tipos de objetos detetados**.

3. No bloco **Tipos de objetos detetados**, selecione as caixas de verificação em frente aos tipos de objetos que pretende que o Kaspersky Endpoint Security detete.

4. Guarde as suas alterações.



Tipos de objetos detetáveis

Editar a lista de aplicações fiáveis

A *lista de aplicações fiáveis* é uma lista de aplicações cujos ficheiros e atividade de rede (incluindo a atividade maliciosa) e o acesso ao registo do sistema não são monitorizados pelo Kaspersky Endpoint Security. Por predefinição, o Kaspersky Endpoint Security monitoriza objetos que sejam abertos, executados ou guardados por qualquer outro processo da aplicação e controla a atividade de todas as aplicações e tráfego de rede gerado pelos mesmos. Após uma aplicação ter sido adicionada à lista de aplicações fiáveis, o Kaspersky Endpoint Security para de monitorizar a atividade da aplicação.

A diferença entre exclusões de verificação e aplicações confiáveis é que, relativamente às exclusões, o Kaspersky Endpoint Security não verifica ficheiros, enquanto que em relação às aplicações confiáveis, não controla os processos iniciados. Se uma aplicação confiável criar um ficheiro malicioso numa pasta que não esteja incluída nas exclusões de verificação, o Kaspersky Endpoint Security detetará o ficheiro e eliminará a ameaça. Se a pasta for adicionada às exclusões, o Kaspersky Endpoint Security ignorará este ficheiro.

Por exemplo, se considerar como seguros objetos utilizados pela aplicação padrão Bloco de Notas do Microsoft Windows, o que significa que confia nesta aplicação, pode adicionar o Bloco de Notas do Microsoft Windows à lista de aplicações fiáveis para que os objetos utilizados por esta aplicação não sejam monitorizados. Esta ação aumentará o desempenho do computador, o que é especialmente importante quando se utiliza aplicações de servidor.

Além disso, algumas ações classificadas pelo Kaspersky Endpoint Security como suspeitas podem ser seguras no contexto da funcionalidade de um conjunto de aplicações. Por exemplo, a interceção de texto introduzido no teclado é um processo de rotina para alternadores de disposição do teclado (como o Punto Switcher). Para ter em consideração as especificidades destas aplicações e excluir a respetiva atividade da monitorização, recomendamos que adicione estas aplicações à lista de aplicações fiáveis.

As aplicações fiáveis ajudam a evitar problemas de compatibilidade entre o Kaspersky Endpoint Security e outras aplicações (por exemplo, o problema de dupla verificação do tráfego de rede de um computador de terceiros pelo Kaspersky Endpoint Security e por outra aplicação antivírus).

Simultaneamente, continua a ser efetuada a verificação da existência de vírus e outro software malicioso no ficheiro executável e no processo da aplicação fiável. Uma aplicação pode ser totalmente excluída da verificação do Kaspersky Endpoint Security com exclusões de verificação.

Como adicionar um aplicação à lista fiável na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Definições gerais** → **Exclusões e tipos de objetos**.
5. No bloco **Analisar exclusões e aplicações fiáveis** → **Aplicações fiáveis**, clique no botão **Definições**.

   Abre-se uma janela que contém a lista das aplicações fiáveis.
6. Selecione a caixa de verificação **Unir valores ao herdar** se pretender criar uma lista consolidada de aplicações fiáveis para todos os computadores da empresa. As listas de aplicações fiáveis nas políticas principais e secundárias serão unidas. As listas serão unidas, desde que a união de valores ao herdar esteja ativada. As aplicações fiáveis da política principal são apresentadas nas políticas secundárias numa visualização apenas de leitura. Não é possível alterar ou eliminar aplicações fiáveis da política principal.
7. Selecione a caixa de verificação **Permitir a utilização de aplicações fiáveis locais** se pretender permitir que o utilizador crie uma lista local de aplicações fiáveis. Desta forma, um utilizador pode criar a sua própria lista local de aplicações fiáveis, além da lista geral de aplicações fiáveis gerada na política. Um administrador pode usar o Kaspersky Security Center para ver, adicionar, editar ou eliminar itens da lista nas propriedades do computador.

   Se a caixa de verificação estiver desmarcada, o utilizador poderá aceder apenas à lista geral de aplicações fiáveis gerada na política. Além disso, se esta caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security oculta a lista consolidada de aplicações fiáveis na interface de utilizador da aplicação.
8. Clique em **Adicionar** e selecione uma ação:

   - **Categoria**. Pode agrupar aplicações fiáveis em categorias separadas. Para criar uma nova categoria, insira o nome da categoria e adicione, pelo menos, uma aplicação fiável à categoria.
   - **Nova exclusão**. O Kaspersky Endpoint Security adiciona a nova aplicação fiável à raiz de uma lista.
   - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e o System Center Configuration Manager, a aplicação inclui *aplicações fiáveis predefinidas*. Também foram adicionadas aplicações fiáveis predefinidas para suportar a configuração de aplicações em ambientes virtuais Citrix e VMware. Tem de selecionar aplicações fiáveis predefinidas dependendo da finalidade do servidor protegido.
   - **Nova exclusão da categoria selecionada**. Para adicionar uma nova aplicação fiável a uma categoria específica, selecione uma categoria.

9. Selecione os critérios de confiança:

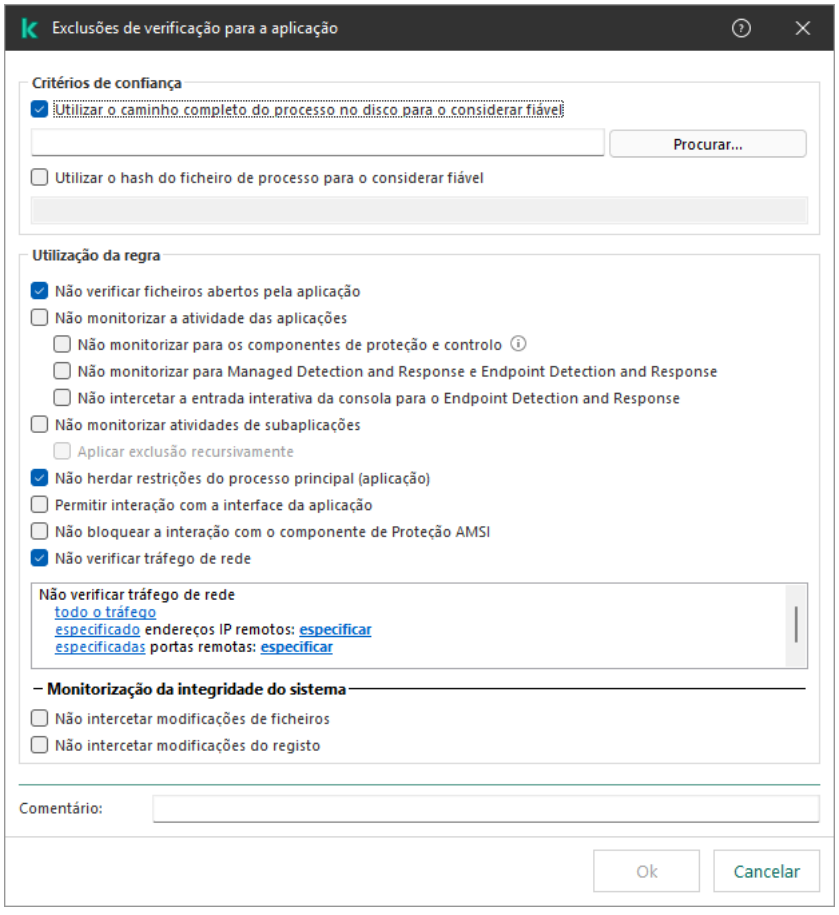
- **Utilizar o caminho completo do processo no disco para o considerar fiável**. Insira o caminho para o ficheiro executável da aplicação fiável.

  O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.

  O Kaspersky Endpoint Security trata o nome do ficheiro de uma aplicação fiável como sensível a maiúsculas e minúsculas. Se o nome do ficheiro introduzido tiver uma letra maiúscula/minúscula errada, o Kaspersky Endpoint Security não reconhecerá a aplicação fiável.

- **Utilizar o hash do ficheiro de processo para o considerar fiável**.

O Kaspersky Endpoint Security não suporta a variável do ambiente `%userprofile%` ao gerar uma lista de aplicações fiáveis na consola do Kaspersky Security Center. Para aplicar a entrada a todas as contas de utilizador, pode utilizar o caractere * (por exemplo, `C:\Users\*\Documents\File.exe`). Sempre que adiciona uma nova variável de ambiente, tem de reiniciar a aplicação.



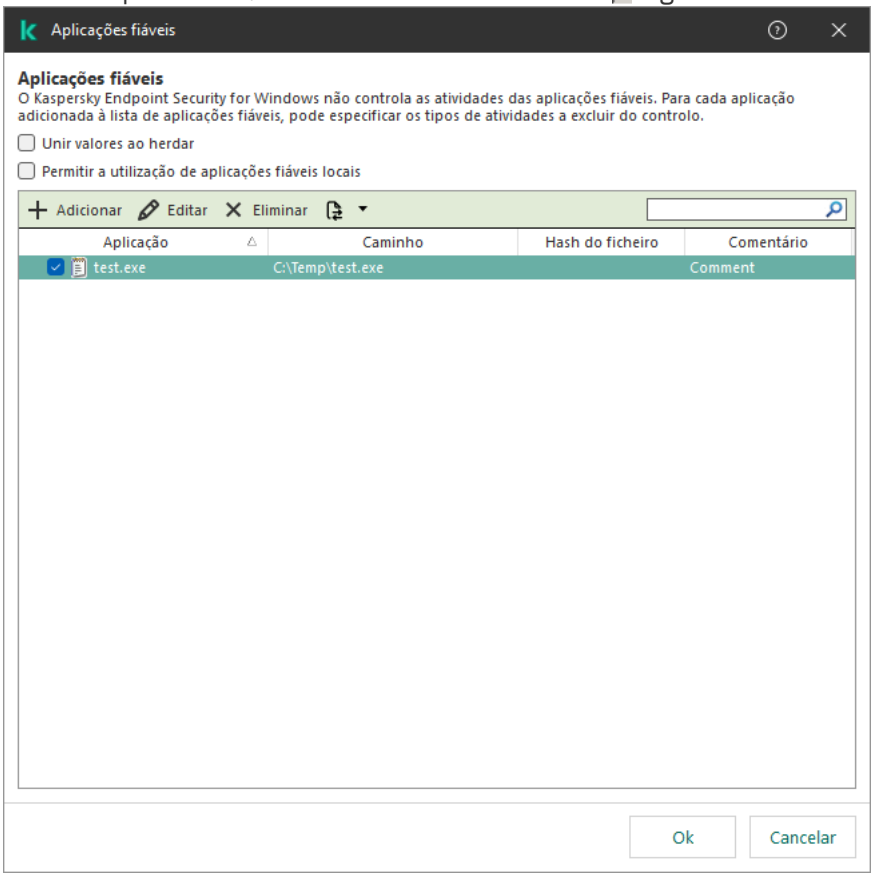
Definições da aplicação fiável

10. Configure as definições avançadas para a aplicação fiável (consulte a tabela abaixo).

11. Clique em **OK**.

    A nova aplicação fiável será adicionada à lista. Pode excluir uma aplicação da zona fiável em qualquer altura, utilizando a caixa de verificação junto ao objeto.

12. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.



A lista de aplicações confiáveis

Como adicionar uma aplicação à lista fiável na Kaspersky Security Center Web Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda à secção **Trusted Zone**.
5. Na janela que abre, clique na ligação **Applications**.

   Abre-se uma janela que contém a lista das aplicações fiáveis.
6. Selecione a caixa de verificação **Merge values when inheriting** se pretender criar uma lista consolidada de aplicações fiáveis para todos os computadores da empresa. As listas de aplicações fiáveis nas políticas principais e secundárias serão unidas. As listas serão unidas, desde que a união de valores ao herdar esteja ativada. As aplicações fiáveis da política principal são apresentadas nas políticas secundárias numa visualização apenas de leitura. Não é possível alterar ou eliminar aplicações fiáveis da política principal.
7. Selecione a caixa de verificação **Allow use of local exclusions** se pretender permitir que o utilizador crie uma lista local de aplicações fiáveis. Desta forma, um utilizador pode criar a sua própria lista local de aplicações fiáveis, além da lista geral de aplicações fiáveis gerada na política. Um administrador pode usar o Kaspersky Security Center para ver, adicionar, editar ou eliminar itens da lista nas propriedades do computador.

   Se a caixa de verificação estiver desmarcada, o utilizador poderá aceder apenas à lista geral de aplicações fiáveis gerada na política. Além disso, se esta caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security oculta a lista consolidada de aplicações fiáveis na interface de utilizador da aplicação.

8. Clique em **Add** e selecione uma ação:

   - **Category**. Pode agrupar aplicações fiáveis em categorias separadas. Para criar uma nova categoria, insira o nome da categoria e adicione, pelo menos, uma aplicação fiável à categoria.
   - **New exclusion**. O Kaspersky Endpoint Security adiciona a nova aplicação fiável à raiz de uma lista.
   - **Select exclusion from list**. Para configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e o System Center Configuration Manager, a aplicação inclui *aplicações fiáveis predefinidas*. Também foram adicionadas aplicações fiáveis predefinidas para suportar a configuração de aplicações em ambientes virtuais Citrix e VMware. Tem de selecionar aplicações fiáveis predefinidas dependendo da finalidade do servidor protegido.

   Para adicionar uma nova aplicação fiável a uma categoria específica, selecione a caixa de verificação ao lado dessa categoria e selecione a opção **New exclusion**.

9. Selecione os critérios de confiança:

   - **Path to the file or folder**. Insira o caminho para o ficheiro executável da aplicação fiável.

     O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.

     O Kaspersky Endpoint Security trata o nome do ficheiro de uma aplicação fiável como sensível a maiúsculas e minúsculas. Se o nome do ficheiro introduzido tiver uma letra maiúscula/minúscula errada, o Kaspersky Endpoint Security não reconhecerá a aplicação fiável.

   - **Application hash**.

   > O Kaspersky Endpoint Security não suporta a variável do ambiente %userprofile% ao gerar uma lista de aplicações fiáveis na consola do Kaspersky Security Center. Para aplicar a entrada a todas as contas de utilizador, pode utilizar o caractere `*` (por exemplo, `C:\Users\*\Documents\File.exe`). Sempre que adiciona uma nova variável de ambiente, tem de reiniciar a aplicação.

10. Configure as definições avançadas para a aplicação fiável (consulte a tabela abaixo).

11. Clique em **OK**.

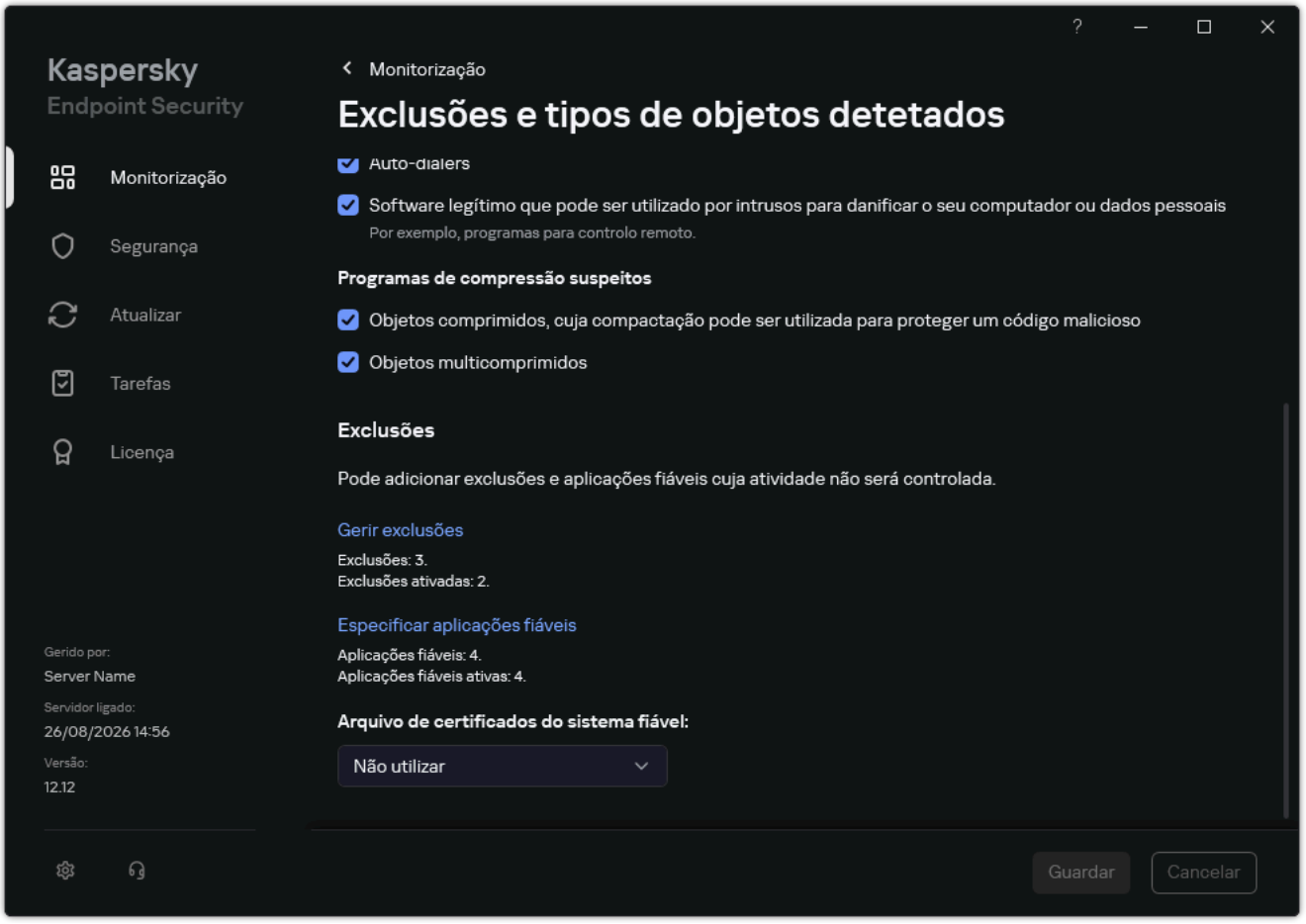
    A nova aplicação fiável será adicionada à lista. Pode excluir uma aplicação da zona fiável em qualquer altura, utilizando a caixa de verificação na coluna **Status**.

12. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como adicionar uma aplicação à lista fiável na interface da aplicação

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Definições gerais → Exclusões e tipos de objetos detetados**.
3. No bloco **Exclusões**, clique na ligação **Especificar aplicações fiáveis**.

O Kaspersky Endpoint Security oculta a lista consolidada de aplicações fiáveis na interface de utilizador da aplicação se a configuração de aplicações fiáveis for bloqueada pelo administrador na consola (símbolo de "cadeado fechado") e se as aplicações fiáveis locais forem proibidas (a caixa de verificação **Permitir a utilização de aplicações fiáveis locais** está desmarcada).



Definições de exclusões

4. Clique em **Adicionar** e selecione uma ação:

   - **Categoria**. Pode agrupar aplicações fiáveis em categorias separadas. Para criar uma nova categoria, insira o nome da categoria e adicione, pelo menos, uma aplicação fiável à categoria.

   - **Nova exclusão**. O Kaspersky Endpoint Security adiciona a nova aplicação fiável à raiz de uma lista.

   - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e o System Center Configuration Manager, a aplicação inclui *aplicações fiáveis predefinidas*. Também foram adicionadas aplicações fiáveis predefinidas para suportar a configuração de aplicações em ambientes virtuais Citrix e VMware. Tem de selecionar aplicações fiáveis predefinidas dependendo da finalidade do servidor protegido.

   Para adicionar uma nova aplicação fiável a uma categoria específica, selecione a caixa de verificação ao lado dessa categoria e selecione a opção **Nova exclusão**.

5. Selecione os critérios de confiança:

   - **Utilizar o caminho completo do processo no disco para o considerar fiável**. Insira o caminho para o ficheiro executável da aplicação fiável.

     O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.

O Kaspersky Endpoint Security trata o nome do ficheiro de uma aplicação fiável como sensível a maiúsculas e minúsculas. Se o nome do ficheiro introduzido tiver uma letra maiúscula/minúscula errada, o Kaspersky Endpoint Security não reconhecerá a aplicação fiável.

- **Utilizar o hash do ficheiro de processo para o considerar fiável**.

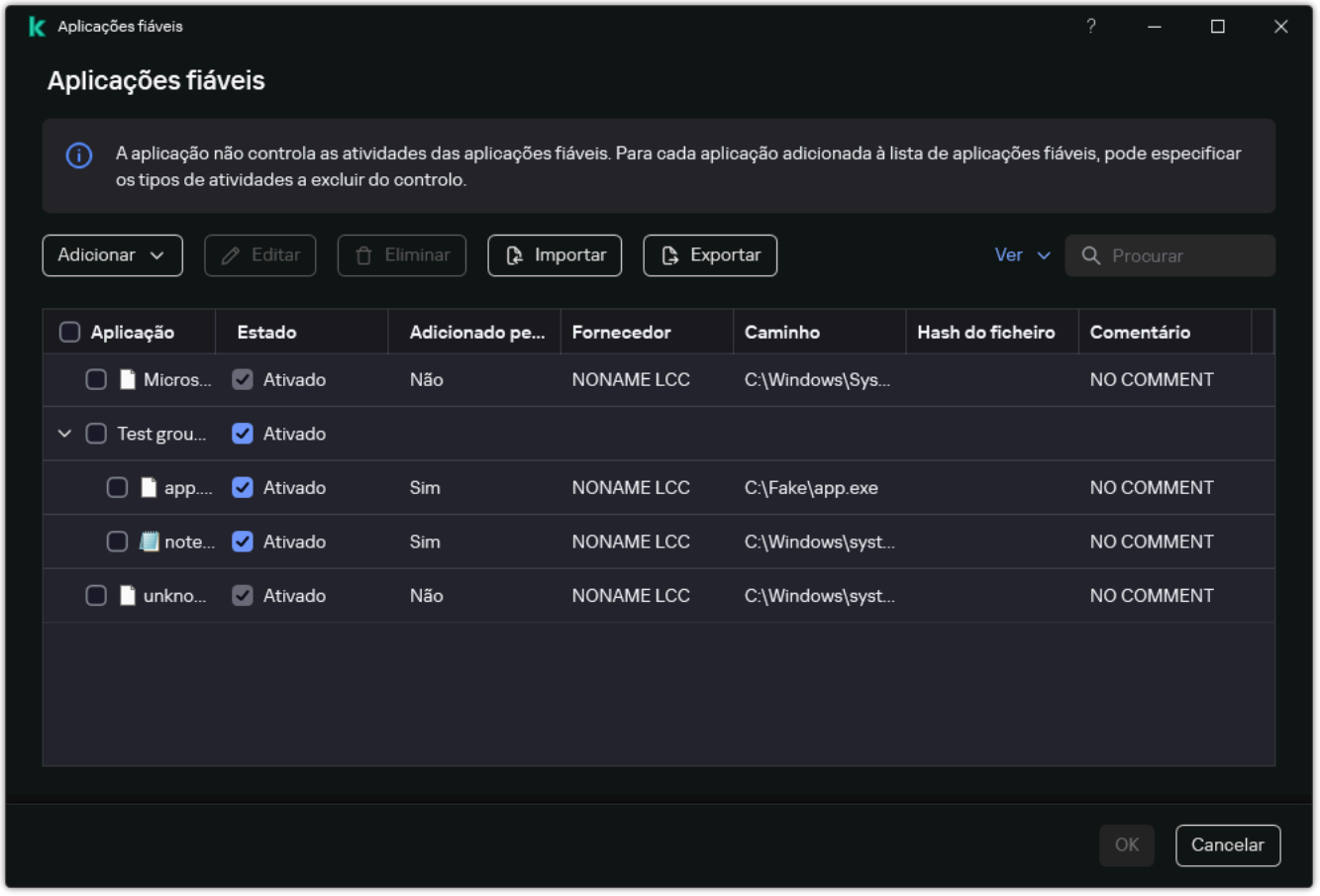
O Kaspersky Endpoint Security suporta variáveis de ambiente e converte o caminho na interface local da aplicação. Por outras palavras, se introduzir o caminho do ficheiro `%userprofile%\Documents\File.exe`, é adicionado um registo `C:\Users\Fred123\Documents\File.exe` na interface local da aplicação para o utilizador Fred123. Por conseguinte, o Kaspersky Endpoint Security ignora o programa fiável `File.exe` para outros utilizadores. Para aplicar a entrada a todas as contas de utilizador, pode utilizar o caractere `*` (por exemplo, `C:\Users\*\Documents\File.exe`). Sempre que adiciona uma nova variável de ambiente, tem de reiniciar a aplicação.

6. Na janela de propriedades da aplicação confiável, configure as definições avançadas.

7. Clique em **OK**.

   A nova aplicação fiável será adicionada à lista. Pode excluir uma aplicação da zona fiável em qualquer altura, utilizando a caixa de verificação na coluna **Estado**.

8. Guarde as suas alterações.



A lista de aplicações confiáveis

Parâmetro	Descrição
Não verificar ficheiros abertos pela aplicação	Todos os ficheiros abertos pela aplicação são excluídos das verificações do Kaspersky Endpoint Security. Por exemplo, se estiver a utilizar aplicações para fazer cópias de segurança de ficheiros, esta funcionalidade ajuda a reduzir o consumo de recursos pelo Kaspersky Endpoint Security.
Não monitorizar a atividade da aplicação	O Kaspersky Endpoint Security não monitoriza a atividade dos ficheiros e da rede da aplicação no sistema operativo. Pode configurar a monitorização da atividade da aplicação para diferentes componentes do Kaspersky Endpoint Security: • **Não monitorizar para os componentes de proteção e controlo**. A atividade da aplicação é monitorizada pelos seguintes componentes: Deteção de comportamento, Prevenção de explorações, Prevenção contra invasões, Motor de remediação e Firewall. • **Não monitorizar o Managed Detection and Response e o Endpoint Detection and Response**. A atividade da aplicação é monitorizada pelo MDR Agent integrado e o EDR (KATA) Agent integrado. • **Não intercetar a entrada interativa da consola para o Endpoint Detection and Response**. O Kaspersky Endpoint Security não envia dados de telemetria sobre a gestão da aplicação na consola. Os dados de telemetria são usados pela Kaspersky Anti Targeted Attack Platform (EDR).
Não monitorizar atividade da aplicação secundária	O Kaspersky Endpoint Security não monitorizará a atividade de ficheiros ou de rede de aplicações iniciadas por esta aplicação. Pode aplicar a exclusão de forma recursiva. Para que a aplicação não monitorize a atividade da cadeia completa de aplicações secundárias.
Não herdar restrições do processo parental (aplicação)	As restrições configuradas para o processo principal não serão aplicadas pelo Kaspersky Endpoint Security a um processo subordinado. O processo principal é iniciado por uma aplicação para a qual os direitos de aplicações (Prevenção contra invasões) e as regras de rede de aplicações (Firewall) estão configurados.
Não monitorizar atividade da aplicação secundária	O Kaspersky Endpoint Security não monitorizará a atividade de ficheiros ou de rede de aplicações iniciadas por esta aplicação. Pode aplicar a exclusão de forma recursiva. Para que a aplicação não monitorize a atividade da cadeia completa de aplicações secundárias.
Permitir interação com a interface da aplicação	A Autodefesa do Kaspersky Endpoint Security bloqueia todas as tentativas de gerir serviços de aplicações a partir de um computador remoto. Se a caixa de verificação estiver selecionada, a aplicação de acesso remoto pode efetuar a gestão das definições do Kaspersky Endpoint Security através da interface do Kaspersky Endpoint Security.
Não bloquear a interação com o componente de Proteção AMSI	O Kaspersky Endpoint Security não monitoriza os pedidos da aplicação fiável para objetos a verificar pelo Componente de proteção AMSI.
Não verificar tráfego de rede	O tráfego de rede iniciado pela aplicação será excluído das verificações do Kaspersky Endpoint Security. Pode excluir todo o tráfego ou apenas o tráfego encriptado das verificações. Também pode excluir endereços IP individuais e números de porta das verificações. A aplicação não suporta a exclusão de tráfego de rede se um hash for especificado para uma aplicação fiável, em vez de um caminho.
Não intercetar modificações de ficheiros *(disponível apenas na Consola do Kaspersky Security Center)*	O Kaspersky Endpoint Security não monitoriza alterações em ficheiros do âmbito de monitorização da Monitorização da integridade do sistema. A aplicação aplica a exclusão a todos os modos de Monitorização da Integridade do Sistema: Monitorização da integridade do sistema em tempo real e Verificação de integridade do sistema mediante pedido.
Não intercetar modificações do registo *(disponível apenas na Consola do Kaspersky Security Center)*	O Kaspersky Endpoint Security não monitoriza alterações nas chaves de registo do âmbito de monitorização da Monitorização da integridade do sistema. A aplicação aplica a exclusão a todos os modos de Monitorização da Integridade do Sistema: Monitorização da integridade do sistema em tempo real e Verificação de integridade do sistema mediante pedido.
Comentário	Se necessário, pode fornecer um breve comentário sobre a aplicação fiável. Os comentários ajudam a simplificar as pesquisas e a classificação das aplicações fiáveis.
Estado	Estado da aplicação fiável: • O estado **Ativo** significa que a aplicação está na zona fiável. • O estado **Inativo** significa que a aplicação foi excluída da zona fiável.

Criar uma zona local fiável

O utilizador pode agora criar a sua própria zona fiável local para um computador específico. Desta forma, os utilizadores podem criar as suas próprias listas locais de exclusões e de aplicações fiáveis, para além da zona fiável geral numa política. Um administrador pode permitir ou bloquear o uso de exclusões locais ou aplicações fiáveis locais nas definições da política. Para o fazer, utilize as caixas de verificação **Permitir a utilização de exclusões locais** e **Permitir a utilização de aplicações fiáveis locais** na secção **Exclusões** da política.

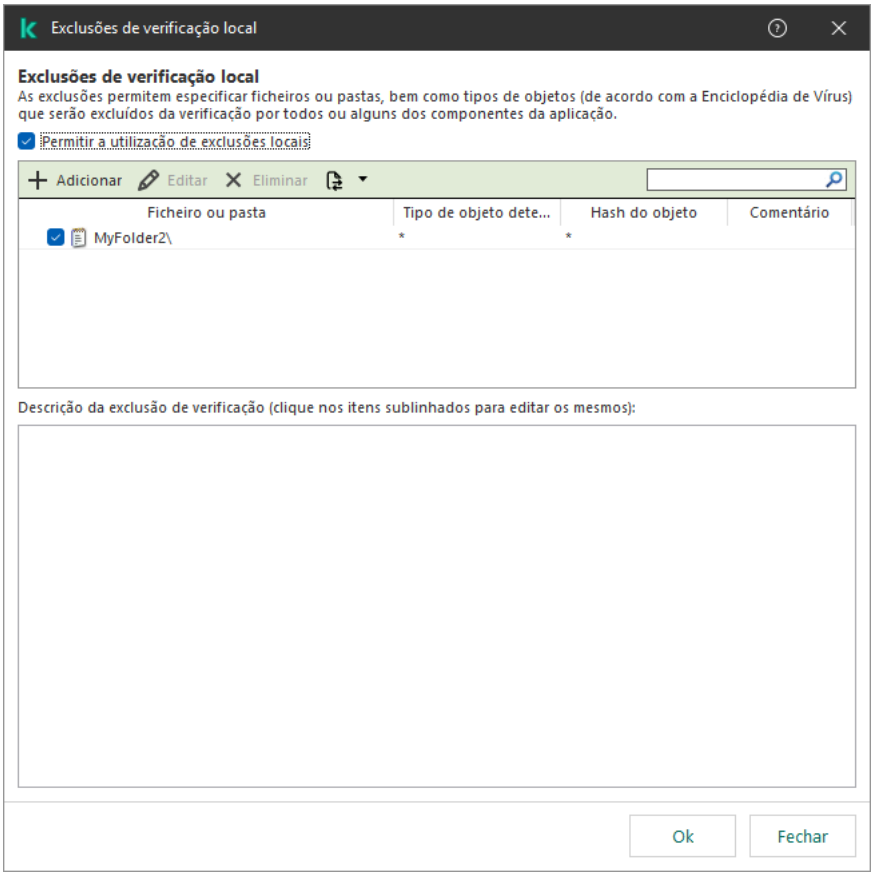
Se a criação de uma zona fiável local for permitida por um administrador, o utilizador poderá adicionar as suas próprias exclusões de verificação e aplicações fiáveis na interface de utilizador da aplicação. Ao mesmo tempo, o utilizador não tem permissão para modificar ou excluir objetos da zona fiável configurada na política. O administrador também pode ver, adicionar, modificar ou excluir itens da lista na consola do Kaspersky Security Center se for necessário adicionar exclusões para um computador individual.

O Kaspersky Endpoint Security oculta as listas de exclusões de verificação e de aplicações fiáveis na interface de utilizador da aplicação se a configuração da zona fiável for bloqueada pelo administrador na consola (símbolo de "cadeado fechado") e se as exclusões de verificação locais e as aplicações fiáveis forem proibidas.

Como adicionar uma aplicação à lista fiável na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Managed devices** da árvore na Consola de Administração, abra a pasta com o nome do grupo de administração ao qual os computadores cliente em questão pertencem.
3. Na área de trabalho, selecione o separador **Devices**.
4. Clique duas vezes para abrir a janela de propriedades do computador.
5. Na janela de propriedades do computador, selecione a secção **Applications**.
6. Na lista de aplicações da Kaspersky instaladas no computador, selecione **Kaspersky Endpoint Security for Windows (14.2)** e clique duas vezes para abrir as propriedades da aplicação.
7. Na janela Application settings, selecione **Definições gerais → Exclusões e tipos de objetos**.
8. No bloco **Analisar exclusões e aplicações fiáveis → Exclusões de verificação local**, clique no botão **Definições**.

É apresentada uma janela que contém uma lista de exclusões.



Definições da Zona fiável

9. Crie uma lista de exclusões de verificação local.

   As regras para criar exclusões de verificação local são iguais às exclusões gerais. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.

10. No bloco **Analisar exclusões e aplicações fiáveis** → **Aplicações fiáveis locais**, clique no botão **Definições**.

    É apresentada uma janela que contém uma lista das aplicações locais fiáveis.

11. Crie uma lista de aplicações locais fiáveis.

    As regras para adicionar aplicações à lista de aplicações locais fiáveis são iguais às regras para adicioná-las à lista geral. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.

12. Guarde as suas alterações.

Como adicionar um objeto à zona local fiável na Kaspersky Security Center Web Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Assets (Devices)**.
2. Clique no nome do computador no qual pretende permitir que um utilizador execute uma ação bloqueada.
3. Selecione o separador **Applications**.
4. Clique em **Kaspersky Endpoint Security for Windows**.

   As definições da aplicação locais são apresentadas.

5. Selecione o separador **Application settings**.

6. Na janela Application settings, selecione **General settings** → **Exclusions and types of detected objects**.
7. No bloco **Scan exclusions and trusted applications**, clique na ligação **Local scan exclusions**.
8. Crie uma lista de exclusões de verificação local.

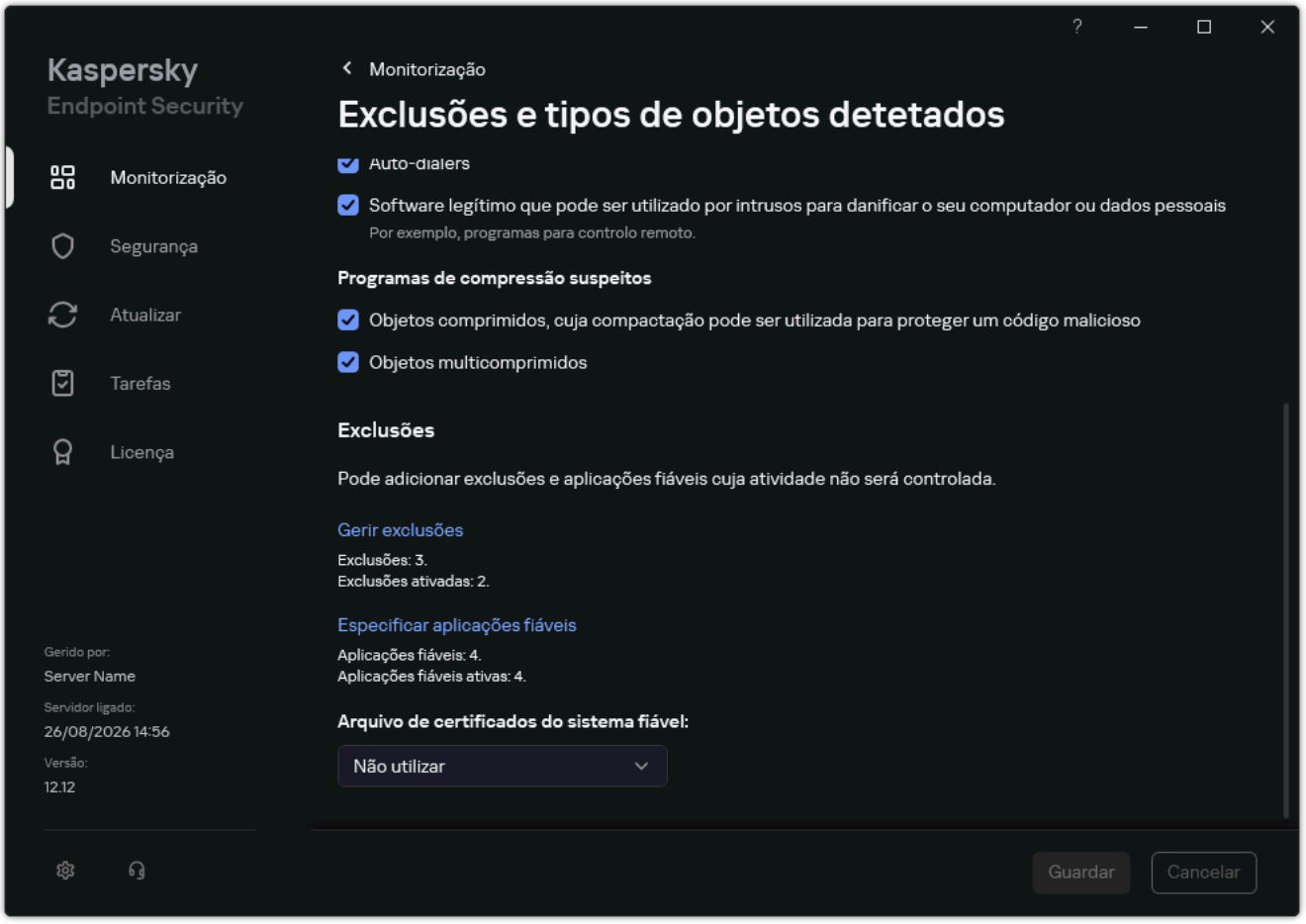
   As regras para criar exclusões locais são iguais às regras para criar exclusões gerais. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres * e ? ao inserir uma máscara.
9. No bloco **Scan exclusions and trusted applications**, clique na ligação **Local trusted applications**.
10. Crie uma lista de aplicações locais fiáveis.

    As regras para adicionar aplicações à lista de aplicações locais fiáveis são iguais às regras para adicioná-las à lista geral. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres * e ? ao inserir uma máscara.
11. Guarde as suas alterações.

Como criar uma exclusão de verificação local na interface da aplicação

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Definições gerais** → **Exclusões e tipos de objetos detetados**.
3. No bloco **Exclusões**, clique na ligação **Gerir exclusões**.

O Kaspersky Endpoint Security oculta a lista de exclusões de verificação na interface de utilizador da aplicação se a configuração de exclusões de verificação for bloqueada pelo administrador na consola (símbolo de "cadeado fechado") e se as exclusões de verificação locais forem proibidas (a caixa de verificação **Permitir a utilização de exclusões locais** está desmarcada).



Definições de exclusões

4. Clique em **Adicionar** e selecione uma ação:

   - **Categoria**. Pode agrupar exclusões de verificação em categorias separadas. Para criar uma nova categoria, insira o nome da categoria e adicione, pelo menos, uma exclusão de verificação à categoria.
   - **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 em servidores SQL, servidores Microsoft Exchange e o System Center Configuration Manager, a aplicação inclui *exclusões de verificação predefinidas*. Também foram adicionadas exclusões de verificação predefinidas para suportar a configuração de aplicações em ambientes virtuais Citrix e VMware. Tem de selecionar exclusões de verificação predefinidas dependendo da finalidade do servidor protegido.

   Para adicionar uma nova exclusão de verificação a uma categoria específica, selecione a caixa de verificação ao lado dessa categoria e selecione a opção **Nova exclusão**.

5. Se quiser excluir um ficheiro ou uma pasta das verificações, selecione o ficheiro ou a pasta clicando no botão **Procurar**.

Também pode introduzir o caminho manualmente. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara:

- O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.

- Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.

- O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.

  Pode utilizar máscaras no início, no meio ou no final do caminho do ficheiro. Por exemplo, se quiser adicionar uma pasta para todos os utilizadores às exclusões, introduza a máscara `?:\Users\*\Folder\`.

  Pode excluir pastas de rede. Para o fazer, insira o caminho para a pasta de rede manualmente (por exemplo, `\\Network Share\*`).

6. Se quiser excluir um tipo específico de objeto das verificações, no campo **Tipo de objeto detetado**, introduza o nome do tipo de objeto de acordo com a classificação da Enciclopédia Kaspersky (por exemplo, `Email-Worm`, `Rootkit` ou `RemoteAdmin`).

   Pode usar máscaras com o caráter `?` (substitui qualquer caráter único) e o caráter `*` (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 quiser excluir um ficheiro individual das verificações, introduza o hash do ficheiro no campo **Hash do objeto**.

   Se o ficheiro for modificado, o hash do ficheiro também será modificado. Se isso acontecer, o ficheiro modificado não será adicionado às exclusões.

8. No bloco **Componentes de proteção**, selecione os componentes aos quais pretende que a exclusão de verificação se aplique.

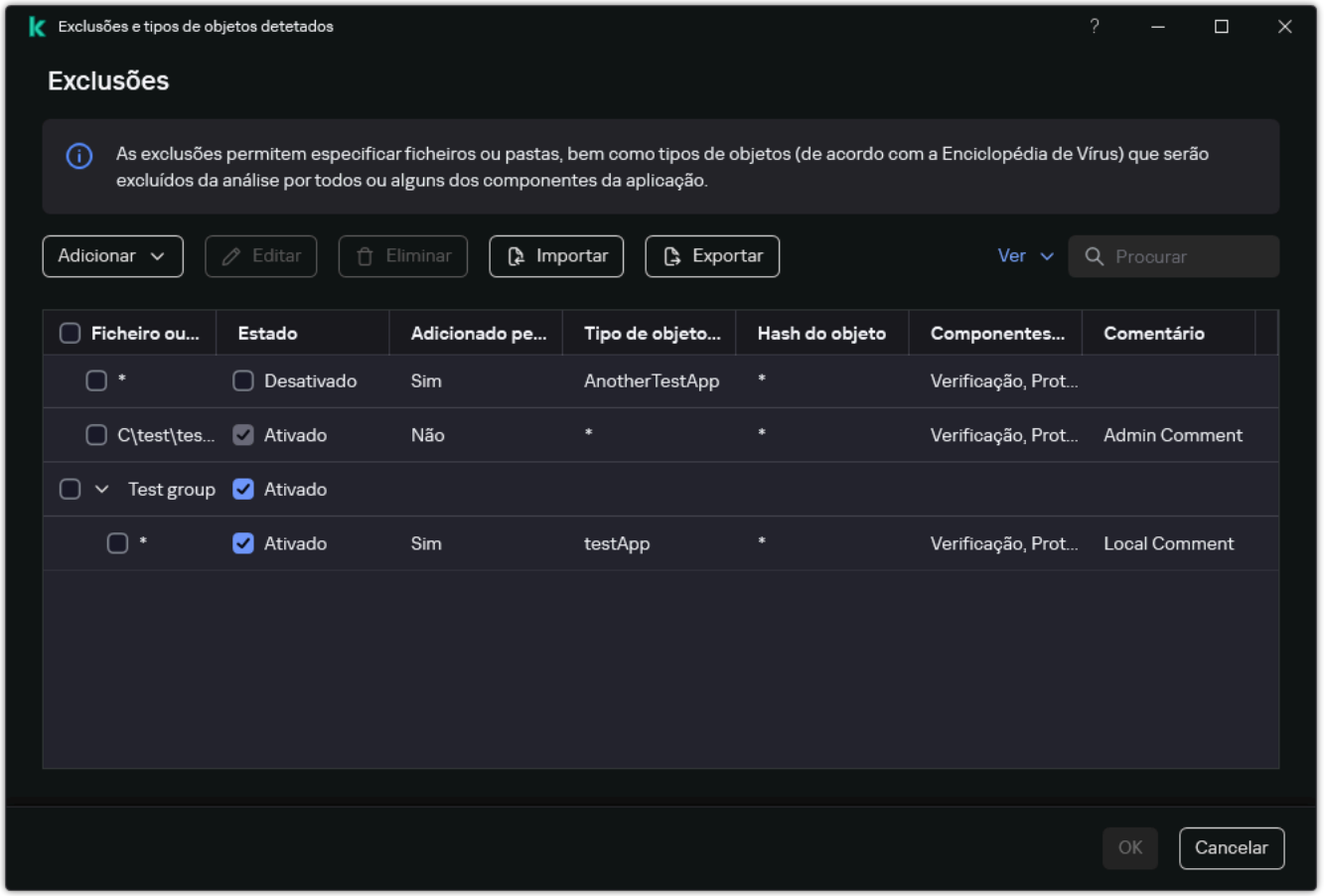
9. Se necessário, no campo **Comentário**, introduza um breve comentário na exclusão de verificação que está a criar.

10. Selecione o estado **Ativo** para a exclusão.

11. Clique em **Adicionar**.

    A nova exclusão será adicionada à lista. Pode desativar a exclusão em qualquer altura utilizando a caixa de verificação na coluna **Estado**.

12. Guarde as suas alterações.

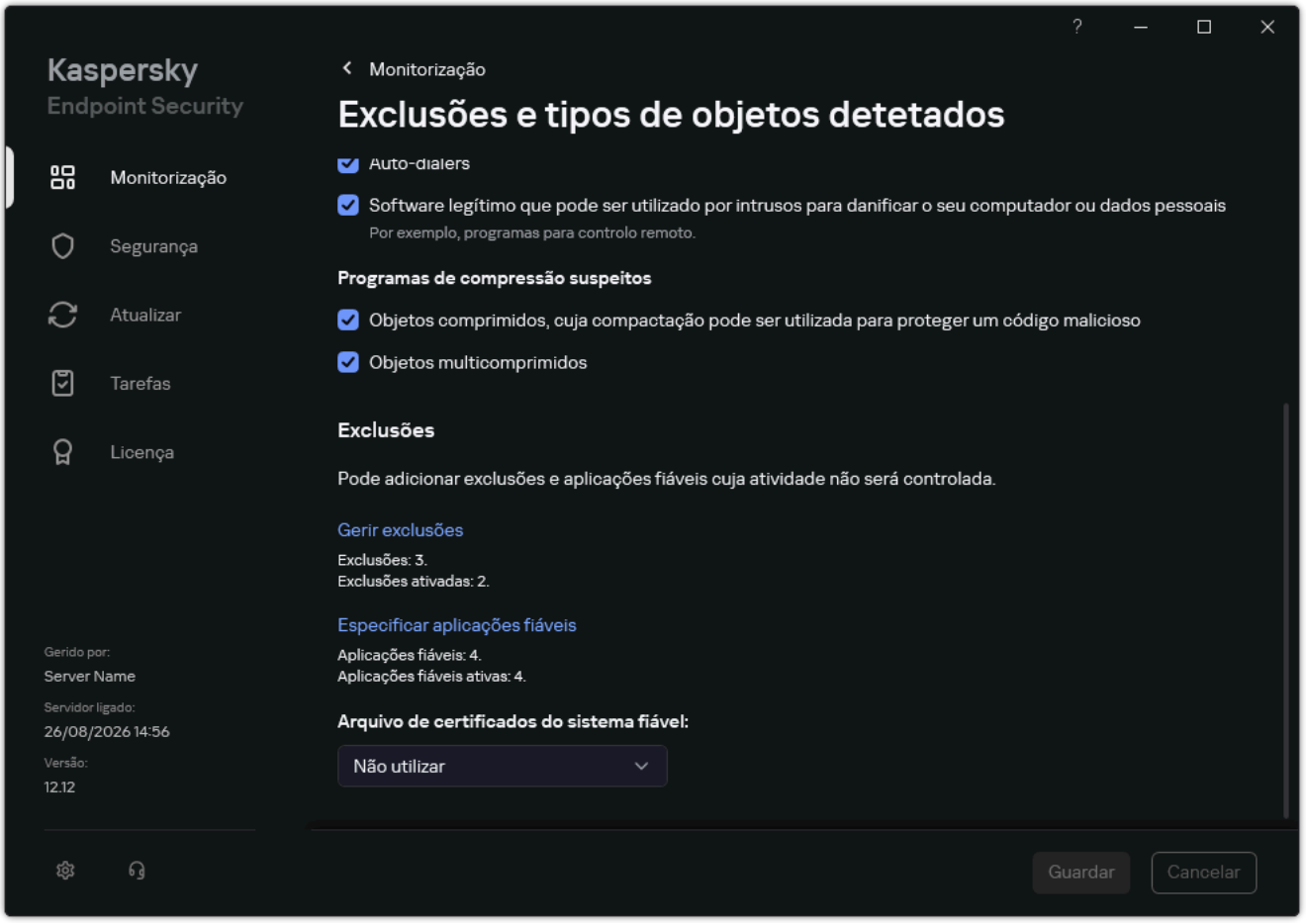


Lista de exclusões

Como adicionar uma aplicação à lista de aplicações locais fiáveis na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais → Exclusões e tipos de objetos detetados**.
3. No bloco **Exclusões**, clique na ligação **Especificar aplicações fiáveis**.

O Kaspersky Endpoint Security oculta a lista consolidada de aplicações fiáveis na interface de utilizador da aplicação se a configuração de aplicações fiáveis for bloqueada pelo administrador na consola (símbolo de "cadeado fechado") e se as aplicações fiáveis locais forem proibidas (a caixa de verificação **Permitir a utilização de aplicações fiáveis locais** está desmarcada).



Definições de exclusões

4. Clique em **Adicionar** e selecione uma ação:

   - **Categoria**. Pode agrupar aplicações fiáveis em categorias separadas. Para criar uma nova categoria, insira o nome da categoria e adicione, pelo menos, uma aplicação fiável à categoria.

   - **Nova exclusão**. O Kaspersky Endpoint Security adiciona a nova aplicação fiável à raiz de uma lista.

   - **Selecionar exclusão da lista**. Para configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e o System Center Configuration Manager, a aplicação inclui *aplicações fiáveis predefinidas*. Também foram adicionadas aplicações fiáveis predefinidas para suportar a configuração de aplicações em ambientes virtuais Citrix e VMware. Tem de selecionar aplicações fiáveis predefinidas dependendo da finalidade do servidor protegido.

   Para adicionar uma nova aplicação fiável a uma categoria específica, selecione a caixa de verificação ao lado dessa categoria e selecione a opção **Nova exclusão**.

5. Selecione os critérios de confiança:

   - **Utilizar o caminho completo do processo no disco para o considerar fiável**. Insira o caminho para o ficheiro executável da aplicação fiável.

     O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.

O Kaspersky Endpoint Security trata o nome do ficheiro de uma aplicação fiável como sensível a maiúsculas e minúsculas. Se o nome do ficheiro introduzido tiver uma letra maiúscula/minúscula errada, o Kaspersky Endpoint Security não reconhecerá a aplicação fiável.

- **Utilizar o hash do ficheiro de processo para o considerar fiável**.

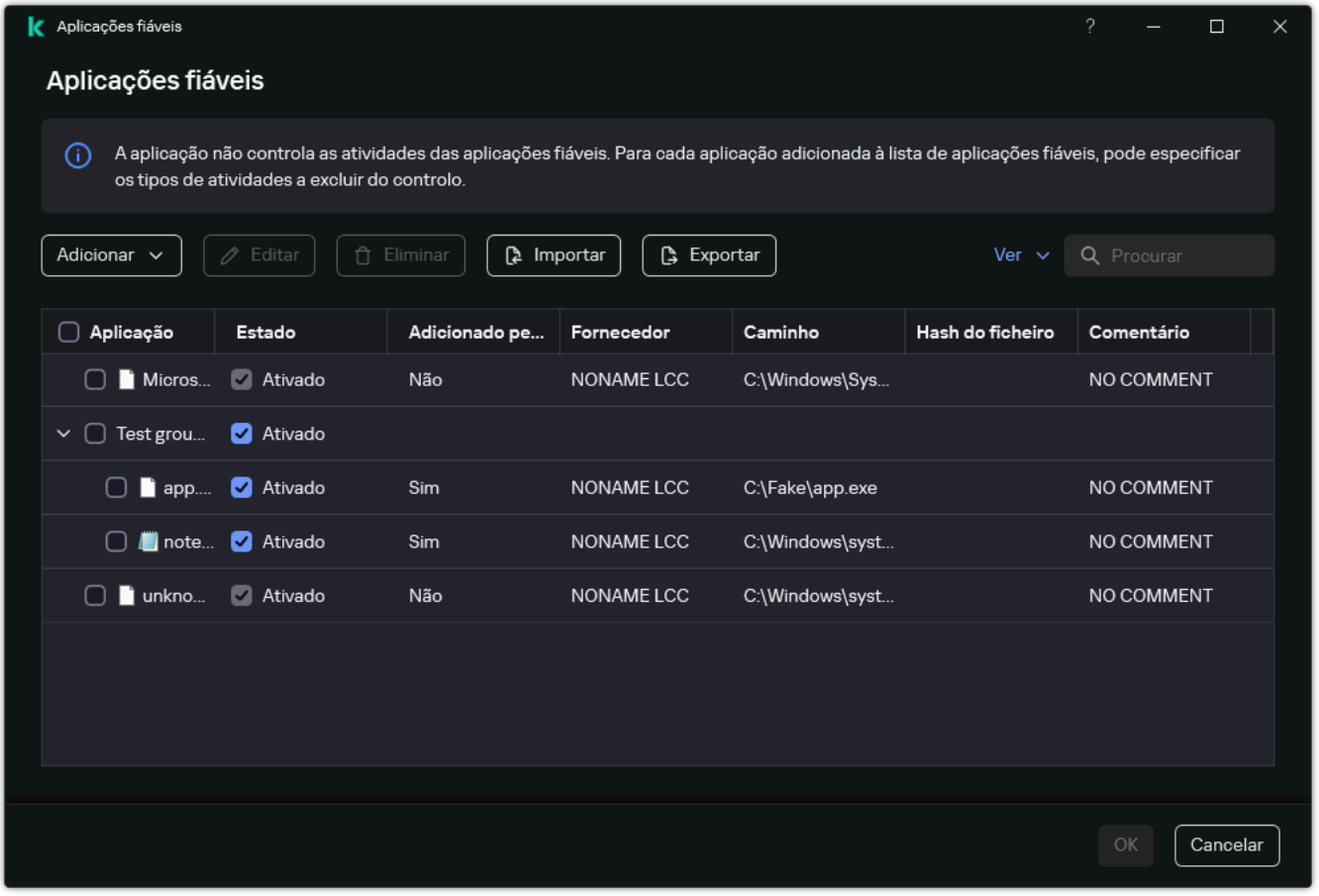
O Kaspersky Endpoint Security suporta variáveis de ambiente e converte o caminho na interface local da aplicação. Por outras palavras, se introduzir o caminho do ficheiro `%userprofile%\Documents\File.exe`, é adicionado um registo `C:\Users\Fred123\Documents\File.exe` na interface local da aplicação para o utilizador Fred123. Por conseguinte, o Kaspersky Endpoint Security ignora o programa fiável `File.exe` para outros utilizadores. Para aplicar a entrada a todas as contas de utilizador, pode utilizar o caractere `*` (por exemplo, `C:\Users\*\Documents\File.exe`). Sempre que adiciona uma nova variável de ambiente, tem de reiniciar a aplicação.

6. Na janela de propriedades da aplicação confiável, configure as definições avançadas.

7. Clique em **OK**.

   A nova aplicação fiável será adicionada à lista. Pode excluir uma aplicação da zona fiável em qualquer altura, utilizando a caixa de verificação na coluna **Estado**.

8. Guarde as suas alterações.



A lista de aplicações confiáveis

Exportar e importar a zona fiável

Uma *zona fiável* consiste numa lista de objetos e aplicações, configurada pelo administrador do sistema, que o Kaspersky Endpoint Security não monitoriza quando está ativo. A zona fiável consiste nas seguintes listas: *exclusões de verificação* e *aplicações fiáveis*. Pode exportar estas listas para ficheiros XML e outros formatos. Em seguida, pode modificar o ficheiro para, por exemplo, adicionar um grande número de exclusões do mesmo tipo. Também pode utilizar a função de exportação/importação para fazer uma cópia de segurança da lista de exclusões e da lista de aplicações fiáveis, ou para migrar as listas para um servidor diferente.

A aplicação utiliza os seguintes formatos para exportar e importar a *lista de exclusões*:

- O XML está disponível na Consola de Administração (MMC), na Consola Web e na Cloud Console.
- O DAT está disponível apenas para importação na Consola de Administração (MMC). O objetivo deste formato é manter a compatibilidade com versões mais antigas da aplicação. Pode converter um ficheiro DAT em XML na Consola de Administração (MMC) para migrar listas de exclusão para a Consola Web.
- O CSV só está disponível na interface local da aplicação.

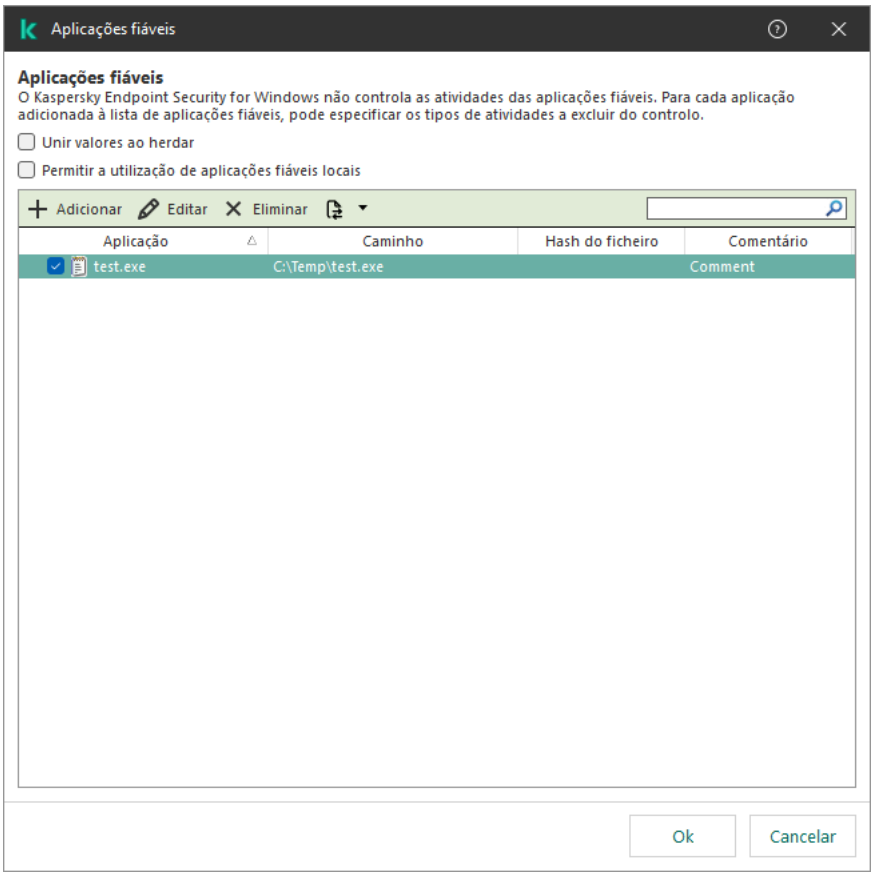
O Kaspersky Endpoint Security utiliza o formato XML para exportar e importar a *lista de aplicações fiáveis*.

Como exportar e importar a zona fiável na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais** → **Exclusões e tipos de objetos**.
4. Sob **Analisar exclusões e aplicações fiáveis**, selecione o componente da zona fiável que deseja exportar ou importar: **Exclusões de verificação** ou **Aplicações fiáveis**.
5. Clique em **Definições**.
6. Para exportar a lista de regras:
   a. Selecione as exclusões que pretende exportar. Para selecionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.
      Se não tiver selecionado nenhuma exclusão, o Kaspersky Endpoint Security exportará todas as exclusões.
   b. Selecione o botão → **Exportar**.
   c. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de exclusões e selecione a pasta onde pretende guardar este ficheiro.

d. Guardar o ficheiro.

O Kaspersky Endpoint Security exporta toda a lista de exclusões para o ficheiro XML. O Kaspersky Endpoint Security também suporta a exportação da lista de exclusões para um ficheiro DAT.



A lista de aplicações confiáveis

7. Para importar a lista de exclusões:

a. Selecione o botão → **Importar**.

b. Na janela que se abre, selecione o ficheiro XML do qual deseja importar a lista de exclusões.

c. Abrir o ficheiro.

Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security irá solicitar-lhe a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro XML. O Kaspersky Endpoint Security também suporta a importação de uma lista de exclusões de um ficheiro DAT.

8. Guarde as suas alterações.

Como exportar ou importar a zona fiável na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.
4. Aceda à secção **Trusted Zone**.

5. Para exportar a lista de regras:

   a. Clique na hiperligação **Malware Scan exclusions**.

   b. Selecione as exclusões que pretende exportar.

   c. Selecione o botão → **Export**.

      O Kaspersky Endpoint Security exporta a lista de exclusões para um ficheiro JSON na pasta de transferências predefinida.

6. Para exportar a lista de aplicações fiáveis:

   a. Selecione as aplicações fiáveis que pretende exportar.

   b. Selecione o botão → **Export**.

      O Kaspersky Endpoint Security exporta a lista de aplicações fiáveis para um ficheiro JSON na pasta de transferências predefinida.

7. Para importar a lista de exclusões:

   a. Clique na hiperligação **Malware Scan exclusions**.

   b. Selecione o botão → **Import**.

      Na janela que se abre, selecione o ficheiro JSON do qual deseja importar a lista de exclusões.

   c. Abrir o ficheiro.

      Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security irá solicitar-lhe a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro JSON.

8. Para importar a lista de aplicações fiáveis:

   a. Clique na hiperligação **Applications**.

   b. Selecione o botão → **Import**.

      Esta ação abre uma janela, onde deve selecionar o ficheiro JSON a partir do qual pretende importar a lista de aplicações fiáveis.

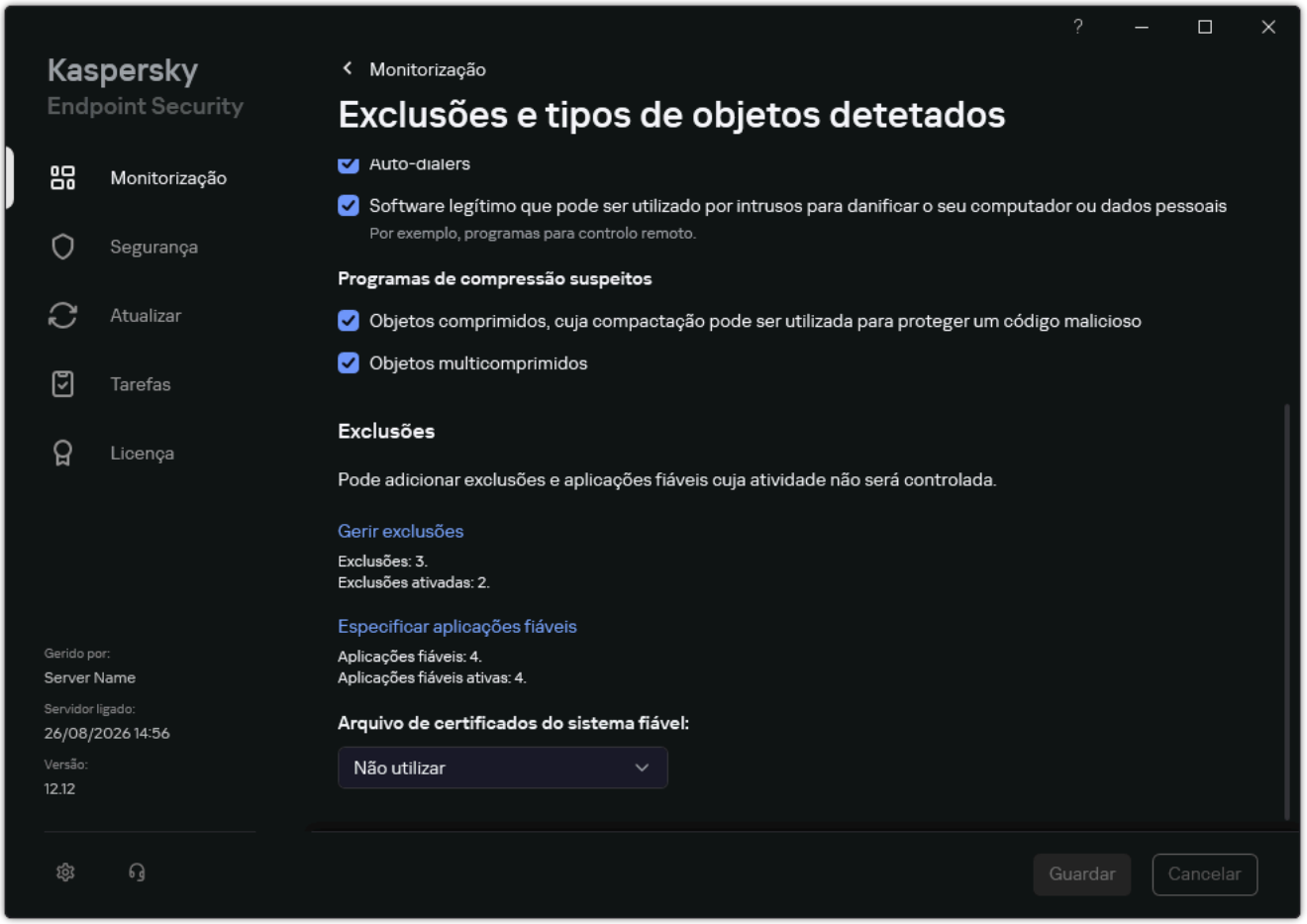
   c. Abrir o ficheiro.

      Se o computador já tiver uma lista de aplicações fiáveis, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas a esta lista a partir do ficheiro JSON.

9. Guarde as suas alterações.

Como exportar ou importar a zona fiável na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais → Exclusões e tipos de objetos detetados**.

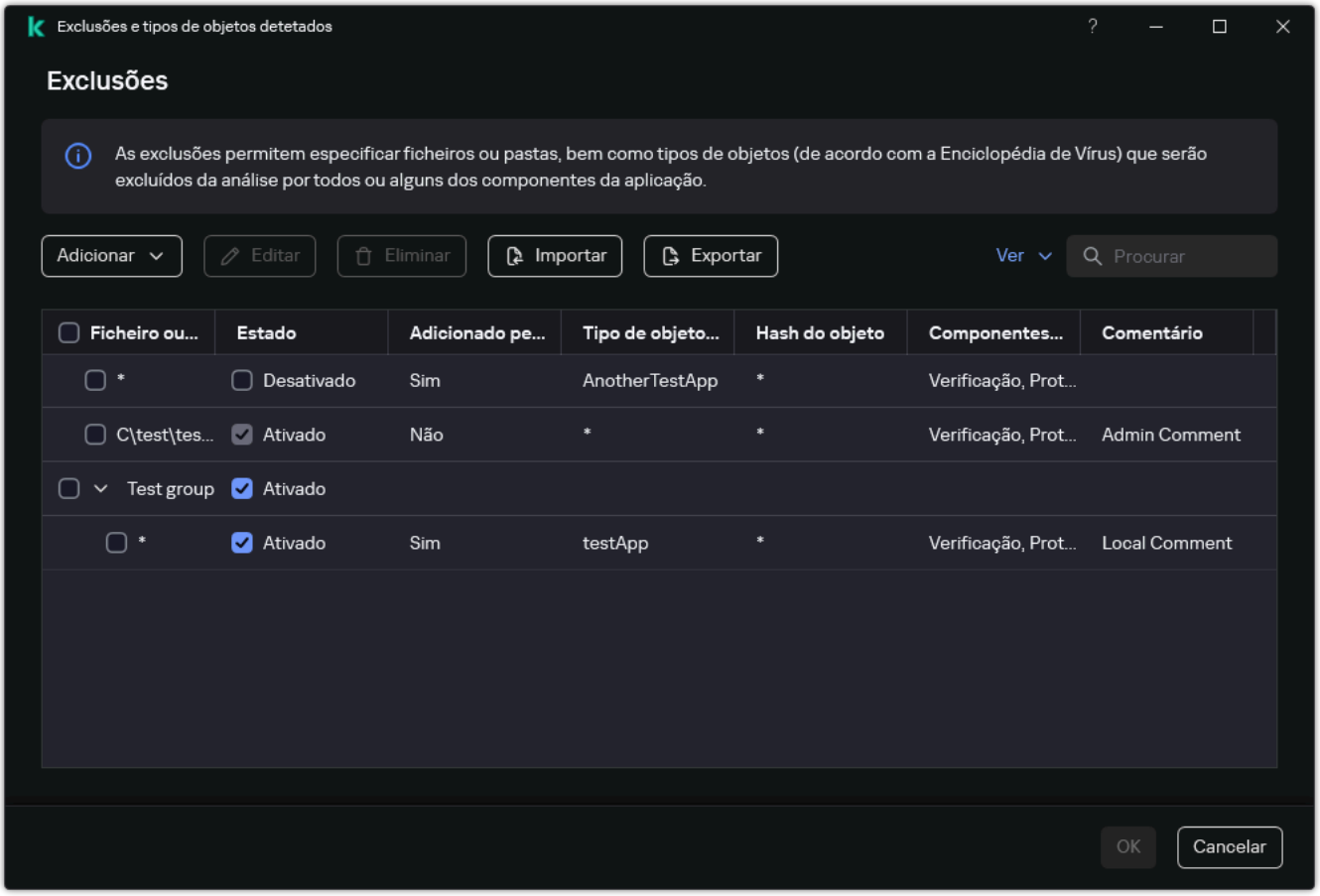


Definições de exclusões

3. Para exportar a lista de regras:
   a. No bloco **Exclusões**, clique na ligação **Gerir exclusões**.
   b. Selecione as exclusões que pretende exportar.
   c. Clique em **Exportar**.
   d. Confirme que quer exportar apenas as exclusões selecionadas ou exportar toda a lista de exclusões.
   e. Na janela que se abre, especifique o nome do ficheiro CSV para o qual pretende exportar a lista de exclusões e selecione a pasta onde pretende guardar este ficheiro.

f. Guardar o ficheiro.

O Kaspersky Endpoint Security exporta toda a lista de exclusões para o ficheiro CSV.



Lista de exclusões

4. Para exportar a lista de aplicações fiáveis:

a. No bloco **Exclusões**, clique na ligação **Especificar aplicações fiáveis**.

b. Selecione as aplicações fiáveis que pretende exportar.

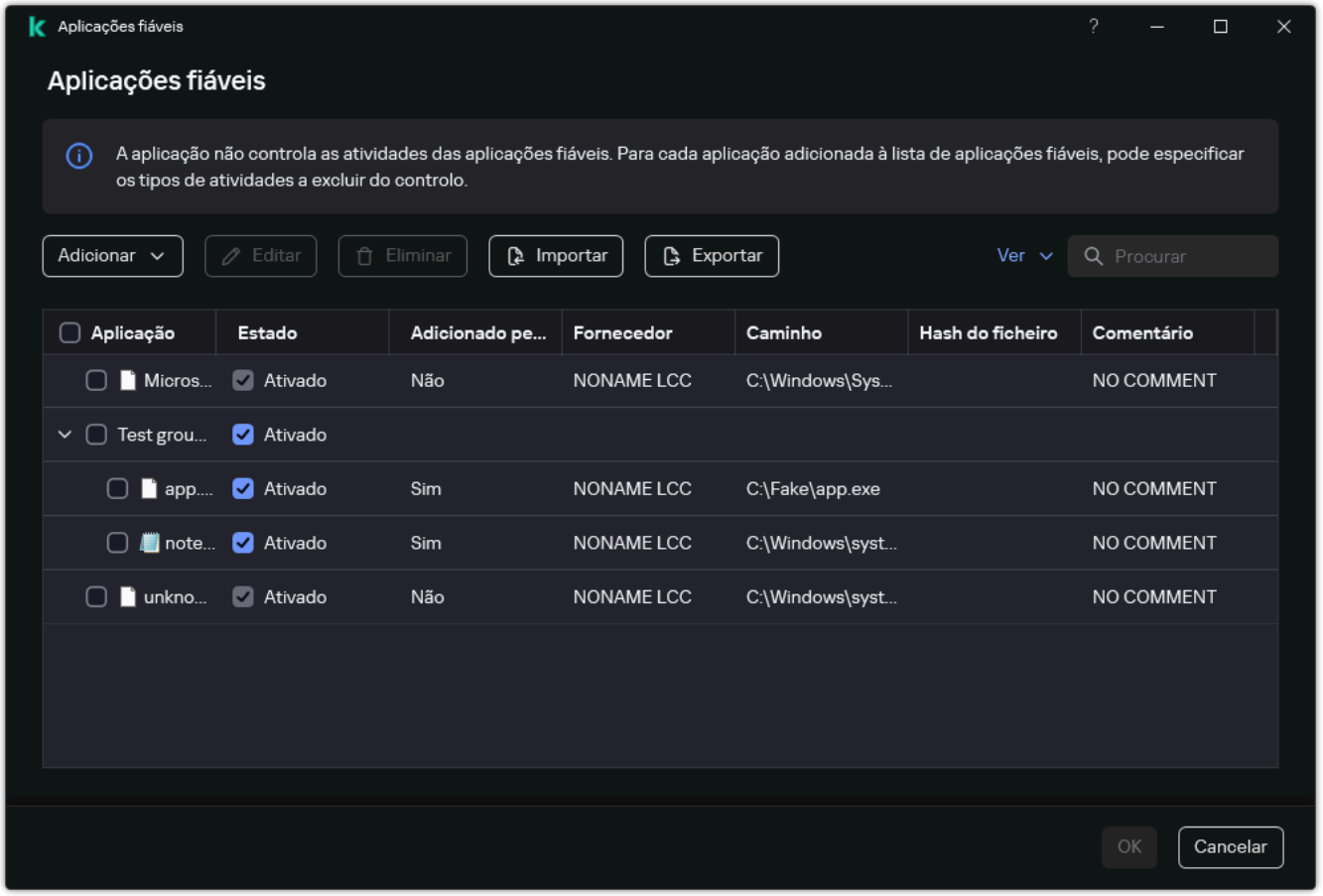
c. Clique em **Exportar**.

d. Confirme que deseja exportar apenas as aplicações fiáveis selecionadas ou exportar a lista inteira.

e. Esta ação abre uma janela, onde deve introduzir o nome do ficheiro XML para o qual pretende exportar a lista de aplicações fiáveis e selecionar a pasta onde pretende guardar este ficheiro.

f. Guardar o ficheiro.

O Kaspersky Endpoint Security exporta toda a lista de aplicações fiáveis para o ficheiro XML.



A lista de aplicações confiáveis

5. Para importar a lista de exclusões:

a. No bloco **Exclusões**, clique na ligação **Gerir exclusões**.

b. Clique em **Importar**.

c. Na janela que se abre, selecione o ficheiro CSV do qual deseja importar a lista de exclusões.

d. Abrir o ficheiro.

Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security irá solicitar-lhe a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro CSV.

6. Para importar a lista de aplicações fiáveis:

a. No bloco **Exclusões**, clique na ligação **Especificar aplicações fiáveis**.

b. Clique em **Importar**.

c. Esta ação abre uma janela, onde deve selecionar o ficheiro XML a partir do qual pretende importar a lista de aplicações fiáveis.

d. Abrir o ficheiro.

Se o computador já tiver uma lista de aplicações fiáveis, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas a esta lista a partir do ficheiro XML.

7. Guarde as suas alterações.

Tratamento de aplicações com uma assinatura digital fiável

A utilização do armazenamento de certificados de sistema permite-lhe excluir aplicações assinadas por uma assinatura digital fiável de verificações de vírus. O Kaspersky Endpoint Security atribui automaticamente essas aplicações ao grupo *Fiáveis*.

Como iniciar a utilização de um armazenamento de certificados de sistema fiável na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais → Exclusões e tipos de objetos**.
4. No bloco **Arquivo de certificados do sistema fiável**, selecione a caixa de verificação **Utilizar arquivo de certificados do sistema fiável**.
5. Na lista pendente, selecione qual o armazenamento do sistema que deve ser considerado fiável pelo Kaspersky Endpoint Security.
6. Guarde as suas alterações.

Como começar a usar um armazenamento de certificados de sistema fiável na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione o separador **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda à secção **Trusted Zone**.
5. Na janela que abre, clique na ligação **Root certificates**.
6. Na janela que abre, selecione a caixa de verificação **Use trusted system certificate store**.
7. Selecione qual o armazenamento do sistema que deve ser considerado fiável pelo Kaspersky Endpoint Security.
8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como iniciar a utilização de um armazenamento de certificados de sistema fiável na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Exclusões e tipos de objetos detetados**.
3. Na lista pendente **Arquivo de certificados do sistema fiável**, selecione qual o armazenamento do sistema que deve ser considerado fiável pelo Kaspersky Endpoint Security.
4. Guarde as suas alterações.

Anexo. Exclusões de verificação predefinidas e aplicações fiáveis

A partir do Kaspersky Endpoint Security 12.6 para Windows, as exclusões de verificação e as aplicações fiáveis são adicionadas à zona fiável. Exclusões de verificação predefinidas e aplicações fiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e System Center Configuration Manager. Isto significa que não é necessário configurar manualmente uma zona fiável para a aplicação nos servidores. A partir do Kaspersky Endpoint Security 12.8 para Windows, pode instalar aplicação no modo Light Agent para proteger ambientes virtuais. As exclusões de verificação predefinidas e as aplicações fiáveis podem ajudá-lo a configurar rapidamente o Kaspersky Endpoint Security em ambientes virtuais Citrix e VMware.

Pode selecionar exclusões predefinidas e aplicações fiáveis das seguintes formas:

- Instalar a aplicação.
  - Instalar a aplicação localmente utilizando o Assistente
  - Propriedades do pacote de instalação
- Definir a política.
  - Novo assistente de políticas
  - Propriedades da política: exclusões de verificação e aplicações fiáveis

Microsoft SQL Server

Ao instalar o Kaspersky Endpoint Security num servidor SQL, tem de criar uma zona fiável a partir de exclusões predefinidas e aplicações fiáveis para garantir que o funcionamento do servidor não sofre interferências.

Exclusões de verificação predefinidas

Caminho	Versão SQL
`%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA\*.mdf`	2012 2014 2016 2017 2019 2022

Caminho	Versão SQL
%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 num servidor Microsoft Exchange, tem de criar uma zona fiável a partir de exclusões predefinidas e aplicações fiáveis para garantir que o funcionamento do servidor não sofre 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
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

Caminho	Versão do Microsoft Exchange
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

Aplicações fiáveis predefinidas

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 operativo do computador protegido, é necessário adicionar uma exclusão predefinida à lista de exclusões de verificação para garantir o funcionamento 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 num ambiente virtual Citrix, tem de criar uma zona fiável a partir de exclusões predefinidas e aplicações fiáveis para garantir que o funcionamento do servidor não sofre interferências.

Exclusões de verificação predefinidas

Caminho
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf

Caminho
%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
*.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

Aplicações fiáveis predefinidas

Caminho	Solução C
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Aplicaçõe ambiente trabalho vi

Caminho	Solução C
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Aplicaçõe ambiente trabalho vi
%SystemRoot%\System32\drivers\CVhdFilter.sys	Aplicaçõe ambiente trabalho vi
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Aplicaçõe ambiente trabalho vi
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Aplicaçõe ambiente trabalho vi

Caminho	Solução C
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Aplicaçõe ambientes trabalho vi
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	Aplicaçã espaço trabalh
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	Aplicaçã espaço trabalh
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	Aplicaçã espaço trabalh
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	Aplicaçã espaço trabalh
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	Aplicaçã espaço trabalh
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	Aplicaçã espaço trabalh
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	Aplicaçã espaço trabalh
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	Aplicaçã espaço trabalh
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	Aplicaçã espaço trabalh
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	Aplicaçã espaço trabalh
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Aprovisiona
%SystemRoot%\System32\drivers\bnistack6.sys	Aprovisiona
%SystemRoot%\System32\drivers\CfsDep2.sys	Aprovisiona
%SystemRoot%\System32\drivers\cnicteam.sys	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Aprovisiona
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Aprovisiona

Caminho	Solução C
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Aprovisiona
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFr
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFr

VMware

Ao instalar o Kaspersky Endpoint Security num ambiente virtual VMware, tem de criar uma zona fiável a partir de aplicações fiáveis predefinidas para garantir que o funcionamento do servidor não sofre interferências.

Aplicações fiáveis predefinidas

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
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

Caminho	Solução VMware
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 operativo Microsoft Windows Server no qual o Kaspersky Endpoint Security está instalado, tem de adicionar uma aplicação fiável predefinida à lista de aplicações fiáveis para otimizar o Kaspersky Endpoint Security e reduzir a carga da CPU.

Aplicações fiáveis predefinidas

Caminho	Versão do Microsoft Windows Server
%SystemRoot%\system32\fsdmhost.exe	Todas as versões suportadas

Gerir Cópias de segurança

A *cópia de segurança* armazena cópias de segurança de ficheiros que foram eliminados ou modificados durante a desinfeção. A *cópia de segurança* é a cópia de um ficheiro criada antes de o ficheiro ser desinfetado ou eliminado. As cópias de segurança dos ficheiros são armazenadas num formato especial e não constituem uma ameaça.

As cópias de segurança de ficheiros são armazenadas na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

Os utilizadores pertencentes aos grupos de administradores obtêm permissões completas de acesso a esta pasta. O utilizador cuja conta foi utilizada para instalar o Kaspersky Endpoint Security recebe direitos de acesso limitado para esta pasta.

O Kaspersky Endpoint Security não disponibiliza a capacidade de configurar as permissões de acesso do utilizador para a realização de cópias de segurança de ficheiros.

Por vezes, não é possível manter a integridade dos ficheiros durante a desinfeção. Se perder acesso, parcial ou totalmente, a informações importantes num ficheiro desinfetado, após a desinfeção, pode tentar recuperar o ficheiro a partir da cópia de segurança para a respetiva pasta original.

Se o Kaspersky Endpoint Security estiver a ser executado sob gestão do Kaspersky Security Center, as cópias de segurança de ficheiros podem ser transmitidas para o Servidor de administração do Kaspersky Security Center. Para obter mais informações sobre a gestão de cópias de segurança de ficheiros no Kaspersky Security Center, consulte o sistema de ajuda do Kaspersky Security Center.

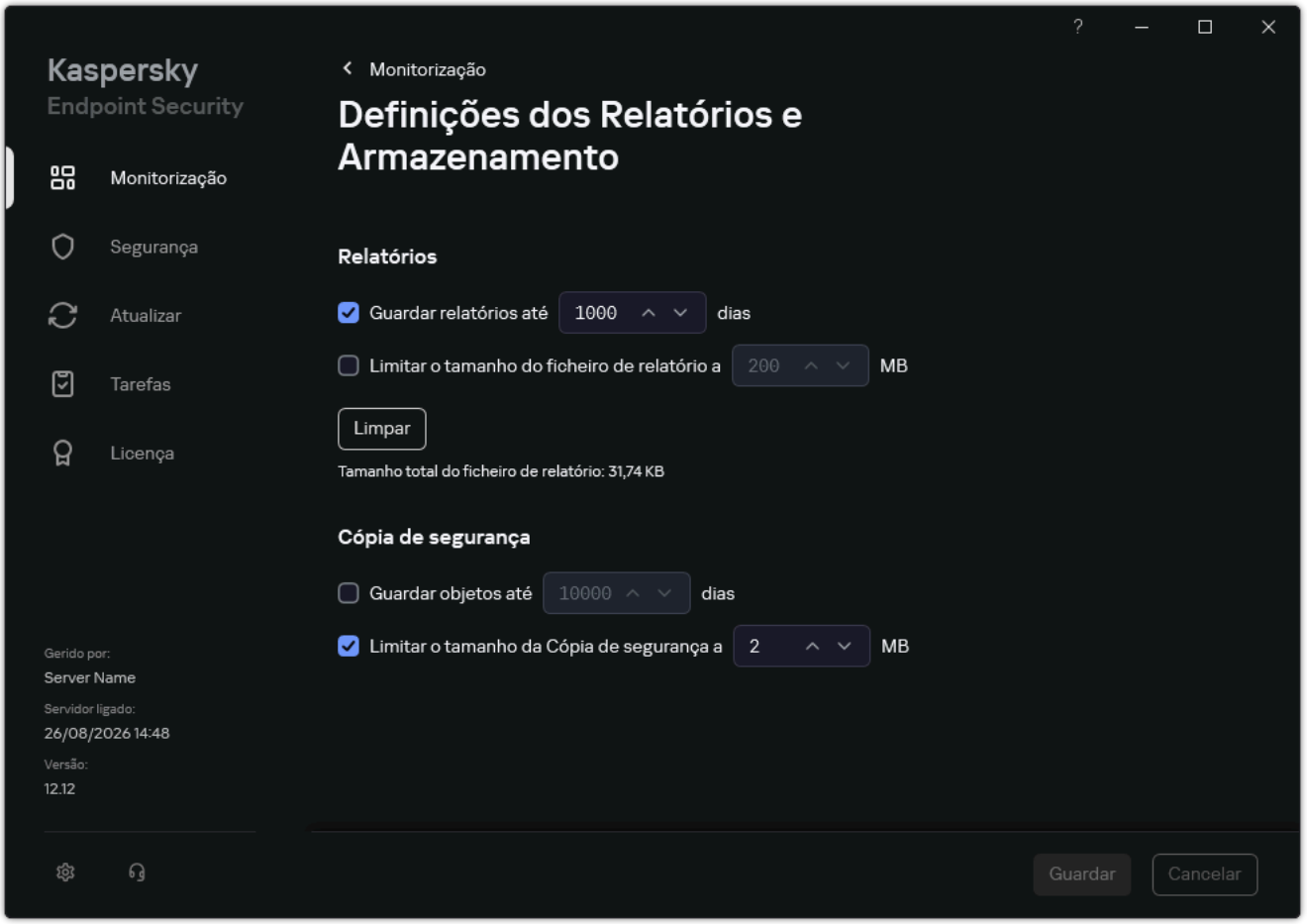
Configurar o período de armazenamento máximo dos ficheiros na Cópia de segurança

O prazo máximo de armazenamento predefinido para as cópias de ficheiros na Cópia de segurança é de 30 dias. Após expirar o prazo máximo de armazenamento, o Kaspersky Endpoint Security elimina os ficheiros mais antigos da Cópia de segurança.

Para configurar o período de armazenamento máximo dos ficheiros na Cópia de segurança:

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela de definições da aplicação, em **Definições gerais** clique no mosaico **Relatórios e armazenamento**.



Definições de cópia de segurança

3. Se quiser limitar o período de armazenamento para cópias de ficheiros em Cópia de Segurança, selecione a caixa de verificação **Guardar objetos até N dias** no bloco **Cópia de segurança**. Introduza a duração de armazenamento máxima para as cópias de ficheiros na Cópia de segurança.

4. Guarde as suas alterações.

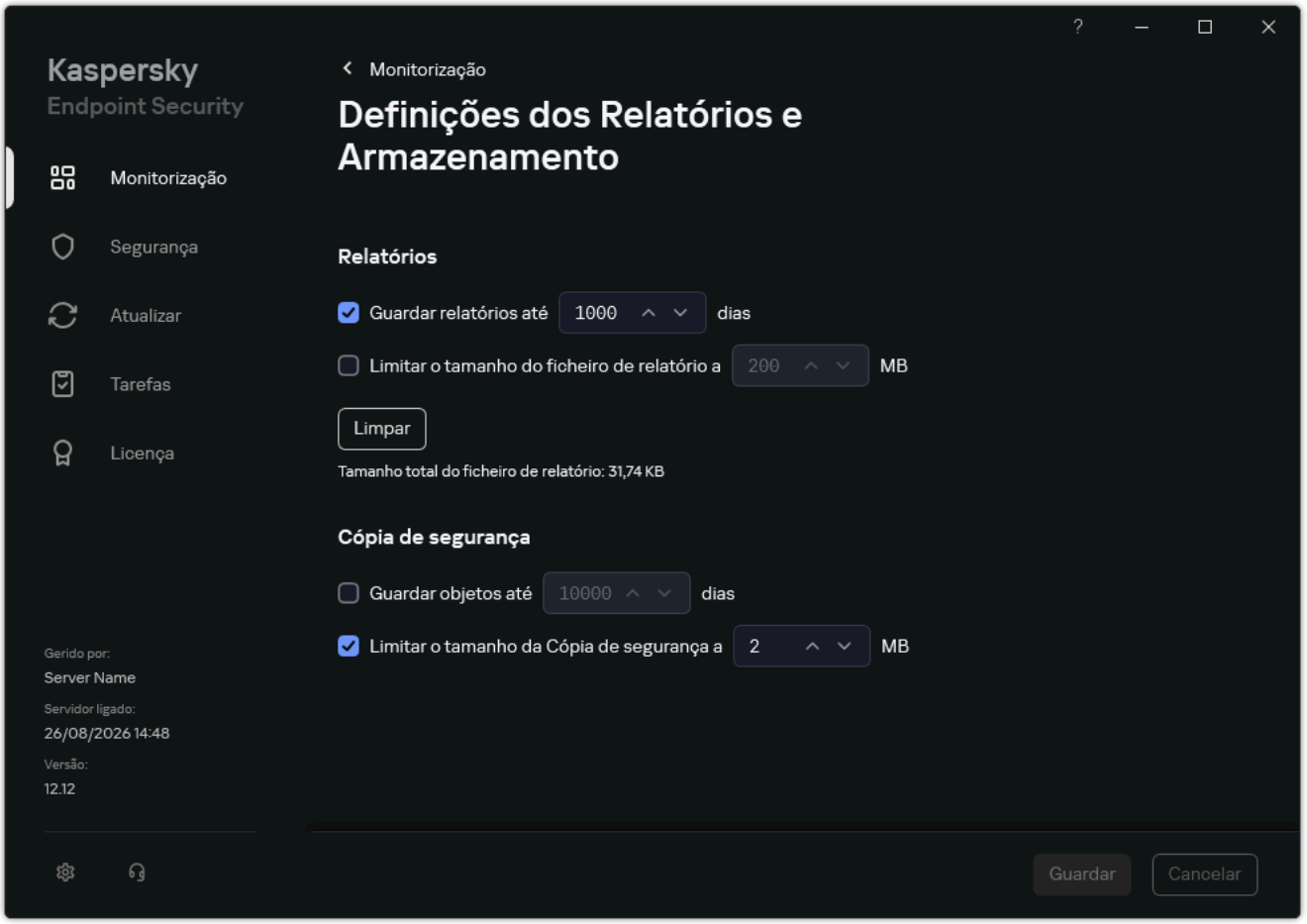
Configure o tamanho máximo da Cópia de segurança

Pode especificar o tamanho máximo da Cópia de Segurança. O tamanho da Cópia de segurança é ilimitado por predefinição. Quando o tamanho máximo é atingido, o Kaspersky Endpoint Security elimina automaticamente os ficheiros mais antigos da Cópia de Segurança.

Para configurar o tamanho máximo da Cópia de segurança:

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela de definições da aplicação, em **Definições gerais** clique no mosaico **Relatórios e armazenamento**.



Definições de cópia de segurança

3. No bloco **Cópia de segurança**, selecione a caixa de verificação **Limitar o tamanho da Cópia de segurança a N MB**. Se a caixa de verificação estiver selecionada, o tamanho máximo de armazenamento será limitado ao valor definido. Por predefinição, o tamanho máximo é de 1024 MB. Para evitar exceder o tamanho máximo de armazenamento, o Kaspersky Endpoint Security elimina automaticamente os ficheiros mais antigos do ficheiro do armazenamento quando o tamanho máximo de armazenamento é atingido.

4. Guarde as suas alterações.

Restaurar ficheiros a partir da Cópia de segurança

Se for detetado código malicioso num ficheiro, o Kaspersky Endpoint Security bloqueia o ficheiro, atribui-lhe o estado de *Não desinfetado*, coloca uma cópia em Cópia de segurança e tenta desinfetá-lo. Se a desinfeção do ficheiro for bem-sucedida, o estado da cópia de segurança do ficheiro é alterado para *Desinfetados*. O ficheiro fica disponível na sua pasta original. Se não for possível desinfetar um ficheiro, o Kaspersky Endpoint Security elimina-o da sua pasta original. Pode restaurar o ficheiro da cópia de segurança para a respetiva pasta original.

As ficheiros com o estado *Será eliminado ao reiniciar o computador* não podem ser restaurados. Reinicie o computador e o estado do ficheiro muda para *Desinfetados* ou *Eliminado*. Pode também restaurar o ficheiro da cópia de segurança para a respetiva pasta original.

Mediante a deteção de código malicioso num ficheiro pertencente à aplicação Windows Store, o Kaspersky Endpoint Security elimina imediatamente o ficheiro sem mover uma cópia do mesmo para a Cópia de Segurança. Pode restaurar a integridade da aplicação da Windows Store ao utilizar as ferramentas adequadas do sistema operativo (consulte os ficheiros de ajuda do Microsoft Windows para obter mais informações sobre a recuperação de uma aplicação da Windows Store).

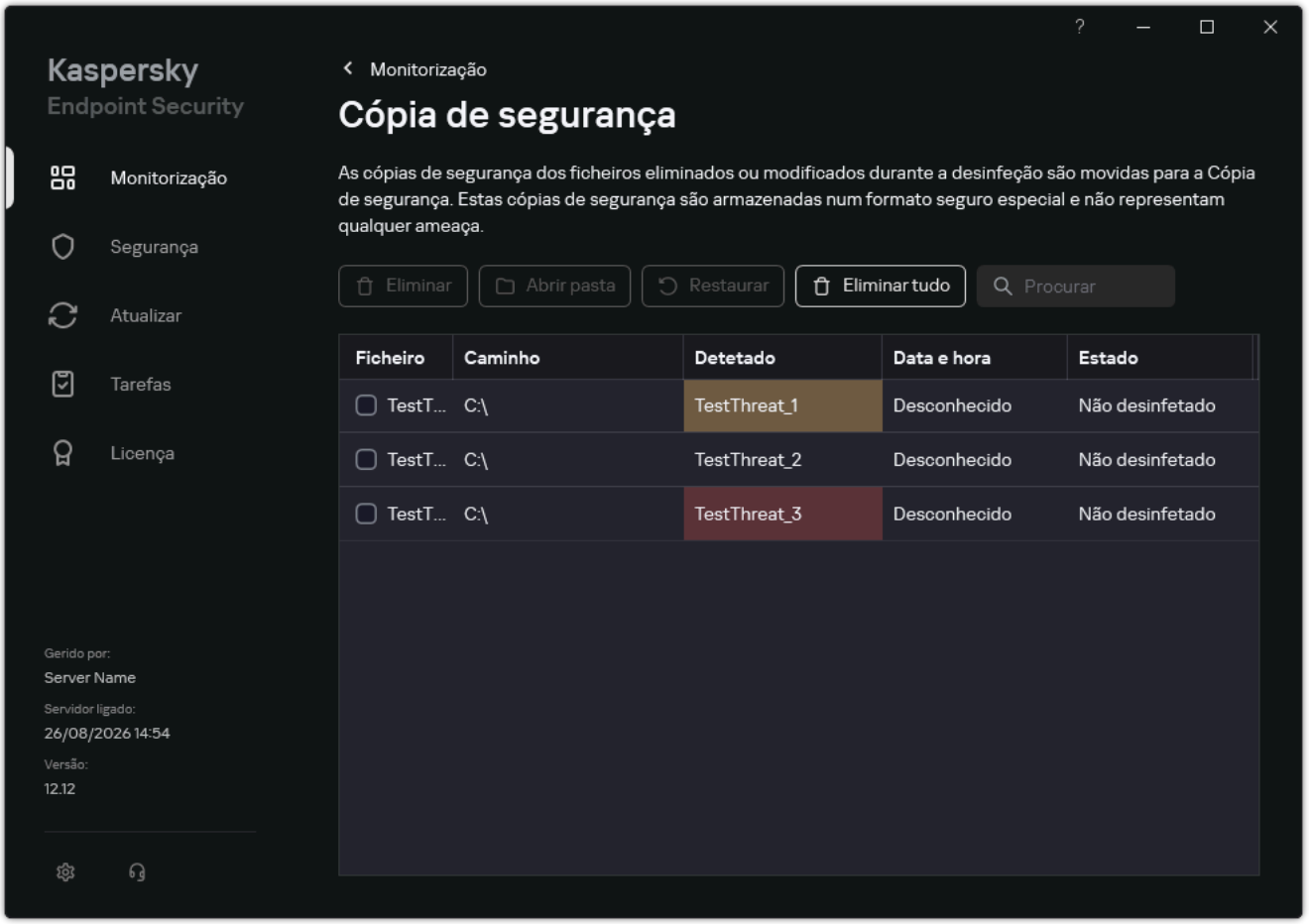
O conjunto de cópias de segurança de ficheiros é apresentado como uma tabela. Para uma cópia de segurança de um ficheiro, é exibido o caminho da pasta original do ficheiro. O caminho da pasta original do ficheiro pode conter dados pessoais.

Se vários ficheiros com nomes idênticos e conteúdos diferentes localizados na mesma pasta forem movidos para a Cópia de segurança, apenas é possível restaurar o último ficheiro que foi colocado na Cópia de segurança.

Para restaurar ficheiros a partir da Cópia de segurança:

1. Na janela principal da aplicação, na secção **Monitorização**, clique em **Cópia de segurança**.
2. Esta ação abre a lista de ficheiros na Cópia de Segurança; nessa lista, selecione os ficheiros que deseja restaurar e clique em **Restaurar**.

O Kaspersky Endpoint Security restaura os ficheiros a partir das cópias de segurança selecionadas para as respetivas pastas originais.



Cópia de segurança

Apagar cópias de segurança de ficheiros da Cópia de segurança

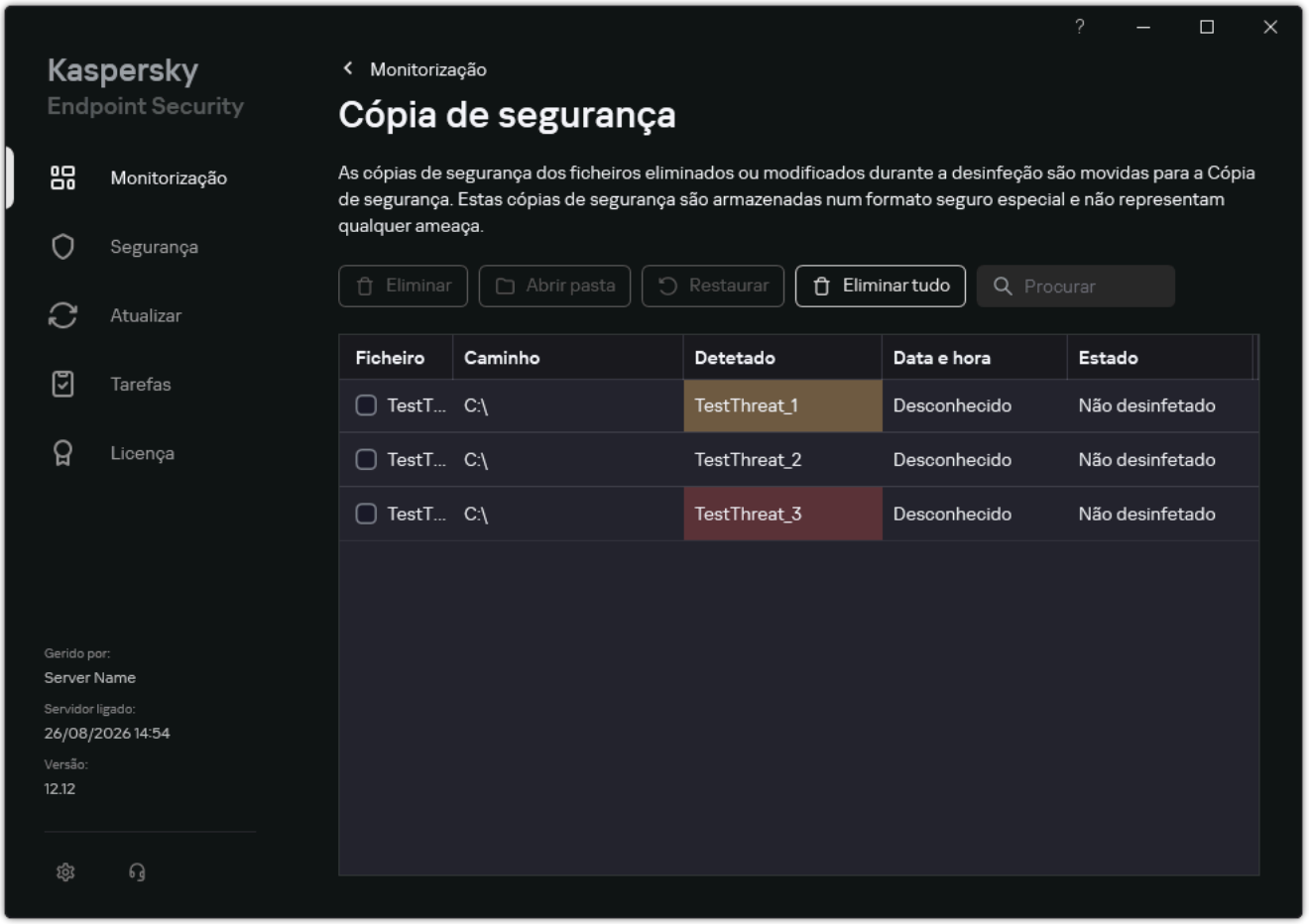
O Kaspersky Endpoint Security elimina automaticamente as cópias de segurança dos ficheiros com qualquer estado da Cópia de segurança, após o prazo de armazenamento configurado nas definições da aplicação ter terminado. Também pode eliminar manualmente qualquer cópia de um ficheiro da Cópia de segurança.

Para apagar cópias de segurança de ficheiros da Cópia de segurança:

1. Na janela principal da aplicação, na secção **Monitorização**, clique em **Cópia de segurança**.

2. Esta ação abre a lista de ficheiros na Cópia de Segurança; nessa lista, selecione os ficheiros que deseja eliminar da Cópia de Segurança e clique em **Eliminar**.

O Kaspersky Endpoint Security elimina as cópias de segurança selecionadas dos ficheiros da Cópia de segurança.



Cópia de segurança

Serviço de notificação

Todos os tipos de eventos decorrem durante o funcionamento do Kaspersky Endpoint Security. As notificações destes eventos podem ser puramente informativas ou conter informações críticas. Por exemplo, as notificações podem informar sobre uma atualização de base de dados e de módulos de aplicação bem-sucedida ou registar os erros de componentes que têm de ser corrigidos.

O Kaspersky Endpoint Security apoia o registo de informações sobre eventos no funcionamento do registo de aplicações do Microsoft Windows e/ou o registo de eventos do Kaspersky Endpoint Security.

O Kaspersky Endpoint Security disponibiliza notificações das seguintes formas:

- ao utilizar notificações pop-up na área de notificação da barra de tarefas do Microsoft Windows;
- por e-mail.

Pode configurar o envio das notificações de eventos. O método de envio da notificação é configurado para cada tipo de evento.

Quando utilizar a tabela de eventos para configurar o serviço de notificações, pode executar as seguintes ações:

- Filtrar eventos do serviço de notificação pelos valores das colunas ou utilizando condições de filtro personalizadas.
- Utilizar a função de procurar para eventos do serviço de notificações.
- Ordenar os eventos do serviço de notificações.
- Alterar a ordem e definir as colunas apresentadas na lista de eventos do serviço de notificações.

Configurar as definições do registo de eventos

Para configurar as definições do registo de eventos:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Interface**.
3. No bloco **Notificações**, clique no botão **Configurar notificações**.

   Os componentes e as tarefas do Kaspersky Endpoint Security são apresentados na parte esquerda da janela. Na parte direita da janela são apresentados os eventos gerados para a tarefa ou componente selecionado.

   Os eventos podem conter os seguintes dados do utilizador:

   - Caminhos para ficheiros verificados pelo Kaspersky Endpoint Security.
   - Caminhos para chaves de registo modificadas durante o funcionamento do Kaspersky Endpoint Security.

- Nome de utilizador do Microsoft Windows.
- Endereços de páginas da Internet abertas pelo utilizador.

4. Na secção esquerda da janela, selecione a tarefa ou componente para o qual pretende configurar as definições de registo de eventos.
5. Selecione as caixas de verificação junto aos eventos pretendidos nas colunas **Guardar no relatório local** e **Guardar no Registo de Eventos do Windows**.

   Os eventos cujas caixas de verificação estão selecionadas na coluna **Guardar no relatório local** são apresentados nos registos da aplicação. Os eventos que têm uma caixa de verificação na coluna **Guardar no Registo de Eventos do Windows** selecionada são apresentados em Registos do Windows no canal `Application`.
6. Guarde as suas alterações.

Configurar a apresentação e o envio de notificações

Para configurar a apresentação e o envio de notificações:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Interface**.
3. No bloco **Notificações**, clique no botão **Configurar notificações**.

   Os componentes e as tarefas do Kaspersky Endpoint Security são apresentados na parte esquerda da janela. Na parte direita da janela são apresentados os eventos gerados para a tarefa ou componente selecionado.

   Os eventos podem conter os seguintes dados do utilizador:

   - Caminhos para ficheiros verificados pelo Kaspersky Endpoint Security.
   - Caminhos para chaves de registo modificadas durante o funcionamento do Kaspersky Endpoint Security.
   - Nome de utilizador do Microsoft Windows.
   - Endereços de páginas da Internet abertas pelo utilizador.
4. Na parte esquerda da janela, selecione a tarefa ou o componente para o qual pretende configurar o envio de notificações.
5. Na coluna **Notificar no ecrã**, selecione as caixas de verificação junto aos eventos relevantes.

   As informações sobre os eventos selecionados são apresentadas no ecrã como mensagens de pop-up na área de notificação da barra de tarefas do Microsoft Windows.
6. Na coluna **Notificar por e-mail**, selecione as caixas de verificação junto aos eventos relevantes.

   As informações sobre os eventos selecionados são enviadas por e-mail se as definições de envio de notificações por e-mail estiverem configuradas.
7. Clique em **OK**.

8. Se ativou as notificações por e-mail, configure as definições para entrega de e-mail:

    a. Clique em **Configurar notificações por e-mail**.

    b. Selecione a caixa de verificação **Notificar sobre eventos** para ativar a entrega de informações sobre os eventos do Kaspersky Endpoint Security selecionados na coluna **Notificar por e-mail**.

    c. Especifique as definições de entrega de notificações por e-mail.

    d. Clique em **OK**.

9. Guarde as suas alterações.

Configurar a apresentação de avisos sobre o estado da aplicação na área de notificação

Para configurar a apresentação de avisos de estado da aplicação na área de notificação:

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Definições gerais** → **Interface**.

3. No bloco **Mostrar o estado da aplicação na área de notificações**, selecione as caixas de verificação à frente das categorias de eventos sobre os quais pretende ver as notificações na área de notificação do Microsoft Windows.

4. Guarde as suas alterações.

Quando os eventos associados às categorias selecionadas ocorrerem, o ícone de aplicação na área de notificação será alterado para ou dependendo da gravidade do aviso.

Mensagens entre utilizadores e o administrador

Os componentes Controlo das Aplicações, Controlo de Dispositivos, Controlo de Internet e Controlo de Anomalias Adaptativo permitem que os utilizadores da rede local tenham o Kaspersky Endpoint Security instalado para enviar mensagens ao administrador.

Poderá ser necessário um utilizador enviar uma mensagem ao administrador local da rede da empresa nos seguintes casos:

- O Controlo de Dispositivos bloqueou o acesso ao dispositivo.

  O modelo de mensagem de um pedido para aceder a um dispositivo bloqueado está disponível na interface do Kaspersky Endpoint Security na secção Controlo de Dispositivos.

- O Controlo das Aplicações bloqueou o arranque de uma aplicação.

  O modelo de mensagem de um pedido para permitir o arranque de uma aplicação bloqueada está disponível na interface do Kaspersky Endpoint Security, na secção Controlo das Aplicações.

- Acesso bloqueado do Controlo de Internet a um recurso da Internet.

  O modelo de mensagem de um pedido para aceder a um recurso da Internet está disponível na interface do Kaspersky Endpoint Security na secção Controlo de Internet.

O método usado para enviar mensagens e o modelo utilizado depende da existência ou não de uma política do Kaspersky Security Center ativa em funcionamento no computador que tem o Kaspersky Endpoint Security instalado e da existência de uma ligação com Servidor de Administração do Kaspersky Security Center. São possíveis os seguintes cenários:

- Se não estiver em execução uma política do Kaspersky Security Center no computador que tem o Kaspersky Endpoint Security instalado, é enviada por e-mail uma mensagem do utilizador ao administrador da rede local.

  Os campos de mensagem estão preenchidos com valores de campos do modelo definidos na interface local do Kaspersky Endpoint Security.

- Se estiver em execução uma política do Kaspersky Security Center no computador que tem o Kaspersky Endpoint Security instalado, é enviada a mensagem padrão para o Servidor de Administração do Kaspersky Security Center.

  Neste caso, as mensagens do utilizador estão disponíveis para visualização no armazenamento de eventos do Kaspersky Security Center (consulte as instruções abaixo). Os campos de mensagem estão preenchidos com os valores dos campos do modelo definidos na política do Kaspersky Security Center.

- Se estiver em funcionamento uma política de ausência do escritório do Kaspersky Security Center no computador com Kaspersky Endpoint Security instalado, o método utilizado para envio de mensagens depende da existência de uma ligação ao Kaspersky Security Center.

  - Se for estabelecida uma ligação com o Kaspersky Security Center, o Kaspersky Endpoint Security envia a mensagem padrão ao Servidor de Administração do Kaspersky Security Center.

  - Se estiver ausente uma ligação com o Kaspersky Security Center, a mensagem do utilizador é enviada ao administrador de rede local através de e-mail.

  Em ambos os casos, os campos de mensagem estão preenchidos com os valores dos campos do modelo definidos na política do Kaspersky Security Center.

Para visualizar uma mensagem de utilizador no armazenamento de eventos do Kaspersky Security Center:

1. Abra a Consola de Administração do Kaspersky Security Center.

2. No nó **Administration Server** da árvore da Consola de Administração, selecione o separador **Events**.

   A área de trabalho do Kaspersky Security Center apresenta todos os eventos que ocorrem durante o funcionamento do Kaspersky Endpoint Security, incluindo as mensagens para o administrador recebidas pelos utilizadores na rede local.

3. Para configurar o filtro de eventos, na lista pendente **Event selections**, selecione **User requests**.

4. Selecione a mensagem enviada ao administrador.

5. Clicar no botão **Open event properties window** na parte direita da área de trabalho da Consola de Administração.

Gerir relatórios

As informações sobre o funcionamento de cada componente do Kaspersky Endpoint Security, eventos de encriptação de dados, o desempenho de cada tarefa de verificação, tarefa de atualização e tarefa de verificação de integridade, bem como sobre o funcionamento geral da aplicação, são registadas nos relatórios.

Os relatórios são armazenados na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\Report`.

Os relatórios podem conter os seguintes dados do utilizador:

- Caminhos para ficheiros verificados pelo Kaspersky Endpoint Security.
- Caminhos para chaves de registo modificadas durante o funcionamento do Kaspersky Endpoint Security.
- Nome de utilizador do Microsoft Windows.
- Endereços de páginas da Internet abertas pelo utilizador.

Os dados no relatório são apresentados em forma tabular. Cada linha da tabela contém informações sobre um evento em separado. Os atributos do evento encontram-se nas colunas da tabela. Algumas colunas são colunas compostas que contêm colunas imbricadas com atributos adicionais. Para visualizar os atributos adicionais, clique no botão ⊞ junto ao nome da coluna. Os eventos registados durante o funcionamento de vários componentes ou durante o desempenho de várias tarefas têm diferentes conjuntos de atributos.

Estão disponíveis os seguintes relatórios:

- Relatório de **Auditoria do sistema**. Contém informações sobre eventos que ocorrem durante a interação entre o utilizador e a aplicação e durante o funcionamento geral da aplicação, sem relação com quaisquer tarefas ou componentes específicos do Kaspersky Endpoint Security.
- Relatórios sobre o funcionamento dos componentes do Kaspersky Endpoint Security.
- Relatórios de tarefas do Kaspersky Endpoint Security.
- Relatório de **Encriptação de dados**. Contém determinadas informações relativas a eventos que ocorrem durante a encriptação de dados e a desencriptação.

Os relatórios usam os seguintes níveis de importância de eventos:

ⓘ **Mensagens informativas**. Eventos de referência que normalmente não contêm informações importantes.

⚠ **Avisos**. Eventos que necessitam da sua atenção, dado que refletem situações importantes no funcionamento do Kaspersky Endpoint Security.

⓪ **Eventos críticos**. Eventos de importância crítica que indicam problemas no funcionamento do Kaspersky Endpoint Security ou vulnerabilidades na proteção do computador do utilizador.

Para um processamento conveniente de relatórios, pode modificar a apresentação de dados no ecrã utilizando os seguintes métodos:

- Filtrar a lista de eventos segundo diversos critérios.
- Utilizar a função de procura para encontrar um evento específico.
- Ver o evento selecionado numa secção em separado.
- Ordenar a lista de eventos por cada coluna de relatório.
- Apresentar e ocultar eventos agrupados pelo filtro de eventos utilizando o botão ⊞.
- Alterar a ordem e disposição das colunas apresentadas no relatório.

Se necessário, pode guardar um relatório gerado num ficheiro de texto. É também possível apagar informações do relatório sobre componentes e tarefas do Kaspersky Endpoint Security combinadas em grupos.

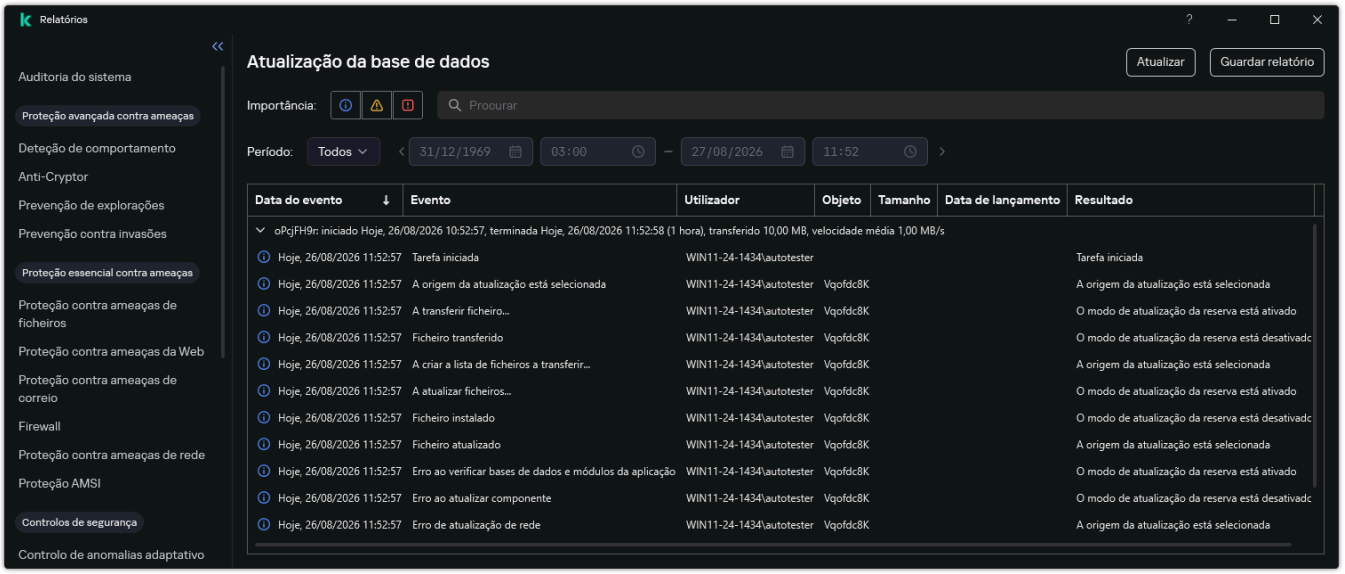
Se o Kaspersky Endpoint Security estiver a ser executado sob gestão do Kaspersky Security Center, informação sobre eventos pode ser transmitida para o Servidor de Administração do Kaspersky Security Center (para obter informação adicional, consulte o Ajuda do Kaspersky Security Center).

Visualizar relatórios

Se o utilizador puder ver relatórios, este também pode visualizar todos os eventos mencionados nos relatórios.

Para visualizar os relatórios:

1. Na janela principal da aplicação, na secção **Monitorização**, clique em **Relatórios**.



Relatórios

2. Na lista de componentes e tarefas, selecione um componente ou tarefa.

   A parte direita da janela exibe um relatório com uma lista de eventos resultante da utilização do componente selecionado ou da tarefa selecionada do Kaspersky Endpoint Security. Pode ordenar os eventos no relatório com base nos valores das células de uma das colunas.

3. Para ver informações detalhadas sobre um evento, selecione o evento no relatório.

É apresentado um bloco com o resumo de evento na parte de baixo da janela.

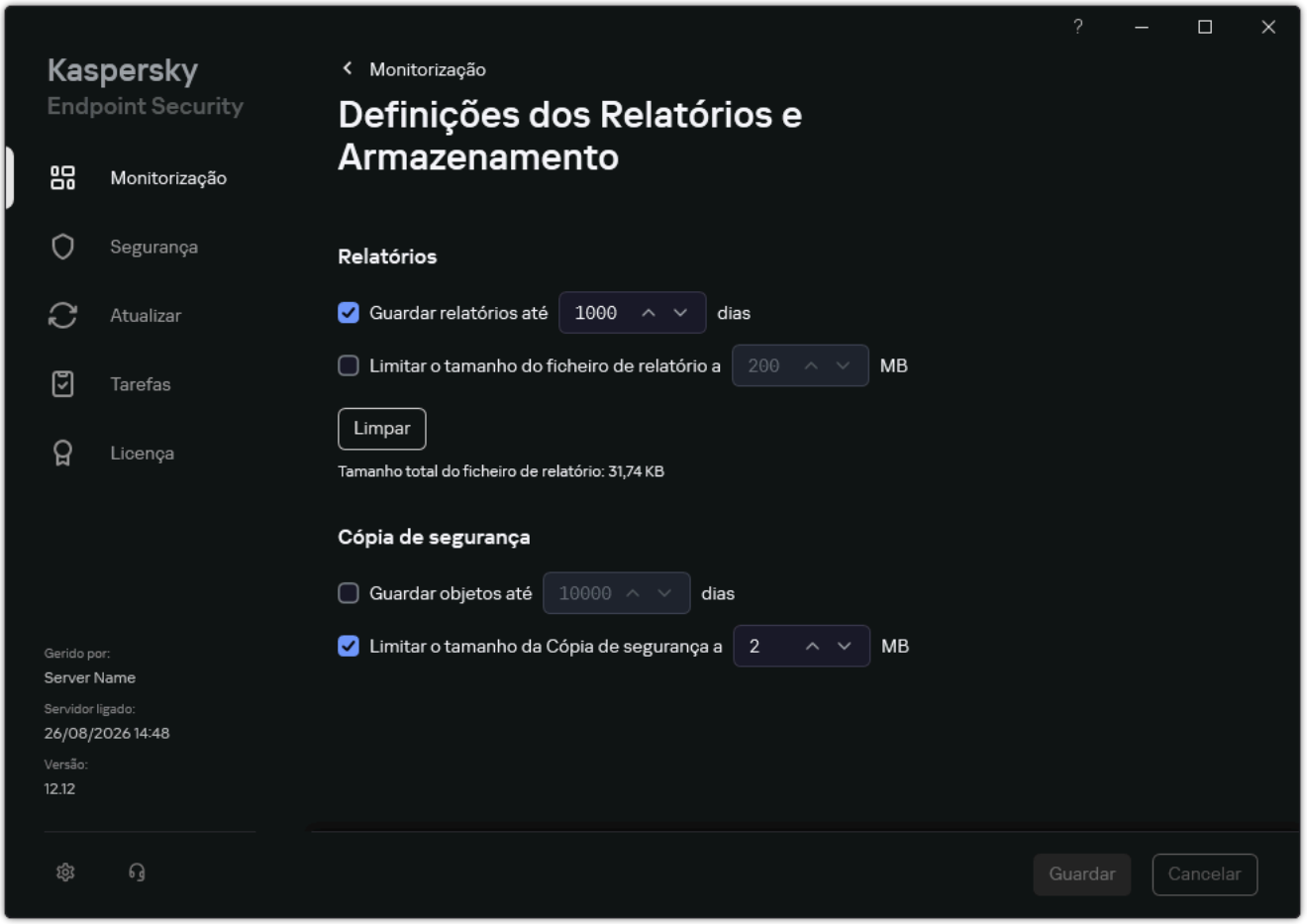
Configurar o prazo máximo de armazenamento de relatórios

O prazo máximo de armazenamento predefinido de relatórios de eventos registados pelo Kaspersky Endpoint Security é de 30 dias. Após esse período, o Kaspersky Endpoint Security apaga automaticamente as entradas mais antigas do ficheiro de relatório.

Para modificar o prazo máximo do armazenamento de relatórios:

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela de definições da aplicação, em **Definições gerais** clique no mosaico **Relatórios e armazenamento**.



Definições do relatório

3. Se quiser limitar o prazo de armazenamento de relatórios, selecione a caixa de verificação **Guardar relatórios até N dias** no bloco **Relatórios**. Defina o prazo máximo de armazenamento de relatórios.

4. Guarde as suas alterações.

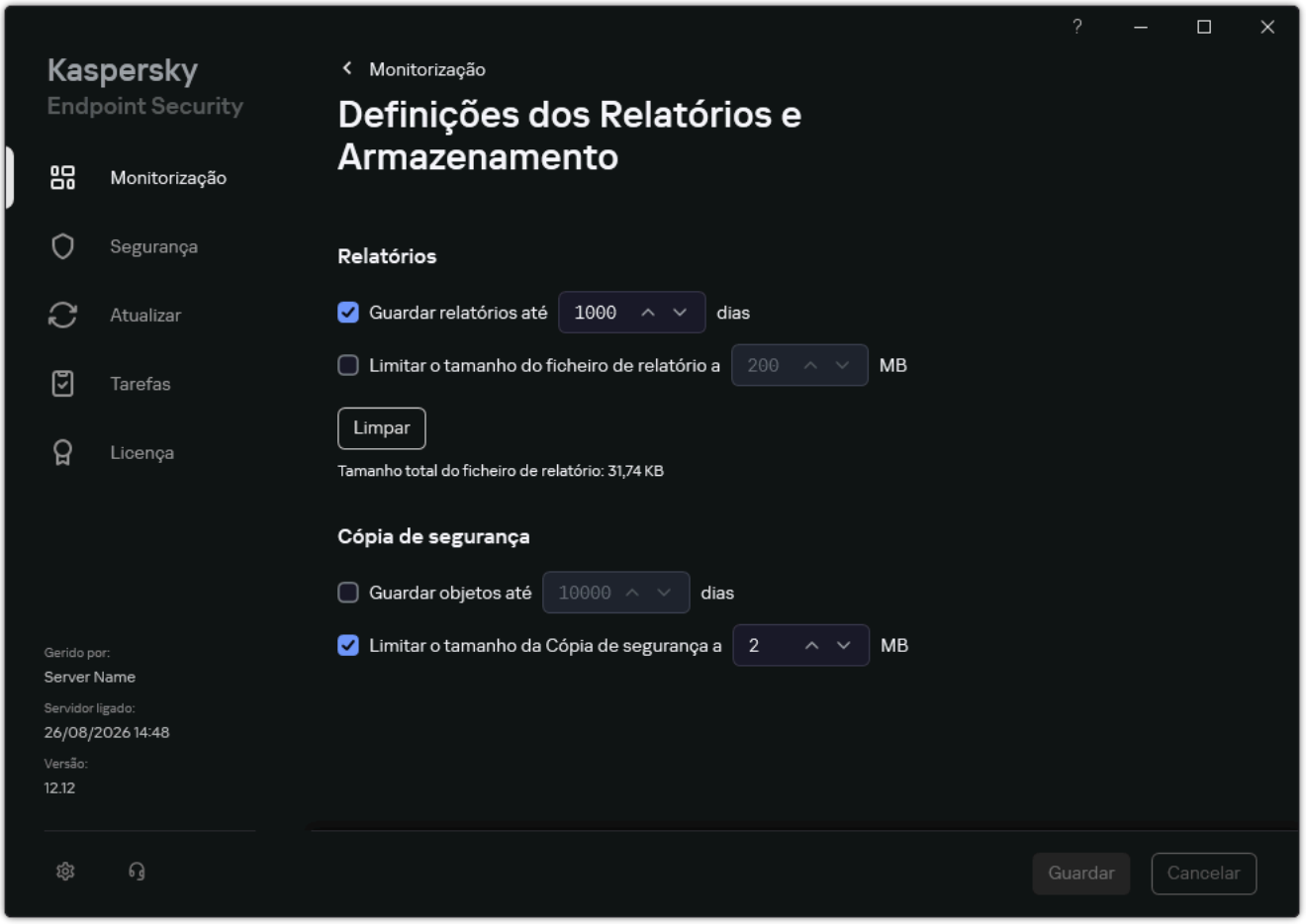
Configurar o tamanho máximo do ficheiro de relatório

Pode especificar o tamanho máximo do ficheiro que contém o relatório. Por predefinição, o tamanho máximo do ficheiro de relatório é de 1024 MB. Para evitar exceder o tamanho máximo do ficheiro de relatórios o Kaspersky Endpoint Security apaga automaticamente as entradas mais antigas do ficheiro de relatórios quando o tamanho máximo do ficheiro de relatório é atingido.

Para configurar o tamanho máximo do ficheiro de relatórios:

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela de definições da aplicação, em **Definições gerais** clique no mosaico **Relatórios e armazenamento**.



Definições do relatório

3. No bloco **Relatórios**, Selecione a caixa de verificação **Limitar o tamanho do ficheiro de relatório a N MB** se quiser limitar o tamanho de um ficheiro de relatório. Defina o tamanho máximo do ficheiro de relatório.

4. Guarde as suas alterações.

Guardar um relatório em ficheiro

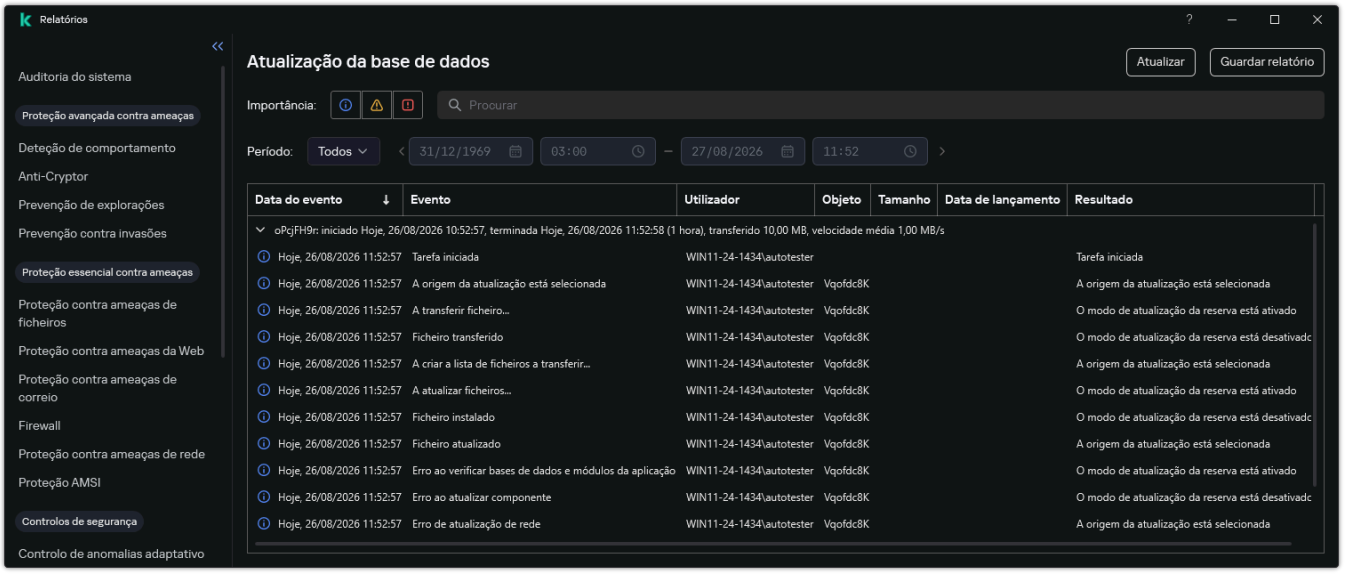
O utilizador é pessoalmente responsável por garantir a segurança da informação de um relatório guardado em ficheiro, e especialmente por controlar e limitar o acesso a esta informação.

Pode guardar o relatório criado num ficheiro de texto (TXT) ou num ficheiro CSV.

O Kaspersky Endpoint Security regista eventos no relatório da mesma forma que são apresentados no ecrã: ou seja, com a mesma ordem e sequência de atributos de evento.

Para guardar um relatório num ficheiro:

1. Na janela principal da aplicação, na secção **Monitorização**, clique em **Relatórios**.



Relatórios

2. Tal abre uma janela; nesta janela, selecione o componente ou a tarefa.

   É apresentado um relatório na parte direita da janela, que contém uma lista de eventos relativos ao funcionamento do componente ou tarefa do Kaspersky Endpoint Security selecionado.

3. Se necessário, pode modificar a apresentação dos dados no relatório:

   - Filtro de eventos
   - Procura de eventos
   - Reordenação de colunas
   - Ordenação de eventos

4. Clique no botão **Guardar relatório** na parte superior direita da janela.

5. Na janela que se abre, especifique a pasta de destino do ficheiro de relatório.

6. Introduza o nome do ficheiro de relatório.

7. Selecione o formato do ficheiro do relatório: TXT ou CSV.

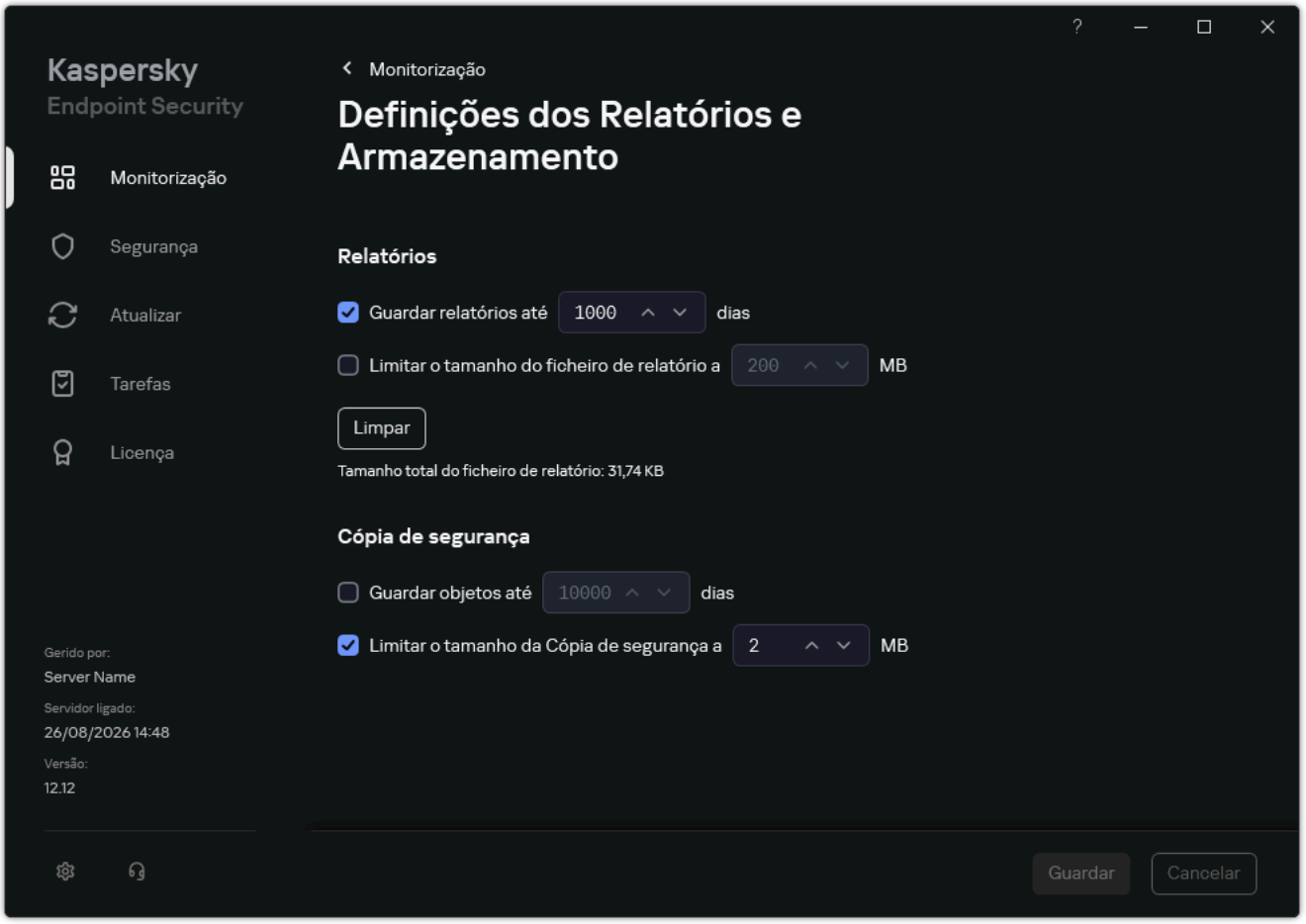
8. Guarde as suas alterações.

Limpar relatórios

Para remover informações dos relatórios:

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela de definições da aplicação, em **Definições gerais** clique no mosaico **Relatórios e armazenamento**.



Definições do relatório

3. No bloco **Relatórios**, clique no botão **Limpar**.

4. Se a Proteção por password está ativada, o Kaspersky Endpoint Security poderá solicitar-lhe as credenciais da conta do utilizador. A aplicação solicita as credenciais da conta se o utilizador não tiver a permissão necessária.

O Kaspersky Endpoint Security eliminará todos os relatórios para todos os componentes e tarefas da aplicação.

Autodefesa do Kaspersky Endpoint Security

O mecanismo de autodefesa impede que outras aplicações 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 disponíveis de Autodefesa para o Kaspersky Endpoint Security dependem se o sistema operativo é de 32 ou 64 bits (consulte a tabela abaixo). A Autodefesa também inclui proteção por password e proteção da ligação ao Servidor de Administração.

A *proteção por password* permite restringir o acesso dos utilizadores ao Kaspersky Endpoint Security de acordo com as permissões que lhes são concedidas (por exemplo, permissão para sair da aplicação).

A proteção da ligação do Servidor de Administração impede a reconexão não autorizada do computador a um servidor não fiável.

Tecnologias de Autodefesa do Kaspersky Endpoint Security

Tecnologia	Descrição	Computador x86	Computador x64
Mecanismo de autodefesa	A tecnologia bloqueia o acesso aos seguintes componentes da aplicação: • ficheiros na pasta de instalação do Kaspersky Endpoint Security e outros ficheiros da aplicação; • chaves de registo com registos que pertencem à aplicação; • Processos que a aplicação executa.	✓	✓
AM-PPL (Antimalware Protected Process Light)	A tecnologia protege os processos do Kaspersky Endpoint Security contra ações maliciosas. Para obter mais informações sobre a tecnologia AM-PPL, visite o website 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 defesa de gestão externa	Esta tecnologia impede que outras aplicações (por exemplo, TeamViewer ou RemotelyAnywhere) obtenham acesso ao Kaspersky Endpoint Security.	✓	– (exceto para o Windows 7)

Ativar e desativar a Autodefesa

O Kaspersky Endpoint Security impede a alteração ou a eliminação dos ficheiros da aplicação no disco rígido, nos processos da memória e nas entradas do registo do sistema.

A tecnologia bloqueia o acesso aos seguintes componentes da aplicação:

- ficheiros na pasta de instalação do Kaspersky Endpoint Security e outros ficheiros da aplicação;
- chaves de registo com registos que pertencem à aplicação;
- Processos que a aplicação executa.

Os mecanismos de Autodefesa não se aplicam aos processos do Kaspersky Endpoint Security iniciados por processos principais não fidedignos.

O mecanismo de Autodefesa do Kaspersky Endpoint Security está ativado por predefinição.

Como ativar ou desativar a Autodefesa na Consola de Administração (MMC)

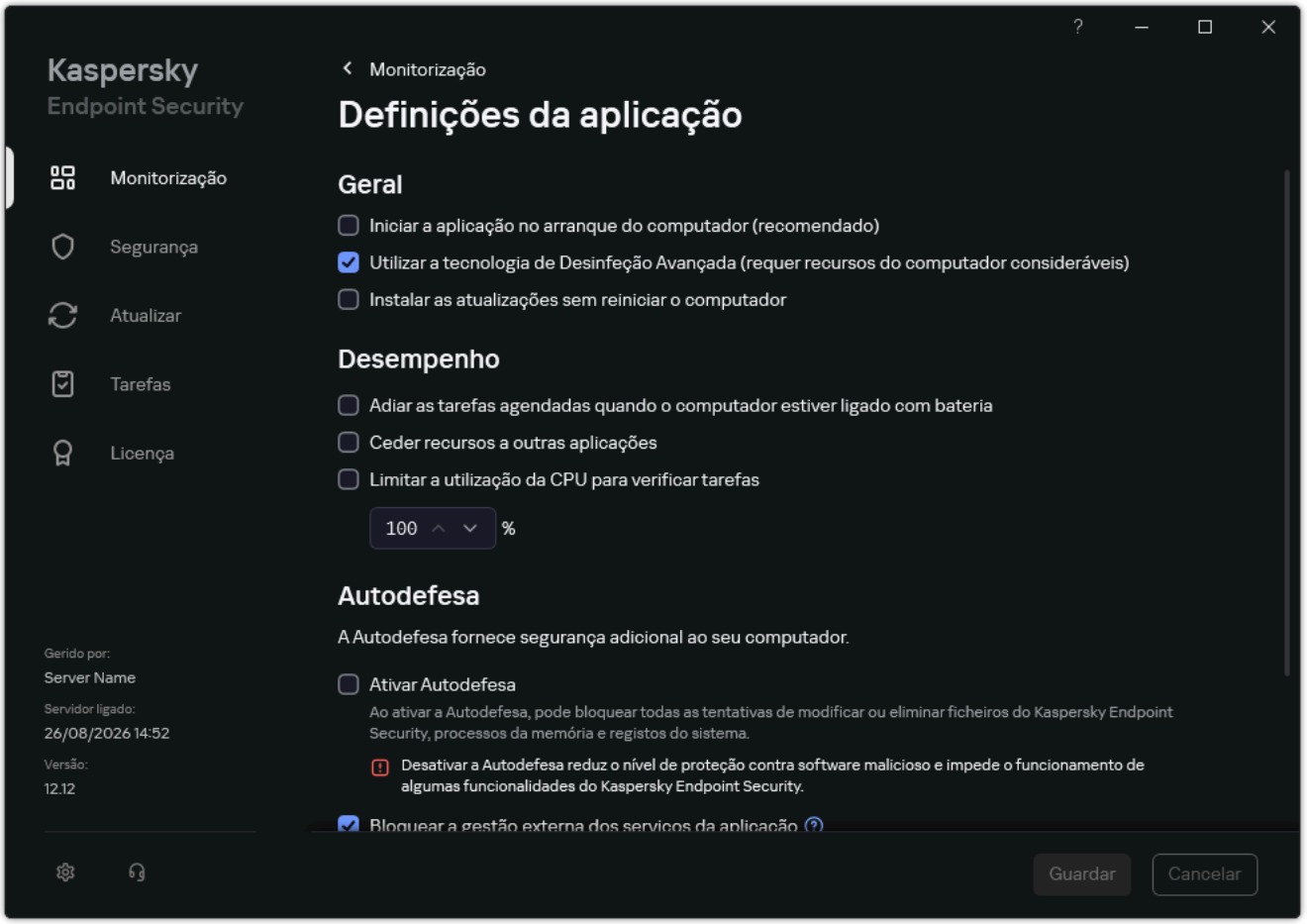
1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais** → **Definições da aplicação**.
4. Use a caixa de verificação **Ativar Autodefesa** para ativar ou desativar o mecanismo de Autodefesa.
5. Guarde as suas alterações.

Como ativar ou desativar a Autodefesa na Web Console e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **Self-Defense**.
5. Use o botão **Self-Defense ENABLED** para ativar ou desativar o mecanismo de Autodefesa.
6. Guarde as suas alterações.

Como ativar ou desativar a Autodefesa na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Definições da aplicação**.



Definições do Kaspersky Endpoint Security for Windows

3. Use a caixa de verificação **Ativar Autodefesa** para ativar ou desativar o mecanismo de Autodefesa.
4. Guarde as suas alterações.

Ativar e desativar o Suporte AM-PPL

O Kaspersky Endpoint Security suporta 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 a aplicação). O AM-PPL permite que apenas os processos fiáveis sejam executados. Os processos do Kaspersky Endpoint Security são assinados de acordo com os requisitos de segurança do Windows e, portanto, são fiáveis. Para obter mais informações sobre a tecnologia AM-PPL, visite o website da Microsoft. A tecnologia AM-PPL está ativada por definição.

O Kaspersky Endpoint Security também inclui mecanismos internos para proteger os processos da aplicação. O suporte do AM-PPL permite delegar funções de segurança do processo ao sistema operacional. Desta forma, pode aumentar a velocidade da aplicação e reduzir o consumo de recursos do computador.

Utilize a tecnologia AM-PPL continuamente. AM-PPL é um componente importante da proteção do sistema operativo. Desativar o suporte AM-PPL pode fazer com que algumas funcionalidades do Kaspersky Endpoint Security deixem de funcionar (por exemplo, a integração da aplicação com o Windows Security Center). A desativação do suporte AM-PPL só é permitida num ambiente de teste separado para fins de 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 da aplicação.

   O mecanismo de autodefesa impede a modificação e a eliminação dos processos de aplicações na memória do computador, incluindo a alteração do estado do AM-PPL.

2. Execute o interpretador de linha de comando (cmd.exe) como administrador.

3. Vá para a pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.

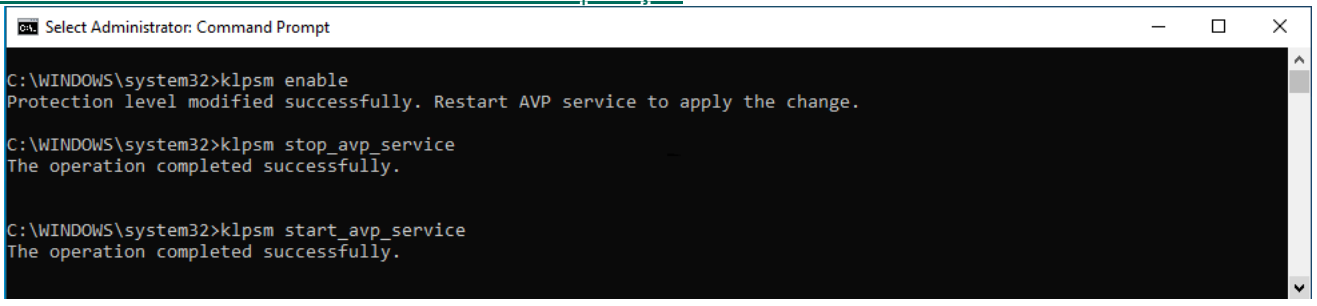
   Pode adicionar o caminho para o ficheiro executável à variável de sistema %PATH% durante a instalação da aplicação.

4. Introduza o seguinte na linha de comando:

   - `klpsm.exe enable` - ativa o suporte da tecnologia AM-PPL (veja a figura abaixo).
   - `klpsm.exe disable` - desativa o suporte da tecnologia AM-PPL.

5. Reiniciar o Kaspersky Endpoint Security.

6. Continue a usar o mecanismo de autodefesa da aplicação.



Ativar suporte da tecnologia AM-PPL

Proteção dos serviços da aplicação contra gestão externa

A proteção dos serviços da aplicação contra gestão externa bloqueia as tentativas dos utilizadores e de outras aplicações para parar os serviços do Kaspersky Endpoint Security. A proteção garante a operação dos seguintes serviços:

- Serviço Kaspersky Endpoint Security (AVP.KES.14.2)
- Serviço Kaspersky Seamless Update Service (AVPSUS.KES.14.2)

Para sair da aplicação a partir da command line, desative a proteção dos serviços do Kaspersky Endpoint Security contra gestão externa.

Apenas pode permitir a gestão externa de serviços de aplicação em computadores que não suportem a tecnologia AM-PPL ou em computadores que tenham a tecnologia desativada.

Como ativar ou desativar a Proteção dos serviços da aplicação contra a gestão externa na Administration Console (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais → Definições da aplicação**.
4. Utilize a caixa de verificação **Bloquear a gestão externa dos serviços da aplicação** para ativar ou desativar a proteção dos serviços do Kaspersky Endpoint Security contra gestão externa.
5. Guarde as suas alterações.

Como ativar ou desativar a Proteção dos serviços da aplicação contra a gestão externa na Web Console e na Cloud Console

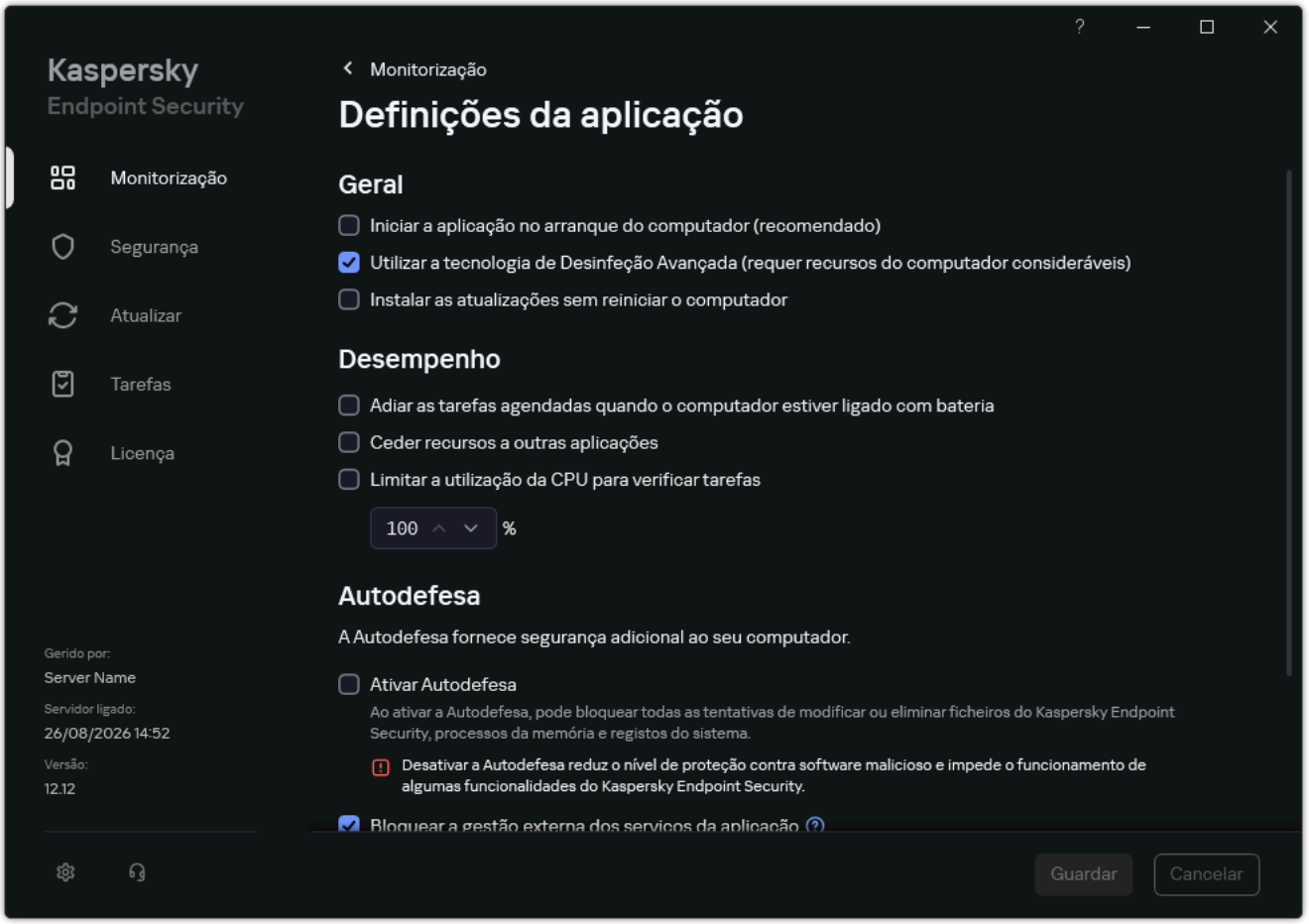
1. Na janela principal da Consola Web, selecione **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings → Self-Defense**.
5. Utilize a caixa de verificação **Block external management of application services** para ativar ou desativar a proteção dos serviços do Kaspersky Endpoint Security contra gestão externa.
6. Guarde as suas alterações.

Como ativar ou desativar a Proteção dos serviços da aplicação contra a gestão externa na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.

2. Na janela Application settings, selecione **Definições gerais → Definições da aplicação**.

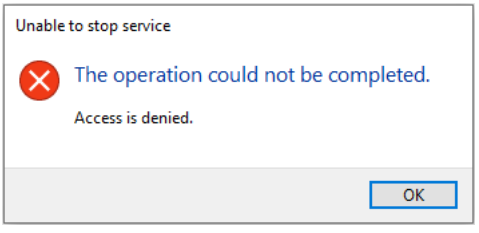


Definições do Kaspersky Endpoint Security for Windows

3. Utilize a caixa de verificação **Bloquear a gestão externa dos serviços da aplicação** para ativar ou desativar a proteção dos serviços do Kaspersky Endpoint Security contra gestão externa.

4. Guarde as suas alterações.

Como resultado, quando um utilizador tentar parar os serviços da aplicação, aparece uma janela do sistema com uma mensagem de erro. O utilizador só pode gerir os serviços da aplicação a partir da interface do Kaspersky Endpoint Security.



Erro de acesso aos serviços da aplicação

Disponibilizar apoio para aplicações de administração remota

Ocasionalmente, poderá ser necessária a utilização de uma aplicação de administração remota quando a defesa de gestão externa está ativada.

Para ativar o funcionamento de aplicações de administração remota:

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Exclusões e tipos de objetos detetados**.
3. No bloco **Exclusões**, clique na ligação **Especificar aplicações fiáveis**.
4. Na janela que abre, clique no botão **Adicionar**.
5. Selecione o ficheiro executável da aplicação de administração remota.

   Também pode introduzir o caminho manualmente. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.
6. Selecione a caixa de verificação **Permitir interação com a interface do Kaspersky Endpoint Security**.
7. Guarde as suas alterações.

Proteção por password

Um computador pode ser partilhado por vários utilizadores com diferentes níveis de conhecimento informático. Se os utilizadores tiverem acesso ilimitado ao Kaspersky Endpoint Security e às suas definições, o nível global de proteção do computador poderá ser reduzido. A proteção por password permite restringir o acesso dos utilizadores ao Kaspersky Endpoint Security de acordo com as permissões que lhes são concedidas (por exemplo, permissão para sair da aplicação).

Se o utilizador que iniciou a sessão do Windows (*utilizador da sessão*) tiver permissão para executar a ação, o Kaspersky Endpoint Security não solicitará o nome de utilizador, a password ou uma password temporária. O utilizador recebe acesso ao Kaspersky Endpoint Security de acordo com as permissões concedidas.

Se um utilizador da sessão não tiver permissão para executar uma ação, poderá obter acesso à aplicação das seguintes formas:

- Digite um nome de utilizador e uma password.

  Este método é adequado para operações do dia-a-dia. Para executar uma ação protegida por password, deve inserir as credenciais da conta de domínio do utilizador com a permissão necessária. Nesse caso, o computador deve estar nesse domínio. Se o computador não estiver no domínio, pode utilizar a conta KLAdmin ou uma conta adicionada manualmente.

- Digite uma password temporária.

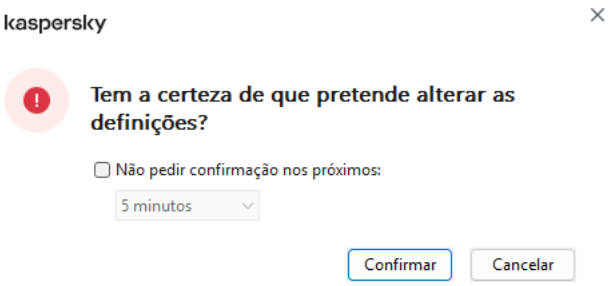
  Esse método é adequado para conceder permissões temporárias para executar ações bloqueadas (por exemplo, sair da aplicação) para utilizadores fora da rede corporativa. Quando uma password temporária expira ou uma sessão termina, o Kaspersky Endpoint Security reverte as suas configurações para o estado anterior.

- Token.

  Este método é adequado para utilizadores privilegiados (como os membros da equipa de Suporte Técnico). A autenticação por token permite utilizar o modo de início de sessão com cartão inteligente no Active Directory. Isto melhora a segurança da infraestrutura da organização.

Quando um utilizador tenta executar uma ação protegida por password, o Kaspersky Endpoint Security solicita ao utilizador o nome de utilizador e a password, a password do token ou a password temporária (veja a figura abaixo).

Na janela de entrada de password, pode alternar os idiomas ao pressionar **ALT+SHIFT**. A utilização de outros atalhos não funciona para a troca de idiomas, mesmo que tenham sido configurados no sistema operativo.



Pedido de password de acesso do Kaspersky Endpoint Security

Utilizador e password

Para aceder ao Kaspersky Endpoint Security, deve introduzir as credenciais da conta. A proteção por password suporta as seguintes contas:

- **KLAdmin**. Uma conta de administrador com acesso sem restrições ao Kaspersky Endpoint Security. A conta KLAdmin tem o direito de executar qualquer ação protegida por password. As permissões para a conta KLAdmin não podem ser revogadas. Quando ativa a proteção por password, o Kaspersky Endpoint Security solicita que defina uma password para a conta do KLAdmin.

- **Conta adicionada manualmente**. Uma conta fora do domínio do Active Directory. Pode utilizar esta conta de serviço em vez do KLAdmin se não quiser partilhar a password de administrador. Pode definir qualquer nome de utilizador e password e configurar permissões individuais.

- **O grupo Todos**. Um grupo interno do Windows que inclui todos os utilizadores dentro da rede corporativa. Os utilizadores do grupo Todos podem aceder à aplicação de acordo com as permissões que lhes são concedidas.

- **Utilizadores individuais ou grupos**. Contas de utilizador para as quais pode configurar permissões individuais. Por exemplo, se uma ação for bloqueada para o grupo Todos, poderá permitir essa ação para um utilizador individual ou um grupo.

- **Utilizador da sessão**. Conta do utilizador que iniciou a sessão do Windows. Pode alternar para outro utilizador da sessão quando for solicitada uma password (a caixa de verificação **Guardar password para a atual sessão**). Nesse caso, o Kaspersky Endpoint Security considera o utilizador cujas credenciais de conta foram inseridas como o utilizador da sessão em vez do utilizador que iniciou a sessão do Windows.

Password temporária

Uma password temporária pode ser usada para conceder acesso temporário ao Kaspersky Endpoint Security para um computador individual fora da rede corporativa. O Administrador gera uma password temporária para um computador individual nas propriedades do computador no Kaspersky Security Center. O Administrador seleciona as ações que serão protegidas com a password temporária e especifica o período de validade da password temporária.

Token

Para aceder às funcionalidades do Kaspersky Endpoint Security, tem de selecionar o certificado de utilizador adequado na lista de certificados armazenados no token ligado e introduzir o seu PIN. A autenticação por token está disponível apenas para utilizadores no domínio do Active Directory. O administrador pode configurar permissões para um utilizador individual ou um grupo. Para que a autenticação por token funcione, tem de implementar uma infraestrutura de PKI fiável e instalar software especial para gerir o token.

Ativar proteção por password

A proteção por password permite restringir o acesso dos utilizadores ao Kaspersky Endpoint Security de acordo com as permissões que lhes são concedidas (por exemplo, permissão para sair da aplicação).

Como ativar Proteção por Password na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais** → **Interface**.
4. No bloco **Proteção por password**, clique no botão **Definições**.

   Esta ação abre uma janela com as definições de proteção por password.
5. Use a caixa de verificação **Ativar proteção por password** para ativar ou desativar o componente.
6. Sob **Permissões**, selecione a conta KLAdmin.

7. Esta ação abre uma janela; nessa janela, clique em **Password** e defina uma password para a conta KLAdmin.

   A conta KLAdmin tem o direito de executar qualquer ação protegida por password.

   > Se se esqueceu da password da sua conta KLAdmin, pode repor a password nas propriedades da política.

8. Volte para a lista de contas.

9. Definir permissões para todos os utilizadores dentro da rede corporativa:

   a. Sob **Permissões**, selecione o grupo "Todos".

      O grupo Todos é um grupo interno do Windows que inclui todos os utilizadores dentro da rede corporativa.

   b. Na janela que abriu, marque as caixas de seleção ao lado das ações que os utilizadores poderão executar sem inserir a password.

      Se uma caixa de seleção estiver desmarcada, os utilizadores serão impedidos de executar a ação. Por exemplo, se a caixa de seleção ao lado da permissão **Sair da aplicação** estiver desmarcada, apenas poderá sair da aplicação se estiver logado como KLAdmin ou como um utilizador individual que tenha a permissão necessária, ou se digitar um password temporária.

      > As permissões de proteção de password têm alguns importantes aspetos a considerar. Certifique-se de que todas as condições para aceder ao Kaspersky Endpoint Security são cumpridas.

10. Guarde as suas alterações.

Como ativar Proteção por Password na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **General Settings** → **Self-Defense**.

5. Sob **Password Protection**, use o botão de alternar da **Password Protection ENABLED** para ativar ou desativar o componente.

6. Especifique a password da conta KLAdmin e confirme-a.

   A conta KLAdmin tem o direito de executar qualquer ação protegida por password.

   > Se se esqueceu da password da sua conta KLAdmin, pode repor a password nas propriedades da política.

7. Volte para a lista de contas.

8. Definir permissões para todos os utilizadores dentro da rede corporativa:

   a. No quadro de contas, selecione o grupo "Todos".

      O grupo Todos é um grupo interno do Windows que inclui todos os utilizadores dentro da rede corporativa.

b. Na janela que abriu, marque as caixas de seleção ao lado das ações que os utilizadores poderão executar sem inserir a password.

Se uma caixa de seleção estiver desmarcada, os utilizadores serão impedidos de executar a ação. Por exemplo, se a caixa de seleção ao lado da permissão **Exit the application** estiver desmarcada, apenas poderá sair da aplicação se estiver logado como KLAdmin ou como um utilizador individual que tenha a permissão necessária, ou se digitar um password temporária.

As permissões de proteção de password têm alguns importantes aspetos a considerar. Certifique-se de que todas as condições para aceder ao Kaspersky Endpoint Security são cumpridas.

9. Guarde as suas alterações.

Como ativar Proteção por Password na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Interface**.
3. Use o botão de alternar da **Proteção por password** para ativar ou desativar o componente.
4. Especifique a password da conta KLAdmin e confirme-a.

A conta KLAdmin tem o direito de executar qualquer ação protegida por password.

Se um computador funcionar no âmbito de uma política, o Administrador poderá redefinir a password da conta KLAdmin nas propriedades da política. Se o computador não estiver ligado ao Kaspersky Security Center e se se tiver esquecido da password da conta KLAdmin, não será possível recuperar a password.

5. Definir permissões para todos os utilizadores dentro da rede corporativa:

a. Na tabela da conta, 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 utilizadores dentro da rede corporativa.

b. Marque as caixas de seleção ao lado das ações que os utilizadores poderão executar sem inserir a password.

Se uma caixa de seleção estiver desmarcada, os utilizadores serão impedidos de executar a ação. Por exemplo, se a caixa de seleção ao lado da permissão **Sair da aplicação** estiver desmarcada, apenas poderá sair da aplicação se estiver logado como KLAdmin ou como um utilizador individual que tenha a permissão necessária, ou se digitar um password temporária.

As permissões de proteção de password têm alguns importantes aspetos a considerar. Certifique-se de que todas as condições para aceder ao Kaspersky Endpoint Security são cumpridas.

6. Guarde as suas alterações.

Quando a proteção por password está ativada, a aplicação restringirá o acesso dos utilizadores ao Kaspersky Endpoint Security de acordo com as permissões concedidas ao grupo Todos. Pode executar as ações que estão bloqueadas para o grupo Todos apenas se usar a conta KLAdmin, outra conta que recebe as permissões necessárias, ou se digitar uma password temporária.

Pode desativar a proteção por password apenas se tiver iniciado a sessão como KLAdmin. Não é possível desativar a proteção por password se estiver a utilizar qualquer outra conta de utilizador ou uma password temporária.

Durante a verificação da password, pode selecionar a caixa de verificação **Guardar password para a atual sessão**. Neste caso, o Kaspersky Endpoint Security não solicitará a password quando um utilizador tentar executar outra ação protegida por password durante toda a sessão.

Conceder permissões a utilizadores ou grupos individuais

A proteção por password permite conceder o acesso do Kaspersky Endpoint Security a contas de utilizador individuais do Active Directory e a contas de utilizador adicionadas manualmente.

Contas de utilizador do Active Directory

Pode conceder acesso ao Kaspersky Endpoint Security a utilizadores individuais ou grupos no domínio do Active Directory. Por exemplo, se a saída da aplicação estiver bloqueado para o grupo Todos, pode conceder a permissão **Sair da aplicação** a um utilizador individual. Como resultado, apenas pode sair da aplicação se estiver ligado a esse utilizador ou como KLAdmin.

Pode usar as credenciais da conta para aceder à aplicação apenas se o computador estiver no domínio. Se o computador não estiver no domínio, pode usar a conta KLAdmin ou uma password temporária.

Contas de utilizador adicionadas manualmente

Pode criar uma conta de utilizador que não esteja presente no Active Directory e atribuir permissões individuais a essa conta de utilizador. Ou seja, pode criar uma *conta de utilizador de serviço* e utilizá-la em vez do KLAdmin. Desta forma, não é necessário partilhar a sua password do KLAdmin com outros utilizadores ou criar novas contas de utilizador do Active Directory. Pode especificar qualquer nome de utilizador e password. Por exemplo, pode conceder a permissão **Ver relatórios** à conta de utilizador do serviço. Consequentemente, se a visualização de relatórios for proibida para o grupo "Todos", pode abrir os relatórios através da conta de utilizador de serviço ou da conta de utilizador KLAdmin.

Conceder permissões a utilizadores ou grupos individuais

Como conceder permissões a utilizadores ou grupos individuais na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais** → **Interface**.
4. No bloco **Proteção por password**, clique no botão **Definições**.

   Esta ação abre uma janela com as definições de proteção por password.
5. Na tabela de contas, clique em **Adicionar**.
6. Selecione o tipo de conta de utilizador que pretende adicionar:

   - **Selecionar um utilizador/grupo do Active Directory** – contas de utilizador do Active Directory.

     Para selecionar uma conta de utilizador, clique em **Selecionar**. Selecione um utilizador ou um grupo no Active Directory e confirme a sua seleção.

   - **Adicionar um utilizador/grupo de utilizadores manualmente** para uma conta de utilizador de serviço adicionada manualmente.

     Para adicionar uma conta de utilizador de serviço, introduza um nome de utilizador e uma password (por exemplo, SecureAdmin).

     Pode repor a password de uma conta de utilizador de serviço nas definições da política. A password da conta de utilizador de serviço tem de ser reposta da mesma forma que a password do KLAdmin. Se a edição das definições da Proteção por password for permitida (o "cadeado" está aberto) ou se não for aplicada nenhuma política ao computador, pode repor a password da conta de utilizador de serviço na interface da aplicação. Para tal, confirme as alterações das informações da conta de utilizador de serviço utilizando a password do KLAdmin.
7. Na lista **Permissões**, selecione as caixas de ação ao lado das ações que o utilizador ou grupo selecionado poderá executar sem lhe ser solicitada uma password.

   Se uma caixa de seleção estiver desmarcada, os utilizadores serão impedidos de executar a ação. Por exemplo, se a caixa de seleção ao lado da permissão **Sair da aplicação** estiver desmarcada, apenas poderá sair da aplicação se estiver logado como KLAdmin ou como um utilizador individual que tenha a permissão necessária, ou se digitar um password temporária.

   As permissões de proteção de password têm alguns importantes aspetos a considerar. Certifique-se de que todas as condições para aceder ao Kaspersky Endpoint Security são cumpridas.
8. Guarde as suas alterações.

Como conceder permissões a utilizadores ou grupos individuais na Web Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **Self-Defense**.
5. No bloco **Password Protection**, clique na ligação **User permissions**.

   Isto abre o formulário para conceder as permissões Ativar password.
6. Clique em **Add**.
7. Selecione o tipo de conta de utilizador que pretende adicionar:

   - **Select from Active Directory** – contas de utilizador do Active Directory.

     Para selecionar uma conta de utilizador, clique em **Edit**. Selecione um utilizador ou um grupo no Active Directory e confirme a sua seleção.
   - **Add manually** para uma conta de utilizador de serviço adicionada manualmente.

     Para adicionar uma conta de utilizador de serviço, introduza um nome de utilizador e uma password (por exemplo, SecureAdmin).

     Pode repor a password de uma conta de utilizador de serviço nas definições da política. A password da conta de utilizador de serviço tem de ser reposta da mesma forma que a password do KLAdmin. Se a edição das definições da Proteção por password for permitida (o "cadeado" está aberto) ou se não for aplicada nenhuma política ao computador, pode repor a password da conta de utilizador de serviço na interface da aplicação. Para tal, confirme as alterações das informações da conta de utilizador de serviço utilizando a password do KLAdmin.
8. Na lista **Permissions**, selecione as caixas de ação ao lado das ações que o utilizador ou grupo selecionado poderá executar sem lhe ser solicitada uma password.

   Se uma caixa de seleção estiver desmarcada, os utilizadores serão impedidos de executar a ação. Por exemplo, se a caixa de seleção ao lado da permissão **Exit the application** estiver desmarcada, apenas poderá sair da aplicação se estiver logado como KLAdmin ou como um utilizador individual que tenha a permissão necessária, ou se digitar um password temporária.

   As permissões de proteção de password têm alguns importantes aspetos a considerar. Certifique-se de que todas as condições para aceder ao Kaspersky Endpoint Security são cumpridas.
9. Clique em **Add**.
10. Guarde as suas alterações.

Como conceder permissões a utilizadores ou grupos individuais na interface do utilizador da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Interface**.

3. Na tabela de contas, clique em **Adicionar**.

4. Selecione o tipo de conta de utilizador que pretende adicionar:

   - **Selecionar um utilizador/grupo do Active Directory** – contas de utilizador do Active Directory.

     Para selecionar uma conta de utilizador, clique em **Selecionar utilizador ou grupo**. Selecione um utilizador ou um grupo no Active Directory e confirme a sua seleção.

   - **Adicionar um utilizador manualmente** para uma conta de utilizador de serviço adicionada manualmente.

     Para adicionar uma conta de utilizador de serviço, introduza um nome de utilizador e uma password (por exemplo, SecureAdmin).

     Pode repor a password de uma conta de utilizador de serviço nas definições da política. A password da conta de utilizador de serviço tem de ser reposta da mesma forma que a password do KLAdmin. Se a edição das definições da Proteção por password for permitida (o "cadeado" está aberto) ou se não for aplicada nenhuma política ao computador, pode repor a password da conta de utilizador de serviço na interface da aplicação. Para tal, confirme as alterações das informações da conta de utilizador de serviço utilizando a password do KLAdmin.

5. Na lista **Permissões**, selecione as caixas de ação ao lado das ações que o utilizador ou grupo selecionado poderá executar sem lhe ser solicitada uma password.

   Se uma caixa de seleção estiver desmarcada, os utilizadores serão impedidos de executar a ação. Por exemplo, se a caixa de seleção ao lado da permissão **Sair da aplicação** estiver desmarcada, apenas poderá sair da aplicação se estiver logado como KLAdmin ou como um utilizador individual que tenha a permissão necessária, ou se digitar um password temporária.

   As permissões de proteção de password têm alguns importantes aspetos a considerar. Certifique-se de que todas as condições para aceder ao Kaspersky Endpoint Security são cumpridas.

6. Guarde as suas alterações.

Como resultado, se o acesso à aplicação for restrito ao grupo Todos, os utilizadores receberão permissões para aceder ao Kaspersky Endpoint Security de acordo com as permissões individuais dos utilizadores.

Usar uma password temporária para conceder permissões

Uma password 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 utilizador execute uma ação bloqueada sem obter as credenciais da conta do KLAdmin. Para usar uma password temporária, o computador deve ser adicionado ao Kaspersky Security Center.

Como permitir que um utilizador execute uma ação bloqueada utilizando uma password temporária através da Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.

2. Na pasta **Managed devices** da árvore na Consola de Administração, abra a pasta com o nome do grupo de administração ao qual os computadores cliente em questão pertencem.

3. Na área de trabalho, selecione o separador **Devices**.

4. Clique duas vezes para abrir a janela de propriedades do computador.

5. Na janela de propriedades do computador, selecione a secção **Applications**.

6. Na lista de aplicações da Kaspersky instaladas no computador, selecione **Kaspersky Endpoint Security for Windows (14.2)** e clique duas vezes para abrir as propriedades da aplicação.

7. Na janela Application settings, selecione **Definições gerais → Interface**.

8. No bloco **Proteção por password**, clique no botão **Definições**.

9. Na janela que abre, no bloco **Password temporária**, clique no botão **Lista de passwords temporárias**.

   A janela de gestão de passwords temporárias é aberta.

10. Clique em **Adicionar**.

11. No campo **Data de validade**, especifique a data de expiração em que a password temporária expirará.

12. Na tabela **Âmbito da password temporária**, selecione as caixas de verificação à frente das operações que devem estar disponíveis para o utilizador enquanto a password temporária for válida.

13. Clique em **Gerar**.

    Abre-se uma janela contendo a password temporária (veja a figura abaixo).

14. Copie a password e forneça-a ao utilizador.

Como permitir que um utilizador execute uma ação bloqueada utilizando uma password temporária através da Consola Web e da Consola da Cloud

1. Na janela principal da Consola Web, selecione **Asset management → Assets (Devices)**.

2. Clique no nome do computador no qual pretende permitir que um utilizador execute uma ação bloqueada.

3. Selecione o separador **Applications**.

4. Clique em **Kaspersky Endpoint Security for Windows**.

   As definições da aplicação locais são apresentadas.

5. Selecione o separador **Application settings**.

6. Na janela Application settings, selecione **General settings → Interface**.

7. No bloco **Temporary passwords**, clique no botão **Add**.

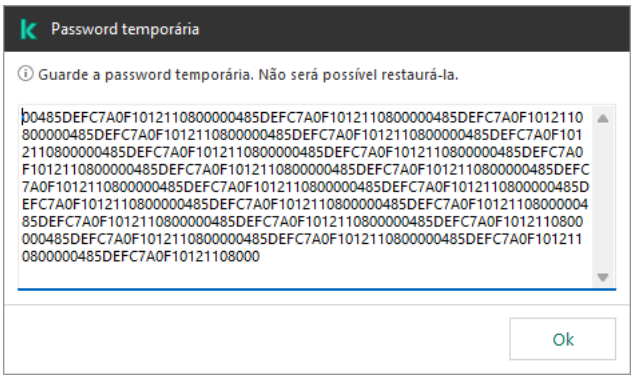
8. No campo **Data de validade**, especifique a data de expiração em que a password temporária expirará.

9. Na tabela **Âmbito da password temporária**, selecione as caixas de verificação à frente das operações que devem estar disponíveis para o utilizador enquanto a password temporária for válida.

10. Clique em **Gerar**.

    É aberta uma janela que contém a password temporária.

11. Copie a password e forneça-a ao utilizador.

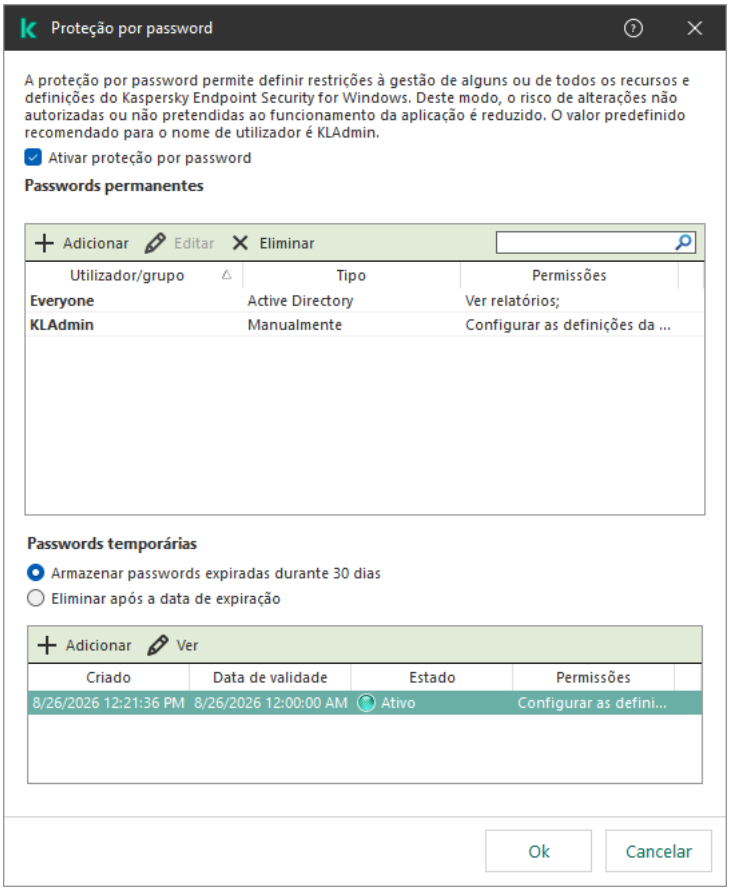


Password temporária

Revogar password temporária

A partir da versão 12.9, o Kaspersky Endpoint Security for Windows inclui a funcionalidade *Gestão de passwords temporárias*. A gestão de passwords temporárias permite-lhe realizar as seguintes ações:

- Guardar o histórico de passwords (até 30 dias).
- Monitorizar o estado da password temporária: *Ativo*, *Expirado*, *Revogado*.
- Revogar passwords temporárias.



Gestão de passwords temporárias

A Gestão de passwords temporárias atualiza o estado da password e revoga a password apenas depois de sincronizar o computador com o Kaspersky Security Center.

Como revogar a password temporária utilizando a Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Managed devices** da árvore na Consola de Administração, abra a pasta com o nome do grupo de administração ao qual os computadores cliente em questão pertencem.
3. Na área de trabalho, selecione o separador **Devices**.
4. Clique duas vezes para abrir a janela de propriedades do computador.
5. Na janela de propriedades do computador, selecione a secção **Applications**.
6. Na lista de aplicações da Kaspersky instaladas no computador, selecione **Kaspersky Endpoint Security for Windows (14.2)** e clique duas vezes para abrir as propriedades da aplicação.
7. Na janela Application settings, selecione **Definições gerais → Interface**.
8. No bloco **Proteção por password**, clique no botão **Definições**.
9. Esta ação abre uma janela; naquela janela abaixo **Password temporária**, configure as definições de armazenamento para passwords expiradas.
10. Clique em **Lista de passwords temporárias**.

    A janela de gestão de passwords temporárias é aberta. A gestão de passwords temporárias apresenta a data de expiração da password, o estado da password e a lista de permissões.
11. Selecione a password temporária ativa que pretende revogar e clique duas vezes na password para abrir as respetivas propriedades.
12. Na janela que abre, clique no botão **Revogar**.
13. Guarde as suas alterações. Para aplicar a política em computadores, feche os cadeados .

Como revogar uma password temporária na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management → Assets (Devices)**.
2. Clique no nome do computador no qual pretende permitir que um utilizador execute uma ação bloqueada.
3. Selecione o separador **Applications**.
4. Clique em **Kaspersky Endpoint Security for Windows**.

    As definições da aplicação locais são apresentadas.
5. Selecione o separador **Application settings**.
6. Na janela Application settings, selecione **General settings → Interface**.
7. Em **Temporary passwords**, configure o armazenamento de passwords expiradas.

8. Clique na hiperligação **Temporary password**.

   A janela de gestão de passwords temporárias é aberta. A gestão de passwords temporárias apresenta a data de expiração da password, o estado da password e a lista de permissões.

9. Selecione a password temporária ativa que deseja revogar.

10. Na janela que abre, clique no botão **Revoke password**.

11. Guarde as suas alterações. Para aplicar a política em computadores, feche os cadeados .

Como resultado, a Gestão de passwords temporárias define o estado da password para *Revogação (sincronização com um anfitrião)*. Depois de sincronizar o computador com o Kaspersky Security Center, a aplicação revoga a password temporária e bloqueia imediatamente as permissões concedidas.

Aspetos especiais de permissões de proteção por password

As permissões de proteção por password têm alguns aspetos e limitações importantes a ter em consideração.

Configurar as definições da aplicação

Se o computador de um utilizador estiver a funcionar no âmbito de uma política, verifique se todas as configurações necessárias da política estão disponíveis para edição (os atributos estão abertos).

Sair da aplicação

Não há considerações ou limitações especiais.

Desativar componentes de proteção

- Não é possível conceder a permissão para desativar os componentes de proteção do grupo Todos. Para permitir que os utilizadores que não sejam o KLAdmin desativem componentes de controlo, adicionar um utilizador ou um grupo que tem a permissão **Desativar componentes de proteção** nas definições de proteção por password.
- Se o computador de um utilizador estiver a funcionar no âmbito de uma política, verifique se todas as configurações necessárias da política estão disponíveis para edição (os atributos estão abertos).
- Para desativar os componentes de proteção nas configurações da aplicação, um utilizador deve ter a permissão **Configurar as definições da aplicação**.
- Para desativar os componentes de proteção a partir do menu contextual (usando o item do menu **Pausar proteção**), um utilizador deve ter a permissão **Desativar componentes de proteção** além da permissão **Desativar componentes de controlo**.

Desativar componentes de controlo

- Não é possível conceder a permissão para desativar os componentes de controlo do grupo Todos. Para permitir que os utilizadores que não sejam o KLAdmin desativem componentes de controlo, adicionar um utilizador ou um grupo que tem a permissão **Desativar componentes de controlo** nas definições de proteção por password.
- Se o computador de um utilizador estiver a funcionar no âmbito de uma política, verifique se todas as configurações necessárias da política estão disponíveis para edição (os atributos estão abertos).
- Para desativar os componentes de controlo nas configurações da aplicação, um utilizador deve ter a permissão **Configurar as definições da aplicação**.
- Para desativar os componentes de controlo do menu contextual (usando o item do menu **Pausar proteção**), um utilizador deve ter a permissão **Desativar componentes de controlo** além da permissão **Desativar componentes de proteção**.

Desativar a política do Kaspersky Security Center

Não pode conceder ao grupo "Todos" a permissão para desativar a política do Kaspersky Security Center. Para permitir que os utilizadores que não sejam o KLAdmin desativem a política, adicionar um utilizador ou um grupo que tem a permissão **Desativar a política do Kaspersky Security Center** nas configurações de proteção por password.

Remover chave

Não há considerações ou limitações especiais.

Remover/modificar/restaurar a aplicação

Se tiver pemitido a remoção, modificação e restauração da aplicação para o grupo “Todos”, o Kaspersky Endpoint Security não pedirá uma password quando o utilizador tentar executar estas operações. Como tal, qualquer utilizador, incluindo os utilizadores fora do domínio, podem instalar, modificar ou restaurar a aplicação.

Restaurar o acesso aos dados na unidade encriptada

Pode restaurar o acesso a dados em unidades encriptadas apenas se estiver logado como KLAdmin. A permissão para executar esta ação não pode ser concedida a nenhum outro utilizador.

Ver relatórios

Não há considerações ou limitações especiais.

Restaurar da cópia de segurança

Não há considerações ou limitações especiais.

Exportar definições

Por defeito, a exportação das definições da aplicação é negada ao grupo "Todos". Pode exportar as definições da aplicação utilizando a conta do utilizador KLAdmin. A exportação das definições da aplicação inclui apenas a criação de um ficheiro de configuração com as definições do Kaspersky Endpoint Security na interface da aplicação. A permissão não restringe a exportação de listas de exclusões de verificação, URL fiáveis, dispositivos fiáveis ou outras listas mantidas por componentes da aplicação.

Redefinir a password do KLAdmin

Se se esqueceu da password da sua conta KLAdmin, pode repor a password nas propriedades da política. Não pode repor a password na interface da aplicação.

Pode executar ações protegidas por password com uma password temporária. Neste caso, não precisa de introduzir as credenciais KLAdmin.

Se o computador não estiver ligado ao Kaspersky Security Center e se se tiver esquecido da password da conta KLAdmin, não será possível recuperar a password.

Como repor a password da conta KLAdmin com a Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais** → **Interface**.
4. No bloco **Proteção por password**, clique no botão **Definições**.
5. Na janela que abre, desmarque a caixa de verificação **Ativar proteção por password**.
6. Guarde as suas alterações.
7. Selecione a caixa de verificação **Ativar proteção por password** novamente.

8. Clique em **OK**.
   Isto abre a janela de password de administrador.
9. Especifique a nova password da conta KLAdmin e confirme-a.
10. Guarde as suas alterações.

Como repor a password da conta KLAdmin na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Assets (Devices)**.
2. Selecione um computador para o qual quer configurar definições da aplicação locais.
   As propriedades do computador são apresentadas.
3. Selecione o separador **Applications**.
4. Clique em **Kaspersky Endpoint Security for Windows 14.2**.
   As definições da aplicação locais são apresentadas.
5. Selecione o separador **Application settings**.
6. Aceda a **General Settings** → **Self-Defense**.
7. Sob **Proteção por password**, desative a opção **Proteção por password**.
8. Guarde as suas alterações.
9. Volte a ativar a opção **Proteção por password**.
10. Especifique a nova password da conta KLAdmin e confirme-a.
11. Guarde as suas alterações.

Como resultado, a password da sua conta KLAdmin é atualizada após a aplicação da política.

Proteção da ligação do Servidor de Administração

A ligação do computador ao Servidor de Administração é conseguida usando o componente *Agente de Rede* do Kaspersky Security Center. Se um intruso tiver direitos suficientes para modificar as definições de ligação ao servidor, existe o risco de ligar o computador a um servidor não fiável. Isto permitiria ao intruso aplicar as suas próprias políticas de grupo e, por exemplo, desativar a autodefesa da aplicação. O Kaspersky Endpoint Security pode impedir a nova ligação não autorizada de um computador a um servidor diferente. Para proteger a ligação ao servidor, a aplicação sugere a definição de uma password e a utilização da Password-Based key Derivation Function (PBKDF2). Por conseguinte, é impossível aceder à aplicação sem uma password.

Para garantir uma proteção abrangente do Kaspersky Endpoint Security e do Agente de Rede contra o acesso não autorizado, recomendamos a ativação de uma proteção adicional. Para o Kaspersky Endpoint Security, recomendamos a ativação da Proteção por password. Para proteger o Agente de Rede, recomendamos a definição de uma password de desinstalação. Para obter informações sobre a proteção do Agente de Rede contra a remoção, consulte a Ajuda do Kaspersky Security Center.

A gestão da ligação do computador ao Servidor de Administração é efetuada através da tarefa *Proteção da ligação do Servidor de Administração*. A tarefa permite-lhe realizar as seguintes ações:

- Definir uma password para proteger a ligação ao servidor.
- Alterar a password.
- Voltar a ligar o computador a um servidor diferente.
- Desativar a proteção da ligação do servidor.

Autenticação do computador quando se liga ao servidor de administração

Depois de definir uma password, a aplicação cria um conjunto de dados utilizando a transformação PBKDF2 da password. A aplicação encripta então este conjunto de dados utilizando a chave do agente de rede. A aplicação utiliza o conjunto de dados encriptados para verificar os direitos e privilégios do servidor de administração para ligações subsequentes.

Posteriormente, sempre que for feita uma tentativa de voltar a ligar o computador ao Servidor de Administração, a aplicação desencripta o conjunto de dados com a chave do Agente de Rede e compara-a com a cópia local. Se não corresponderem, o acesso à aplicação é restringido.

Proteção da ligação do Servidor de Administração

Como definir uma password para proteção da ligação do servidor na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

Selecione **Kaspersky Endpoint Security for Windows (14.2) → Proteção da ligação do Servidor de Administração**.

Passo 2. Proteger a ligação do Servidor de Administração

Defina uma password para proteger a ligação do Servidor de Administração:

1. Em **Proteção da ligação do Servidor de Administração**, selecione **Proteger com password**.
2. Na lista pendente **Servidor de Administração**, selecione **Novo servidor**.
3. No campo **Password para ligação ao Servidor de Administração**, defina uma password para ligar ao Servidor de Administração e confirme-a.

   Se se esquecer da password, pode alterá-la através de uma tarefa.
4. Se tiver o Kaspersky Endpoint Security 12.7 ou uma versão anterior da aplicação implementada, selecione a caixa de verificação **Ative a compatibilidade da encriptação de passwords para versões anteriores da aplicação (12.7 e inferior)**.

   A partir do Kaspersky Endpoint Security 12.8 para Windows, a aplicação utiliza uma encriptação de password mais forte. Se tiver o Kaspersky Endpoint Security 12.8 ou posterior implementado, recomendamos que desmarque esta caixa de verificação e utilize a encriptação de password mais forte. As versões anteriores da aplicação não suportam a encriptação de passwords fortes. Para executar a tarefa, tem de marcar a caixa de verificação.

Passo 3. Selecionar a conta para executar a tarefa

Selecione **Default account**. Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com a conta de utilizador do sistema (SYSTEM).

Passo 4. Configurar um agendamento de início de uma tarefa

Em **Scheduled start**, selecione **Manually**.

Passo 5. Definir o nome da tarefa

Introduza um nome para a tarefa, por exemplo, *Password de ligação ao servidor principal*.

Passo 6. Completar a criação da tarefa

Conclua o assistente. Selecione a caixa de verificação **Run the task after the wizard finishes** ou execute a tarefa manualmente. Pode controlar o progresso da tarefa nas propriedades da tarefa.

Como definir uma password para proteção da ligação ao servidor na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **Administration Server connection protection**.

   c. No campo **Task name**, introduza uma breve descrição, por exemplo, *Password de ligação ao servidor principal*.

   d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Avance para o passo seguinte.

5. Selecione uma conta de utilizador predefinida. Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com a conta de utilizador do sistema (SYSTEM).

6. Conclua o assistente.

   Será apresentada uma nova tarefa na lista de tarefas.

7. Clique na tarefa **Administration Server connection protection** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

8. Selecione o separador **Application settings**.

9. Em **Administration Server connection protection**, selecione **Protect with a password**.

10. Na lista pendente **Connection to the Administration Server**, selecione **New password**.

11. No campo **Password for connection to the Administration Server**, defina uma password para ligar ao Servidor de Administração e confirme-a.

    Se se esquecer da password, pode alterá-la através de uma tarefa.

12. Se tiver o Kaspersky Endpoint Security 12.7 ou uma versão anterior da aplicação implementada, selecione a caixa de verificação **Enable password encryption compatibility for previous application versions (12.7 and lower)**.

    A partir do Kaspersky Endpoint Security 12.8 para Windows, a aplicação utiliza uma encriptação de password mais forte. Se tiver o Kaspersky Endpoint Security 12.8 ou posterior implementado, recomendamos que desmarque esta caixa de verificação e utilize a encriptação de password mais forte. As versões anteriores da aplicação não suportam a encriptação de passwords fortes. Para executar a tarefa, tem de marcar a caixa de verificação.

13. Guarde as suas alterações.

14. Selecione a caixa de verificação junto à tarefa.

15. Clique em **Start**.

Pode controlar o estado da tarefa e o número de dispositivos nos quais a tarefa foi concluída com êxito ou concluída com um erro.

Voltar a ligar o computador a um Servidor de Administração diferente

Voltar a ligar o computador a um Servidor de Administração diferente implica os seguintes passos:

1. Na consola do servidor `[KSC1]` atual, execute a tarefa *Change Administration Server* para o Agente de Rede.

   Depois de executar a tarefa, o computador é ligado novamente ao novo servidor `[KSC2]`.

   O computador é apresentado na consola do servidor `[KSC1]` com o estado *Critical*. É impossível configurar a aplicação utilizando políticas ou executar tarefas remotamente no computador.

2. Na consola do novo servidor `[KSC2]`, crie uma nova tarefa *Proteção da ligação do Servidor de Administração* para o Kaspersky Endpoint Security. Nas propriedades da tarefa, introduza a password do servidor anterior e defina uma password para o novo servidor.

   Como definir uma nova password para voltar a ligar a um novo servidor na Consola de Administração (MMC)

   1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Tasks**.

      A lista de tarefas é aberta.

   2. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Proteção da ligação do Servidor de Administração**.

Passo 2. Proteger a ligação do Servidor de Administração

Defina uma password para proteger a ligação ao novo Servidor de Administração:

1. Em **Proteção da ligação do Servidor de Administração**, selecione **Proteger com password**.

2. Na lista pendente **Servidor de Administração**, selecione **Voltar a ligar a partir de outro servidor**.

3. No campo **Password atual**, introduza a password definida para a ligação ao servidor de confiança utilizado anteriormente.

4. No campo **Nova password**, defina uma password para ligar ao novo servidor de administração e confirme-a.

   Se se esquecer da password, pode alterá-la através de uma tarefa.

5. Se tiver o Kaspersky Endpoint Security 12.7 ou uma versão anterior da aplicação implementada, selecione a caixa de verificação **Ative a compatibilidade da encriptação de passwords para versões anteriores da aplicação (12.7 e inferior)**.

   A partir do Kaspersky Endpoint Security 12.8 para Windows, a aplicação utiliza uma encriptação de password mais forte. Se tiver o Kaspersky Endpoint Security 12.8 ou posterior implementado, recomendamos que desmarque esta caixa de verificação e utilize a encriptação de password mais forte. As versões anteriores da aplicação não suportam a encriptação de passwords fortes. Para executar a tarefa, tem de marcar a caixa de verificação.

Passo 3. Selecionar a conta para executar a tarefa

Selecione **Default account**. Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com a conta de utilizador do sistema (SYSTEM).

Passo 4. Configurar um agendamento de início de uma tarefa

Em **Scheduled start**, selecione **Manually**.

Passo 5. Definir o nome da tarefa

Introduza um nome para a tarefa, por exemplo, *Password de ligação ao servidor principal*.

Passo 6. Completar a criação da tarefa

Conclua o assistente. Selecione a caixa de verificação **Run the task after the wizard finishes** ou execute a tarefa manualmente. Pode controlar o progresso da tarefa nas propriedades da tarefa.

Como definir uma nova password para voltar a ligar a um novo servidor na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **Administration Server connection protection**.

   c. No campo **Task name**, introduza uma breve descrição, por exemplo, *Password de ligação ao servidor principal*.

   d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Avance para o passo seguinte.

5. Selecione uma conta de utilizador predefinida. Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com a conta de utilizador do sistema (SYSTEM).

6. Conclua o assistente.

   Será apresentada uma nova tarefa na lista de tarefas.

7. Clique na tarefa **Administration Server connection protection** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

8. Selecione o separador **Application settings**.

9. Em **Administration Server connection protection**, selecione **Protect with a password**.

10. Na lista pendente **Connection to the Administration Server**, selecione **Reconnect from another server**.

11. No campo **Current password**, introduza a password definida para a ligação ao servidor de confiança utilizado anteriormente.

12. No campo **New password**, defina uma password para ligar ao novo servidor de administração e confirme-a.

    Se se esquecer da password, pode alterá-la através de uma tarefa.

13. Se tiver o Kaspersky Endpoint Security 12.7 ou uma versão anterior da aplicação implementada, selecione a caixa de verificação **Enable password encryption compatibility for previous application versions (12.7 and lower)**.

    A partir do Kaspersky Endpoint Security 12.8 para Windows, a aplicação utiliza uma encriptação de password mais forte. Se tiver o Kaspersky Endpoint Security 12.8 ou posterior implementado, recomendamos que desmarque esta caixa de verificação e utilize a encriptação de password mais forte. As versões anteriores da aplicação não suportam a encriptação de passwords fortes. Para executar a tarefa, tem de marcar a caixa de verificação.

14. Guarde as suas alterações.

15. Selecione a caixa de verificação junto à tarefa.

16. Clique em **Start**.

    Pode controlar o estado da tarefa e o número de dispositivos nos quais a tarefa foi concluída com êxito ou concluída com um erro.

Depois de concluir a tarefa, certifique-se de que na consola do novo servidor `[KSC2]`, o computador apresenta o estado *OK*🖥. Teste se pode executar tarefas remotamente e configurar a aplicação utilizando políticas.

Repor a password de ligação do servidor de administração

Se se tiver esquecido da password de ligação do servidor de administração ou se a password estiver comprometida, pode repor a password nas propriedades da tarefa. Também pode repor a password e definir uma nova password para um grupo de computadores com diferentes estados de proteção da ligação do servidor de administração. Ou seja, se alguns computadores tiverem a proteção ativada e outros a tiverem desativada, a tarefa define uma password para todos os computadores.

Apenas pode repor a password de ligação do servidor de administração na consola do servidor fiável ao qual o computador está ligado.

Como repor a password de ligação do servidor de administração com a Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Tasks**.
3. Selecione a tarefa **Proteção da ligação do Servidor de Administração** e clique duas vezes para abrir as propriedades da tarefa.
4. Na janela de propriedades da tarefa, selecione a secção **Definições**.
5. Em **Proteção da ligação do Servidor de Administração**, selecione **Proteger e alterar password**.
6. No campo **Password para ligação ao Servidor de Administração**, defina uma nova password para ligar ao servidor fiável atual e confirme a password.
7. Guarde as suas alterações.
8. Execute a tarefa.

Como repor a password de ligação do servidor de administração na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.
2. Clique na tarefa **Administration Server connection protection** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.
3. Selecione o separador **Application settings**.
4. Em **Administration Server connection protection**, selecione **Protect and change password**.
5. No campo **Password for connection to the Administration Server**, defina uma nova password para ligar ao servidor fiável atual e confirme a password.
6. Guarde as suas alterações.
7. Selecione a caixa de verificação junto à tarefa.
8. Clique em **Start**.

Como resultado, a password de ligação do servidor de administração é reposta após a conclusão da tarefa.

Desativar a proteção da ligação do Servidor de Administração

Apenas pode desativar remotamente a proteção de ligação do servidor de administração na consola do servidor fiável ao qual o computador está ligado. Também pode desativar a proteção localmente na linha de comandos.

Como desativar a proteção da ligação do servidor na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Tasks**.
3. Selecione a tarefa **Proteção da ligação do Servidor de Administração** e clique duas vezes para abrir as propriedades da tarefa.
4. Na janela de propriedades da tarefa, selecione a secção **Definições**.
5. Em **Proteção da ligação do Servidor de Administração**, selecione **Não proteger**.
6. Guarde as suas alterações.
7. Execute a tarefa.

   Pode controlar o estado 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 ligação ao servidor na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.
2. Clique na tarefa **Administration Server connection protection** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.
3. Selecione o separador **Application settings**.
4. Em **Administration Server connection protection**, selecione **Do not protect with a password**.
5. Guarde as suas alterações.
6. Selecione a caixa de verificação junto à tarefa.
7. Clique em **Start**.

   Pode controlar o estado 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 ligação do servidor na linha de comandos

1. Execute o interpretador de linha de comando (cmd.exe) como administrador.
2. Vá para a pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.
3. Execute o seguinte comando:

   ```
   avp.com SERVERBINDINGDISABLE [/password=<password>]
   ```

   onde `<password>` é a password da conta do utilizador KL Admin ou a password da tarefa *Proteção da ligação do Servidor de Administração*. Se o parâmetro não for especificado, o Kaspersky Endpoint Security pede-lhe para introduzir uma password na linha seguinte.

   Para executar este comando, a proteção por password deve estar ativada.

Exemplo

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

Encriptação de dados

O Kaspersky Endpoint Security permite encriptar ficheiros e pastas armazenados em unidades locais e amovíveis ou em unidades amovíveis e unidades de disco rígido completas. A encriptação de dados minimiza o risco de fugas de informação que podem ocorrer devido à eventual perda ou roubo de um computador portátil, unidade amovível ou unidade de disco rígido, ou ao acesso não autorizado aos dados por utilizadores ou aplicações. O Kaspersky Endpoint Security utiliza o algoritmo de encriptação Advanced Encryption Standard (AES).

Se a licença expirou, a aplicação não encripta novos dados, e os dados encriptados antigos permanecem encriptados e disponíveis para serem utilizados. Neste caso, a encriptação de novos dados exige que a aplicação seja ativada com uma nova licença que permita a utilização da encriptação.

Se o Kaspersky Endpoint Security estiver instalado num computador baseado em Arm, apenas a Encriptação de Unidade BitLocker estará disponível. A aplicação não suporta outros componentes de encriptação de dados.

Se a licença tiver expirado, o Contrato de Licença do Utilizador Final tiver sido violado, a chave de licença, o Kaspersky Endpoint Security ou os componentes de encriptação tiverem sido removidos, o estado encriptado de ficheiros encriptados anteriormente não é garantido. A razão para isso prende-se com o facto de algumas aplicações, tais como o Microsoft Office Word, criarem uma cópia temporária de ficheiros durante a edição. Quando o ficheiro original é guardado, a cópia temporária substitui o ficheiro original. Em consequência, num computador que não tenha a funcionalidade de encriptação ou que esteja inacessível, o ficheiro permanece desencriptado.

O Kaspersky Endpoint Security oferece os seguintes aspetos da proteção de dados:

- **Encriptação ao nível dos ficheiros unidades locais do computador**. Pode compilar listas de ficheiros por extensão ou grupos de extensões e listas de pastas armazenadas em unidades de leitura locais e criar regras para encriptar ficheiros que são criados por aplicações específicas. Após a aplicação de uma política, o Kaspersky Endpoint Security encripta e desencripta os seguintes ficheiros:
  - ficheiros adicionados individualmente a listas de encriptação e desencriptação;
  - ficheiros armazenados em pastas adicionados a listas de encriptação e desencriptação;
  - ficheiros criados por aplicações separadas.
- **Encriptação de unidades amovíveis**. Pode especificar uma regra de encriptação predefinida, segundo a qual a aplicação aplica a mesma ação a todas as unidades amovíveis, ou especificar regras de encriptação para unidades amovíveis individuais.

  A regra de encriptação predefinida tem uma prioridade menor relativamente às regras de encriptação criadas para unidades amovíveis individuais. As regras de encriptação criadas para unidades amovíveis do modelo de dispositivo especificado têm uma prioridade menor do que as regras de encriptação criadas para unidades amovíveis com o ID de dispositivo especificado.

Para selecionar uma regra de encriptação para ficheiros numa unidade amovível, o Kaspersky Endpoint Security verifica se o modelo e ID do dispositivo são ou não conhecidos. A aplicação executa então uma das seguintes operações:

- Se apenas o modelo do dispositivo for conhecido, a aplicação utiliza a regra de encriptação (caso exista) que foi criada para unidades amovíveis do modelo de dispositivo especificado.
- Se apenas o ID do dispositivo for conhecido, a aplicação utiliza a regra de encriptação (caso exista) que foi criada para unidades amovíveis com o ID do dispositivo especificado.
- Se o modelo e ID do dispositivo forem conhecidos, a aplicação aplica a regra de encriptação (caso exista) que foi criada para unidades amovíveis com o ID de dispositivo específico. Se essa regra não existir, mas existir uma regra de encriptação criada para unidades amovíveis com o modelo de dispositivo específico, a aplicação aplica esta regra. Se não for especificada nenhuma regra de encriptação para o ID de dispositivo específico nem para o modelo de dispositivo específico, a aplicação aplica a regra de encriptação predefinida.
- Se nem o modelo nem o ID do dispositivo forem conhecidos, a aplicação utiliza a regra de encriptação predefinida.

A aplicação permite preparar uma unidade amovível para utilizar dados encriptados armazenados na mesma, em modo portátil. Após a ativação do modo portátil, pode aceder aos ficheiros encriptados em unidades amovíveis ligadas a um computador sem funcionalidade de encriptação.

- **Gerir regras de acesso às aplicações para ficheiros encriptados**. Para qualquer aplicação, pode criar uma regra de acesso a ficheiros encriptados, que bloqueia o acesso a ficheiros encriptados ou que permite o acesso a ficheiros encriptados apenas como texto cifrado, uma sequência de caracteres obtidos quando a encriptação é aplicada.
- **Criar pacotes encriptados**. Pode criar arquivos encriptados e proteger o acesso a esses arquivos com uma password. Os conteúdos dos arquivos encriptados apenas podem ser acedidos com a introdução de passwords com as quais protegeu o acesso a esses arquivos. Esses arquivos podem ser transmitidos de forma segura através de redes ou em unidades amovíveis.
- **Encriptação de disco completa**. Pode selecionar uma tecnologia de encriptação: Encriptação de disco Kaspersky ou Encriptação de Unidade BitLocker (aqui também referida simplesmente como "BitLocker").

  BitLocker é uma tecnologia que faz parte do sistema operativo Windows. Se um computador estiver equipado com um Trusted Platform Module (TPM), o BitLocker utiliza-o para armazenar chaves de recuperação que fornecem acesso a uma unidade de disco rígido encriptada. Quando o computador inicia, o BitLocker solicita as chaves de recuperação da unidade de disco rígido do Trusted Platform Module e desbloqueia a unidade. Pode configurar a utilização de uma password e/ou código PIN para aceder às chaves de recuperação.

  Pode especificar a regra predefinida de encriptação de disco completa e criar uma lista de unidades de disco rígido a excluir da encriptação. O Kaspersky Endpoint Security realiza a encriptação de disco completa por setor, depois de a política do Kaspersky Security Center ser aplicada. A aplicação encripta todas as partições lógicas das unidades de disco rígido em simultâneo.

  Após a encriptação das unidades de disco rígido do sistema, no próximo arranque do computador, o utilizador tem de efetuar a autenticação utilizando o Agente de Autenticação antes de as unidades de disco rígido poderem ser acedidas e o sistema operativo ser carregado. Para tal é necessário introduzir a password do token ou smart card ligado ao computador ou o nome de utilizador e a password da conta do Agente de Autenticação criada pelo administrador da rede local utilizando a tarefa de *Gestão das contas de Agente de Autenticação*. Estas contas são baseadas em contas do Microsoft Windows com as quais os utilizadores iniciam sessão no sistema operativo. Pode também utilizar a tecnologia Single Sign-On (SSO) que permite iniciar sessão no sistema operativo automaticamente, utilizando o nome de utilizador e a password da conta do Agente de Autenticação.

Se criar uma cópia de segurança de um computador, encriptar os dados do computador e, em seguida, restaurar a cópia de segurança do computador e encriptar os dados do computador novamente, o Kaspersky Endpoint Security cria duplicados das contas do Agente de Autenticação. Para remover as contas duplicadas, tem de utilizar o utilitário klmover com a chave `dupfix`. O utilitário klmover está incluído na compilação do Kaspersky Security Center. Pode ler mais sobre o seu funcionamento na Ajuda do Kaspersky Security Center.

O acesso a unidades de disco rígido encriptadas é possível apenas a partir de computadores nos quais o Kaspersky Endpoint Security com a funcionalidade de encriptação de disco completa esteja instalado. Esta precaução minimiza o risco de perda de dados de uma unidade de disco rígido encriptada quando ocorre uma tentativa de acesso exterior à rede local da empresa.

Para encriptar unidades de disco rígido e unidades amovíveis, pode utilizar a função Encriptar apenas espaço de disco utilizado. Recomenda-se que utilize esta função apenas para novos dispositivos que não tenham sido utilizados anteriormente. Se estiver a aplicar encriptação num dispositivo que já esteja em utilização, recomenda-se que encripte o dispositivo inteiro. Esta ação assegura que todos os dados estão protegidos – até mesmo dados apagados que ainda possam conter informação recuperável.

Antes do início da encriptação, o Kaspersky Endpoint Security obtém o mapa dos setores do sistema de ficheiros. A primeira fase da encriptação inclui setores que estão ocupados por ficheiros no momento em que a encriptação é iniciada. A segunda fase da encriptação inclui setores que foram escritos depois de a encriptação começar. Após a conclusão da encriptação, todos os setores que contêm dados estão encriptados.

Após a conclusão da encriptação e quando um utilizador elimina um ficheiro, os setores onde estava armazenado o ficheiro apagado ficam disponíveis para armazenar informações novas no nível de sistema de ficheiros, mas permanecem encriptados. Assim, à medida que os ficheiros são escritos num novo dispositivo e o dispositivo é encriptado regularmente com a função **Encriptar apenas espaço de disco utilizado** ativada, passado algum tempo todos os setores serão encriptados.

Os dados necessários para desencriptar os ficheiros são fornecidos pelo Servidor de Administração do Kaspersky Security Center que controlava o computador na altura da encriptação. Se o computador com os objetos encriptados for gerido por um Servidor de Administração diferente, pode obter acesso aos dados encriptados de um dos seguintes modos:

- Servidores de Administração na mesma hierarquia:
  - Não é necessário efetuar ações adicionais. O utilizador mantém o acesso aos objetos encriptados. As chaves de encriptação são distribuídas a todos os Servidores de administração.
- Servidores de administração separados:
  - Solicitar o acesso aos objetos encriptados ao administrador da rede local.
  - Restaure os dados nos dispositivos encriptados utilizando a Ferramenta de Restauro.
  - Restaure a configuração do Servidor de administração do Kaspersky Security Center que controlava o computador no momento da encriptação a partir de uma cópia de segurança e utilize esta configuração no Servidor de administração que controla agora o computador com os objetos encriptados.

Se não houver acesso aos dados encriptados, cumpra as instruções especiais para trabalhar com dados encriptados (Restaurar acesso a ficheiros encriptados, Trabalhar com dispositivos encriptados quando não há acesso a eles).

Limitações da funcionalidade de encriptação

A Encriptação de Dados tem as seguintes limitações:

- A aplicação cria ficheiros de serviço durante a encriptação. São necessários cerca de 0.5% de espaço disponível não fragmentado no disco rígido para armazenar os mesmos. Se não existir espaço livre não fragmentado suficiente na unidade de disco rígido, a encriptação não será iniciada até libertar espaço suficiente.

- Pode fazer a gestão de todos os componentes da encriptação de dados na Consola de Administração do Kaspersky Security Center e na Consola Web do Kaspersky Security Center. Na Cloud Console do Kaspersky Security Center, apenas pode fazer a gestão do Bitlocker.

- A encriptação de dados só está disponível quando se utiliza o Kaspersky Endpoint Security com o sistema de administração do Kaspersky Security Center ou a Cloud Console do Kaspersky Security Center (apenas BitLocker). Não é possível a Encriptação de Dados quando usar o Kaspersky Endpoint Security no modo offline porque o Kaspersky Endpoint Security armazena as chaves de encriptação no Kaspersky Security Center.

- Se o Kaspersky Endpoint Security estiver instalado num computador com o Microsoft Windows for Servers, apenas está disponível a encriptação de disco completa com a tecnologia de Encriptação de Unidade BitLocker. Se o Kaspersky Endpoint Security estiver instalado num computador com o Windows para estações de trabalho, a funcionalidade de encriptação de dados está totalmente disponível.

- Se o Kaspersky Endpoint Security estiver instalado num computador baseado em Arm, apenas estará disponível a encriptação completa do disco através da tecnologia BitLocker Drive Encryption; os restantes componentes de encriptação não são suportados.

A encriptação de disco completa utilizando a tecnologia de Encriptação de disco Kaspersky não está disponível para unidades de disco rígido que não cumpram os requisitos de hardware e de software.

A compatibilidade entre a funcionalidade de encriptação completa do disco do Kaspersky Endpoint Security e o Kaspersky Anti-Virus for UEFI não é suportada. O Kaspersky Anti-Virus para UEFI inicia-se antes do carregamento do sistema operativo. Quando utilizar a encriptação completa do disco, a aplicação detetará a ausência de um sistema operativo instalado no computador. Como resultado, o funcionamento do Kaspersky Anti-Virus para UEFI terminará com um erro. A Encriptação ao nível dos ficheiros (FLE) não afeta a operação do Kaspersky Anti-Virus for UEFI.

O Kaspersky Endpoint Security suporta as seguintes configurações:

- HDD, SSD e unidades USB.

  A tecnologia de Encriptação de Disco Kaspersky (FDE) suporta o trabalho com SSD enquanto preserva o desempenho e a vida útil das unidades SSD.

- Unidades ligadas via barramento: SCSI, ATA, IEEE1934, USB, RAID, SAS, SATA, NVME.

- Unidades não amovíveis ligadas via barramento SD ou MMC.

- Unidades com setores de 512 bytes.

- Unidades com setores de 4096 bytes que emulam 512 bytes.

- Unidades com os seguintes tipos de partições: GPT, MBR e VBR (unidades amovíveis).
- Software integrado do padrão UEFI 64 e BIOS Legado.
- Software integrado do padrão UEFI com suporte para Inicialização Segura.

  A *Inicialização Segura* é uma tecnologia concebida para verificar assinaturas digitais para aplicações e controladores do carregador UEFI. A Inicialização Segura bloqueia a inicialização de aplicações e controladores UEFI não assinadas ou assinadas por editores desconhecidos. A Encriptação de Disco Kaspersky (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), poderá ser instalada uma lista desatualizada de certificados de verificação de assinatura digital por predefinição. Antes de encriptar a unidade, precisa de atualizar a lista de certificados.
- Software integrado do padrão UEFI com suporte para Inicialização Rápida (Fast Boot).

  A *Inicialização Rápida* é uma tecnologia que ajuda o computador a inicializar mais rapidamente. Quando a tecnologia Inicialização Rápida está ativada, normalmente o computador carrega apenas o conjunto mínimo de controladores UEFI necessários para iniciar o sistema operativo. Quando a tecnologia Inicialização Rápida está ativada, os teclados USB, ratos, tokens USB, touchpads e ecrãs tácteis podem não funcionar enquanto o Agente de Autenticação está a ser executado.

  Para usar a Encriptação de Disco Kaspersky (FDE), recomendamos a desativação da tecnologia Inicialização Rápida. Pode usar o Utilitário de teste FDE para testar a operação da Encriptação de Disco Kaspersky (FDE).

O Kaspersky Endpoint Security não suporta as seguintes configurações:

- O carregador de arranque está localizado numa unidade enquanto o sistema operativo está localizado numa unidade diferente.
- O sistema contém o software integrado da norma UEFI 32.
- O sistema dispõe da Tecnologia Rapid Start da Intel® e unidades que têm uma partição de hibernação mesmo quando a Tecnologia Rapid Start da Intel® está desativada.
- Unidades no formato MBR com mais de 10 partições expandidas.
- O sistema possui um ficheiro de troca localizado numa unidade que não é do sistema.
- Sistema Multiboot com vários sistemas operativos instalados em simultâneo.
- Partições dinâmicas (são suportadas apenas as partições primárias).
- Unidades com menos de 0.5% de espaço em unidade de disco livre por desfragmentar.
- 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 comprimidos.

- A tecnologia de Encriptação de Disco Kaspersky (FDE) é incompatível com outras tecnologias de encriptação de disco completa (como BitLocker, McAfee Drive Encryption e WinMagic SecureDoc).
- A tecnologia de Encriptação de Disco Kaspersky (FDE) é incompatível com a tecnologia ExpressCache.
- A criação, eliminação e modificação de partições numa unidade encriptada não é suportada. Pode ocorrer a perda de dados.
- A formatação do sistema de ficheiros não é suportada. Pode ocorrer a perda de dados.

  Se precisar de formatar uma unidade que foi encriptada com a tecnologia de Encriptação de Disco Kaspersky (FDE), formate a unidade num computador que não tenha o Kaspersky Endpoint Security for Windows e use apenas a encriptação de disco completa.

  Uma unidade encriptada formatada com a opção de formatação rápida poderá ser erradamente identificada como encriptada na próxima vez que for ligada a um computador com o Kaspersky Endpoint Security for Windows instalado. Os dados do utilizador ficarão indisponíveis.
- O Agente de Autenticação não suporta mais de 100 contas.
- A tecnologia Single Sign-On é incompatível com outras tecnologias de programadores de terceiros.
- A tecnologia de Encriptação de Disco Kaspersky (FDE) não é suportada nos seguintes modelos de dispositivos:
  - Dell Latitude E6410 (modo UEFI)
  - HP Compaq nc8430 (modo BIOS legado)
  - Lenovo ThinkCenter 8811 (modo BIOS legado)
- O Agente de Autenticação não suporta o trabalho com tokens USB quando o Legacy USB Support está ativado. Apenas a autenticação baseada em password será possível no computador.
- Ao encriptar uma unidade no modo BIOS legado, é aconselhável ativar o 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
- HP Compaq dx2450 Microtower PC
- 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 (motherboard)

Alterar o comprimento da chave de encriptação (AES56 / AES256)

O Kaspersky Endpoint Security utiliza o algoritmo de encriptação AES (Padrão de Encriptação Avançado). O Kaspersky Endpoint Security suporta o algoritmo de encriptação AES com um comprimento de chave de 256 ou 56 bits. O algoritmo de encriptação de dados depende da biblioteca de encriptação AES incluída no pacote de distribuição: *Encriptação forte (AES256)* ou *Encriptação leve (AES56).* A biblioteca de encriptação AES é instalada juntamente com a aplicação.

A alteração do comprimento da chave de encriptação só está disponível para o Kaspersky Endpoint Security 11.2.0 ou posterior.

A alteração do comprimento da chave de encriptação consiste nas seguintes etapas:

1. Desencriptar objetos que o Kaspersky Endpoint Security encriptou antes de começar a alterar o comprimento da chave de encriptação:

   a. Desencriptar unidades de disco rígido.

   b. Desencriptar ficheiros em unidades locais.

   c. Desencriptar unidades amovíveis.

   Depois da alteração do comprimento da chave de encriptação, os objetos que foram anteriormente encriptados ficam indisponíveis.

2. Remover o Kaspersky Endpoint Security.

3. Instalar o Kaspersky Endpoint Security a partir do pacote de distribuição do Kaspersky Endpoint Security que contém uma biblioteca de encriptação diferente.

Também pode alterar o comprimento da chave de encriptação atualizando a aplicação. O comprimento da chave pode ser alterado através de uma atualização da aplicação apenas se as seguintes condições forem satisfeitas:

- O Kaspersky Endpoint Security versão 10 Service Pack 2 ou posterior está instalado no computador.
- Os componentes de encriptação de dados (Encriptação ao nível dos ficheiros, Encriptação de disco completa) não estão instalados no computador.

  Por defeito, os componentes de encriptação de dados não estão incluídos no Kaspersky Endpoint Security. O componente BitLocker Management não afeta a alteração do comprimento da chave de encriptação.

Para alterar o comprimento da chave de encriptação, execute o ficheiro kes_win.msi ou setup_kes. exe a partir do pacote de distribuição que contém a biblioteca de encriptação necessária. Também pode atualizar remotamente a aplicação utilizando o pacote de instalação.

Não é possível alterar o comprimento da chave de encriptação com o pacote de distribuição da mesma versão da aplicação instalada no seu computador sem primeiro desinstalar a aplicação.

Encriptação de disco Kaspersky

O Encriptação de disco Kaspersky não é compatível com computadores baseados em Arm.

A Encriptação de disco Kaspersky só está disponível em computadores que executem um sistema operativo Windows para estações de trabalho. Para computadores que executam um sistema operativo Windows para servidores, utilize a tecnologia de Encriptação de Unidade BitLocker.

O Kaspersky Endpoint Security suporta a encriptação de disco completa nos sistemas de ficheiros FAT32, NTFS e exFat.

Antes de iniciar a encriptação de disco completa, a aplicação executa várias verificações para determinar se o dispositivo pode ser encriptado, o que inclui verificar se o disco rígido do sistema tem compatibilidade com o Agente de Autenticação ou os componentes de encriptação BitLocker. Para verificar a compatibilidade, é necessário reiniciar o computador. Após o computador reiniciar, a aplicação efetua todas as verificações necessárias automaticamente. Se a verificação de compatibilidade for bem-sucedida, a encriptação de disco completa é iniciada depois de o sistema operativo carregar e de a aplicação ser iniciada. Se a unidade de disco rígido do sistema não for compatível com o Agente de Autenticação ou com os componentes de encriptação BitLocker, o computador tem de ser reiniciado premindo o botão Reiniciar hardware. O Kaspersky Endpoint Security regista informações sobre a incompatibilidade. Com base nestas informações, a aplicação não inicia a encriptação de disco completa no arranque do sistema operativo. As informações sobre este evento são registadas nos relatórios do Kaspersky Security Center.

Se a configuração de hardware do computador tiver sido alterada, a informação de incompatibilidade registada pela aplicação durante a verificação anterior deve ser apagada para que a unidade de disco rígido do sistema seja verificada quanto à compatibilidade com o Agente de Autenticação e com os componentes de encriptação BitLocker. Para tal, antes da encriptação de disco completa, introduza `avp pbatestreset` na command line. Se o sistema operativo não carregar após a verificação da unidade de disco rígido do sistema quanto a compatibilidade pelo Agente de Autenticação, remova os objetos e os dados restantes após a operação de teste do Agente de Autenticação utilizando a Ferramenta de Restauro e, em seguida, inicie o Kaspersky Endpoint Security e execute o comando `avp pbatestreset` novamente.

Após iniciar a encriptação de disco completa, o Kaspersky Endpoint Security encripta todos os dados gravados nas unidades de disco rígido.

Se o utilizador encerrar ou reiniciar o computador durante a encriptação de disco completa, o Agente de Autenticação é carregado antes do próximo arranque do sistema operativo. O Kaspersky Endpoint Security retoma a encriptação de disco completa após a autenticação com êxito no Agente de Autenticação e o arranque do sistema operativo.

Se o sistema operativo passar para o modo de hibernação durante a encriptação de disco completa, o Agente de Autenticação é carregado quando o sistema operativo sair do modo de hibernação. O Kaspersky Endpoint Security retoma a encriptação de disco completa após a autenticação com êxito no Agente de Autenticação e o arranque do sistema operativo.

Se o sistema operativo entrar em modo de suspensão durante a encriptação de disco completa, o Kaspersky Endpoint Security retoma a encriptação de disco completa quando o sistema operativo sair do modo de suspensão sem carregar o Agente de Autenticação.

A autenticação do utilizador no Agente de Autenticação pode ser efetuada de duas formas:

- Introduzindo o nome e a password da conta do Agente de Autenticação criada pelo administrador da rede da empresa utilizando as ferramentas do Kaspersky Security Center.
- Introduza a password de um token ou smart card ligado ao computador.

  A utilização de um token ou smart-card está disponível apenas se as unidades de disco rígido do computador tiverem sido encriptadas ao utilizar o algoritmo de encriptação AES256. Se os discos rígidos do computador foram encriptados através do algoritmo de encriptação AES56, a adição do ficheiro de certificado eletrónico ao comando será negada.

O agente de autenticação suporta esquemas de teclado para os idiomas seguintes:

- Inglês (Reino Unido)
- Inglês (EUA)

- Árabe (Argélia, Marrocos, Tunísia, esquema AZERTY)
- Castelhano (América Latina)
- Italiano
- Alemão (Alemanha e Áustria)
- Alemão (Suíça)
- Português (Brasil, esquema ABNT2)
- Russo (para IBM de 105 teclas/teclados Windows com esquema QWERTY)
- Turco (esquema QWERTY)
- Francês (França)
- Francês (Suíça)
- Francês (Bélgica, esquema AZERTY)
- Japonês (para teclados de 106 teclas com esquema QWERTY)

Um esquema de teclado fica disponível no Agente de Autenticação se este esquema tiver sido adicionado nas definições de idioma e região do sistema operativo e estiver disponível no ecrã de boas-vindas do Microsoft Windows.

Se o nome da conta do Agente de Autenticação incluir símbolos que não podem ser introduzidos utilizando os esquemas do teclado disponíveis no Agente de Autenticação, as unidades de disco rígido encriptadas podem ser acedidas apenas após serem restauradas utilizando a Ferramenta de Restauro ou após o nome e a password da conta de agente de autenticação serem recuperados.

Funcionalidades especiais de encriptação de unidade SSD

A aplicação suporta a encriptação de unidades SSD, unidades SSHD híbridas e unidades com a funcionalidade Intel Smart Response. A aplicação não suporta a encriptação de unidades com a funcionalidade Intel Rapid Start. Desative a funcionalidade Intel Rapid Start antes de encriptar esta unidade.

A encriptação de unidades SSD tem as seguintes funcionalidades especiais:

- Se uma unidade SSD for nova e não contiver dados confidenciais, ative a encriptação apenas do espaço ocupado. Isso permite substituir os setores relevantes da unidade.
- Se uma unidade SSD estiver a ser utilizada e tiver dados confidenciais, selecione uma das seguintes opções:
  - Limpe totalmente a unidade SSD (Secure Erase), instale o sistema operativo e execute a encriptação da unidade SSD com a opção de encriptar apenas o espaço ocupado ativado.
  - Execute a encriptação da unidade SSD com a opção de encriptar apenas o espaço ocupado desativado.

A encriptação de uma unidade SSD requer 5 a 10 GB de espaço livre. Os requisitos de espaço livre para armazenar dados de administração de encriptação estão indicados na tabela abaixo.

Requisitos de espaço livre para armazenamento de dados de administração de encriptação

Tamanho da unidade SSD (GB)	Espaço livre na partição principal da unidade SSD (MB)	Espaço livre na partição secundária da unidade SSD (MB)
128	250	64
256	250	640
512	300	128

A iniciar a encriptação de disco Kaspersky

Antes de iniciar a encriptação de disco completa, certifique-se de que o mesmo não está infetado. Para tal, inicie a tarefa de Verificação Completa ou Verificação de Áreas Críticas. A execução da encriptação de disco completa num computador infetado por um rootkit pode fazer com que o computador deixe de funcionar.

Antes de iniciar a encriptação do disco, tem de verificar as definições das contas do Agente de Autenticação. O Agente de Autenticação é necessário para trabalhar com unidades protegidas com a tecnologia Encriptação de disco Kaspersky (FDE). Antes de o sistema operativo ser carregado, o utilizador tem de concluir a autenticação com o Agente. O Kaspersky Endpoint Security permite criar automaticamente contas do Agente de Autenticação antes de encriptar uma unidade. Pode ativar a criação automática de contas do Agente de Autenticação nas Definições da política de Encriptação de disco completa (consulte as instruções abaixo). Pode também usar a tecnologia de autenticação única (SSO).

O Kaspersky Endpoint Security permite criar automaticamente o Agente de Autenticação para os seguintes grupos de utilizadores:

- **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 do 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 em algum momento.
- **Conta de serviço com uma password única**. A conta de serviço é necessária para obter acesso ao computador, por exemplo, quando o utilizador se esquece da password. Também pode utilizar a conta de serviço como uma conta de reserva. Tem de inserir o nome da conta (por defeito, `ServiceAccount`). O Kaspersky Endpoint Security cria uma password automaticamente. Pode encontrar a password na consola do Kaspersky Security Center.
- **Administrador local**. O Kaspersky Endpoint Security cria uma conta de utilizador do Agente de Autenticação para o administrador local do computador.
- **Gestor do computador**. O Kaspersky Endpoint Security cria uma conta de utilizador do Agente de Autenticação para a conta do gestor do computador. Pode ver qual é a conta que tem a função de gestor do computador nas propriedades do computador no Active Directory. Por defeito, a função de gestor do computador não está definida, ou seja, não corresponde a uma conta.
- **Conta ativa**. O Kaspersky Endpoint Security cria automaticamente uma conta do Agente de Autenticação para a conta que está ativa no momento da encriptação do disco.

A tarefa *Gestão das contas de Agente de Autenticação* foi concebida para definir as definições de autenticação do utilizador. Pode utilizar esta tarefa para adicionar contas novas, modificar as definições de contas atuais ou remover contas, se necessário. 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 a Encriptação de disco Kaspersky através da Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Encriptação de dados → Encriptação de disco completa**.
4. Na lista pendente **Tecnologia de encriptação**, selecione **Encriptação de disco Kaspersky**.

   A tecnologia de encriptação de disco Kaspersky não pode ser utilizada se o computador tiver unidades de disco rígido que foram encriptadas pelo BitLocker.

5. Na lista pendente **Modo de encriptação**, selecione **Encriptar todas as unidades de discos rígido**.

   Se o computador tiver vários sistemas operativos instalados, após encriptar todos os discos rígidos apenas será possível carregar o sistema operativo que tem a aplicação instalada.

   Se for necessário excluir algumas das unidades de disco rígido da encriptação, crie uma lista com essas unidades de disco rígido.

6. Configure as opções avançadas da Encriptação de disco Kaspersky (consulte a tabela abaixo).
7. Guarde as suas alterações.

Como executar a Encriptação de disco Kaspersky através da Consola Web e da Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Data Encryption → Full Disk Encryption**.
5. Selecione a tecnologia **Kaspersky Disk Encryption**.

   A tecnologia de encriptação de disco Kaspersky não pode ser utilizada se o computador tiver unidades de disco rígido que foram encriptadas pelo BitLocker.

6. No bloco **Action on devices**, selecione **Encrypt all hard drives**.

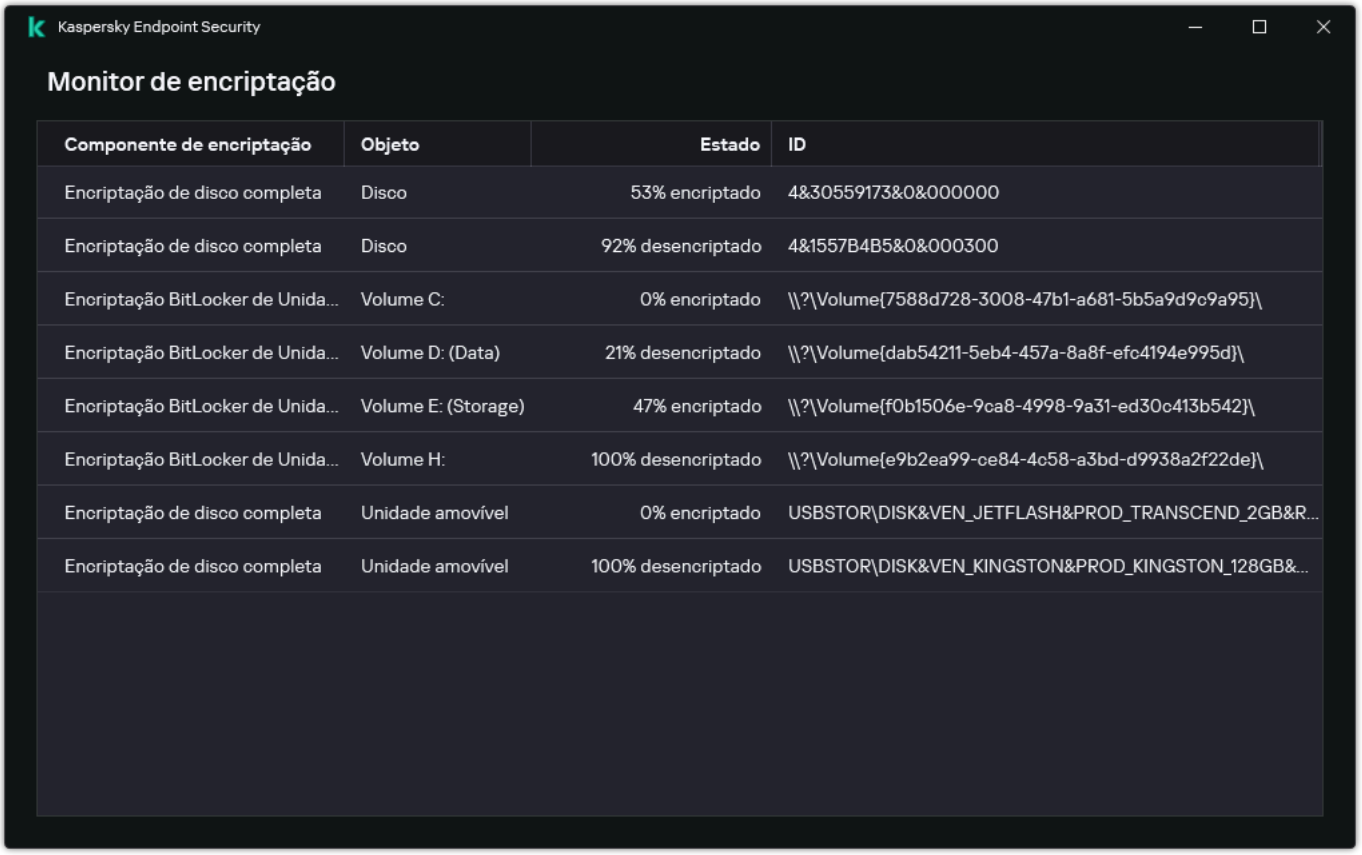
Se o computador tiver vários sistemas operativos instalados, após a encriptação, apenas será possível carregar o sistema operativo em que a encriptação foi realizada.

Se for necessário excluir algumas das unidades de disco rígido da encriptação, crie uma lista com essas unidades de disco rígido.

7. Configure as opções avançadas da Encriptação de disco Kaspersky (consulte a tabela abaixo).

8. Guarde as suas alterações.

Pode utilizar a ferramenta Monitor de Encriptação para controlar o processo de encriptação ou desencriptação de disco no computador de um utilizador. Pode executar a ferramenta Monitor de Encriptação na janela principal da aplicação.



Monitor de encriptação

Se as unidades de disco rígido do sistema estiverem encriptadas, o Agente de Autenticação é carregado antes do arranque do sistema operativo. Utilize o Agente de Autenticação para concluir a autenticação para obter o acesso a unidades de disco rígido do sistema encriptadas e para carregar o sistema operativo. Após a conclusão bem-sucedida do procedimento de autenticação, o sistema operativo é carregado. O processo de autenticação é repetido sempre que o sistema operativo é reiniciado.

Parâmetro	Descrição
Criar automaticamente contas do Agente de Autenticação para utilizadores durante a encriptação	Se esta caixa de verificação estiver selecionada, a aplicação cria contas do Agente de Autenticação com base na lista de contas de utilizador do Windows no computador. Por predefinição, o Kaspersky Endpoint Security utiliza todas as contas locais e de domínio com as quais o utilizador iniciou a sessão no sistema operativo ao longo dos últimos 30 dias.
Criar automaticamente contas do Agente de Autenticação para todos os utilizadores deste computador ao iniciar sessão	Se esta caixa de verificação estiver selecionada, a aplicação verifica as informações sobre as contas de utilizador do Windows no computador antes de iniciar o Agente de Autenticação. Se o Kaspersky Endpoint Security detetar uma conta de utilizador do Windows sem conta do Agente de Autenticação, a aplicação criará uma nova conta para aceder às unidades encriptadas. A nova conta do Agente de Autenticação terá as seguintes definições predefinidas: início de sessão protegido apenas por password e alteração da password na primeira autenticação. Como tal, não é necessário adicionar manualmente contas do Agente de Autenticação através da tarefa *Gestão das contas de Agente de Autenticação* para computadores com unidades já encriptadas.
Guardar o nome de utilizador introduzir no Agente de Autenticação	Se a caixa de verificação for selecionada, a aplicação guarda o nome da conta do Agente de Autenticação. Não será solicitada a introdução do nome da conta da próxima vez que tentar concluir a autorização no Agente de Autenticação com a mesma conta.
Encriptar apenas espaço utilizado do disco (reduz tempo de encriptação)	Esta caixa ativa/desativa a opção que limita a área de encriptação a setores ocupados do disco rígido. Este limite permite reduzir o tempo de encriptação. Ativar ou desativar a funcionalidade **Encriptar apenas espaço utilizado do disco (reduz tempo de encriptação)** após o início da encriptação não altera esta definição até que os discos rígidos sejam desencriptados. Tem de selecionar ou desmarcar a caixa de verificação antes de iniciar a encriptação. Se a caixa de verificação estiver selecionada, são encriptadas apenas as partes do disco rígido que estiverem ocupadas por ficheiros. O Kaspersky Endpoint Security encripta automaticamente dados novos quando são adicionados. Se a caixa de verificação estiver selecionada, é encriptado o disco rígido completo, incluindo os fragmentos residuais de ficheiros anteriormente eliminados e modificados. Recomenda-se esta opção para discos rígidos novos cujos dados não tenham sido modificados ou eliminados. Se estiver a aplicar encriptação num disco rígido que já esteja em utilização, recomenda-se encriptar o disco rígido completo. Dessa forma, assegura a proteção de todos os dados, mesmo os dados eliminados que sejam potencialmente recuperáveis. Por padrão, a caixa de verificação está desmarcada.
Utilizar Legacy USB Support (não recomendado)	Esta caixa de seleção ativa ou desativa a funcionalidade Legacy USB Support. O *Suporte de USB legado* **é** uma função BIOS/UEFI que permite usar dispositivos USB (como um token de segurança) durante a fase de inicialização do computador antes de iniciar o sistema operativo (modo BIOS). O Legacy USB Support não afeta o suporte para dispositivos USB após iniciar o sistema operativo. Se a caixa de verificação estiver selecionada, o suporte de dispositivos USB durante o arranque inicial do computador é ativado. Quando a função Legacy USB Support está ativa, o Agente de autenticação no modo BIOS não suporta trabalho com tokens via USB. Recomenda-se utilizar esta opção apenas quando existir um problema de compatibilidade de hardware e só para os computadores nos quais o problema ocorreu.

Criar uma lista de unidades de disco rígido excluídas da encriptação

Pode criar uma lista de exclusões da encriptação apenas para a tecnologia de Encriptação de disco Kaspersky.

Para formar uma lista de unidades de disco rígido excluídas da encriptação:

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Encriptação de dados → Encriptação de disco completa**.
4. Na lista pendente **Tecnologia de encriptação**, selecione **Encriptação de disco Kaspersky**.

   As entradas correspondentes a unidades de disco rígido excluídas da encriptação são apresentadas na tabela **Não encriptar as unidades de disco rígido seguintes**. Esta tabela está vazia caso não tenha sido previamente formada uma lista de unidades de disco rígido excluídas da encriptação.
5. Para adicionar unidades de disco rígido à lista de unidades de disco rígido excluídas da encriptação:

   a. Clique em **Adicionar**.

   b. Na janela que se abre, especifique os valores para **Nome do dispositivo**, **Computador**, **Tipo de disco**, **Encriptação de disco Kaspersky**.

   c. Clique em **Atualizar**.

   d. Na coluna **Nome**, selecione as caixas de verificação nas linhas da tabela correspondentes às unidades de disco rígido que pretende adicionar à lista de unidades de disco rígido excluídas da encriptação.

   e. Clique em **Ok**.

   As unidades de disco rígido selecionadas são apresentadas na tabela **Não encriptar as unidades de disco rígido seguintes**.
6. Guarde as suas alterações.

Exportar e importar uma lista de discos rígidos excluídos da encriptação

Pode exportar a lista de exclusões de encriptação do disco rígido para um ficheiro XML. Em seguida, pode modificar o ficheiro para, por exemplo, adicionar um grande número de exclusões do mesmo tipo. Também pode usar a função de exportação/importação para fazer uma cópia de segurança da lista de exclusões ou para migrar as exclusões para um servidor diferente.

Como exportar e importar uma lista de exclusões de encriptação do disco rígido na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Encriptação de dados → Encriptação de disco completa**.
4. Na lista pendente **Tecnologia de encriptação**, selecione **Encriptação de disco Kaspersky**.

   As entradas correspondentes a unidades de disco rígido excluídas da encriptação são apresentadas na tabela **Não encriptar as unidades de disco rígido seguintes**.

5. Para exportar a lista de exclusões:

   a. Selecione as exclusões que pretende exportar. Para selecionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.

      Se não tiver selecionado nenhuma exclusão, o Kaspersky Endpoint Security exportará todas as exclusões.

   b. Selecione o botão → **Exportar**.

   c. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de exclusões e selecione a pasta onde pretende guardar este ficheiro.

   d. Guardar o ficheiro.

      O Kaspersky Endpoint Security exporta toda a lista de exclusões para o ficheiro XML.

6. Para importar a lista de regras:

   a. Selecione o botão → **Importar**.

   b. Na janela que se abre, selecione o ficheiro XML do qual deseja importar a lista de exclusões.

   c. Abrir o ficheiro.

      Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security irá solicitar-lhe a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro XML.

7. Guarde as suas alterações.

Como exportar e importar uma lista de exclusões de encriptação do disco rígido na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Data Encryption** → **Full Disk Encryption**.

   Selecione a tecnologia **Kaspersky Disk Encryption**.

5. Clique na hiperligação **Exclusions**.

   Abre-se a lista de exclusões.

6. Para exportar a lista de regras:

   a. Selecione as exclusões que pretende exportar.

   b. Selecione o botão → **Export**.

      O Kaspersky Endpoint Security exporta a lista de exclusões para um ficheiro JSON na pasta de transferências predefinida.

7. Para importar a lista de exclusões:

   a. Selecione o botão → **Import**.

      Na janela que se abre, selecione o ficheiro JSON do qual deseja importar a lista de exclusões.

b. Abrir o ficheiro.

Se o computador já tiver uma lista de exclusões, o Kaspersky Endpoint Security irá solicitar-lhe a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro JSON.

8. Guarde as suas alterações.

Ativação da tecnologia de autenticação única (SSO)

A tecnologia de Single Sign-On (SSO) permite que efetue o início de sessão automaticamente no sistema operativo usando as credenciais do Agente de Autenticação. Isto significa que um utilizador apenas precisa de introduzir uma password uma única vez ao iniciar sessão no Windows (password da conta do Agente de Autenticação). A tecnologia Início de Sessão Único também lhe permite atualizar automaticamente a password da conta do Agente de Autenticação quando a password da conta Windows é alterada.

Ao usar a tecnologia de autenticação única, o Agente de Autenticação ignora os requisitos de segurança da password especificados no Kaspersky Security Center. Pode definir os requisitos de segurança da password nas definições do sistema operativo.

Ativação da tecnologia de autenticação única

Como ativar a utilização da tecnologia de autenticação única na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Encriptação de dados → Definições de encriptação comuns**.
4. No bloco **Definições de password**, clique no botão **Definições**.
5. Na janela que surgir, no separador **Agente de Autenticação**, selecione a caixa de verificação **Utilizar a tecnologia SSO (Single Sign-On)**.
6. Se estiver a utilizar um fornecedor de credenciais de terceiros, selecione a caixa de verificação **Envolver fornecedores de credenciais de terceiros**.
7. Guarde as suas alterações.

Como resultado, o utilizador precisa de concluir o procedimento de autenticação apenas uma vez com o Agente. O procedimento de autenticação não é necessário para iniciar o sistema operativo. O sistema operativo é iniciado automaticamente.

Como ativar a utilização da tecnologia de autenticação única na Consola da Web

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.

4. Aceda a **Data Encryption → Full Disk Encryption**.

5. Selecione a tecnologia **Kaspersky Disk Encryption**.

6. No bloco **Password settings**, selecione a caixa de verificação **Use Single Sign-On (SSO) technology**.

7. Se estiver a utilizar um fornecedor de credenciais de terceiros, selecione a caixa de verificação **Wrap third-party credential providers**.

8. Guarde as suas alterações.

Como resultado, o utilizador precisa de concluir o procedimento de autenticação apenas uma vez com o Agente. O procedimento de autenticação não é necessário para iniciar o sistema operativo. O sistema operativo é iniciado automaticamente.

Para a tecnologia de autenticação única (SSO) funcionar, a password da conta do Windows e a password da conta do Agente de Autenticação devem corresponder. Se as passwords não corresponderem, o utilizador precisa de executar o procedimento de autenticação duas vezes: na interface do Agente de Autenticação e antes de iniciar o sistema operativo. Estas ações precisam de ser executadas apenas uma vez para sincronizar as passwords. Depois disso, o Kaspersky Endpoint Security substitui a password da conta do Agente de Autenticação pela password da conta do Windows. Quando a password da conta do Windows é alterada, a aplicação atualiza automaticamente a password da conta do Agente de Autenticação.

Fornecedores de credenciais de terceiros

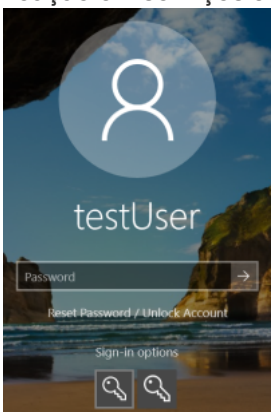
O Kaspersky Endpoint Security suporta o fornecedor de credenciais de terceiros ADSelfService Plus.

Ao trabalhar com fornecedores de credenciais de terceiros, o Agente de Autenticação interceta a password antes de o sistema operativo ser carregado. Isto significa que um utilizador apenas precisa de introduzir uma password uma única vez ao iniciar sessão no Windows. Depois de iniciar sessão no Windows, o utilizador pode utilizar as capacidades de um fornecedor de credenciais de terceiros para realizar a autenticação em serviços empresariais, por exemplo. Os fornecedores de credenciais de terceiros também permitem aos utilizadores repor a sua própria password de forma independente. Neste caso, o Kaspersky Endpoint Security irá atualizar automaticamente a password do Agente de Autenticação.

Se estiver a utilizar um fornecedor de credenciais de terceiros que não seja suportado pela aplicação, poderá encontrar algumas limitações no funcionamento da tecnologia de Início de Sessão Único. Ao iniciar sessão no Windows, estarão disponíveis dois perfis para o utilizador: o fornecedor de credenciais no sistema e o fornecedor de credenciais de terceiros. Os ícones destes perfis serão idênticos (consulte a figura abaixo). O utilizador terá as seguintes opções para continuar:

- Se o utilizador selecionar o *fornecedor de credenciais de terceiros*, o Agente de Autenticação não poderá sincronizar a password com a conta do Windows. Portanto, se o utilizador tiver alterado a password da conta do Windows, o Kaspersky Endpoint Security não pode atualizar a password da conta do Agente de Autenticação. Como resultado, o utilizador precisa de executar o procedimento de autenticação duas vezes: na interface do Agente de Autenticação e antes de iniciar o sistema operativo. Neste caso, o utilizador pode utilizar as capacidades de um fornecedor de credenciais de terceiros para realizar a autenticação em serviços empresariais, por exemplo.

- Se o utilizador selecionar o *fornecedor de credenciais no sistema*, o Agente de Autenticação irá sincronizar as passwords com a conta do Windows. Neste caso, o utilizador não pode utilizar as capacidades de um fornecedor de terceiros para realizar a autenticação em serviços empresariais, por exemplo.



Perfil de autenticação do sistema e perfil de autenticação de terceiros para início de sessão do Windows

Gestão de contas do agente de autenticação

O Agente de Autenticação é necessário para trabalhar com unidades protegidas com a tecnologia Encriptação de disco Kaspersky (FDE). Antes de o sistema operativo ser carregado, o utilizador tem de concluir a autenticação com o Agente. A tarefa *Manage Authentication Agent accounts* foi concebida para definir as definições de autenticação do utilizador. Pode usar tarefas locais para computadores individuais, bem como tarefas de grupo para computadores de grupos de administração separados ou uma seleção de computadores.

Não pode configurar um agendamento para iniciar a tarefa *Manage Authentication Agent accounts*. É igualmente impossível interromper uma tarefa à força.

Como criar a tarefa Gerir contas do Agente de Autenticação na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Gestão das contas de Agente de Autenticação**.

Passo 2. Selecionar um comando de gestão da conta do Agente de Autenticação

Gere uma lista de comandos de gestão da conta do Agente de Autenticação. Os comandos de gestão permitem adicionar, modificar e eliminar contas do Agente de Autenticação (consulte as instruções abaixo). Somente utilizadores com uma conta do Agente de Autenticação podem concluir o procedimento de autenticação, carregar o sistema operativo e obter acesso à unidade encriptada.

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

Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 4. Definir o nome da tarefa

Digite um nome para a tarefa, por exemplo, *Contas de Administrador*.

Passo 5. Completar a criação da tarefa

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa.

Como resultado, após a conclusão da tarefa no próximo arranque do computador, somente utilizadores com uma conta do Agente de Autenticação podem concluir o procedimento de autenticação, carregar o sistema operativo e obter acesso à unidade encriptada.

Como criar a tarefa Gerir contas do Agente de Autenticação na Consola da Web

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

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

Passo 1. Configurar definições da tarefa geral

Configurar definições da tarefa geral:

1. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.
2. Na lista pendente **Task type**, selecione **Manage Authentication Agent accounts**.
3. No campo **Task name**, introduza uma breve descrição, por exemplo, *Administrator accounts*.
4. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

Passo 2. Gestão das contas do Agente de Autenticação

Gere uma lista de comandos de gestão da conta do Agente de Autenticação. Os comandos de gestão permitem adicionar, modificar e eliminar contas do Agente de Autenticação (consulte as instruções abaixo). Somente utilizadores com uma conta do Agente de Autenticação podem concluir o procedimento de autenticação, carregar o sistema operativo e obter acesso à unidade encriptada.

Passo 3. Completar a criação da tarefa

Conclua o assistente. Será apresentada uma nova tarefa na lista de tarefas.

Para executar uma tarefa, selecione a caixa de seleção em frente da tarefa e clique no botão **Start**.

Como resultado, após a conclusão da tarefa no próximo arranque do computador, somente utilizadores com uma conta do Agente de Autenticação podem concluir o procedimento de autenticação, carregar o sistema operativo e obter acesso à unidade encriptada.

Para adicionar uma conta do Agente de Autenticação, tem de adicionar um comando especial à tarefa *Manage Authentication Agent accounts*. É conveniente usar uma tarefa de grupo, por exemplo, para adicionar uma conta de administrador a todos os computadores.

O Kaspersky Endpoint Security permite criar automaticamente contas do Agente de Autenticação antes de encriptar uma unidade. Pode ativar a criação automática de contas do Agente de Autenticação nas Definições da política de Encriptação de disco completa. Pode também usar a tecnologia de autenticação única (SSO).

Como adicionar uma conta do Agente de Autenticação através da Consola de Administração (MMC)

1. Abra as propriedades da tarefa *Gestão das contas de Agente de Autenticação*.
2. Nas propriedades da tarefa, selecione a secção **Definições**.
3. Clique em **Adicionar → Comando de adição de conta**.
4. Na janela que surgir, no campo **Conta do Windows**, especifique o nome da conta de utilizador do Microsoft Windows utilizada para criar a conta do Agente de Autenticação.
5. Se introduziu manualmente o nome de uma conta do Windows, clique no botão **Permitir** para definir o identificador de segurança (SID) da conta.

   Se optar por não determinar o identificador de segurança (SID), clicando no botão **Permitir**, este será determinado quando 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 fiável, a tarefa *Gestão das contas de Agente de Autenticação* terminará com um erro.

6. Selecione a caixa de verificação **Substituir conta existente** se pretender que a conta existente previamente criada para o Agente de Autenticação seja substituída pela conta que está a ser criada.

   > Este passo está disponível quando adiciona um comando de criação de conta do Agente de Autenticação nas propriedades de uma tarefa de grupo para gestão de contas de agente de autenticação. Este passo está disponível quando adiciona um comando de criação de conta do Agente de Autenticação nas propriedades de uma tarefa local de *Gestão das contas de Agente de Autenticação*.

7. No campo **Nome de utilizador**, introduza o nome da conta do Agente de Autenticação que tem de ser introduzido durante a autenticação para aceder a unidades de disco rígido encriptadas.
8. Selecione a caixa de verificação **Permitir autenticação baseada em password** se pretender que a aplicação solicite ao utilizador a introdução da password da conta do Agente de Autenticação, durante a autenticação para aceder às unidades de disco rígido encriptadas. Defina uma password para a conta do Agente de Autenticação. Se necessário, pode solicitar uma nova password ao utilizador após a primeira autenticação.
9. Selecione a caixa de verificação **Permitir autenticação baseada em certificado** se pretender que a aplicação solicite ao utilizador a ligação de um token ou de um smart-card ao computador durante a autenticação da conta do Agente de Autenticação para aceder às unidades de disco rígido encriptadas. Selecione um ficheiro de certificado para autenticação com um cartão inteligente ou token.
10. Se solicitado, no campo **Descrição do comando**, introduza os detalhes da conta do Agente de Autenticação necessários para a gestão do comando.
11. No bloco **Acesso à autenticação no Agente de Autenticação**, configure o acesso à autenticação no Agente de Autenticação para o utilizador que utiliza a conta especificada no comando.
12. Guarde as suas alterações.

Como adicionar uma conta do Agente de Autenticação através da Consola da Web

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Manage Authentication Agent accounts** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

3. Selecione o separador **Application settings**.

4. Na lista de contas do Agente de Autenticação, clique no botão **Add** e selecione o tipo de comando **Add account**.

5. Selecione uma conta de utilizador. Pode selecionar uma conta na lista de contas de domínio ou inserir manualmente o nome da conta. Avance para o passo seguinte.

   O Kaspersky Endpoint Security determina o identificador de segurança da conta (Security Identifier, SID). Isto é necessário para verificar a conta. Se tiver digitado o nome de utilizador incorretamente, o Kaspersky Endpoint Security encerrará a tarefa com um erro.

6. Configure as definições da conta do Agente de Autenticação.

   - **Create a new Authentication Agent account to replace the existing account**. O Kaspersky Endpoint Security verifica as contas existentes no computador. Se a ID de segurança do utilizador no computador e na tarefa corresponderem, o Kaspersky Endpoint Security alterará as definições da conta do utilizador de acordo com a tarefa.

   - **User name**. O nome de utilizador padrão da conta do Agente de Autenticação corresponde ao nome de domínio do utilizador.

   - **Allow password-based authentication**. Defina uma password para a conta do Agente de Autenticação. Se necessário, pode solicitar uma nova password ao utilizador após a primeira autenticação. Assim, cada utilizador terá sua própria password exclusiva. Pode também definir os requisitos de segurança da password para a conta do Agente de Autenticação na política.

   - **Allow certificate-based authentication**. Selecione um ficheiro de certificado para autenticação com um cartão inteligente ou token. Dessa forma, o utilizador terá de digitar a password do cartão inteligente ou token.

   - **Account access to encrypted data**. Configure o acesso do utilizador à unidade encriptada. Pode, por exemplo, desativar temporariamente a autenticação do utilizador em vez de eliminar a conta do Agente de Autenticação.

   - **Comment**. Digite uma descrição da conta, se necessário.

7. Guarde as suas alterações.

8. Selecione a caixa de verificação junto à tarefa e clique no botão **Start**.

   Como resultado, após a conclusão da tarefa no próximo arranque do computador, somente utilizadores com uma conta do Agente de Autenticação podem concluir o procedimento de autenticação, carregar o sistema operativo e obter acesso à unidade encriptada.

Para alterar a password e outras definições da conta do Agente de Autenticação, tem de adicionar um comando especial à tarefa *Manage Authentication Agent accounts*. É conveniente usar uma tarefa de grupo, por exemplo, para substituir o certificado do token do administrador em todos os computadores.

Como alterar uma conta do Agente de Autenticação através da Consola de Administração (MMC)

1. Abra as propriedades da tarefa *Gestão das contas de Agente de Autenticação*.

2. Nas propriedades da tarefa, selecione a secção **Definições**.

3. Clique em **Adicionar** → **Comando de edição de conta**.

4. Na janela que surgir, no campo **Conta do Windows**, especifique o nome da conta de utilizador do Microsoft Windows que pretende alterar.

5. Se introduziu manualmente o nome de uma conta do Windows, clique no botão **Permitir** para definir o identificador de segurança (SID) da conta.

   Se optar por não determinar o identificador de segurança (SID), clicando no botão **Permitir**, este será determinado quando 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 fiável, a tarefa *Gestão das contas de Agente de Autenticação* terminará com um erro.

6. Selecione a caixa de verificação **Alterar nome de utilizador** e introduza um nome novo para a conta do Agente de Autenticação se pretender que o Kaspersky Endpoint Security altere o nome de utilizador 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 introduzido no campo abaixo.

7. Selecione a caixa de verificação **Modificar definições de autenticação baseada em password** para tornar editáveis as definições de autenticação baseada em password.

8. Selecione a caixa de verificação **Permitir autenticação baseada em password** se pretender que a aplicação solicite ao utilizador a introdução da password da conta do Agente de Autenticação, durante a autenticação para aceder às unidades de disco rígido encriptadas. Defina uma password para a conta do Agente de Autenticação.

9. Selecione a caixa de verificação **Editar a regra da alteração de password ao autenticar no Agente de Autenticação** se pretender que o Kaspersky Endpoint Security altere o valor da definição de alteração de password para todas as contas do Agente de Autenticação criadas utilizando a conta do Microsoft Windows com o nome indicado no campo **Conta do Windows** para o valor da definição especificado abaixo.

10. Especifique o valor da definição de alteração de password ao efetuar a autenticação no Agente de Autenticação.

11. Selecione a caixa de verificação **Modificar definições de autenticação baseada em certificado** para tornar editáveis as definições de autenticação baseada no certificado eletrónico de um token ou smart card.

12. Selecione a caixa de verificação **Permitir autenticação baseada em certificado** se pretender que a aplicação solicite ao utilizador a introdução da password do token ou smart card ligado ao computador, durante o processo de autenticação para aceder às unidades de disco rígido encriptadas. Selecione um ficheiro de certificado para autenticação com um cartão inteligente ou token.

13. Selecione a caixa de verificação **Editar a descrição do comando** e edite a descrição do comando se pretender que o Kaspersky Endpoint Security altere a descrição do comando para todas as contas do Agente de Autenticação criadas utilizando a conta do Microsoft Windows com o nome indicado no campo **Conta do Windows**.

14. Selecione a caixa de verificação **Editar a regra de acesso à autenticação no Agente de Autenticação** se pretender que o Kaspersky Endpoint Security altere a regra para o acesso do utilizador à caixa de diálogo no Agente de Autenticação para o valor especificado abaixo para todas as contas do Agente de Autenticação criadas utilizando a conta do Microsoft Windows com o nome indicado no campo **Conta do Windows**.

15. Especificar a regra para acesso à caixa de diálogo de autenticação no Agente de Autenticação.

16. Guarde as suas alterações.

Como alterar uma conta do Agente de Autenticação através da Consola da Web

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique na tarefa **Manage Authentication Agent accounts** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

3. Selecione o separador **Application settings**.

4. Na lista de contas do Agente de Autenticação, clique no botão **Add** e selecione o tipo de comando **Edit account**.

5. Selecione uma conta de utilizador. Pode selecionar uma conta na lista de contas de domínio ou inserir manualmente o nome da conta. Avance para o passo seguinte.

   O Kaspersky Endpoint Security determina o identificador de segurança da conta (Security Identifier, SID). Isto é necessário para verificar a conta. Se tiver digitado o nome de utilizador incorretamente, o Kaspersky Endpoint Security encerrará a tarefa com um erro.

6. Selecione as caixas de verificação junto às definições que pretende editar.

7. Configure as definições da conta do Agente de Autenticação.

   - **Create a new Authentication Agent account to replace the existing account**. O Kaspersky Endpoint Security verifica as contas existentes no computador. Se a ID de segurança do utilizador no computador e na tarefa corresponderem, o Kaspersky Endpoint Security alterará as definições da conta do utilizador de acordo com a tarefa.

   - **User name**. O nome de utilizador padrão da conta do Agente de Autenticação corresponde ao nome de domínio do utilizador.

   - **Allow password-based authentication**. Defina uma password para a conta do Agente de Autenticação. Se necessário, pode solicitar uma nova password ao utilizador após a primeira autenticação. Assim, cada utilizador terá sua própria password exclusiva. Pode também definir os requisitos de segurança da password para a conta do Agente de Autenticação na política.

   - **Allow certificate-based authentication**. Selecione um ficheiro de certificado para autenticação com um cartão inteligente ou token. Dessa forma, o utilizador terá de digitar a password do cartão inteligente ou token.

   - **Account access to encrypted data**. Configure o acesso do utilizador à unidade encriptada. Pode, por exemplo, desativar temporariamente a autenticação do utilizador em vez de eliminar a conta do Agente de Autenticação.

   - **Comment**. Digite uma descrição da conta, se necessário.

8. Guarde as suas alterações.

9. Selecione a caixa de verificação junto à tarefa e clique no botão **Start**.

Para eliminar uma conta do Agente de Autenticação, tem de adicionar um comando especial à tarefa *Manage Authentication Agent accounts*. É conveniente usar uma tarefa de grupo, por exemplo, para eliminar a conta de um funcionário despedido.

Como eliminar uma conta do Agente de Autenticação através da Consola de Administração (MMC)

1. Abra as propriedades da tarefa *Gestão das contas de Agente de Autenticação*.
2. Nas propriedades da tarefa, selecione a secção **Definições**.
3. Clique em **Adicionar → Comando de eliminação de conta**.
4. Na janela que surgir, no campo **Conta do Windows**, especifique o nome da conta de utilizador do Windows utilizada para criar a conta do Agente de Autenticação que pretende eliminar.
5. Se introduziu manualmente o nome de uma conta do Windows, clique no botão **Permitir** para definir o identificador de segurança (SID) da conta.

   Se optar por não determinar o identificador de segurança (SID), clicando no botão **Permitir**, este será determinado quando 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 fiável, a tarefa *Gestão das contas de Agente de Autenticação* terminará com um erro.

6. Guarde as suas alterações.

Como eliminar uma conta do Agente de Autenticação através da Consola da Web

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.
2. Clique na tarefa **Manage Authentication Agent accounts** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.
3. Selecione o separador **Application settings**.
4. Na lista de contas do Agente de Autenticação, clique no botão **Add** e selecione o tipo de comando **Remove account**.
5. Selecione uma conta de utilizador. Pode selecionar uma conta na lista de contas de domínio ou inserir manualmente o nome da conta.
6. Guarde as suas alterações.
7. Selecione a caixa de verificação junto à tarefa e clique no botão **Start**.

Como resultado, após a conclusão da tarefa no próximo arranque do computador, o utilizador não pode concluir o procedimento de autenticação e carregar o sistema operativo. O Kaspersky Endpoint Security negará o acesso aos dados encriptados.

Para consultar a lista de utilizadores que podem concluir a autenticação com o Agente e carregar o sistema operativo, tem de aceder às propriedades do computador gerido.

Como consultar a lista de contas do Agente de Autenticação através da Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Devices**.
3. Clique duas vezes para abrir a janela de propriedades do computador.
4. Na janela de propriedades do computador, selecione a secção **Tasks**.
5. Na lista de tarefas, selecione **Gestão das contas de Agente de Autenticação** e abra as propriedades da tarefa ao clicar duas vezes.
6. Nas propriedades da tarefa, selecione a secção **Definições**.

Como resultado, pode aceder a uma lista de contas do Agente de Autenticação neste computador. Somente utilizadores da lista podem concluir a autenticação com o Agente e carregar o sistema operativo.

1. Na janela principal da Consola Web, selecione **Asset management → Assets (Devices)**.
2. Clique no nome do computador no qual pretende consultar a lista de contas do Agente de Autenticação.
3. Nas propriedades do computador, selecione o separador **Tasks**.
4. Na lista de tarefas, selecione **Manage Authentication Agent accounts**.
5. Na janela de propriedades da tarefa, selecione a secção **Application settings**.

Como resultado, pode aceder a uma lista de contas do Agente de Autenticação neste computador. Somente utilizadores da lista podem concluir a autenticação com o Agente e carregar o sistema operativo.

Utilizar um token e um smart-card com o Agente de Autenticação

Pode ser utilizado um token ou um smart-card ou simbólico pode ser usado para a autenticação ao aceder às unidades de disco rígido encriptadas. Para tal, deve adicionar o ficheiro de certificado eletrónico de um token ou cartão inteligente à tarefa *Gestão das contas de Agente de Autenticação*.

A utilização de um token ou smart-card está disponível apenas se as unidades de disco rígido do computador tiverem sido encriptadas ao utilizar o algoritmo de encriptação AES256. Se os discos rígidos do computador foram encriptados através do algoritmo de encriptação AES56, a adição do ficheiro de certificado eletrónico ao comando será negada.

O Kaspersky Endpoint Security suporta os tokens, leitores de smart card e smart cards seguintes:

- 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 ficheiro de certificado eletrónico de token ou smart-card ao comando para criar uma conta de Agente de Autenticação, comece por guardar o ficheiro utilizando software de terceiros para gerir certificados.

O certificado do token ou smart-card tem de ter as propriedades seguintes:

- O certificado tem de ser compatível com a norma X.509 e o ficheiro de certificado tem de ter codificação DER.
- O certificado contém uma chave RSA com um comprimento de pelo menos 1024 bits.

Se o certificado eletrónico do token ou cartão inteligente não cumprir estes requisitos, não pode carregar o ficheiro 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 o objetivo do certificado. Se o parâmetro tiver um valor diferente, o Kaspersky Security Center transfere o ficheiro de certificado, mas apresenta um aviso.

Se um utilizador tiver perdido um token ou smart card, o administrador tem de adicionar o ficheiro de um certificado eletrónico de token ou smart card ao comando para criar uma conta de Agente de Autenticação. Em seguida, o utilizador tem de concluir o procedimento para obter acesso a dispositivos encriptados ou para restaurar dados em dispositivos encriptados.

Desencriptação de unidade de disco rígido

Pode desencriptar unidades de disco rígido mesmo que não exista nenhuma licença atual que permita a encriptação de dados.

Para desencriptar unidades de disco rígido:

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.

3. Na janela de política, selecione **Encriptação de dados → Encriptação de disco completa**.

4. Na lista pendente **Tecnologia de encriptação**, selecione a tecnologia com a qual foram encriptados os discos rígidos.

5. Execute uma das ações seguintes:

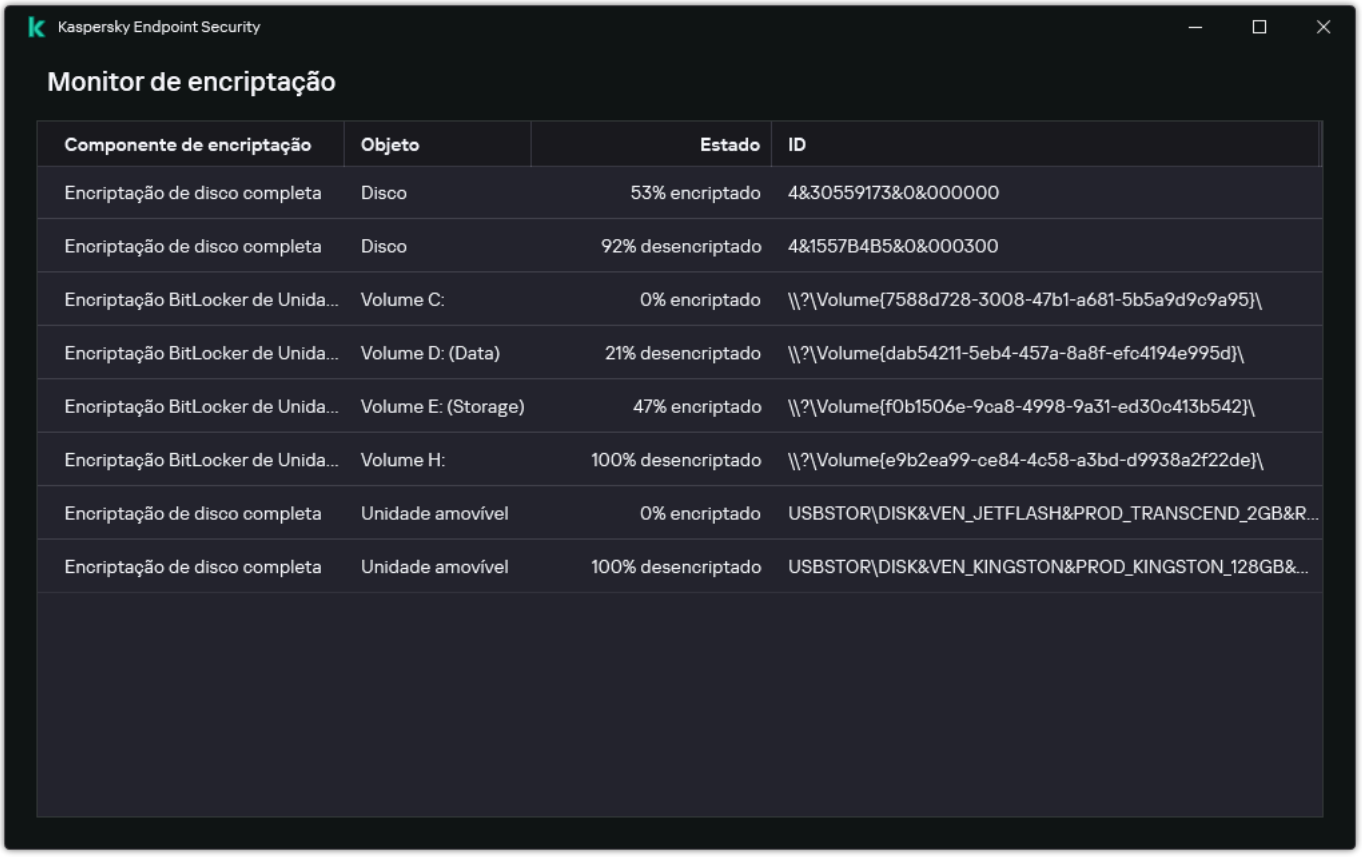
   - Na lista pendente **Modo de encriptação**, selecione a opção **Desencriptar todas as unidades de discos rígido** se pretender desencriptar todas as unidades de disco rígido encriptadas.

   - Adicione as unidades de disco rígido que pretende desencriptar à tabela **Não encriptar as unidades de disco rígido seguintes**.

     Esta opção está disponível apenas para a tecnologia de Encriptação de disco Kaspersky.

6. Guarde as suas alterações.

Pode utilizar a ferramenta Monitor de Encriptação para controlar o processo de encriptação ou desencriptação de disco no computador de um utilizador. Pode executar a ferramenta Monitor de Encriptação na janela principal da aplicação.



Monitor de encriptação

Se o utilizador encerra ou reinicia o computador durante a desencriptação de unidades de disco rígido encriptadas através da tecnologia de Encriptação de disco Kaspersky, o Agente de Autenticação é carregado antes do próximo arranque do sistema operativo. O Kaspersky Endpoint Security retoma a desencriptação da unidade de disco rígido após a autenticação com êxito no agente de autenticação e arranque do sistema operativo.

Se o sistema operativo passar para o modo de hibernação durante a desencriptação de unidades de disco rígido encriptadas através da tecnologia de Encriptação de disco Kaspersky, o Agente de Autenticação é carregado quando o sistema operativo sai do modo de hibernação. O Kaspersky Endpoint Security retoma a desencriptação da unidade de disco rígido após a autenticação com êxito no agente de autenticação e arranque do sistema operativo. Após a desencriptação da unidade de disco rígido, o modo de hibernação está indisponível até o primeiro reinício do sistema operativo.

Se o sistema operativo entrar em modo de descanso durante a desencriptação da unidade de disco rígido, o Kaspersky Endpoint Security retoma a desencriptação da unidade de disco rígido quando o sistema operativo sair do modo de descanso sem carregar o Agente de Autenticação.

Restaurar acesso a uma unidade protegida pela tecnologia Encriptação de disco Kaspersky

Se um utilizador se tiver esquecido da password para aceder a um disco rígido protegido pela tecnologia Encriptação de disco Kaspersky, será necessário iniciar o procedimento de recuperação (Pedido-Resposta). Também pode utilizar a conta de serviço para obter acesso ao disco rígido se esta funcionalidade estiver ativada nas definições de encriptação do disco.

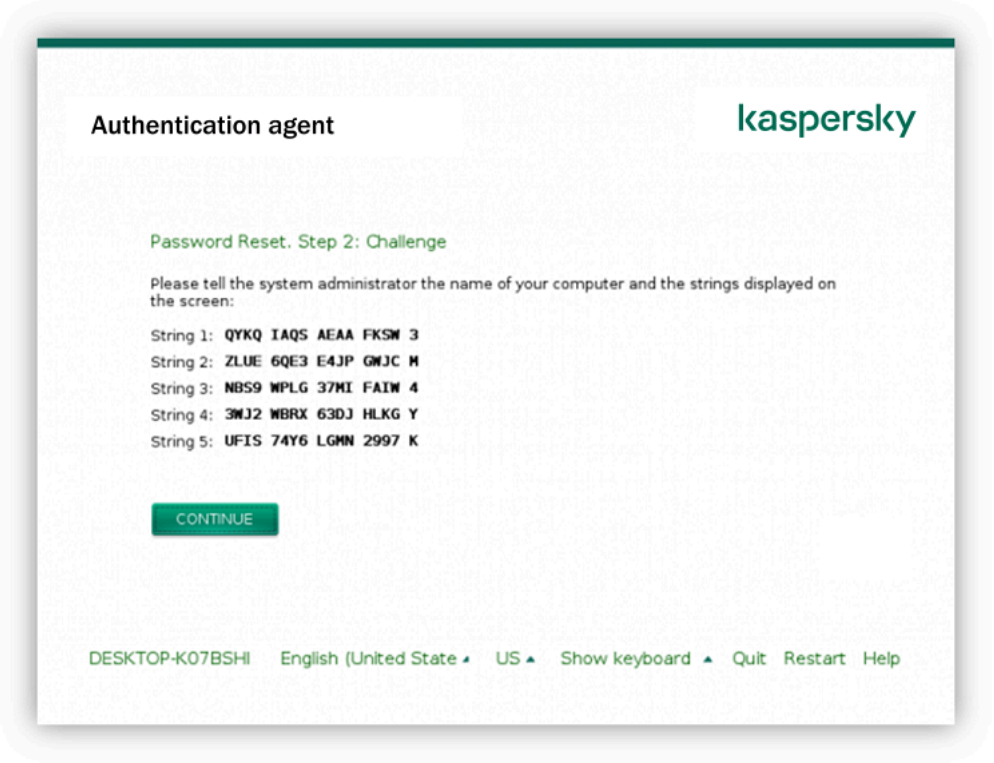
Restaurar o acesso ao disco rígido do sistema

A restauração do acesso a um disco rígido do sistema protegido pela tecnologia Encriptação de disco Kaspersky consiste nas seguintes etapas:

1. O utilizador reporta os blocos de pedido ao administrador (ver a figura abaixo).

2. O administrador introduz os blocos de pedido no Kaspersky Security Center, recebe os blocos de resposta e relata os blocos de resposta ao utilizador.

3. O utilizador introduz 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 Encriptação de disco Kaspersky

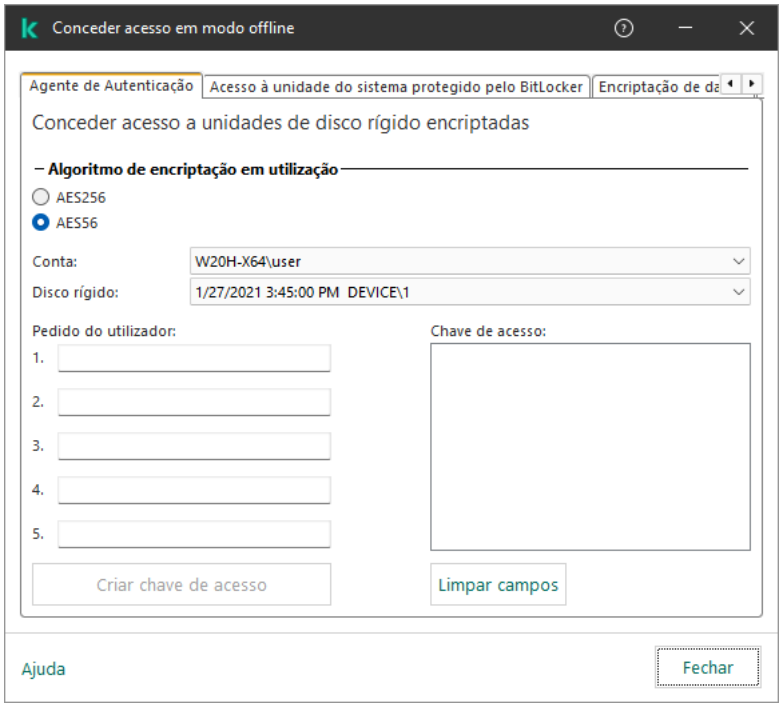
Para iniciar o procedimento de recuperação, o utilizador deve clicar no botão **Forgot your password** na interface do Agente de Autenticação.

Como obter blocos de resposta para um disco rígido do sistema protegido pela tecnologia Encriptação de disco Kaspersky na Consola de administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Devices**.
3. No separador **Devices**, selecione o computador do utilizador que solicitou acesso a dados encriptados, e clique com o botão direito do rato para abrir o menu de contexto.
4. No menu de contexto, selecione **Conceder acesso em modo offline**.
5. Esta ação abre uma janela; nessa janela, selecione o separador **Agente de Autenticação**.
6. No bloco **Algoritmo de encriptação em utilização**, selecione um algoritmo de encriptação: **AES56** ou **AES256**.

   O algoritmo de encriptação de dados depende da biblioteca de encriptação AES incluída no pacote de distribuição: *Strong encryption (AES256)* ou *Lite encryption (AES56)*. A biblioteca de encriptação AES é instalada juntamente com a aplicação.
7. Na lista pendente **Conta**, selecione o nome da conta do Agente de Autenticação do utilizador que solicitou a recuperação do acesso a uma unidade.
8. Na lista pendente **Disco rígido**, selecione a unidade de disco rígido encriptada para a qual necessita de recuperar o acesso.
9. No bloco **Pedido do utilizador**, introduza os bloqueios de pedidos ditados pelo utilizador.

Como resultado, os conteúdos dos blocos da resposta ao pedido do utilizador para recuperação do nome de utilizador e password de uma conta do Agente de Autenticação serão apresentados no campo **Chave de acesso**. Transmitir o conteúdo dos blocos de resposta para o utilizador.



Conceder acesso no modo offline

Como obter blocos de resposta para um disco rígido do sistema protegido pela tecnologia Encriptação de disco Kaspersky na Consola da Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Assets (Devices)**.
2. Selecione a caixa de verificação ao lado do nome do computador a cuja unidade pretende restaurar o acesso.
3. Clique em **Grant access to the device in offline mode**.
4. Na janela que surgir, selecione a secção **Authentication Agent**.
5. Na lista pendente **Account**, selecione o nome da conta do Agente de Autenticação criada para o utilizar que solicita a recuperação do nome e password da conta do Agente de Autenticação.
6. Introduza os blocos do pedido transmitidos pelo utilizador.

   Os conteúdos das secções da resposta ao pedido do utilizador para recuperação do nome de utilizador e password de uma conta do Agente de Autenticação serão apresentados no fundo da janela. Transmitir o conteúdo dos blocos de resposta para o utilizador.

Após concluir o procedimento de recuperação, o Agente de Autenticação solicitará a alteração da password pelo utilizador.

Restaurar o 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 Encriptação de disco Kaspersky consiste nas seguintes etapas:

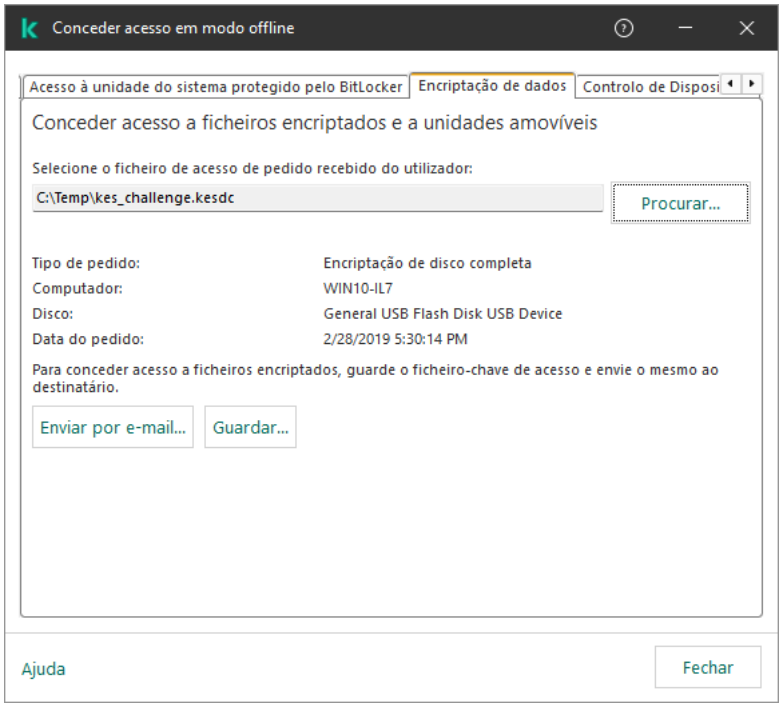
1. O utilizador envia um ficheiro de pedido de acesso ao administrador.
2. O administrador adiciona o ficheiro de pedido de acesso ao Kaspersky Security Center, cria um ficheiro de chave de acesso e envia-o ao utilizador.
3. O utilizador adiciona o ficheiro de chave de acesso ao Kaspersky Endpoint Security e obtém acesso ao disco rígido.

Para iniciar o procedimento de recuperação, o utilizador precisa tentar aceder a um disco rígido. Como resultado, o Kaspersky Endpoint Security irá criar um ficheiro de pedido de acesso (um ficheiro com a extensão KESDC), que o utilizador precisa de enviar ao administrador, por exemplo, por e-mail.

Como obter um ficheiro de chave de acesso para um disco rígido encriptado que não é do sistema na Consola de administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Devices**.
3. No separador **Devices**, selecione o computador do utilizador que solicitou acesso a dados encriptados, e clique com o botão direito do rato para abrir o menu de contexto.
4. No menu de contexto, selecione **Conceder acesso em modo offline**.
5. Esta ação abre uma janela; nessa janela, selecione o separador **Encriptação de dados**.
6. No separador **Encriptação de dados**, clique no botão **Procurar**.
7. Na janela para selecionar um ficheiro de pedido de acesso, especifique o caminho para o ficheiro recebido do utilizador.

Verá informações acerca do pedido do utilizador. O Kaspersky Security Center gera um ficheiro-chave. Envie por email o ficheiro-chave de acesso a dados encriptados gerado para o utilizador. Ou guarde o ficheiro de acesso e utilize qualquer método disponível para transferir o ficheiro.



Conceder acesso no modo offline

Como obter um ficheiro de chave de acesso encriptado que não é do sistema na Consola da Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Assets (Devices)**.
2. Selecione a caixa de verificação ao lado do nome do computador a cujos dados pretende restaurar o acesso.
3. Clique em **Grant access to the device in offline mode**.
4. Selecione **Data Encryption**.
5. Clique no botão **Select file** e selecione o ficheiro de pedido de acesso recebido do utilizador (um ficheiro com a extensão KESDC).

   A consola da Web apresentará informações acerca do pedido. Isto incluirá o nome do computador ao qual o utilizador está a solicitar acesso ao ficheiro.
6. Clique no botão **Save key** e selecione uma pasta onde guardar os dados encriptados (um ficheiro com a extensão KESDR).

Como resultado, poderá obter a chave de acesso a dados encriptados, que terá de transferir para o utilizador.

Iniciar sessão com a conta de serviço do Agente de Autenticação

O Kaspersky Endpoint Security permite adicionar uma conta de serviço do Agente de Autenticação ao encriptar uma unidade. A conta de serviço é necessária para obter acesso ao computador, por exemplo, quando o utilizador se esquece da password. Também pode utilizar a conta de serviço como uma conta de reserva. Para adicionar uma conta, selecione uma conta de serviço nas definições de encriptação do disco e introduza o nome da conta de utilizador (por defeito, `ServiceAccount`). Para autenticar com o agente, irá precisar de uma password de utilização única.

Como descobrir a password de utilização única na Consola de administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Devices**.
3. Clique duas vezes para abrir a janela de propriedades do computador.
4. Na janela de propriedades do computador, selecione a secção **Tasks**.
5. Na lista de tarefas, selecione **Gestão das contas de Agente de Autenticação** e abra as propriedades da tarefa ao clicar duas vezes.
6. Na janela de propriedades da tarefa, selecione a secção **Definições**.
7. Na lista de contas, selecione a conta de serviço do Agente de Autenticação (por exemplo, `WIN10-USER\ServiceAccount`).
8. Na lista pendente **Ação**, selecione **Ver conta**.
9. Nas propriedades da conta, selecione a caixa de verificação **Mostrar password original**.
10. Copie a password de utilização única para iniciar sessão com a conta de serviço.

Como descobrir a password de utilização única na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management → Assets (Devices)**.
2. Clique no nome do computador no qual pretende consultar a lista de contas do Agente de Autenticação.

   As propriedades do computador são apresentadas.
3. Nas propriedades do computador, selecione o separador **Tasks**.
4. Na lista de tarefas, selecione **Manage Authentication Agent accounts**.
5. Na janela de propriedades da tarefa, selecione a secção **Application settings**.
6. Na lista de contas, selecione a conta de serviço do Agente de Autenticação (por exemplo, `WIN10-USER\ServiceAccount`).

7. Nas propriedades da conta, selecione a caixa de verificação **Show password**.

8. Copie a password de utilização única para iniciar sessão com a conta de serviço.

O Kaspersky Endpoint Security atualiza automaticamente a password sempre que um utilizador se autentica com a conta de serviço. Depois de autenticar com o agente, tem de inserir a password da conta do Windows. Ao iniciar sessão com a conta de serviço, não pode utilizar a tecnologia SSO.

Atualizar o sistema operativo

Há várias considerações especiais para atualizar o sistema operativo de um computador protegido pela Encriptação de disco completa (FDE). Atualize o sistema operativo da seguinte forma: primeiro, atualize o sistema operativo num computador, depois atualize o sistema operativo numa pequena parte dos computadores e, em seguida, atualize o sistema operativo em todos os computadores da rede.

Se estiver a utilizar a tecnologia de Encriptação de disco Kaspersky, o Agente de Autenticação será carregado antes de o sistema operativo ser iniciado. Utilizando o Agente de Autenticação, o utilizador pode entrar no sistema e aceder às unidades encriptadas. Depois, o sistema operativo começa a ser carregado. Se iniciar uma atualização do sistema operativo num computador protegido com a tecnologia de Encriptação de disco Kaspersky, o Assistente de Atualização do sistema operativo removerá o Agente de Autenticação. Como resultado, o computador pode ser bloqueado porque o carregador do SO não poderá aceder à unidade encriptada.

Recursos da atualização do sistema operativo:

- **Atualizar o SO através do WSUS**. Pode atualizar o sistema operativo da forma habitual.
- **Atualizar o SO a partir do ISO**. Para atualizar o sistema operativo, tem de especificar a pasta com os controladores de encriptação de disco da Kaspersky. A aplicação copia automaticamente os controladores para uma pasta separada. Execute as seguintes ações:

  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 estará disponível somente se o computador estiver a executar o Windows 10 1607 (RS1) ou superior. Para atualizar versões anteriores do sistema operativo, recomenda-se que primeiro desencripte o disco, efetue uma atualização do SO e, em seguida, encripte o disco.

Se estiver a utilizar a tecnologia de Encriptação de Unidade BitLocker, não é necessário desencriptar os discos rígidos para atualizar o Windows 10. Para obter mais informações sobre o BitLocker, visite o website da Microsoft.

A eliminar erros da atualização da funcionalidade de encriptação

A Encriptação de disco completa é atualizada quando a versão anterior da aplicação é atualizada para o Kaspersky Endpoint Security for Windows 14.2.

Os seguintes erros podem ocorrer ao iniciar a atualização da funcionalidade da Encriptação de disco completa:

- Não é possível inicializar a atualização.
- O dispositivo é incompatível com o Agente de autenticação.

Para eliminar erros que tenham ocorrido quando inicia o processo de atualização da funcionalidade de Encriptação de disco completa na nova versão da aplicação:

1. Desencriptar unidades de disco rígido.
2. Encriptar unidades de disco rígido novamente.

Os seguintes erros podem ocorrer durante a atualização da funcionalidade da Encriptação de disco completa:

- Não é possível completar a atualização.
- Reversão da atualização da Encriptação de disco completa concluída com um erro.

Para eliminar erros que tenham ocorrido durante o processo de atualização da funcionalidade da Encriptação de disco completa,

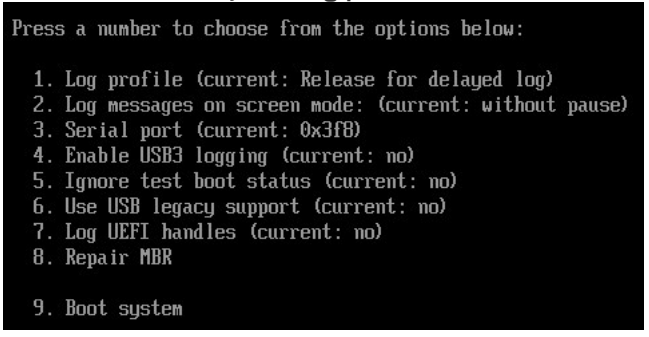
restaure o acesso um dispositivo encriptado utilizando o Ferramenta de Restauro.

Rastrear o Agente de Autenticação

A aplicação regista informação de serviço sobre o funcionamento do Agente de Autenticação e informações sobre as operações do utilizador com o Agente de Autenticação no ficheiro de rastreio.

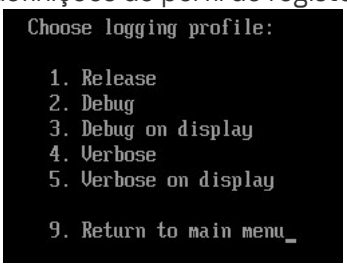
Para ativar o rastreamento do Agente de Autenticação:

1. Ativar o rastreamento do Kaspersky Endpoint Security.
2. Reinicie o computador.
3. Assim que o computador com as unidades de disco rígido encriptadas é iniciado, prima o botão **F3** para invocar uma janela para configurar as definições do Agente de Autenticação.
4. Assim que o carregador de arranque de FDE iniciar, selecione o gestor de arranque **KES (FDE <version>)**.
5. No menu do gestor de arranque, aceda às definições **Log profile**.



Menu do gestor de arranque

6. Selecione o nível de rastreio na janela de definições do perfil do registo:



Níveis de rastreamento do Agente de Autenticação

- **Release**. Se esta opção estiver selecionada, a aplicação não regista a informação sobre eventos do Agente de Autenticação no ficheiro de rastreio.
- **Debug**. Se esta opção estiver selecionada, a aplicação regista informação sobre o funcionamento do Agente de Autenticação e as operações do utilizador realizadas com o Agente de Autenticação no ficheiro de rastreio.
- **Debug on display**. Se esta opção estiver selecionada, a aplicação regista informação relativa ao funcionamento do Agente de Autenticação e as operações do utilizador realizadas com o Agente de Autenticação no ficheiro de rastreio e transmite essas informações através da porta COM.

  Se um computador com as unidades de disco rígidos encriptadas estiver ligado a outro computador através da porta COM, os eventos do Agente de Autenticação podem ser examinados a partir deste computador.
- **Verbose**. Se esta opção estiver selecionada, a regista informação detalhada sobre o funcionamento do Agente de Autenticação e as operações do utilizador realizadas com o Agente de Autenticação no ficheiro de rastreio.

  O nível de detalhe das entradas sob esta opção é superior quando comparado com o nível da opção **Debug**. Um elevado nível de detalhe das entradas pode tornar mais lento o arranque do Agente de Autenticação e do sistema operativo.
- **Verbose on display**. Se esta opção estiver selecionada, a aplicação regista informação detalhada relativa ao funcionamento do Agente de Autenticação e as operações do utilizador realizadas com o Agente de Autenticação no ficheiro de rastreio e transmite essas informações através da porta COM.

  O nível de detalhe das entradas sob esta opção é superior quando comparado com o nível da opção **Debug on display**. Um elevado nível de detalhe das entradas pode tornar mais lento o arranque do Agente de Autenticação e do sistema operativo.

Depois de selecionar um nível de rastreamento, o gestor de arranque exibe o menu novamente.

7. No menu do gestor de arranque, selecione **Boot system**.

   O gestor de arranque de FDE inicia o Agente de Autenticação.

   Reproduza o problema.

   Os dados são gravados no ficheiro de rastreio do Agente de Autenticação se existirem unidades de disco rígido encriptadas no computador ou durante a encriptação de disco completa.

8. Para interromper o processo de rastreio, regresse à janela Ferramentas de suporte e desative o rastreio.

Como resultado, são criados ficheiros de rastreio de funcionamento do Agente de Autenticação KES.SRV na pasta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. O ficheiro de rastreio do Agente de Autenticação

não é enviado para a Kaspersky, ao contrário de outros ficheiros de rastreio da aplicação. Se necessário, pode enviar manualmente o ficheiro de rastreio do Agente de Autenticação para a Kaspersky para análise.

Editar as mensagens de ajuda do Agente de Autenticação

Antes de editar mensagens de ajuda do Agente de Autenticação, consulte a lista de caracteres suportados num ambiente de pré-carregamento (ver abaixo).

Para editar as mensagens de ajuda do Agente de Autenticação:

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Encriptação de dados** → **Definições de encriptação comuns**.
4. No bloco **Modelos**, clique no botão **Ajuda**.
5. Na janela que surgir, faça o seguinte:
   - Selecione o separador **Autenticação** para editar o texto de ajuda apresentado na janela Agente de Autenticação quando as credenciais de conta estão a ser introduzidas.
   - Selecione o separador **Alterar password** para editar o texto de ajuda apresentado na janela do Agente de Autenticação quando a password para a conta do Agente de Autenticação estiver a ser alterada.
   - Selecione o separador **Recuperar password** para editar o texto de ajuda apresentado na janela do Agente de Autenticação quando a password para a conta do Agente de Autenticação está a ser recuperada.
6. Editar mensagens de ajuda.

   Se pretender restaurar o texto original, clique no botão **Por defeito**.

   Pode introduzir texto de ajuda com 16 linhas ou menos. O comprimento máximo de uma linha é 64 carateres.
7. Guarde as suas alterações.

O suporte limitado para caracteres nas mensagens de ajuda do Agente de Autenticação

Num ambiente de pré-carregamento, são suportados os seguintes caracteres Unicode:

- Alfabeto latino básico (0000 - 007F)
- Alfabeto latino adicional-1 caracter (0080 - 00FF)
- Alfabeto latino alargado-A (0100 - 017F)

- Alfabeto latino alargado-B (0180 - 024F)
- Caracteres de ID alargados não combinados (02B0 - 02FF)
- Sinais diacríticos combinados (0300 - 036F)
- Alfabetos grego e copta (0370 - 03FF)
- Cirílico (0400 - 04FF)
- Hebraico (0590 - 05FF)
- Escrita árabe (0600 - 06FF)
- Alfabeto latino alargado adicional (1E00 - 1EFF)
- Sinais de pontuação (2000 - 206F)
- Símbolos de moeda (20A0 - 20CF)
- Símbolos semelhantes a letras (2100 - 214F)
- Figuras geométricas (25A0 - 25FF)
- Formulários de apresentação de Escrita árabe-B (FE70 - FEFF)

Os caracteres não especificados nesta lista não são suportados num ambiente de pré-carregamento. Não é recomendada a utilização destes caracteres em mensagens de ajuda do Agente de Autenticação.

Remover objetos e dados restantes após testar o funcionamento do Agente de Autenticação

Durante a desinstalação da aplicação, se o Kaspersky Endpoint Security detetar objetos e dados restantes na unidade de disco rígido do sistema após a operação de teste do Agente de Autenticação, a desinstalação da aplicação é interrompida e deixa de ser possível até que os objetos e dados sejam removidos.

Os objetos e os dados podem permanecer na unidade de disco rígido do sistema após a operação de teste do Agente de Autenticação apenas em casos excecionais. Por exemplo, tal pode acontecer se o computador não tiver sido reiniciado após uma política do Kaspersky Security Center com definições de encriptação ter sido aplicada ou se a aplicação não iniciar após a operação de teste do Agente de Autenticação.

É possível remover os objetos e os dados que restaram na unidade de disco rígido do sistema após a operação de teste do Agente de Autenticação das seguintes maneiras:

- Utilizando a política do Kaspersky Security Center.
- Utilizando o Utilitário de Restauro.

Para utilizar uma política do Kaspersky Security Center para remover os objetos e os dados restantes após a operação de teste do Agente de Autenticação:

1. Aplicar uma política do Kaspersky Security Center com as definições configuradas para desencriptar todas as unidades de disco rígido no computador.
2. Iniciar o Kaspersky Endpoint Security.

Para utilizar um Utilitário de Restauro para remover os objetos e os dados restantes após a operação de teste do Agente de Autenticação:

1. Execute o ficheiro chamado fdert.exe, que é o ficheiro executável do utilitário de restauro. Este ficheiro é criado pelo Kaspersky Endpoint Security.
2. Na janela do Utilitário de Restauro, selecione o dispositivo necessário.
3. Clique em **Verificar**.
4. Se, após o diagnóstico do disco rígido do sistema, receber uma mensagem a indicar que permanecem objetos e dados da operação de teste do Agente de Autenticação, clique em **Eliminar artefactos do Agente de Autenticação**.

   O botão **Eliminar artefactos do Agente de Autenticação** só está disponível se forem detetados objetos e dados restantes após a operação de teste do Agente de Autenticação.

Para remover a informação sobre a incompatibilidade da aplicação com o Agente de Autenticação,

introduza o comando `avp pbatestreset` na command line.

Gestão de BitLocker

BitLocker é uma tecnologia de encriptação integrada nos sistemas operativos Windows. O Kaspersky Endpoint Security permite controlar e gerir o Bitlocker utilizando a infraestrutura do Kaspersky Next. O BitLocker encripta volumes lógicos. Não pode utilizar o BitLocker para a encriptação de unidades removíveis. Para obter mais informações sobre o BitLocker, consulte a documentação da Microsoft.

Ao criptografar o disco, o BitLocker coloca o carregador de inicialização e outros ficheiros auxiliares no system partition. Esta partição não está encriptada. O sistema operativo cria a partição do sistema automaticamente durante a instalação do Windows. Se o disco estiver totalmente particionado antes da instalação do Windows, o sistema operativo não poderá criar uma partição do sistema. Neste caso, quando inicia a encriptação de disco do BitLocker, o sistema operativo solicita que faça uma repartição do disco e crie uma partição do sistema. Depois de criar uma partição do sistema, o sistema operativo inicia a encriptação do BitLocker.

O algoritmo de criptografia BitLocker não depende da versão da Biblioteca AES incluída no pacote de distribuição (AES256 ou AES56). A criptografia utiliza a biblioteca de criptografia integrada do sistema operativo.

Por predefinição, a aplicação utiliza o algoritmo de encriptação BitLocker com um comprimento de chave efetivo de 256 bits para encriptar dispositivos que nunca foram encriptados. Para um dispositivo que tenha sido encriptado antes da instalação da aplicação, o algoritmo de encriptação pode ser diferente. Para obter informações detalhadas sobre a seleção do algoritmo de encriptação, 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 encriptados anteriormente por aplicações de terceiros para o Kaspersky Security Center.

O BitLocker fornece armazenamento seguro de chaves de acesso ao utilizar um módulo de plataforma fiável. Um *Trusted Platform Module* (TPM) é um microchip desenvolvido para fornecer funções básicas relacionadas com segurança (por exemplo, para armazenar chaves de encriptação). Habitualmente, é instalado um Trusted Platform Module (TPM) na motherboard do computador e interage com todos os outros componentes do sistema através do barramento de hardware. Utilizar o TPM é a forma mais segura de armazenar chaves de acesso do BitLocker, uma vez que o TPM fornece verificação integrada do sistema antes do arranque. Ainda pode encriptar unidades num computador sem um TPM. Neste caso, a chave de acesso será encriptada com uma password. O BitLocker utiliza os seguintes métodos de autenticação:

- TPM.
- TPM e PIN.
- Password.

Depois de encriptar o disco rígido do sistema, o utilizador precisa passar pela autenticação do BitLocker para inicializar o sistema operativo. Após a autenticação, o BitLocker permite que o utilizador inicie sessão. O BitLocker não oferece suporte à tecnologia de início de sessão único (SSO).

Depois de encriptar uma unidade, o BitLocker cria uma chave de recuperação. O Kaspersky Endpoint Security envia a chave de recuperação ao Kaspersky Security Center para que possa restaurar o acesso ao disco, por exemplo, se um utilizador se esqueceu da password.

Se um utilizador encriptar um disco utilizando o BitLocker, o Kaspersky Endpoint Security enviará a chave de recuperação e informações sobre a encriptação do disco ao Kaspersky Security Center.

Se estiver a utilizar políticas de grupo do Windows, desative a gestão do BitLocker nas definições de política. As definições de política do Windows podem entrar em conflito com as definições de política do Kaspersky Endpoint Security. Ao encriptar uma unidade, podem ocorrer erros.

Iniciar a Encriptação de Unidade BitLocker

Antes de iniciar a encriptação de disco completa, certifique-se de que o mesmo não está infetado. Para tal, inicie a tarefa de Verificação Completa ou Verificação de Áreas Críticas. A execução da encriptação de disco completa num computador infetado por um rootkit pode fazer com que o computador deixe de funcionar.

Para utilizar a Encriptação de Unidade BitLocker nos computadores com sistemas operativos Windows para servidores, pode ser necessário instalar o componente Encriptação de Unidade BitLocker. Instale o componente utilizando as ferramentas do sistema operativo (Assistente para Adicionar Funções e Componentes). Para mais informações sobre como instalar a Encriptação de Unidade BitLocker, consulte a documentação Microsoft.

Como executar a Encriptação de Unidade BitLocker através da Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Encriptação de dados → Encriptação de disco completa**.
4. Na lista pendente **Tecnologia de encriptação**, selecione **Encriptação BitLocker de Unidade**.
5. Na lista pendente **Modo de encriptação**, selecione **Encriptar todas as unidades de discos rígido**.

   Se o computador tiver vários sistemas operativos instalados, após a encriptação, apenas será possível carregar o sistema operativo em que a encriptação foi realizada.

6. Configure as opções avançadas da Encriptação de Unidade BitLocker (consulte a tabela abaixo).
7. Guarde as suas alterações.

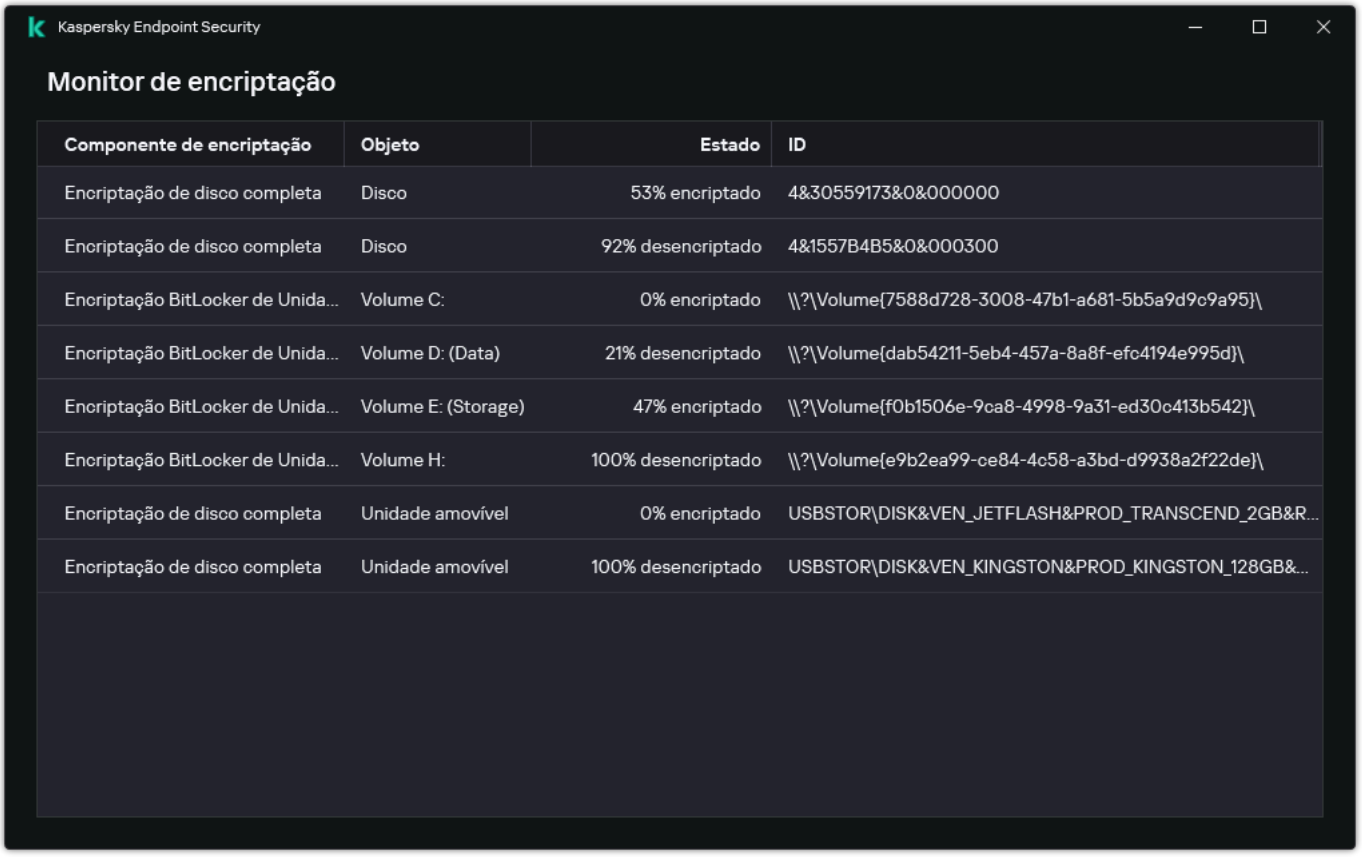
Como executar a Encriptação BitLocker de Unidade através da Web Console

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Data Encryption → Full Disk Encryption**.
5. Selecione a tecnologia **BitLocker Disk Encryption**.
6. No bloco **Action on devices**, selecione **Encrypt all hard drives**.

   Se o computador tiver vários sistemas operativos instalados, após a encriptação, apenas será possível carregar o sistema operativo em que a encriptação foi realizada.

7. Configure as opções avançadas da Encriptação de Unidade BitLocker (consulte a tabela abaixo).
8. Guarde as suas alterações.

Pode utilizar a ferramenta Monitor de Encriptação para controlar o processo de encriptação ou desencriptação de disco no computador de um utilizador. Pode executar a ferramenta Monitor de Encriptação na janela principal da aplicação.



Monitor de encriptação

Assim que a política for aplicada, a aplicação irá apresentar as seguintes consultas, dependendo das definições de autenticação:

- Apenas TPM. Não é necessária a introdução do utilizador. O disco será encriptado quando o computador for reiniciado.
- TPM + PIN/Password. Se um módulo TPM estiver disponível, é apresentada uma janela de código PIN. Se um módulo TPM não estiver disponível, será apresentada uma janela de palavra-passa para autenticação pré-arranque.
- Apenas password. Verá uma janela de pedido de password para autenticação de pré-arranque.

Se o modo de compatibilidade padrão do Tratamento de Informação Federal estiver ativado no sistema operativo do computador, é apresentado um pedido de ligação de um dispositivo de armazenamento para guardar o ficheiro-chave de recuperação no Windows 8 e versões anteriores do sistema operativo. Pode guardar vários ficheiros de chave de recuperação num único dispositivo de armazenamento.

Depois de definir uma password ou um PIN, o BitLocker pedirá para reiniciar o computador para concluir a encriptação. Em seguida, o utilizador tem de seguir o procedimento de autenticação do BitLocker. Após o procedimento de autenticação, o utilizador deve iniciar sessão no sistema. Após o carregamento do sistema operativo, o BitLocker concluirá a encriptação.

Se não existir acesso a chaves de encriptação, o utilizador pode solicitar que o administrador da rede local forneça uma chave de recuperação (caso a chave de recuperação não tenha sido guardada anteriormente no dispositivo de armazenamento ou se tenha perdido).

Definições do componente Encriptação de Unidade BitLocker

Parâmetro	Descrição
Ativar utilização de autenticação BitLocker que exija introdução por teclado de pré-arranque em tablets	Utilizar a autenticação que requer a entrada de dados num ambiente de pré-arranque, mesmo que a plataforma não tenha a capacidade para a entrada de pré-arranque (por exemplo, no caso dos teclados táteis no ecrã nos tablets). O ecrã tátil dos tablets não está disponível no meio de pré-arranque. Para concluir a autenticação com BitLocker em tablets, o utilizador deve ligar, por exemplo, um teclado USB. Se a caixa de verificação estiver selecionada, é permitida a utilização da autenticação com entrada de pré-arranque. Recomendamos a utilização desta definição apenas para dispositivos que tenham ferramentas de entrada de dados alternativas num ambiente de pré-arranque como, por exemplo, um teclado USB adicionalmente aos teclados do ecrã tátil. Se a caixa de verificação estiver desmarcada, não é possível executar a Encriptação de Unidade BitLocker em tablets.
Utilizar encriptação de hardware (Windows 8 e versões mais recentes)	Se a caixa de verificação estiver selecionada, a aplicação aplica a encriptação de hardware. O que lhe permite aumentar a velocidade da encriptação e utilizar menos recursos do computador.
Encriptar apenas espaço utilizado do disco (Windows 8 e versões mais recentes)	Esta caixa ativa/desativa a opção que limita a área de encriptação a setores ocupados do disco rígido. Este limite permite reduzir o tempo de encriptação. Ativar ou desativar a funcionalidade **Encriptar apenas espaço utilizado do disco (reduz tempo de encriptação)** após o início da encriptação não altera esta definição até que os discos rígidos sejam desencriptados. Tem de selecionar ou desmarcar a caixa de verificação antes de iniciar a encriptação. Se a caixa de verificação estiver selecionada, são encriptadas apenas as partes do disco rígido que estiverem ocupadas por ficheiros. O Kaspersky Endpoint Security encripta automaticamente dados novos quando são adicionados. Se a caixa de verificação estiver selecionada, é encriptado o disco rígido completo, incluindo os fragmentos residuais de ficheiros anteriormente eliminados e modificados. Recomenda-se esta opção para discos rígidos novos cujos dados não tenham sido modificados ou eliminados. Se estiver a aplicar encriptação num disco rígido que já esteja em utilização, recomenda-se encriptar o disco rígido completo. Dessa forma, assegura a proteção de todos os dados, mesmo os dados eliminados que sejam potencialmente recuperáveis. Por padrão, a caixa de verificação está desmarcada.

Parâmetro	Descrição
Método de autenticação	**Apenas password (Windows 8 e versões mais recentes)** Se esta opção estiver selecionada, o Kaspersky Endpoint Security pede uma password ao utilizador quando este tenta aceder a unidade encriptada. Esta opção pode ser selecionada quando um Trusted Platform Module (TPM) não está a ser utilizado. **Trusted platform module (TPM)** Se esta opção estiver selecionada, o BitLocker utiliza um Trusted Platform Module (TPM). Um *Trusted Platform Module* (TPM) é um microchip desenvolvido para fornecer funções básicas relacionadas com segurança (por exemplo, para armazenar chaves de encriptação). Um Trusted Platform Module está normalmente instalado na placa principal (motherboard) e interage com todos os outros componentes de sistema através do hardware de barramento. No caso de computadores a executar o Windows 7 ou Windows Server 2008 R2, só está disponível encriptação utilizando um módulo TPM. Se um módulo TPM não estiver instalado, a encriptação do BitLocker não será possível. O uso de uma password nestes computadores não é suportado. Um dispositivo equipado com um Trusted Platform Module pode criar chaves de encriptação que apenas podem ser desencriptadas com o dispositivo. Um Trusted Platform Module encripta as chaves de encriptação com a sua própria chave de armazenamento de raiz. A chave de armazenamento de raiz está armazenada dentro do Trusted Platform Module. Isto fornece um nível adicional de proteção contra tentativas de penetração nas chaves de encriptação. Esta ação está selecionada por predefinição. Pode definir uma camada adicional de proteção para o acesso à chave de encriptação, e encriptar a chave com uma password ou um PIN: • **Utilizar PIN para TPM**. Se esta caixa de verificação estiver selecionada, um utilizador pode utilizar um código PIN para obter o acesso a uma chave de encriptação que esteja armazenada num Trusted Platform Module (TPM). Se esta caixa de verificação estiver desmarcada, os utilizadores estão proibidos de utilizar códigos PIN. Para aceder à chave de encriptação, um utilizador deverá introduzir a password. • **Trusted platform module (TPM) ou password se o TPM não estiver disponível**. Se esta opção estiver selecionada, o utilizador pode utilizar uma password para obter acesso a chaves de encriptação quando um Trusted Platform Module (TPM) não está disponível. Se a caixa de verificação não estiver selecionada e o TPM não estiver disponível, a encriptação de disco completa não é iniciada. O método de autenticação selecionado tem de ser configurado ao especificar os requisitos de password ou PIN: • **Comprimento mínimo do PIN (carateres)** (o valor predefinido é 6). • **Comprimento mínimo da password (carateres)** (o valor predefinido é 8). • **Número máximo de palavras-passe/PINs armazenados** (o valor predefinido é 5). • **Limitar período de validade de password/PIN para TPM (dias)** (desativado por predefinição). • **Utilizar PIN melhorado (letras e números)**. O *PIN avançado* permite a utilização de outros caracteres além dos caracteres numéricos: letras latinas maiúsculas e minúsculas, caracteres especiais e espaços. Desativado por predefinição.
Recriar automaticamente a chave de recuperação (dias)	Atualizar automaticamente a password para restaurar o acesso a uma unidade protegida por BitLocker. Se a caixa de verificação estiver selecionada, especifique o período de validade da password da chave de recuperação. Isto ajuda a evitar a reutilização da password da chave de recuperação.

Desencriptar um disco rígido protegido por BitLocker

Os utilizadores podem desencriptar um disco utilizando o sistema operativo (a função *Desativar o BitLocker*). Depois disso, o Kaspersky Endpoint Security solicitará ao utilizador para encriptar o disco novamente. O Kaspersky Endpoint Security solicitará a encriptação do disco, a menos que ative a desencriptação do disco na política.

Como desencriptar um disco rígido protegido por BitLocker através da Consola de Administração (MMC)

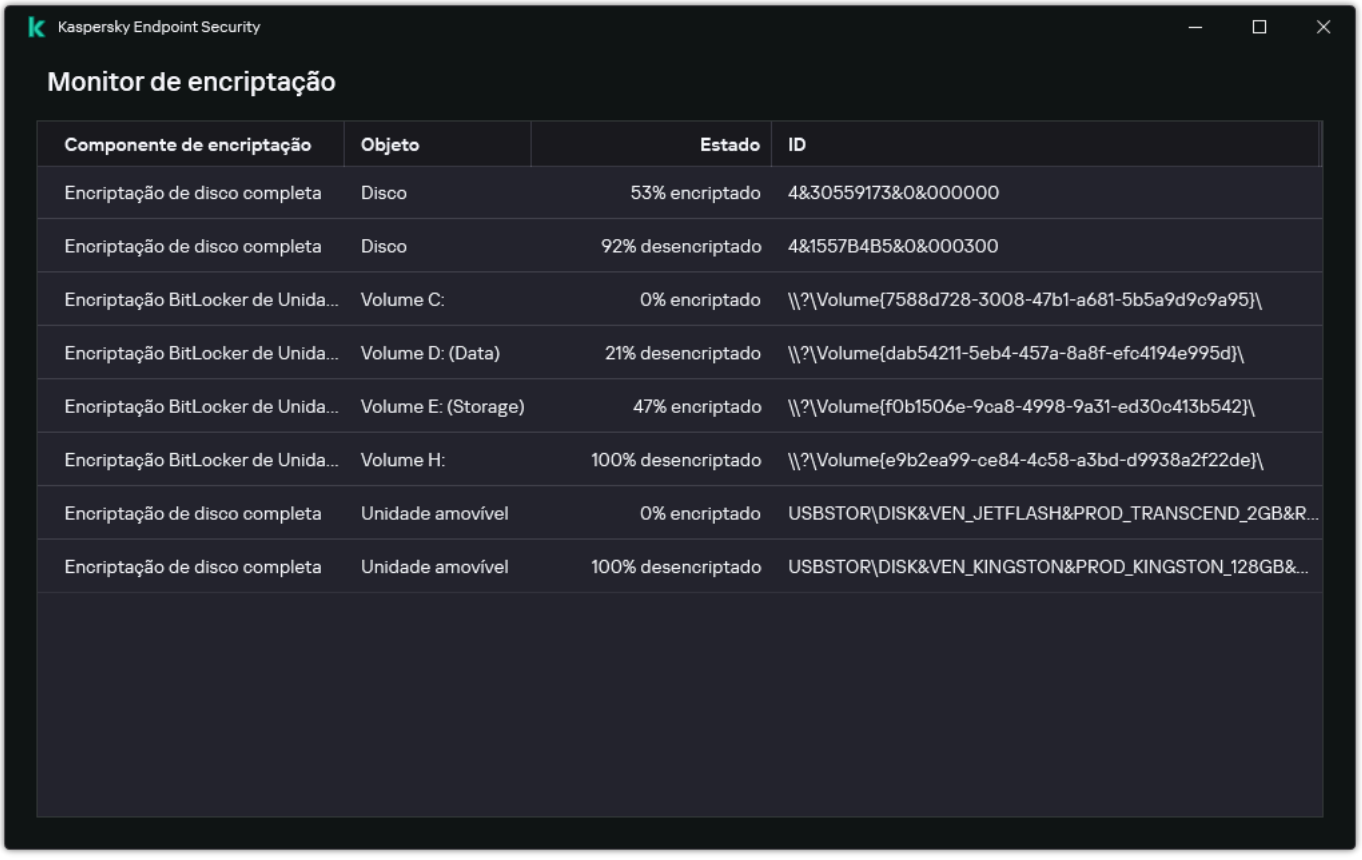
1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Encriptação de dados → Encriptação de disco completa**.

4. Na lista pendente **Tecnologia de encriptação**, selecione **Encriptação BitLocker de Unidade**.
5. Na lista pendente **Modo de encriptação**, selecione **Desencriptar todas as unidades de discos rígido**.
6. Guarde as suas alterações.

Como desencriptar um disco rígido encriptado com BitLocker através da Consola Web e da Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Data Encryption** → **Full Disk Encryption**.
5. Selecione a tecnologia **BitLocker Disk Encryption**.
6. No bloco **Action on devices**, selecione **Decrypt all hard drives**.
7. Guarde as suas alterações.

Pode utilizar a ferramenta Monitor de Encriptação para controlar o processo de encriptação ou desencriptação de disco no computador de um utilizador. Pode executar a ferramenta Monitor de Encriptação na janela principal da aplicação.



Monitor de encriptação

Restaurar acesso a uma unidade protegida por BitLocker

Se um utilizador se tiver esquecido da password para aceder a um disco rígido encriptado pelo BitLocker, terá de iniciar o procedimento de recuperação (Pedido-Resposta).

Se o sistema operativo do computador tiver o modo de compatibilidade padrão do Tratamento de Informação Federal (FIPS) ativado, no Windows 8 e versões anteriores, o ficheiro de chave de recuperação será guardado na unidade amovível antes da encriptação. Para restaurar o acesso à unidade, insira a unidade amovível e siga as instruções no ecrã.

A restauração do acesso a um disco rígido encriptado pelo BitLocker consiste nas seguintes etapas:

1. O utilizador informa o administrador da ID da chave de recuperação (ver a figura abaixo).
2. O administrador verifica a ID da chave de recuperação nas propriedades do computador no Kaspersky Security Center. A ID que o utilizador forneceu deve corresponder à ID apresentada nas propriedades do computador.
3. Se as IDs da chave de recuperação corresponderem, o administrador fornece ao utilizador a chave de recuperação ou envia um ficheiro da chave de recuperação.

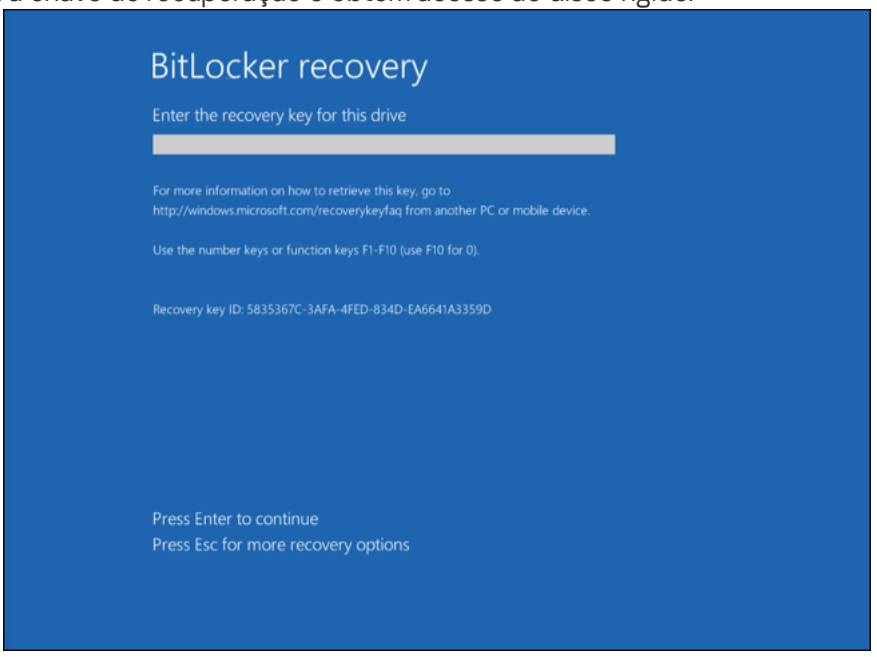
   Um ficheiro da chave de recuperação é utilizado para computadores a executar os seguintes sistemas operativos:

   - Windows 7
   - Windows 8
   - Windows Server 2008
   - Windows Server 2011
   - Windows Server 2012

   Para todos os outros sistemas operativos, uma chave de recuperação é utilizada.

   Para evitar a reutilização da password da chave de recuperação, pode configurar a atualização automática da password nas definições da política.

4. O utilizador introduz a chave de recuperação e obtém acesso ao disco rígido.



Restaurar o acesso a um disco rígido encriptado pelo BitLocker

Restaurar o acesso a uma unidade do sistema

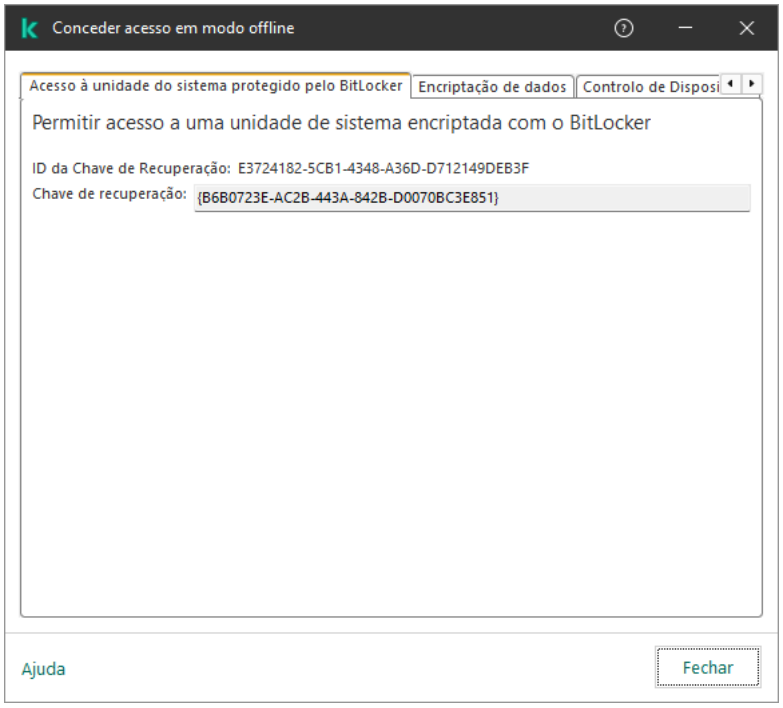
Para iniciar o procedimento de recuperação, o utilizador tem de premir a tecla **Esc** na etapa de autenticação pré-inicialização.

Como ver a chave de recuperação de uma unidade do sistema encriptada pelo BitLocker na Consola de administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Managed devices**.
3. No separador **Devices**, selecione o computador do utilizador que solicitou acesso a dados encriptados, e clique com o botão direito do rato para abrir o menu de contexto.
4. No menu de contexto, selecione **Conceder acesso em modo offline**.
5. Esta ação abre uma janela; nessa janela, selecione o separador **Acesso à unidade do sistema protegido pelo BitLocker**.
6. Solicitar ao utilizador o ID da chave de recuperação indicado na janela de introdução da password do BitLocker e compará-lo com o ID no campo **ID da Chave de Recuperação**.

   Se os IDs não forem correspondentes, esta chave não é válida para restaurar o acesso à unidade de sistema especificada. Certifique-se de que o nome do computador selecionado corresponde ao nome do computador do utilizador.

Como resultado, terá acesso à chave de recuperação ou ao ficheiro da chave de recuperação, que terá de ser transferida para o utilizador.



Repor o acesso a uma unidade encriptada com BitLocker

Como consultar a chave de recuperação de uma unidade de sistema encriptada pelo BitLocker na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Assets (Devices)**.
2. Selecione a caixa de verificação ao lado do nome do computador a cuja unidade pretende restaurar o acesso.
3. Clique em **Grant access to the device in offline mode**.
4. Na janela que surgir, selecione a secção **BitLocker**.
5. Verifique a ID da chave de recuperação. A ID fornecida pelo utilizador deve corresponder à ID apresentada nas definições do computador.

   Se os IDs não forem correspondentes, esta chave não é válida para restaurar o acesso à unidade de sistema especificada. Certifique-se de que o nome do computador selecionado corresponde ao nome do computador do utilizador.

6. Clique em **Receive key**.

Como resultado, terá acesso à chave de recuperação ou ao ficheiro da chave de recuperação, que terá de ser transferida para o utilizador.

Depois de o sistema operativo ser carregado, o Kaspersky Endpoint Security solicita ao utilizador que altere a password ou o código PIN. Depois de definir uma nova password ou um novo código PIN, o BitLocker criará uma nova chave de recuperação e enviará a chave para o Kaspersky Security Center. Como resultado, a chave de recuperação e o ficheiro da chave de recuperação serão atualizados. Se o utilizador não alterar a password, pode usar a chave de recuperação antiga quando voltar a iniciar o sistema operativo.

Os computadores com Windows 7 não permitem alterar a password ou o código PIN. Depois de a chave de recuperação ser introduzida e o sistema operativo carregado, o Kaspersky Endpoint Security não irá solicitar ao utilizador que altere a password ou o código PIN. Como tal, é impossível definir uma nova password ou código PIN. Este problema resulta das peculiaridades do sistema operativo. Para continuar, é necessário voltar a encriptar o disco rígido.

Restaurar o acesso a uma unidade que não é do sistema

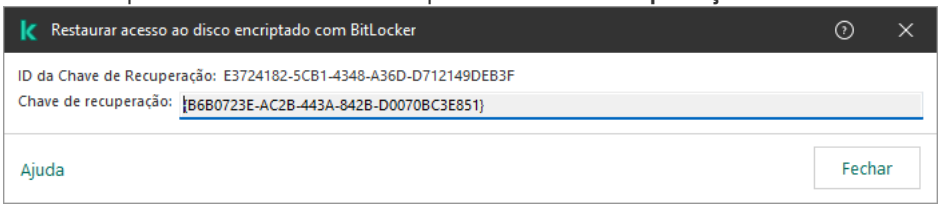
Para iniciar o procedimento de recuperação, o utilizador tem de clicar na hiperligação **Forgot your password** na janela que fornece acesso à unidade. Depois de obter acesso à unidade encriptada, o utilizador pode ativar o desbloqueio automático da unidade durante a autenticação do Windows nas definições do BitLocker.

Como consultar a chave de recuperação de uma unidade que não é do sistema encriptada pelo BitLocker na Consola de administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da Consola de Administração, selecione a pasta **Advanced** → **Data encryption and protection** → **Encrypted drives**.
3. Na área de trabalho, selecione o dispositivo encriptado para o qual pretende criar um ficheiro-chave de acesso e, no menu de contexto do dispositivo, selecione **Obtenha acesso ao dispositivo em Kaspersky Endpoint Security**.
4. Solicitar ao utilizador o ID da chave de recuperação indicado na janela de introdução da password do BitLocker e compará-lo com o ID no campo **ID da Chave de Recuperação**.

   Se os IDs não forem correspondentes, esta chave não é válida para restaurar o acesso à unidade especificada. Certifique-se de que o nome do computador selecionado corresponde ao nome do computador do utilizador.

5. Envie ao utilizador a chave que está indicada no campo **Chave de recuperação**.



Repor o acesso a uma unidade encriptada com BitLocker

Como consultar a chave de recuperação de uma unidade não pertencente ao sistema encriptada pelo BitLocker na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Operations → Data encryption and protection → Encrypted drives**.
2. Selecione a caixa de verificação ao lado do nome do computador a cuja unidade pretende restaurar o acesso.
3. Clique em **Grant access to the device in offline mode**.

   Isto inicia o Assistente para conceder acesso a um dispositivo.
4. Cumpra as instruções do Assistente para conceder acesso a um dispositivo:

   a. Selecione o plug-in **Kaspersky Endpoint Security for Windows**

   b. Verifique a ID da chave de recuperação. A ID fornecida pelo utilizador deve corresponder à ID apresentada nas definições do computador.

   > Se os IDs não forem correspondentes, esta chave não é válida para restaurar o acesso à unidade de sistema especificada. Certifique-se de que o nome do computador selecionado corresponde ao nome do computador do utilizador.

   c. Clique em **Receive key**.

Como resultado, terá acesso à chave de recuperação ou ao ficheiro da chave de recuperação, que terá de ser transferida para o utilizador.

Pausar a proteção por BitLocker para atualizar o software

Há uma série de considerações especiais para atualizar o sistema operativo, instalar pacotes de atualização para o sistema operativo ou atualizar outro software com proteção por BitLocker ativada. A instalação de atualizações pode exigir reiniciar o computador várias vezes. Após cada reinício, o utilizador deve concluir a autenticação do BitLocker. Para garantir que as atualizações são instaladas corretamente, pode desativar temporariamente a autenticação do BitLocker. Nesse caso, o disco permanece encriptado e o utilizador tem acesso aos dados após entrar no sistema. Para gerir a autenticação do BitLocker, pode usar a tarefa *Gestão de segurança BitLocker*. Pode utilizar esta tarefa para especificar o número de reinícios do computador que não exigem autenticação do BitLocker. Deste modo, após as atualizações serem instaladas e a tarefa *Gestão de segurança BitLocker* ser concluída, a autenticação do BitLocker é ativada automaticamente. Pode ativar a autenticação do BitLocker a qualquer momento.

Como pausar a proteção por BitLocker utilizando a Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Tasks**.

   A lista de tarefas é aberta.
2. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Gestão de segurança BitLocker**.

Passo 2. Gestão de segurança BitLocker

Configure a autenticação do BitLocker. Para pausar a proteção por BitLocker, selecione **Permitir temporariamente ignorar a autenticação do BitLocker** e introduza o número de reinícios sem autenticação do BitLocker (1 a 15 vezes). Se necessário, introduza uma data e hora de expiração para a tarefa. Na hora especificada, a tarefa é desligada automaticamente e o utilizador deve concluir a autenticação do BitLocker quando o computador for reiniciado.

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

Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 4. Definir o nome da tarefa

Introduza o nome da tarefa, por exemplo *A atualizar para Windows 10*.

Passo 5. Completar a criação da tarefa

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso da tarefa nas propriedades da tarefa.

Como pausar a proteção por BitLocker utilizando a Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

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

Passo 1. Configurar definições da tarefa geral

Configurar definições da tarefa geral:

1. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows**.
2. Na lista pendente **Task type**, selecione **BitLocker Protection Management**.
3. No campo **Task name**, introduza uma breve descrição, por exemplo, *Updating to Windows 10*.
4. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

Passo 2. Gestão de segurança BitLocker

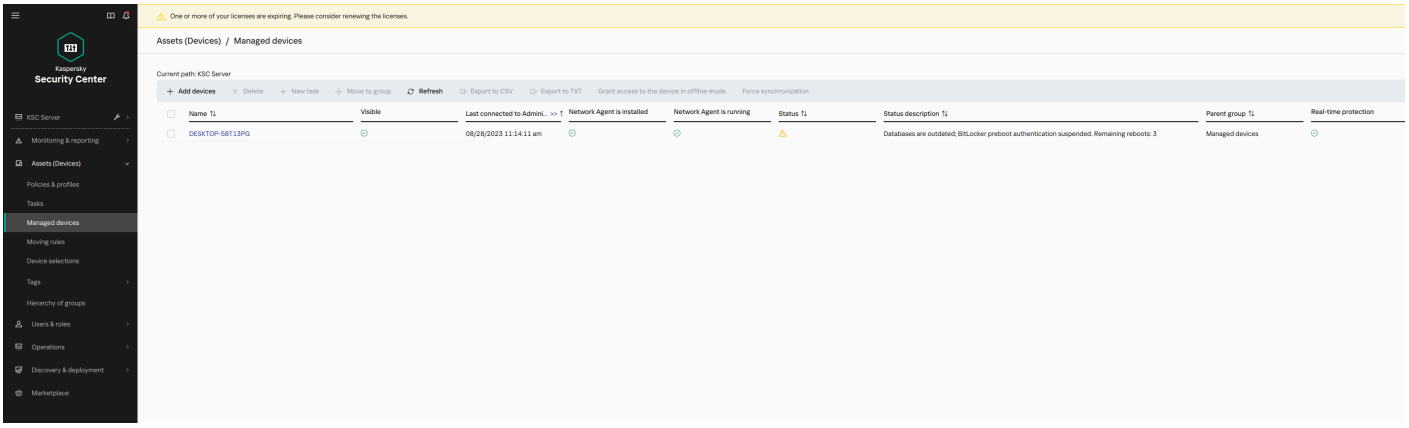
Configure a autenticação do BitLocker. Para pausar a proteção por BitLocker, selecione **Temporarily allow skipping BitLocker authentication** e introduza o número de reinícios sem autenticação do BitLocker (1 a 15 vezes). Se necessário, introduza uma data e hora de expiração para a tarefa. Na hora especificada, a tarefa é desligada automaticamente e o utilizador deve concluir a autenticação do BitLocker quando o computador for reiniciado.

Passo 3. Completar a criação da tarefa

Conclua o assistente. Será apresentada uma nova tarefa na lista de tarefas.

Para executar uma tarefa, selecione a caixa de seleção em frente da tarefa e clique no botão **Start**.

Como resultado, ao executar a tarefa, após o próximo reinício do computador, o BitLocker não solicita a autenticação do utilizador. Após cada reinício do computador sem autenticação do BitLocker, o Kaspersky Endpoint Security gera um evento correspondente e regista o número de reinícios restantes. Depois, o Kaspersky Endpoint Security envia o evento ao Kaspersky Security Center para ser monitorizado pelo administrador. Pode também ver o número de reinícios restantes na pasta **Managed devices** da consola do Kaspersky Security Center na descrição do estado do dispositivo.



A lista dos dispositivos geridos

Quando o número especificado de reinícios ou o tempo de expiração da tarefa é atingido, a autenticação do BitLocker é ativada automaticamente. Para obter acesso aos dados, o utilizador deve concluir a autenticação do BitLocker.

Em computadores com o Windows 7, o BitLocker não pode contar os reinícios do computador. A contagem de reinícios em computadores com Windows 7 é feita pelo Kaspersky Endpoint Security. Portanto, para ativar automaticamente a autenticação do BitLocker após cada reinício, o Kaspersky Endpoint Security deve ser iniciado.

Para ativar a autenticação do BitLocker com antecedência, abra as propriedades da tarefa *Gestão de segurança BitLocker* e selecione **Solicitar sempre autenticação no pré-arranque**.

Encriptação ao nível dos ficheiros em unidades locais do computador

A encriptação de ficheiros não é suportada em computadores baseados em Arm.

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para estações de trabalho. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para servidores.

A encriptação de ficheiros possui os seguintes recursos especiais:

- O Kaspersky Endpoint Security encripta/desencripta ficheiros em pastas predefinidas apenas para perfis de utilizadores locais do sistema operativo. O Kaspersky Endpoint Security não encripta ou desencripta ficheiros em pastas predefinidas de perfis de utilizadores em roaming, perfis de utilizador obrigatórios, perfis de utilizador temporários ou pastas redirecionadas.
- O Kaspersky Endpoint Security não encripta ficheiros cuja modificação possa prejudicar o sistema operativo e aplicações instaladas. Por exemplo, os seguintes ficheiros e pastas com todas as pastas imbricadas estão na lista de exclusões da encriptação:
  - %WINDIR%;
  - %PROGRAMFILES% e %PROGRAMFILES(X86)%;
  - Ficheiros de registo do Windows.

  A lista de exclusões de encriptação não pode ser visualizada nem editada. Embora os ficheiros e as pastas na lista de exclusões de encriptação possam ser adicionados à lista de encriptação, não serão encriptados durante encriptação de um ficheiro.

Encriptar ficheiros nas unidades locais do computador

O Kaspersky Endpoint Security não encripta ficheiros localizados no armazenamento na nuvem do OneDrive ou noutras pastas que tenham OneDrive como nome. O Kaspersky Endpoint Security também bloqueia a cópia de ficheiros encriptados para as pastas do OneDrive se esses ficheiros não forem adicionados à regra de desencriptação.

Para encriptar ficheiros em unidades locais:

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Data Encryption** → **File Level Encryption**.
4. Na lista pendente **Modo de encriptação**, selecione **De acordo com as regras**.
5. No separador **Encriptação**, clique no botão **Adicionar** e selecione um dos seguintes itens na lista pendente:
   a. Selecione o item **Pastas predefinidas** para adicionar ficheiros de pastas de perfis de utilizador locais sugeridos por peritos da Kaspersky para uma regra de encriptação.
      - **Documentos**. Ficheiros na pasta *Documentos* padrão do sistema operativo e as respetivas subpastas.
      - **Favoritos**. Ficheiros na pasta *Favoritos* padrão do sistema operativo e respetivas subpastas.
      - **Ambiente de trabalho**. Ficheiros na pasta *Ambiente de trabalho* padrão do sistema operativo e respetivas subpastas.
      - **Ficheiros temporários**. Ficheiros temporários relacionados com o funcionamento das aplicações instaladas no computador. Por exemplo, as aplicações do Microsoft Office criam ficheiros temporários que contêm cópias de segurança dos documentos.

        Não é recomendado encriptar ficheiros temporários, uma vez que pode causar a perda de dados. Por exemplo, o Microsoft Word cria ficheiros temporários ao processar um documento. Se os ficheiros temporários forem encriptados, mas o ficheiro original não for, o utilizador poderá receber o erro *Acesso negado* ao tentar guardar o documento. Além disso, o Microsoft Word pode guardar o ficheiro, mas não será possível abrir o documento na próxima vez, ou seja, os dados serão perdidos.

      - **Ficheiros do Outlook**. Ficheiros relacionados com o funcionamento do cliente de e-mail do Outlook: ficheiros de dados (PST), ficheiros de dados offline (OST), ficheiros do livro de endereços offline (OAB) e ficheiros do livro de endereços pessoal (PAB).

   b. Selecione o item **Pasta predefinida** para adicionar um caminho de pasta introduzido manualmente para uma regra de encriptação.

Ao adicionar um caminho de pasta, cumpra as seguintes regras:

- Use uma variável de ambiente (por exemplo, `%FOLDER%\UserFolder\`). Pode usar uma variável de ambiente apenas uma vez e só no início do caminho.
- Não use caminhos relativos.
- Não use os carateres `*` e `?`.
- Não use caminhos UNC.
- Use `;` ou `,` como um caráter separador.

c. Selecione o item **Ficheiros por extensão** para adicionar extensões de ficheiro individuais a uma regra de encriptação. O Kaspersky Endpoint Security encripta ficheiros com as extensões especificadas em todas as unidades locais do computador.

d. Selecione o item **Ficheiros por grupos de extensões** para adicionar grupos de extensões de ficheiro a uma regra de encriptação (por exemplo, *Documentos do Microsoft Office*). O Kaspersky Endpoint Security encripta ficheiros que têm as extensões de ficheiro listadas nos grupos de extensões em todas as unidades locais do computador.

6. Guarde as suas alterações.

Assim que a política é aplicada, o Kaspersky Endpoint Security encripta ficheiros que estão incluídos na lista de encriptação e que não estão incluídos na regra de desencriptação.

A encriptação de ficheiros possui os seguintes recursos especiais:

- Se o mesmo ficheiro for adicionado às regras de encriptação e desencriptação, o Kaspersky Endpoint Security executará as seguintes ações:
  - Se o ficheiro não estiver encriptado, o Kaspersky Endpoint Security não encripta este ficheiro.
  - Se o ficheiro estiver encriptado, o Kaspersky Endpoint Security desencripta este ficheiro.
- O Kaspersky Endpoint Security continua a encriptar novos ficheiros se estes corresponderem à regra de encriptação. Por exemplo, quando altera as propriedades de um ficheiro não encriptado (caminho ou extensão), o ficheiro atende aos critérios da regra de encriptação. O Kaspersky Endpoint Security encripta este ficheiro.
- Quando o utilizador cria um novo ficheiro cujas propriedades cumprem os critérios das regras de encriptação, o Kaspersky Endpoint Security encripta o ficheiro logo que este é aberto.
- O Kaspersky Endpoint Security adia a encriptação de ficheiros abertos até que estes sejam fechados.
- Se mover um ficheiro encriptado para outra pasta na unidade local, o ficheiro permanece encriptado, independentemente deste ficheiro estar ou não incluído na regra de encriptação.
- Se desencriptar um ficheiro e copiá-lo para outra pasta local que não esteja incluída na regra de desencriptação, uma cópia do ficheiro pode ser encriptada. Para impedir que o ficheiro copiado seja encriptado, crie uma regra de desencriptação para a pasta de destino.

Formar regras de acesso a ficheiros encriptados para aplicações

Por predefinição, todas as aplicações trabalham com ficheiros encriptados num estado desencriptado. Se utilizar frequentemente determinadas aplicações (por exemplo, navegadores ou editores de texto), pode criar regras de acesso a ficheiros encriptados para proteger as informações.

Recomendamos a criação de uma regra de acesso a ficheiros encriptados para os navegadores Microsoft Internet Explorer e Microsoft Edge. Devido à forma como estes navegadores funcionam, se carregar um ficheiro encriptado para um site (por exemplo, armazenamento na nuvem), o ficheiro é automaticamente desencriptado. Isto pode causar uma fuga de dados. Não é possível carregar um ficheiro encriptado utilizando estes navegadores. Recomendamos a configuração da regra **Conceder acesso aos ficheiros encriptados apenas em texto cifrado**. Não precisa de criar uma regra para outros navegadores (como o Google Chrome).

Para formar regras de acesso a ficheiros encriptados para aplicações:

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Data Encryption → File Level Encryption**.
4. Na lista pendente **Modo de encriptação**, selecione **De acordo com as regras**.

   As regras de acesso são aplicadas apenas no modo **De acordo com as regras**. Depois de aplicar as regras de acesso no modo **De acordo com as regras**, se mudar para o modo **Manter inalterado**, o Kaspersky Endpoint Security ignorará todas as regras de acesso. Todas as aplicações terão acesso a todos os ficheiros encriptados.

5. Na parte direita da janela, selecione o separador **Regras de aplicações**.
6. Se quiser selecionar aplicações exclusivamente a partir da lista do Kaspersky Security Center, clique no botão **Adicionar** e na lista pendente selecione o item **Aplicações da lista do Kaspersky Security Center**.
   a. Especifique os filtros para reduzir a lista de aplicações na tabela. Para tal, especifique os valores dos parâmetros **Aplicação**, **Fornecedor** e **Período adicionado**, bem como todas as caixas de verificação do bloco **Grupo**.
   b. Clique em **Atualizar**.
   c. A tabela apresenta a lista de aplicações que correspondem aos filtros aplicados.
   d. Na coluna **Aplicação**, selecione as caixas de verificação em frente às aplicações para as quais pretende formar regras de acesso aos ficheiros encriptados.
   e. Na lista pendente **Regra de Aplicações**, selecione a regra que determinará o acesso de aplicações a ficheiros encriptados.
   f. Na lista pendente **Ações para as aplicações selecionadas anteriormente**, selecione a ação a executar pelo Kaspersky Endpoint Security nas regras de acesso a ficheiros encriptados formuladas anteriormente para essas aplicações.

Os detalhes de uma regra de acesso a ficheiros encriptados para aplicações são apresentados na tabela no separador **Regras de aplicações**.

7. Se pretender selecionar manualmente aplicações, clique no botão **Adicionar** e na lista pendente selecione o item **Aplicações personalizadas**.

   a. No campo de entrada, introduza o nome ou a lista de nomes de ficheiros de aplicações executáveis, incluindo as respetivas extensões.

      Também pode adicionar os nomes de ficheiros executáveis de aplicações a partir da lista do Kaspersky Security Center, clicando no botão **Adicionar da lista do Kaspersky Security Center**.

   b. Se necessário, no campo **Descrição**, introduza uma descrição da lista de aplicações.

   c. Na lista pendente **Regra de Aplicações**, selecione a regra que determinará o acesso de aplicações a ficheiros encriptados.

   Os detalhes de uma regra de acesso a ficheiros encriptados para aplicações são apresentados na tabela no separador **Regras de aplicações**.

8. Guarde as suas alterações.

Encriptar ficheiros criados ou alterados por aplicações específicas

Pode criar uma regra segundo a qual o Kaspersky Endpoint Security encriptará todos os ficheiros criados ou alterados pelas aplicações especificadas na regra.

> Os ficheiros criados ou modificados pelas aplicações especificadas antes de a regra de encriptação ser aplicada não serão encriptados.

Para configurar a encriptação de ficheiros criados ou alterados por aplicações específicas:

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Data Encryption → File Level Encryption**.

4. Na lista pendente **Modo de encriptação**, selecione **De acordo com as regras**.

   > As regras de encriptação são aplicadas apenas ao modo **De acordo com as regras**. Depois de aplicar as regras de encriptação no modo **De acordo com as regras**, se mudar para o modo **Manter inalterado**, o Kaspersky Endpoint Security ignorará todas as regras de encriptação. Os ficheiros que foram encriptados anteriormente permanecerão encriptados.

5. Na parte direita da janela, selecione o separador **Regras de aplicações**.

6. Se quiser selecionar aplicações exclusivamente a partir da lista do Kaspersky Security Center, clique no botão **Adicionar** e na lista pendente selecione o item **Aplicações da lista do Kaspersky Security Center**.

   a. Especifique os filtros para reduzir a lista de aplicações na tabela. Para tal, especifique os valores dos parâmetros **Aplicação**, **Fornecedor** e **Período adicionado**, bem como todas as caixas de verificação do bloco **Grupo**.

   b. Clique em **Atualizar**.

      A tabela apresenta a lista de aplicações que correspondem aos filtros aplicados.

   c. Na coluna **Aplicação**, selecione as caixas de verificação ao lado das aplicações cujos ficheiros criados pretende encriptar.

   d. Na lista pendente **Regra de Aplicações**, selecione **Encriptar todos os ficheiros criados**.

   e. Na lista pendente **Ações para as aplicações selecionadas anteriormente**, selecione a ação a executar pelo Kaspersky Endpoint Security nas regras de encriptação de ficheiros formuladas anteriormente para essas aplicações.

   A informação sobre a regra de encriptação para ficheiros criados ou alterados pelas aplicações selecionadas é apresentada na tabela no separador **Regras de aplicações**.

7. Se pretender selecionar manualmente aplicações, clique no botão **Adicionar** e na lista pendente selecione o item **Aplicações personalizadas**.

   a. No campo de entrada, introduza o nome ou a lista de nomes de ficheiros de aplicações executáveis, incluindo as respetivas extensões.

      Também pode adicionar os nomes de ficheiros executáveis de aplicações a partir da lista do Kaspersky Security Center, clicando no botão **Adicionar da lista do Kaspersky Security Center**.

   b. Se necessário, no campo **Descrição**, introduza uma descrição da lista de aplicações.

   c. Na lista pendente **Regra de Aplicações**, selecione **Encriptar todos os ficheiros criados**.

   A informação sobre a regra de encriptação para ficheiros criados ou alterados pelas aplicações selecionadas é apresentada na tabela no separador **Regras de aplicações**.

8. Guarde as suas alterações.

Criar uma regra de desencriptação

Para criar uma regra de desencriptação:

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Data Encryption → File Level Encryption**.

4. Na lista pendente **Modo de encriptação**, selecione **De acordo com as regras**.

5. No separador **Desencriptação**, clique no botão **Adicionar** e selecione um dos seguintes itens na lista pendente:

   a. Selecione o item **Pastas predefinidas** para adicionar ficheiros de pastas de perfis de utilizador locais sugeridos por peritos da Kaspersky para uma regra de desencriptação.

   b. Selecione o item **Pasta predefinida** para adicionar um caminho de pasta introduzido manualmente para uma regra de desencriptação.

   c. Selecione o item **Ficheiros por extensão** para adicionar extensões de ficheiro individuais a uma regra de desencriptação. O Kaspersky Endpoint Security não encripta ficheiros com as extensões especificadas em todas as unidades locais do computador.

   d. Selecione o item **Ficheiros por grupos de extensões** para adicionar grupos de extensões de ficheiro a uma regra de desencriptação (por exemplo, *Documentos do Microsoft Office*). O Kaspersky Endpoint Security não encripta ficheiros que têm as extensões de ficheiro listadas nos grupos de extensões em todas as unidades locais do computador.

6. Guarde as suas alterações.

Se o mesmo ficheiro tiver sido adicionado à regra de encriptação e à regra de desencriptação, o Kaspersky Endpoint Security não encripta este ficheiro se este não estiver encriptado, e desencripta o ficheiro, caso este esteja encriptado.

Desencriptar ficheiros nas unidades locais do computador

Para desencriptar ficheiros em unidades locais:

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Data Encryption → File Level Encryption**.
4. Na parte direita da janela, selecione o separador **Encriptação**.
5. Remova da lista de encriptação os ficheiros e pastas que pretende desencriptar. Para tal, selecione os ficheiros e selecione o item **Eliminar regra e desencriptar ficheiros** no menu de contexto do botão **Eliminar**.

   Os ficheiros e as pastas removidos da lista de encriptação são automaticamente adicionados à lista de desencriptação.
6. Formar uma lista de desencriptação de ficheiros.
7. Guarde as suas alterações.

Assim que a política for aplicada, o Kaspersky Endpoint Security desencripta os ficheiros encriptados que foram adicionados à lista de desencriptação.

O Kaspersky Endpoint Security desencripta ficheiros encriptados se os respetivos parâmetros (caminho de ficheiro/nome de ficheiro/extensão de ficheiro) forem alterados para corresponder aos parâmetros de objetos adicionados à lista de desencriptação.

O Kaspersky Endpoint Security adia a desencriptação de ficheiros abertos até que estes sejam fechados.

Criar pacotes encriptados

Para proteger os seus dados ao enviar ficheiros para utilizadores fora da rede empresarial, pode utilizar pacotes encriptados. Os pacotes encriptados podem ser convenientes para transferir ficheiros grandes em unidades amovíveis, pois os clientes de e-mail têm restrições de tamanho dos ficheiros.

Antes de criar pacotes encriptados, o Kaspersky Endpoint Security solicita a password ao utilizador. Para proteger os dados com confiança, pode ativar a verificação dos requisitos de segurança da password e especificar os requisitos de segurança da password. Esta ação vai impedir que os utilizadores utilizem passwords curtas e simples, por exemplo, `1234`.

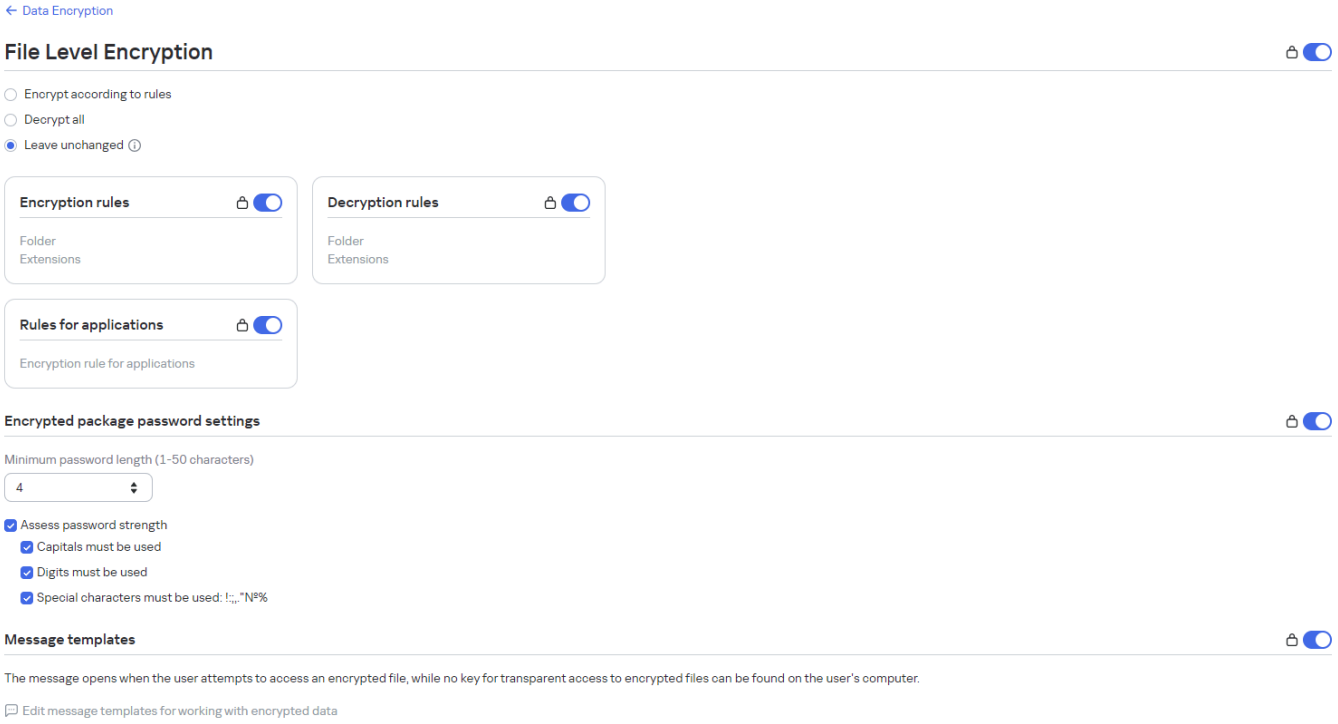
Como ativar a verificação dos requisitos de segurança da password ao criar arquivos encriptados na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Encriptação de dados** → **Definições de encriptação comuns**.
4. No bloco **Definições de password**, clique no botão **Definições**.
5. Esta ação abre uma janela; nessa janela, selecione o separador **Pacotes encriptados**.
6. Configure as definições de complexidade da password ao criar pacotes encriptados.

Como ativar a verificação dos requisitos de segurança da password ao criar arquivos encriptados na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Data Encryption** → **File Level Encryption**.

5. No bloco **Encrypted package password settings**, configure os critérios de segurança da password necessários para a criação de pacotes encriptados.



Definições de encriptação de ficheiros

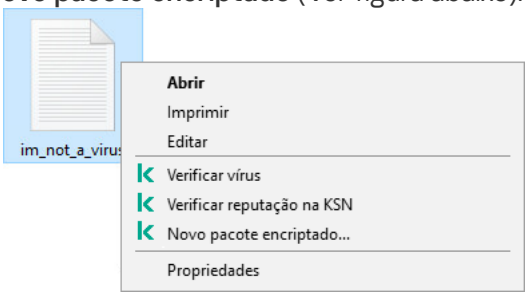
Pode criar pacotes encriptados em computadores com o Kaspersky Endpoint Security instalado com a Encriptação ao nível dos ficheiros disponível.

Ao adicionar um ficheiro ao pacote encriptado cujo conteúdo esteja localizado no armazenamento da nuvem do OneDrive, o Kaspersky Endpoint Security transfere os conteúdos do ficheiro e executa a encriptação.

Para criar um pacote encriptado:

1. Em qualquer gestor de ficheiros, selecione os ficheiros ou pastas que desejar adicionar ao pacote encriptado. Clique com o botão direito do rato para abrir o menu de contexto respetivo.

2. No menu de contexto, selecione **Novo pacote encriptado** (Ver figura abaixo).



Criar um pacote encriptado

3. Na janela surgir, especifique a password e confirme-a.

   A password deve cumprir aos critérios de complexidade especificados na política.

4. Clique em **Criar**.

   O processo de criação do pacote encriptado é iniciado. O Kaspersky Endpoint Security não executa a compressão de ficheiros quando cria um pacote encriptado. Quando o processo terminar, é criado um pacote encriptado autoextraível e protegido por password (um ficheiro executável com a extensão .exe – ) na pasta de destino selecionada.

Para aceder a ficheiros num pacote encriptado, clique duas vezes no mesmo para iniciar o Assistente de Descompactação e introduza a password. Se se esqueceu ou perdeu a sua password, não é possível recuperá-la e aceder ao pacote encriptado. Pode recriar o pacote encriptado.

Restaurar o acesso aos ficheiros encriptados

Quando os arquivos são encriptados, o Kaspersky Endpoint Security recebe uma chave de encriptação necessária para aceder diretamente os ficheiros encriptados. Ao utilizar esta chave de encriptação, um utilizador que esteja a trabalhar com qualquer conta de utilizador do Windows que estava ativa durante a encriptação de ficheiros pode aceder diretamente aos ficheiros encriptados. Os utilizadores que estejam a trabalhar com contas Windows que estavam inativas durante a encriptação de ficheiros têm de estabelecer ligação ao Kaspersky Security Center para acederem aos ficheiros encriptados.

Os ficheiros encriptados poderão não estar acessíveis nas seguintes circunstâncias:

- o computador do utilizador armazena chaves de encriptação, mas não existe ligação ao Kaspersky Security Center para gestão das mesmas. Neste caso, o utilizador deve solicitar o acesso aos ficheiros encriptados ao administrador de rede local.

  Se o acesso ao Kaspersky Security Center não existir, tem de:

  - solicitar uma chave de acesso para aceder a ficheiros encriptados em discos rígidos do computador;
  - para aceder a ficheiros encriptados armazenados em unidades amovíveis, tem de solicitar chaves de acesso diferentes para ficheiros encriptados em cada unidade amovível.

- Os componentes de encriptação são eliminados do computador do utilizador. Neste caso, o utilizador pode abrir ficheiros encriptados em discos amovíveis e locais, mas os conteúdos daqueles ficheiros aparecerão encriptados.

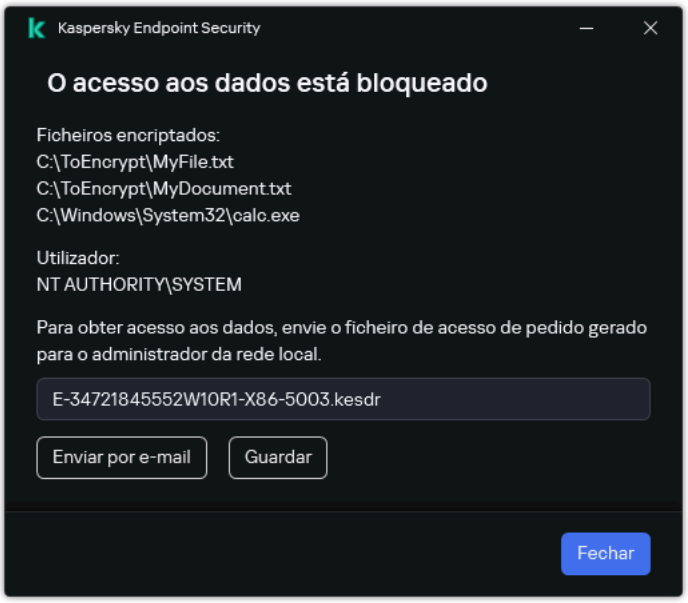
  O utilizador pode trabalhar com ficheiros encriptados nas seguintes circunstâncias:

  - Os ficheiros são colocados dentro de pacotes encriptados criados num computador com o Kaspersky Endpoint Security instalado.
  - Os ficheiros são armazenados em unidades amovíveis nas quais o modo portátil tenha sido permitido.

Para obter acesso aos arquivos encriptados, o utilizador precisa de iniciar o procedimento de recuperação (Pedido-Resposta).

A recuperação do acesso a ficheiros encriptados consiste nas seguintes etapas:

1. O utilizador envia um ficheiro de pedido de acesso ao administrador (ver a figura abaixo).
2. O administrador adiciona o ficheiro de pedido de acesso ao Kaspersky Security Center, cria um ficheiro de chave de acesso e envia-o ao utilizador.
3. O utilizador adiciona o ficheiro da chave de acesso ao Kaspersky Endpoint Security e obtém acesso aos ficheiros.



Restaurar o acesso aos ficheiros encriptados

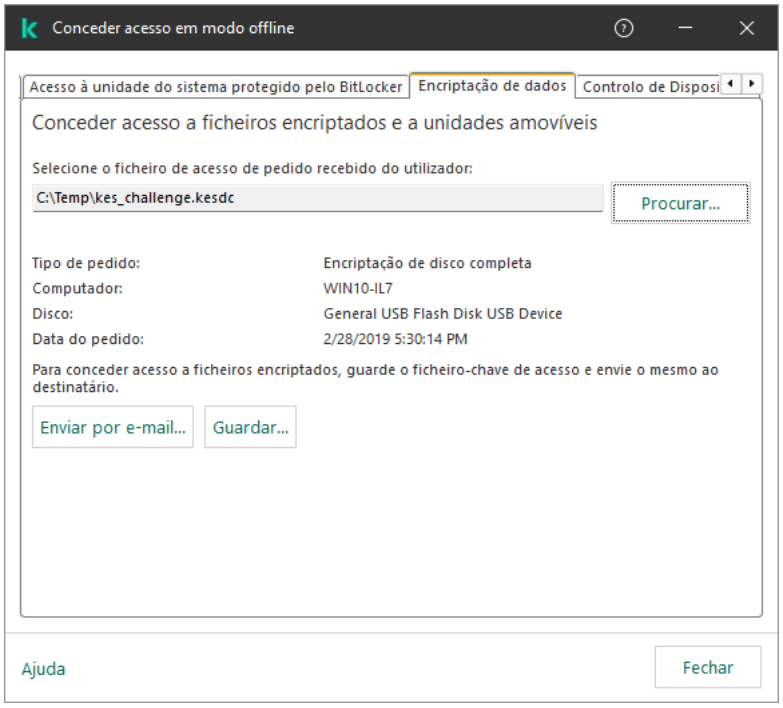
Para iniciar o procedimento de recuperação, o utilizador precisa tentar aceder um ficheiro. Como resultado, o Kaspersky Endpoint Security irá criar um ficheiro de pedido de acesso (um ficheiro com a extensão KESDC), que o utilizador precisa de enviar ao administrador, por exemplo, por e-mail.

O Kaspersky Endpoint Security gera um ficheiro de pedido de acesso para aceder a todos os ficheiros encriptados armazenados na unidade do computador (unidade local ou unidade amovível).

Como obter um ficheiro da chave de acesso a dados encriptados na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Devices**.
3. No separador **Devices**, selecione o computador do utilizador que solicitou acesso a dados encriptados, e clique com o botão direito do rato para abrir o menu de contexto.
4. No menu de contexto, selecione **Conceder acesso em modo offline**.
5. Esta ação abre uma janela; nessa janela, selecione o separador **Encriptação de dados**.
6. No separador **Encriptação de dados**, clique no botão **Procurar**.
7. Na janela para selecionar um ficheiro de pedido de acesso, especifique o caminho para o ficheiro recebido do utilizador.

Verá informações acerca do pedido do utilizador. O Kaspersky Security Center gera um ficheiro-chave. Envie por email o ficheiro-chave de acesso a dados encriptados gerado para o utilizador. Ou guarde o ficheiro de acesso e utilize qualquer método disponível para transferir o ficheiro.



Conceder acesso no modo offline

Como obter um ficheiro da chave de acesso a dados encriptados na Consola da Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Assets (Devices)**.
2. Selecione a caixa de verificação ao lado do nome do computador a cujos dados pretende restaurar o acesso.
3. Clique em **Grant access to the device in offline mode**.
4. Selecione **Data Encryption**.
5. Clique no botão **Select file** e selecione o ficheiro de pedido de acesso recebido do utilizador (um ficheiro com a extensão KESDC).

   A consola da Web apresentará informações acerca do pedido. Isto incluirá o nome do computador ao qual o utilizador está a solicitar acesso ao ficheiro.
6. Clique no botão **Save key** e selecione uma pasta onde guardar os dados encriptados (um ficheiro com a extensão KESDR).

Como resultado, poderá obter a chave de acesso a dados encriptados, que terá de transferir para o utilizador.

Após receber o ficheiro da chave de acesso a dados encriptados, o utilizador precisa de executar o ficheiro clicando duas vezes nele. Como resultado, o Kaspersky Endpoint Security concederá acesso a todos os ficheiros encriptados armazenados na unidade. Para aceder a ficheiros encriptados que estão armazenados noutras unidades, tem de obter um ficheiro-chave de acesso individual para cada unidade.

Restaurar o acesso a dados encriptados após uma falha do sistema operativo

Pode restaurar o acesso aos dados após a falha do sistema operacional apenas para encriptação ao nível de ficheiro (FLE). Você não pode restaurar o acesso aos dados se a encriptação de disco completo (FDE) for usada.

Para restaurar o acesso a dados encriptados após uma falha do sistema operativo:

1. Reinstale o sistema operativo sem formatar a unidade de disco rígido.
2. Instalar o Kaspersky Endpoint Security.
3. Estabeleça uma ligação entre o computador e o Servidor de Administração do Kaspersky Security Center que estava a controlar o computador quando os dados foram encriptados.

O acesso aos dados encriptados será concedido com as mesmas condições aplicadas antes da falha do sistema operativo.

Editar modelos de mensagens de acesso a ficheiros encriptados

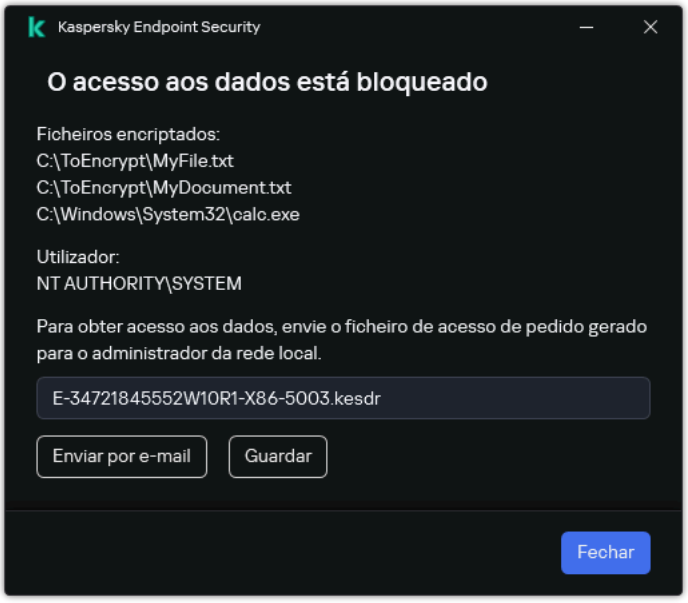
Para editar modelos de mensagens de acesso a ficheiros encriptados:

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Encriptação de dados** → **Definições de encriptação comuns**.
4. No bloco **Modelos**, clique no botão **Modelos**.
5. Na janela que surgir, faça o seguinte:
   - Se pretender editar o modelo de mensagem de utilizador, selecione o separador **Mensagem do utilizador**. A janela seguinte é aberta quando o utilizador tenta aceder a um ficheiro encriptado sem uma chave disponível no computador para aceder aos ficheiros encriptados (veja a figura abaixo). Ao clicar no botão **Enviar por e-mail** é criada automaticamente uma mensagem do utilizador. Esta mensagem é enviada ao administrador da rede da empresa local com conjunto com o ficheiro a solicitar acesso a ficheiros encriptados.
   - Se pretender editar o modelo de mensagem de administrador, selecione o separador **Mensagem do administrador**. O utilizador recebe esta mensagem após ser concedido acesso aos ficheiros encriptados.
6. Editar os modelos da mensagem.

   Para adicionar uma variável ao texto do modelo, coloque o cursor na posição desejada, clique em **Variável** e selecione a variável necessária na lista de opções disponíveis.

   Também pode restaurar o texto do modelo padrão ao clicar em **Por defeito**.

7. Guarde as suas alterações.



Restaurar o acesso aos ficheiros encriptados

Encriptação de unidades amovíveis

A encriptação de unidades removíveis não é suportada em computadores baseados em Arm.

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para estações de trabalho. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para servidores.

O Kaspersky Endpoint Security suporta a encriptação de ficheiros nos sistemas de ficheiros FAT32 e NTFS. Se uma unidade amovível com um sistema de ficheiros não suportado for ligada ao computador, a tarefa de encriptação desta unidade amovível termina com um erro e o Kaspersky Endpoint Security atribui o estado apenas de leitura à unidade amovível.

Para proteger dados em unidades amovíveis, pode usar os seguintes tipos de encriptação:

- Full Disk Encryption (FDE).

  Encriptação de toda a unidade amovível, incluindo o sistema de ficheiros.

  Não é possível aceder a dados encriptados fora da rede empresarial. Também é impossível aceder a dados encriptados dentro da rede empresarial se o computador não estiver ligado ao Kaspersky Security Center (ou seja, num computador convidado).

- File Level Encryption (FLE).

  Encriptação só de ficheiros numa unidade amovível. O sistema de ficheiros permanece inalterado.

A encriptação de ficheiros em unidades amovíveis fornece a capacidade de aceder a dados fora da rede empresarial através de um modo especial chamado *Modo portátil*.

Durante a encriptação, o Kaspersky Endpoint Security cria uma chave mestra. O Kaspersky Endpoint Security guarda a chave mestra nos seguintes repositórios:

- Kaspersky Security Center.
- Computador do utilizador.

  A chave mestra é encriptada com a chave secreta do utilizador.
- Unidade amovível.

  A chave mestra é encriptada com a chave pública do Kaspersky Security Center.

Após a conclusão da encriptação, os dados na unidade amovível podem ser acedidos na rede empresarial como se estivessem numa unidade amovível convencional não encriptada.

Aceder a dados encriptados

Quando uma unidade amovível com dados encriptados é ligada, o Kaspersky Endpoint Security executa as seguintes ações:

1. Verifica se há uma chave mestra no armazenamento local no computador do utilizador.

   Se a chave mestra for encontrada, o utilizador obterá acesso aos dados na unidade amovível.

   Se a chave mestra não for encontrada, o Kaspersky Endpoint Security executa as seguintes ações:

   a. Envia um pedido ao Kaspersky Security Center.

      Após receber o pedido, o Kaspersky Security Center envia uma resposta que contém a chave mestra.

   b. O Kaspersky Endpoint Security guarda a chave mestra no armazenamento local no computador do utilizador para operações subsequentes com a unidade amovível encriptada.
2. Desencripta os dados.

Recursos especiais de encriptação de unidade amovível

A encriptação de unidades amovíveis possui os seguintes recursos especiais:

- A política com predefinições para encriptação de unidades amovíveis é formada por um grupo específico de computadores geridos. Como tal, o resultado da aplicação da política do Kaspersky Security Center configurada para a encriptação/desencriptação de unidades amovíveis depende do computador ao qual a unidade amovível está ligada.
- O Kaspersky Endpoint Security não encripta/desencripta ficheiros apenas de leitura que estão armazenados em unidades amovíveis.

- Os seguintes tipos de dispositivos são suportados como unidades amovíveis:
  - Suportes de dados ligados pelo bus USB
  - unidades de disco rígido ligadas por bus USB e bus FireWire
  - unidades SSD ligadas por barramentos USB e FireWire

Iniciar a encriptação de unidades amovíveis

Pode usar uma política para desencriptar uma unidade amovível. Uma política com definições definidas para a encriptação de unidades amovíveis é gerada para um grupo de administração específico. Deste modo, o resultado da desencriptação de dados em unidades amovíveis depende do computador ao qual a unidade amovível está ligada.

O Kaspersky Endpoint Security suporta a encriptação de ficheiros nos sistemas de ficheiros FAT32 e NTFS. Se uma unidade amovível com um sistema de ficheiros não suportado for ligada ao computador, a tarefa de encriptação desta unidade amovível termina com um erro e o Kaspersky Endpoint Security atribui o estado apenas de leitura à unidade amovível.

Antes de encriptar ficheiros numa unidade amovível, 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 encriptação do ficheiro pode falhar com um erro.

Para encriptar unidades amovíveis:

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Encriptação de dados** → **Encriptação de unidades amovíveis**.
4. Na lista pendente **Modo de encriptação**, selecione a ação predefinida que pretende que o Kaspersky Endpoint Security execute nas unidades removíveis:
   - **Encriptar unidade amovível completa** (FDE). O Kaspersky Endpoint Security encripta o conteúdo de um setor de uma unidade amovível por setor. Como resultado, a aplicação encripta não só os ficheiros armazenados na unidade amovível, mas também os seus sistemas de ficheiros, incluindo os nomes dos ficheiros e estruturas da pasta na unidade amovível.
   - **Encriptar todos os ficheiros** (FLE). O Kaspersky Endpoint Security encripta todos os ficheiros armazenados nas unidades removíveis. A aplicação não encripta os sistemas de ficheiros de unidades amovíveis, incluindo nomes de ficheiros e estruturas de pastas.
   - **Encriptar apenas os ficheiros novos** (FLE). O Kaspersky Endpoint Security encripta apenas os ficheiros que foram adicionados a unidades amovíveis ou que foram armazenados em unidades amovíveis e foram modificados após a última aplicação da política do Kaspersky Security Center.

   O Kaspersky Endpoint Security não volta a encriptar uma unidade amovível que já tenha sido encriptada.

5. Se quiser usar o modo portátil para a encriptação de unidades amovíveis, selecione a caixa de verificação **Modo portátil**.

   O *Modo portátil* é um modo de encriptação de ficheiros (FLE) em unidades amovíveis que disponibiliza a capacidade de aceder a dados fora de uma rede empresarial. O modo portátil também permite que trabalhe com dados encriptados em computadores nos quais o Kaspersky Endpoint Security não está instalado.

6. Se quer encriptar uma nova unidade amovível, recomendamos a seleção da caixa de verificação **Encriptar apenas espaço de disco utilizado**. Se a caixa de verificação for desmarcada, o Kaspersky Endpoint Security irá encriptar todos os ficheiros, incluindo os fragmentos residuais dos ficheiros eliminados ou modificados.

7. Se quiser configurar a encriptação para unidades amovíveis individuais, defina regras de encriptação.

8. Se quiser utilizar a encriptação de disco completo de unidades amovíveis no Modo offline, selecione a caixa de verificação **Permitir encriptação de unidades amovíveis no modo offline**.

   O Modo de encriptação offline refere-se à encriptação de unidades amovíveis (FDE) quando não há ligação ao Kaspersky Security Center. Durante a encriptação, o Kaspersky Endpoint Security guarda a chave mestra apenas no computador do utilizador. O Kaspersky Endpoint Security irá enviar a chave mestra para o Kaspersky Security Center na próxima sincronização.

   > Não será possível obter acesso à unidade amovível se o computador no qual a chave mestra é guardada for corrompido e os dados não forem enviados para o Kaspersky Security Center.

   A encriptação da unidade amovível não será possível se a caixa de verificação **Permitir encriptação de unidades amovíveis no modo offline** for desmarcada e não houver ligação ao Kaspersky Security Center.

9. Guarde as suas alterações.

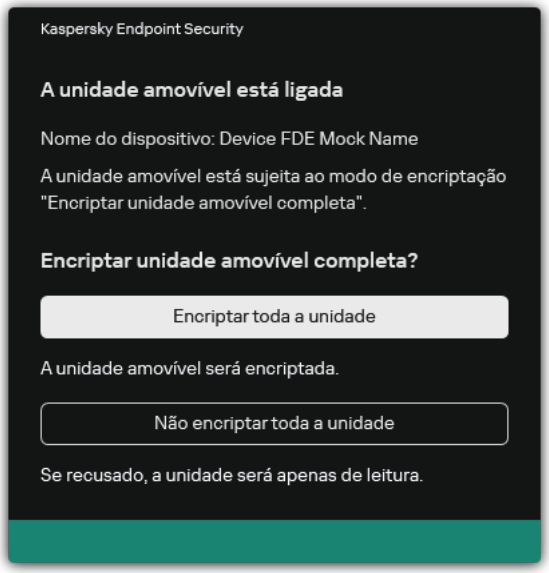
Após a aplicação da política, quando o utilizador liga uma unidade amovível ou se uma unidade amovível já estiver ligada, o Kaspersky Endpoint Security solicita ao utilizador uma confirmação para executar a operação de encriptação (ver a figura abaixo).

A aplicação permite-lhe realizar as seguintes ações:

- Se o utilizador confirmar o pedido de encriptação, o Kaspersky Endpoint Security encripta os dados.
- Se o utilizador recusar o pedido de encriptação, o Kaspersky Endpoint Security deixa os dados inalterados e atribui acesso apenas de leitura a esta unidade amovível.
- Se o utilizador não responder ao pedido de encriptação, o Kaspersky Endpoint Security mantém os dados inalterados e atribui acesso apenas de leitura a esta unidade removível. A aplicação solicita confirmação novamente ao aplicar posteriormente uma política ou da próxima vez que esta unidade amovível for ligada novamente.

Se o utilizador inicia a remoção segura de uma unidade amovível durante a encriptação de dados, o Kaspersky Endpoint Security interrompe o processo de encriptação de dados e permite a remoção da unidade amovível antes da conclusão do processo de encriptação. A encriptação de dados continuará na próxima vez que a unidade removível for conectada a este computador.

Se a encriptação de uma unidade amovível falhar, consulte o relatório de **Encriptação de dados** na interface do Kaspersky Endpoint Security. O acesso aos ficheiros pode ser bloqueado por outra aplicação. Nesse caso, tente remover a unidade amovível do computador e introduzi-la novamente.



Pedido de encriptação de unidade amovível

Adicionar uma regra de encriptação para unidades amovíveis

Para adicionar uma regra de encriptação para unidades amovíveis:

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Encriptação de dados** → **Encriptação de unidades amovíveis**.
4. Clique em **Adicionar** e na lista pendente selecione um dos seguintes itens:
   - Se pretender adicionar regras de encriptação para unidades amovíveis incluídas na lista de dispositivos fiáveis do componente de Controlo de Dispositivos, selecione **Na lista de dispositivos fiáveis desta política**.
   - Se pretender adicionar regras de encriptação para unidades amovíveis incluídas na lista do Kaspersky Security Center, selecione **Da lista de dispositivos do Kaspersky Security Center**.
5. Na lista pendente **Modo de encriptação para os dispositivos selecionados**, selecione a ação a executar pelo Kaspersky Endpoint Security em ficheiros armazenados nas unidades amovíveis selecionadas.

6. Selecione a caixa de verificação **Modo portátil** se pretender que o Kaspersky Endpoint Security prepare as unidades amovíveis antes da encriptação, possibilitando a utilização de ficheiros encriptados armazenados nessas unidades no modo portátil.

   O modo portátil permite utilizar ficheiros encriptados armazenados em unidades amovíveis que estejam ligadas a computadores sem a funcionalidade de encriptação.

7. Selecione a caixa de verificação **Encriptar apenas espaço de disco utilizado** se pretender que o Kaspersky Endpoint Security encripte apenas os setores de disco que estão ocupados por ficheiros.

   Se estiver a aplicar encriptação numa unidade que já está em utilização, é recomendado encriptar a unidade inteira. Esta ação assegura que todos os dados estão protegidos – até mesmo dados apagados que ainda possam conter informação recuperável. A função **Encriptar apenas espaço de disco utilizado** é recomendada para novas unidades que não tenham sido utilizadas anteriormente.

   Se um dispositivo tiver sido encriptado anteriormente utilizando a função **Encriptar apenas espaço de disco utilizado**, depois de aplicar uma política no modo **Encriptar unidade amovível completa**, os setores que não estejam ocupados por ficheiros continuarão sem ser encriptados.

8. Na lista pendente **Ações para os dispositivos selecionados anteriormente**, selecione a ação a ser executada pelo Kaspersky Endpoint Security de acordo com as regras de encriptação que foram previamente definidas para as unidades amovíveis:

   - Se pretender que a regra de encriptação criada anteriormente para a unidade amovível permaneça inalterada, selecione **Ignorar**.
   - Se pretender que a regra de encriptação criada anteriormente para a unidade amovível seja substituída pela nova regra, selecione **Atualizar**.

9. Guarde as suas alterações.

As regras de encriptação adicionadas para unidades amovíveis serão aplicadas a unidades amovíveis ligadas a qualquer computador na organização.

Exportar e importar uma lista de regras de encriptação para unidades amovíveis

Pode exportar a lista de regras de encriptação da unidade amovível para um ficheiro XML. Em seguida, pode modificar o ficheiro para, por exemplo, adicionar um grande número de regras para o mesmo tipo de unidades amovíveis. Também pode usar a função de exportação/importação para fazer uma cópia de segurança da lista de regras ou para migrar as regras para um servidor diferente.

Como exportar e importar uma lista de regras de encriptação da unidade amovível na Consola de Administração (MMC)

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.
4. Aceda a **Data Encryption** → **Encryption of removable drives**.

5. No bloco **Encryption rules for selected devices**, clique na ligação **<N> rules**.

   Abre-se uma lista de regras de encriptação para unidades amovíveis.

6. Para exportar a lista de regras de encriptação de unidades amovíveis:

   a. Selecione as regras que pretende exportar.

   b. Clique em **Export**.

   c. Confirme que deseja exportar apenas as regras selecionadas ou exportar a lista inteira.

   d. Guardar o ficheiro.

      O Kaspersky Endpoint Security exporta a lista de regras para um ficheiro XML na pasta de transferências predefinida.

7. Para importar a lista de regras:

   a. Clique na hiperligação **Import**.

      Na janela que se abre, selecione o ficheiro XML a partir do qual pretende importar a lista de regras.

   b. Abrir o ficheiro.

      Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro XML.

8. Guarde as suas alterações.

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Encriptação de dados → Encriptação de unidades amovíveis**.

4. Para exportar a lista de regras de encriptação de unidades amovíveis:

   a. Selecione as regras que pretende exportar. Para selecionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.

      Se não tiver selecionado nenhuma regra, o Kaspersky Endpoint Security exportará todas as regras.

   b. Clique na hiperligação **Exportar**.

   c. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de regras e selecione a pasta onde pretende guardar este ficheiro.

   d. Guardar o ficheiro.

      O Kaspersky Endpoint Security exporta a lista de regras para o ficheiro XML.

5. Para importar uma lista de regras de encriptação de unidades amovíveis:

   a. Clique na hiperligação **Importar**.

      Na janela que se abre, selecione o ficheiro XML a partir do qual pretende importar a lista de regras.

b. Abrir o ficheiro.

Se o computador já tiver uma lista de regras, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas à mesma a partir do ficheiro XML.

6. Guarde as suas alterações.

Modo portátil para aceder a ficheiros encriptados em unidades amovíveis

O *Modo portátil* é um modo de encriptação de ficheiros (FLE) em unidades amovíveis que disponibiliza a capacidade de aceder a dados fora de uma rede empresarial. O modo portátil também permite que trabalhe com dados encriptados em computadores nos quais o Kaspersky Endpoint Security não está instalado.

O modo portátil é conveniente para utilizar nos seguintes casos:

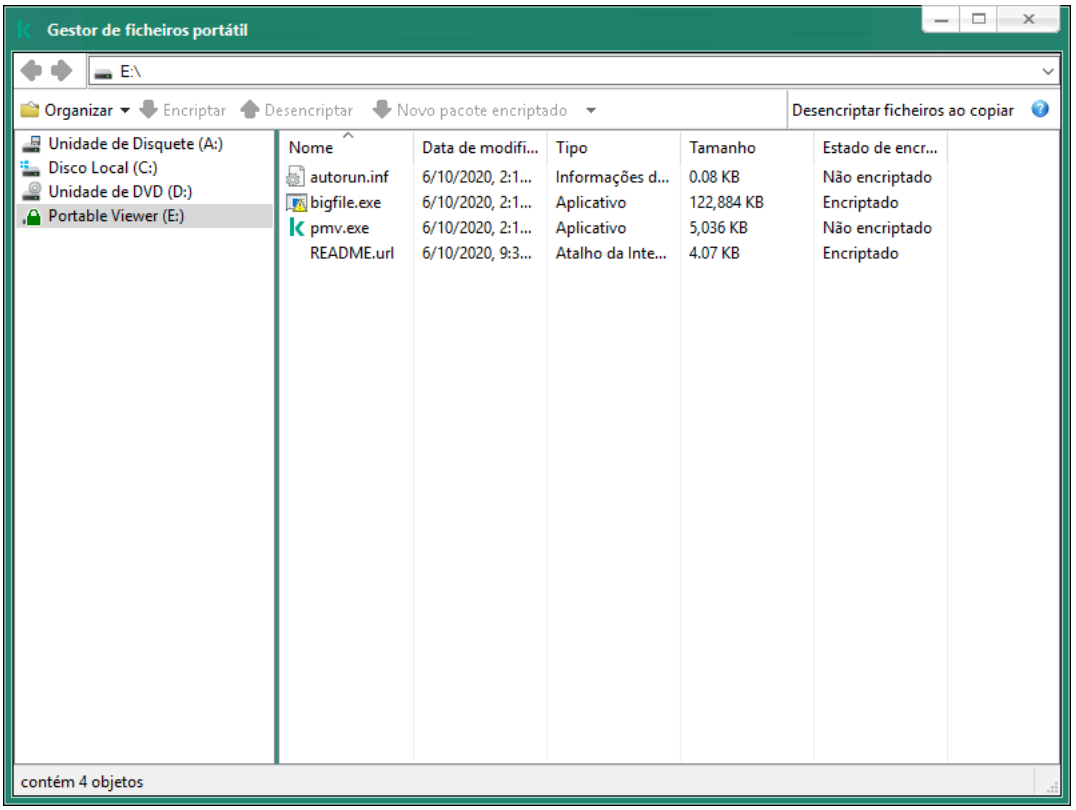
- Não há ligação entre o computador e o Servidor de Administração do Kaspersky Security Center.
- A infraestrutura mudou com a alteração do Servidor de Administração do Kaspersky Security Center.
- O Kaspersky Endpoint Security não está instalado no computador.

Gestor de ficheiros portátil

Para trabalhar no modo portátil, o Kaspersky Endpoint Security instala um módulo de encriptação especial chamado *Gestor de ficheiros portátil* numa unidade amovível. O Gestor de ficheiros portátil fornece uma interface para trabalhar com dados encriptados se o Kaspersky Endpoint Security não estiver instalado no computador (ver a figura abaixo). Se o Kaspersky Endpoint Security estiver instalado no computador, poderá trabalhar com unidades amovíveis encriptadas utilizando o gestor de ficheiros usual (por exemplo, o Explorador).

O Gestor de ficheiros portátil armazena uma chave para encriptar ficheiros numa unidade amovível. A chave é encriptada com a password do utilizador. O utilizador define uma password antes de encriptar ficheiros numa unidade amovível.

O Gestor de ficheiros portátil é iniciado automaticamente quando uma unidade amovível é ligada a um computador no qual o Kaspersky Endpoint Security não está instalado. Se a inicialização automática de aplicações estiver desativada no computador, inicie manualmente o Gestor de ficheiros portátil. Para fazer isso, execute o ficheiro chamado pmv.exe que está armazenado na unidade amovível.



Gestor de ficheiros portátil

Suporte para o modo portátil para trabalhar com ficheiros encriptados

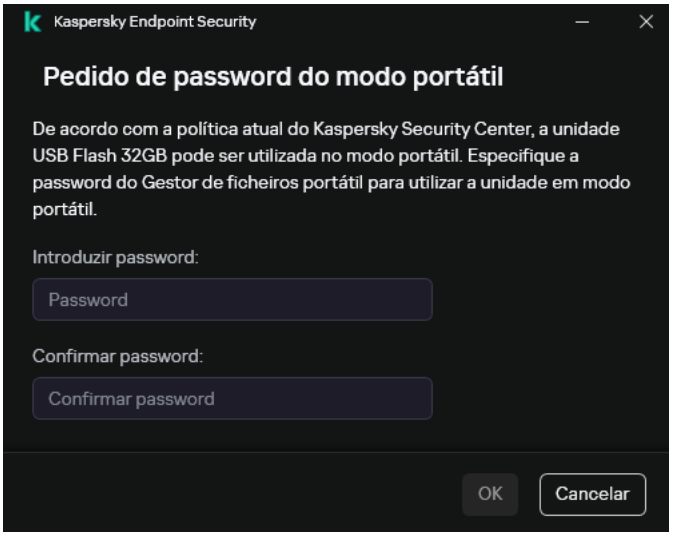
Como ativar o suporte ao modo portátil para trabalhar com ficheiros encriptados em unidades amovíveis no Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Encriptação de dados → Encriptação de unidades amovíveis**.
4. Na lista pendente **Modo de encriptação para os dispositivos selecionados**, selecione **Encriptar todos os ficheiros** ou **Encriptar apenas os ficheiros novos**.

   O modo portátil está disponível apenas com Encriptação ao nível dos ficheiros (FLE). Não é possível ativar o suporte ao modo portátil para Encriptação de disco completa (FDE).

5. Selecione a caixa de verificação **Modo portátil**.
6. Se necessário, adicione regras de encriptação para unidades amovíveis individuais.
7. Guarde as suas alterações.
8. Após aplicar a política, ligue a unidade amovível ao computador.
9. Confirme a operação de encriptação da unidade amovível.

Isto abre uma janela na qual pode criar uma password para o Gestor de ficheiros portátil.



Pedido de password do modo portátil

10. Especifique uma password que cumpra os requisitos de força e confirme-a.
11. Guarde as suas alterações.

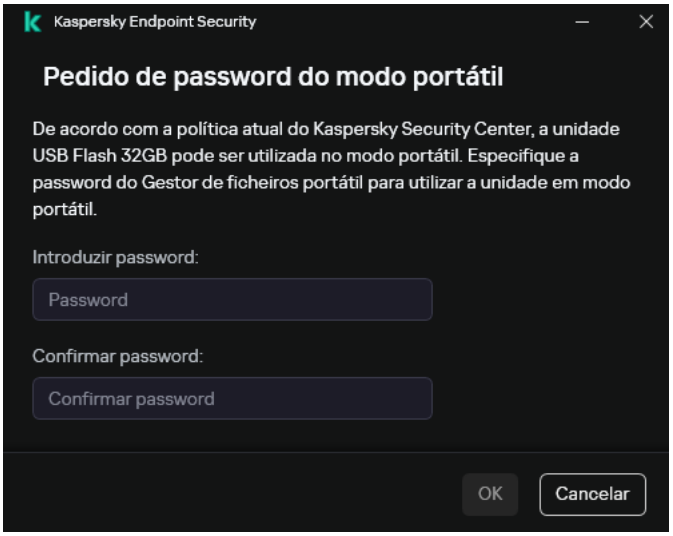
Como ativar o suporte do modo portátil para trabalhar com ficheiros encriptados em unidades amovíveis no consola da Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Data Encryption** → **Encryption of removable drives**.
5. No bloco **Default action**, selecione **Encrypt all files** ou **Encrypt new files only**.

   O modo portátil está disponível apenas com Encriptação ao nível dos ficheiros (FLE). Não é possível ativar o suporte ao modo portátil para Encriptação de disco completa (FDE).

6. Selecione a caixa de verificação **Portable mode**.
7. Se necessário, adicione regras de encriptação para unidades amovíveis individuais.
8. Guarde as suas alterações.
9. Após aplicar a política, ligue a unidade amovível ao computador.
10. Confirme a operação de encriptação da unidade amovível.

Isto abre uma janela na qual pode criar uma password para o Gestor de ficheiros portátil.



Pedido de password do modo portátil

11. Especifique uma password que cumpra os requisitos de força e confirme-a.

12. Guarde as suas alterações.

O Kaspersky Endpoint Security encriptará os ficheiros na unidade amovível. O Gestor de ficheiros portátil utilizado para trabalhar com ficheiros encriptados também será adicionado à unidade amovível. Se já houver ficheiros encriptados na unidade amovível, o Kaspersky Endpoint Security irá encriptar estes ficheiros novamente utilizando a sua própria chave. Isto permite que o utilizador aceda a todos os ficheiros na unidade amovível no modo portátil.

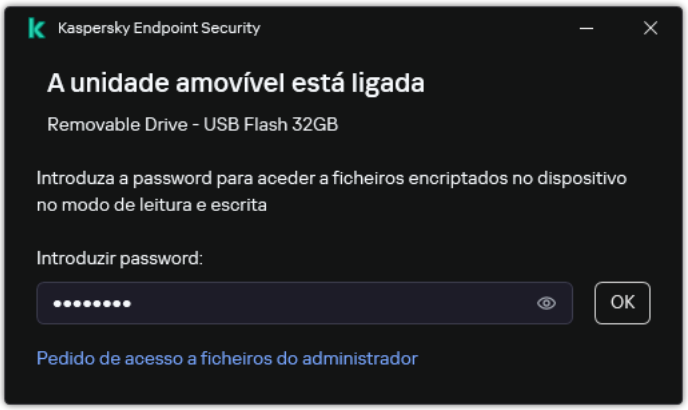
Aceder a ficheiros encriptados numa unidade amovível

Depois de encriptar os ficheiros numa unidade amovível com suporte do modo portátil, estão disponíveis os seguintes métodos de acesso a ficheiros:

- Se o Kaspersky Endpoint Security não estiver instalado no computador, o Gestor de ficheiros portátil solicitará a introdução de uma password. Terá de introduzir a password sempre que reiniciar o computador ou reconectar a unidade amovível.

- Se o computador estiver localizado fora da rede empresarial e o Kaspersky Endpoint Security estiver instalado, a aplicação solicitará a introdução de uma password ou o envio ao administrador de um pedido de acesso aos ficheiros. Depois de obter acesso aos ficheiros numa unidade amovível, o Kaspersky Endpoint Security guarda a chave secreta no armazenamento de chaves do computador. Isto permitirá o acesso a ficheiros no futuro sem ter de introduzir uma password ou pedir ao administrador (veja a figura abaixo).

- Se o computador estiver localizado dentro da rede empresarial e o Kaspersky Endpoint Security estiver instalado no computador, terá acesso ao dispositivo sem ter de introduzir uma password. O Kaspersky Endpoint Security receberá a chave secreta do Servidor de Administração do Kaspersky Security Center ao qual o computador está ligado.



Aceder a ficheiros encriptados numa unidade amovível

Recuperar a password para trabalhar no modo portátil

Caso se tenha esquecido da password para trabalhar no modo portátil, terá de ligar a unidade amovível a um computador com o Kaspersky Endpoint Security instalado na rede empresarial. Terá acesso aos ficheiros porque a chave secreta é armazenada no armazenamento de chaves do computador ou no Servidor de Administração. Desencripte e encripte novamente os ficheiros com uma nova password.

Recursos do modo portátil ao ligar uma unidade amovível a um computador de outra rede

Se o computador estiver localizado fora da rede empresarial e o Kaspersky Endpoint Security estiver instalado, pode aceder aos ficheiros das seguintes maneiras:

- **Acesso baseado em password**

  Após introduzir a password, poderá ver, modificar e guardar ficheiros na unidade amovível (*acesso transparente*). O Kaspersky Endpoint Security pode definir um direito de acesso de leitura apenas para uma unidade amovível se os seguintes parâmetros estiverem configurados nas definições de política para encriptação de unidades amovíveis:

  - O suporte ao modo portátil está desativado.
  - O modo **Encriptar todos os ficheiros** ou o modo **Encriptar apenas os ficheiros novos** está selecionado.

  Em todos os outros casos, terá acesso total à unidade amovível (permissão de leitura/gravação). Poderá adicionar e eliminar ficheiros.

  Pode alterar as permissões de acesso à unidade amovível, até mesmo quando a unidade amovível estiver ligada ao computador. Se as permissões de acesso à unidade amovível forem alteradas, o Kaspersky Endpoint Security bloqueia o acesso aos ficheiros e vai lhe solicitar a password novamente.

  Após introduzir a password, não poderá aplicar as definições da política de encriptação para a unidade amovível. Neste caso, é impossível desencriptar ou encriptar novamente os ficheiros na unidade amovível.

- **Peça ao administrador o acesso aos ficheiros**

Se tiver esquecido da password para trabalhar no modo portátil, solicite o acesso aos ficheiros ao administrador. Para aceder aos ficheiros, o utilizador precisa de enviar ao administrador um ficheiro de pedido de acesso (um ficheiro com a extensão KESDC). O utilizador pode enviar o ficheiro de pedido de acesso por e-mail, por exemplo. O administrador enviará um ficheiro de acesso a dados encriptados (um ficheiro com a extensão KESDR).

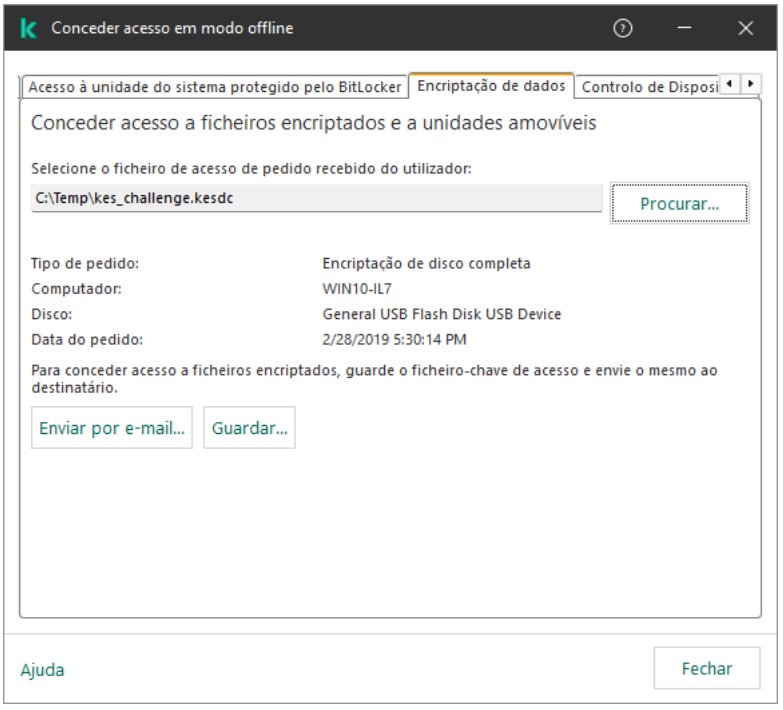
Depois de concluir o procedimento de Pedido/Resposta de recuperação da password, vai receber acesso transparente aos ficheiros na unidade amovível e acesso total à unidade amovível (permissão de leitura/gravação).

Pode aplicar uma política de encriptação de unidade amovível e desencriptar ficheiros, por exemplo. Após ter recuperado a password ou quando a política for atualizada, o Kaspersky Endpoint Security solicitará que confirme as alterações.

Como obter um ficheiro de acesso a dados encriptados na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Devices**.
3. No separador **Devices**, selecione o computador do utilizador que solicitou acesso a dados encriptados, e clique com o botão direito do rato para abrir o menu de contexto.
4. No menu de contexto, selecione **Conceder acesso em modo offline**.
5. Esta ação abre uma janela; nessa janela, selecione o separador **Encriptação de dados**.
6. No separador **Encriptação de dados**, clique no botão **Procurar**.
7. Na janela para selecionar um ficheiro de pedido de acesso, especifique o caminho para o ficheiro recebido do utilizador.

   Verá informações acerca do pedido do utilizador. O Kaspersky Security Center gera um ficheiro-chave. Envie por email o ficheiro-chave de acesso a dados encriptados gerado para o utilizador. Ou guarde o ficheiro de acesso e utilize qualquer método disponível para transferir o ficheiro.



Conceder acesso no modo offline

Como obter um ficheiro de acesso a dados encriptados na consola da Web

1. Na janela principal da Consola Web, selecione **Asset management → Assets (Devices)**.
2. Selecione a caixa de verificação ao lado do nome do computador a cujos dados pretende restaurar o acesso.
3. Clique em **Grant access to the device in offline mode**.
4. Selecione **Data Encryption**.
5. Clique no botão **Select file** e selecione o ficheiro de pedido de acesso recebido do utilizador (um ficheiro com a extensão KESDC).

   A consola da Web apresentará informações acerca do pedido. Isto incluirá o nome do computador ao qual o utilizador está a solicitar acesso ao ficheiro.
6. Clique no botão **Save key** e selecione uma pasta onde guardar os dados encriptados (um ficheiro com a extensão KESDR).

Como resultado, poderá obter a chave de acesso a dados encriptados, que terá de transferir para o utilizador.

Desencriptação de unidades amovíveis

Pode usar uma política para desencriptar uma unidade amovível. Uma política com definições definidas para a encriptação de unidades amovíveis é gerada para um grupo de administração específico. Deste modo, o resultado da desencriptação de dados em unidades amovíveis depende do computador ao qual a unidade amovível está ligada.

Para desencriptar unidades amovíveis:

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Encriptação de dados → Encriptação de unidades amovíveis**.
4. Se pretende desencriptar todos os ficheiros encriptados que estão armazenados em unidades amovíveis, na lista pendente **Modo de encriptação** selecione **Desencriptar unidade amovível completa**.

5. Para desencriptar dados armazenados em unidades amovíveis individuais, edite as regras de encriptação para unidades amovíveis cujos dados pretende desencriptar. Para tal:

   a. Na lista de unidades amovíveis para as quais as regras de encriptação foram configuradas, selecione uma entrada correspondente à unidade amovível de que necessita.

   b. Clique no botão **Definir uma regra** para editar a regra de encriptação para a unidade amovível selecionada.

   c. No menu de contexto do botão **Definir uma regra**, selecione **Desencriptar unidade amovível completa**.

6. Guarde as suas alterações.

Como resultado, se um utilizador ligar uma unidade amovível ou se esta já estiver ligada, o Kaspersky Endpoint Security desencripta a unidade amovível. A aplicação avisa o utilizador de que o processo de desencriptação pode demorar algum tempo. Se o utilizador inicia a remoção segura de uma unidade amovível durante a desencriptação de dados, o Kaspersky Endpoint Security interrompe o processo de desencriptação de dados e permite a remoção da unidade amovível antes da conclusão da operação de desencriptação. A desencriptação de dados continuará na próxima vez que a unidade removível for conectada a este computador.

Se a desencriptação de uma unidade amovível falhar, consulte o relatório de **Encriptação de dados** na interface do Kaspersky Endpoint Security. O acesso aos ficheiros pode ser bloqueado por outra aplicação. Nesse caso, tente remover a unidade amovível do computador e introduzi-la novamente.

Ver detalhes da encriptação de dados

Enquanto as tarefas de encriptação e desencriptação decorrem, o Kaspersky Endpoint Security transmite informação sobre o estado dos parâmetros de encriptação aplicados a computadores cliente para o Kaspersky Security Center.

Visualizar o estado de encriptação

Pode ver o estado para monitorizar a encriptação de dados. O Kaspersky Endpoint Security atribui os seguintes estados de encriptação:

- **Does not meet the policy; canceled by user**. O utilizador cancelou a encriptação de dados.
- **Does not meet the policy due to an error**. Erro de encriptação de dados, por exemplo, a licença está em falta.
- **Applying the policy; restart is required**. A encriptação de dados está a decorrer no computador. Reinicie o computador para concluir a encriptação de dados.
- **No encryption policy specified**. A encriptação de dados está desativada nas definições da política.
- **Not supported**. Os componentes da encriptação de dados não estão instalados no computador.
- **Applying the policy**. A encriptação e/ou desencriptação de dados está a decorrer no computador.

Para ver o estado de encriptação dos dados do computador:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Managed devices**.
3. No separador **Devices** da área de trabalho, faça deslizar a barra de deslocamento totalmente para a direita. Se a coluna **Encryption status** não for exibida, adicione esta coluna nas definições da consola do Kaspersky Security Center.

   A coluna **Encryption status** apresenta o estado de encriptação de dados em computadores do grupo de administração selecionado. Este estado é formado com base em informações sobre a encriptação de ficheiros nas unidades locais do computador e encriptação de disco completa.
4. Se o estado da encriptação de dados do computador for **Applying policy**, pode monitorizar o painel de progresso da encriptação:
   a. Abra as propriedades do computador com o estado **Applying policy** ao clicar duas vezes no mesmo.
   b. Na janela de propriedades do computador, selecione a secção **Applications**.
   c. Na lista de aplicações da Kaspersky instaladas no computador, selecione **Kaspersky Endpoint Security for Windows**.
   d. Clique em **Statistics**.
   e. Sob **Encryption of devices**, pode ver o progresso atual da encriptação de dados como uma percentagem.

Ver estatísticas de encriptação nos painéis do Kaspersky Security Center

Para ver o estado de encriptação nos painéis do Kaspersky Security Center:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione o **Administration Server**.
3. Na área de trabalho, à direita da árvore da Consola de Administração, selecione o separador **Statistics**.
4. Crie uma nova página com painéis de detalhes que contenham as estatísticas de encriptação de dados. Para tal:
   a. No separador **Statistics**, clique no botão **Customize view**.
   b. Na janela que abre, clique no botão **Add**.
   c. Esta ação abre uma janela; nessa janela, na secção **General**, introduza o nome da página.
   d. Na secção **Information panels**, clique no botão **Add**.
   e. Na janela que abre no grupo **Protection status**, selecione o item **Encryption of devices**.
   f. Clique em **OK**.

g. Se for necessário, edite as definições do painel de detalhes. Para tal, utilize as secções **View** e **Devices**.

h. Clique em **OK**.

i. Repita os passos d – h das instruções, selecionando o item **Encryption of removable drives** na secção **Protection status**.

Os painéis de detalhes adicionados são apresentados na lista **Information panels**.

j. Clique em **OK**.

O nome da página com painéis de detalhes criada nos passos anteriores é apresentado na lista **Pages**.

k. Selecione o botão **Close**.

5. No separador **Statistics**, abra a página criada nos passos anteriores das instruções.

Os painéis de detalhes são visualizados, apresentando o estado de encriptação dos computadores e unidades amovíveis.

Visualizar os erros de encriptação de ficheiros em unidades do computador locais

Para visualizar os erros de encriptação de ficheiros em unidades locais:

1. Abra a Consola de Administração do Kaspersky Security Center.

2. Na árvore da consola, selecione **Managed devices**.

3. No separador **Devices**, selecione o nome do computador na lista e clique com o botão direito do rato para abrir o menu de contexto.

4. No menu de contexto do computador, selecione **Properties**. Na janela que surgir, selecione a secção **Protection**.

5. Clique na ligação **View data encryption errors** para abrir a janela **Data encryption errors**.

Esta janela apresenta os detalhes de erros de encriptação de ficheiros em unidades de leitura locais. Quando um erro é corrigido, o Kaspersky Security Center remove os detalhes do erro da janela **Data encryption errors**.

Ver o relatório de encriptação de dados

O Kaspersky Security Center permite criar relatórios de encriptação de dados:

- **Report on encryption status of managed devices**. O relatório inclui informações sobre se o estado da encriptação do computador está em conformidade com a política de encriptação.

- **Report on encryption status of mass storage devices**. O relatório inclui informações sobre o estado da encriptação dos dispositivos externos e dos dispositivos de armazenamento.

- **Report on rights to access encrypted drives**. O relatório inclui informações sobre o estado das contas que têm acesso a unidades encriptadas.

- **Report on file encryption errors**. O relatório inclui informações sobre os erros ocorridos durante a execução de tarefas de encriptação ou desencriptação de dados em computadores.
- **Report on blockage of access to encrypted files**. O relatório inclui informações sobre as aplicações que são impedidas de obter acesso a ficheiros encriptados.

Para ver o relatório de encriptação de dados:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. No nó **Administration Server** da árvore da Consola de Administração, selecione o separador **Reports**.
3. Selecione o botão **New report template**.

   O novo Assistente de Modelos de Relatório é iniciado.
4. Siga as instruções do Assistente de Modelos de Relatório. Na janela **Selecting the report template type**, na secção **Other**, selecione um dos seguintes relatórios de encriptação de dados.

   Depois de concluir o Novo Assistente de Modelos de Relatório, o novo modelo de relatório é apresentado na tabela no separador **Reports**.
5. Selecione o modelo de relatório que foi criado nos passos prévios das instruções.
6. No menu de contexto do modelo, selecione **Show report**.

O processo de criação do relatório é iniciado. O relatório é apresentado numa nova janela.

Trabalhar com dispositivos encriptados quando não existe acesso aos mesmos

Obter acesso a dispositivos encriptados

Um utilizador pode ser obrigado a solicitar o acesso a dispositivos encriptados nos seguintes casos:

- o disco rígido foi encriptado num computador diferente.
- a chave de encriptação de um dispositivo não está no computador (por exemplo, depois da primeira tentativa de aceder à unidade amovível encriptada no computador) e o computador não está ligado ao Kaspersky Security Center.

  depois de o utilizador ter aplicado a chave de acesso ao dispositivo encriptado, o Kaspersky Endpoint Security guarda a chave de encriptação no computador do utilizador e permite o acesso a este dispositivo depois de tentativas de acesso subsequentes, mesmo que não exista ligação ao Kaspersky Security Center.

O acesso a dispositivos encriptados pode ser obtido da seguinte forma:

1. O utilizador utiliza a interface da aplicação do Kaspersky Endpoint Security para criar um ficheiro de acesso de pedido com a extensão kesdc e envia-a ao administrador da rede local empresarial.
2. O administrador utiliza a Consola de Administração do Kaspersky Security Center para criar um ficheiro-chave de acesso com a extensão kesdr e envia-a ao utilizador.
3. O utilizador aplica a chave de acesso.

Restaurar dados em dispositivos encriptados

Um utilizador pode utilizar a Ferramenta de Restauro de Dispositivo Encriptado (doravante designada Ferramenta de Restauro) para trabalhar com dispositivos encriptados. Tal pode ser necessário nos seguintes casos:

- O procedimento para utilizar uma chave de acesso para obter acesso foi malsucedido.
- Os componentes de encriptação não foram instalados no computador com o dispositivo encriptado.

Os dados necessários para restaurar o acesso a dispositivos encriptados ao utilizar a Ferramenta de Restauro estão na memória do computador do utilizador na forma desencriptada durante algum tempo. Para reduzir o risco de acesso não autorizado a esses dados, recomendamos que restaure o acesso aos dispositivos encriptados em computadores fiáveis.

Os dados em dispositivos encriptados podem ser restaurados da seguinte forma:

1. O utilizador utiliza a Ferramenta de Restauro para criar um ficheiro de acesso de pedido com a extensão fdertc e envia-a ao administrador da rede local empresarial.
2. O administrador utiliza a Consola de Administração do Kaspersky Security Center para criar um ficheiro-chave de acesso com a extensão fdertr e envia-a ao utilizador.
3. O utilizador aplica a chave de acesso.

Para restaurar dados em discos rígidos de sistema encriptados, o utilizador também pode especificar as credenciais da conta de Agente de Autenticação na Ferramenta de Restauro. Se os metadados da conta do Agente de Autenticação tiverem sido corrompidos, o utilizador deve concluir o procedimento de restauro ao utilizar um ficheiro de acesso de pedido.

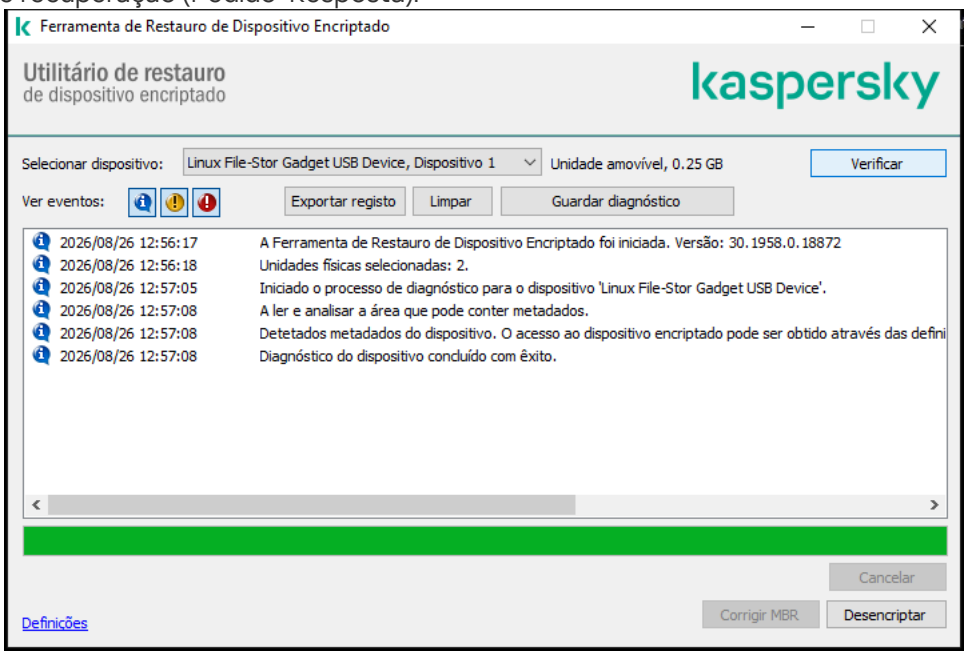
Antes de restaurar dados em dispositivos encriptados, recomenda-se que cancele a política do Kaspersky Security Center ou desative a encriptação nas definições da política do Kaspersky Security Center no computador onde o procedimento será executado. Este procedimento impede que o dispositivo seja encriptado novamente.

Recuperar dados utilizando Utilitário de Restauro FDERT

Se o disco rígido falhar, o sistema de ficheiros pode estar corrompido. Se for esse o caso, os dados protegidos pela tecnologia Encriptação de disco Kaspersky não estarão disponíveis. Pode desencriptar os dados e copiá-los para uma nova unidade.

A recuperação de dados numa unidade protegida pela tecnologia Encriptação de disco Kaspersky consiste nas seguintes etapas:

1. Crie um utilitário de restauro autónomo (ver a figura abaixo).
2. Ligue uma unidade a um computador que não tenha os componentes de encriptação do Kaspersky Endpoint Security instalados.
3. Execute o utilitário de restauro e diagnostique o disco rígido.
4. Aceda aos dados na unidade. Para tal, introduza as credenciais do agente de autenticação ou inicie o procedimento de recuperação (Pedido-Resposta).



Utilitário de Restauro FDERT

Criar um utilitário de restauro autónomo

Para criar o ficheiro executável da Ferramenta de Restauro:

1. Na janela principal da aplicação, clique no botão .
2. Na janela que abre, clique no botão **Restaurar dispositivo encriptado**.

   O Ferramenta de Restauro de dispositivo encriptado é iniciado.

3. Clique no botão **Criar Ferramenta de Restauro autónoma** na janela do Ferramenta de Restauro.

4. Guarde o utilitário de restauro autónomo na memória do computador.

Como resultado, o ficheiro executável do utilitário de restauro (fdert.exe) será guardado na pasta especificada. Copie o utilitário de restauro para um computador que não possua componentes de encriptação do Kaspersky Endpoint Security. Este procedimento impede que a unidade seja encriptada novamente.

Os dados necessários para restaurar o acesso a dispositivos encriptados ao utilizar a Ferramenta de Restauro estão na memória do computador do utilizador na forma desencriptada durante algum tempo. Para reduzir o risco de acesso não autorizado a esses dados, recomendamos que restaure o acesso aos dispositivos encriptados em computadores fiáveis.

Recuperar dados num disco rígido

Para restaurar o acesso um dispositivo encriptado utilizando o Ferramenta de Restauro:

1. Execute o ficheiro chamado fdert.exe, que é o ficheiro executável do utilitário de restauro. Este ficheiro é criado pelo Kaspersky Endpoint Security.

2. Na janela Utilitário de Restauro, selecione o dispositivo encriptado para o qual pretende restaurar o acesso.

3. Clique no botão **Verificar** para permitir que o utilitário defina as ações que devem ser executadas no dispositivo: se deve ser desbloqueado ou desencriptado.

   Se o computador tiver acesso à funcionalidade de encriptação do Kaspersky Endpoint Security, a Ferramenta de Restauro solicita que desbloqueie o dispositivo. Uma vez que o desbloqueio do dispositivo não o desencripta, o dispositivo fica diretamente acessível em consequência de estar desbloqueado. Se o computador não tiver acesso à funcionalidade de encriptação do Kaspersky Endpoint Security, a Ferramenta de Restauro solicita que desencripte o dispositivo.

4. Se quiser importar informações de diagnóstico, clique no botão **Guardar diagnóstico**.

   O utilitário guardará um arquivo com ficheiros contendo informações de diagnóstico.

5. Clique no botão **Corrigir MBR** se o diagnóstico do disco rígido do sistema encriptado tiver devolvido uma mensagem acerca de problemas relacionados com o registo de arranque principal (MBR) do dispositivo.

   A correção do registo de arranque principal do dispositivo pode acelerar o processo de recolha de informações necessárias para desbloquear ou desencriptar o dispositivo.

6. Clique no botão **Desbloquear** ou **Desencriptar**, dependendo dos resultados do diagnóstico.

7. Se quiser restaurar dados utilizando uma conta do Agente de Autenticação, selecione a opção **Utilizar definições da conta do Agente de Autenticação** e introduza as credenciais do Agente de Autenticação.

   Este método só é possível quando restaurar dados num disco rígido do sistema. Se o disco rígido do sistema foi corrompido e os dados da conta do Agente de Autenticação se tiverem perdido, deve obter uma chave de acesso do administrador da rede local empresarial para restaurar os dados num dispositivo encriptado.

8. Se quiser iniciar o procedimento de recuperação, faça o seguinte:

    a. selecione a opção **Indicar chave de acesso ao dispositivo manualmente**.

    b. Clique no botão **Receber chave de acesso** e guarde o ficheiro de pedido de acesso à solicitação na memória do computador (um ficheiro com a extensão FDERTC).

    c. Envie o ficheiro de acesso de pedido ao administrador da rede local empresarial.

    Não feche a janela **Receber chave de acesso ao dispositivo** enquanto não tiver recebido a chave de acesso. Quando esta janela for aberta novamente, não será capaz de aplicar a chave de acesso que foi criada anteriormente pelo administrador.

    d. Receba e guarde o ficheiro de acesso (um ficheiro com a extensão FDERTR) criado e enviado a si pelo administrador da LAN empresarial (consulte as instruções abaixo).

    e. Transfira o ficheiro de acesso na janela **Receber chave de acesso ao dispositivo**.

9. Se estiver a desencriptar um dispositivo, deve definir definições adicionais de desencriptação:

    - Especificar a área para desencriptar:
        - Se pretender desencriptar o dispositivo completo, selecione a opção **Desencriptar todo o dispositivo**.
        - Se quiser desencriptar uma porção dos dados num dispositivo, selecione a opção **Desencriptar áreas individuais do dispositivo** e especificar os limites da área de desencriptação.
    - Selecione o local de escrita dos dados desencriptados:
        - Se pretender que os dados no dispositivo original sejam reescritos com os dados desencriptados, desmarque a caixa de verificação **Desencriptar para ficheiro de imagem de disco**.
        - Se pretender guardar os dados desencriptados separadamente dos dados encriptados originais, selecione a caixa de verificação **Desencriptar para ficheiro de imagem de disco** e utilize o botão **Procurar** para especificar o caminho onde guardar o ficheiro VHD.

10. Clique em **OK**.

O processo de desbloqueio/desencriptação do dispositivo é iniciado.

Como criar um ficheiro de acesso a dados encriptados na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.

2. Na árvore da Consola de Administração, selecione a pasta **Advanced** → **Data encryption and protection** → **Encrypted drives**.

3. Na área de trabalho, selecione o dispositivo encriptado para o qual pretende criar um ficheiro-chave de acesso e, no menu de contexto do dispositivo, selecione **Obtenha acesso ao dispositivo em Kaspersky Endpoint Security**.

   Se não tiver a certeza para que computador foi gerado o ficheiro de pedido de acesso, na árvore da Consola de Administração, selecione a pasta **Advanced → Data encryption and protection** e na área de trabalho, clique em **Obtenha a chave de encriptação em Kaspersky Endpoint Security**.

4. Na janela apresentada, selecione o algoritmo de encriptação a utilizar: AES256 ou AES56.

   O algoritmo de encriptação de dados depende da biblioteca de encriptação AES incluída no pacote de distribuição: *Strong encryption (AES256)* ou *Lite encryption (AES56)*. A biblioteca de encriptação AES é instalada juntamente com a aplicação.

5. Clique **Procurar** para abrir uma janela; nesta janela, especifique o caminho para o ficheiro de pedido com a extensão fdertc que foi recebido do utilizador.

6. Clique em **Desbloquear**.

Verá informações acerca do pedido do utilizador. O Kaspersky Security Center gera um ficheiro-chave. Envie por email o ficheiro-chave de acesso a dados encriptados gerado para o utilizador. Ou guarde o ficheiro de acesso e utilize qualquer método disponível para transferir o ficheiro.

Como criar um ficheiro de acesso a dados encriptados na Consola da Web

1. Na janela principal da Consola Web, selecione **Operations → Data encryption and protection → Encrypted drives**.

2. Selecione a caixa de verificação ao lado do nome do computador no qual pretende recuperar dados.

3. Clique em **Grant access to the device in offline mode**.

   Isto inicia o Assistente para conceder acesso a um dispositivo.

4. Cumpra 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 encriptação a utilizar: AES256 ou AES56.

      O algoritmo de encriptação de dados depende da biblioteca de encriptação AES incluída no pacote de distribuição: *Strong encryption (AES256)* ou *Lite encryption (AES56)*. A biblioteca de encriptação AES é instalada juntamente com a aplicação.

   c. Selecione o ficheiro de pedido de acesso recebido do utilizador (um ficheiro com a extensão FDERTC).

   d. Selecione uma pasta onde guardar o ficheiro-chave de acesso aos dados encriptados (um ficheiro com a extensão FDERTR).

Como resultado, poderá obter a chave de acesso a dados encriptados, que terá de transferir para o utilizador.

Criar um disco de recuperação do sistema operativo

O disco de recuperação do sistema operativo pode ser útil quando não é possível aceder a uma unidade de disco rígido encriptada e o sistema operativo não inicia.

Pode carregar uma imagem do sistema operativo do Windows utilizando o disco de recuperação e recuperar o acesso à unidade de disco rígido encriptada utilizando o Ferramenta de Restauro incluindo na imagem do sistema operativo.

Para criar um disco de recuperação do sistema operativo:

1. Crie um ficheiro executável para a Ferramenta de Restauro de Dispositivo Encriptado.

2. Crie uma imagem personalizada o ambiente de pré-carregamento do Windows. Ao criar a imagem personalizada do ambiente de pré-carregamento do Windows, adicione o ficheiro executável do Ferramenta de Restauro à imagem.

3. Guarde a imagem personalizada do ambiente de pré-instalação do Windows num suporte de arranque como, por exemplo, um CD ou uma unidade amovível.

   Consulte os ficheiros de ajuda da Microsoft para obter instruções para criar uma imagem personalizada do ambiente de pré-carregamento do Windows (por exemplo, no recurso Microsoft TechNet).

Soluções Detection and Response

As soluções Kaspersky Detection and Response são sistemas de segurança para detetar ameaças avançadas e indicadores de ataque em diferentes níveis da infraestrutura de uma organização. As soluções Detection and Response fornecem informações sobre a ameaça detetada e permitem gerir ações de resposta a ameaças.

Assim, a solução Detection and Response faz o seguinte:

- Recebe informações sobre a operação de um computador, servidor ou outros dispositivos (telemetria).
- Analisa automaticamente informações para detetar ameaças.
- Gera detalhes de alerta como colunas da cadeia de ações de uma ameaça 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 suporta soluções Detection and Response utilizando um agente integrado. O agente integrado envia telemetria para servidores de soluções e realiza Ações de Resposta a Ameaças. O agente integrado suporta:

- 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

Pode utilizar o Kaspersky Endpoint Security com a solução Detection and Response em várias configurações, por exemplo, [EDR Optimum+MDR].

Licenciamento MDR e EDR Optimum

O Kaspersky Endpoint Security suporta a funcionalidade das soluções do Kaspersky Managed Detection and Response (MDR) e do Kaspersky Endpoint Detection and Response Optimum (EDR Optimum). Pode usar o Kaspersky Endpoint Security com estas soluções em várias configurações e construir um sistema de proteção personalizado que satisfaça os seus requisitos particulares. Para o fazer, tem de adquirir uma licença para cada uma das soluções. A licença pode abranger o direito de utilização de uma única solução (por exemplo, apenas o Suplemento do MDR) ou de várias soluções, Suplemento [EDR Optimum+MDR].

O MDR e o EDR Optimum suportam os seguintes métodos de licenciamento:

- A funcionalidade do MDR ou do EDR Optimum é abrangida pela licença Kaspersky Endpoint Security for Windows.

  A funcionalidade está imediatamente disponível após a ativação do Kaspersky Endpoint Security for Windows. Apenas precisa de adicionar uma chave.

- Licenças separadas para MDR ou EDR Optimum (MDR Add-on, EDR Optimum Add-on, [EDR Optimum+MDR] Add-on).

  A funcionalidade fica disponível depois de adicionar uma chave separada para o Suplemento MDR, Suplemento EDR Optimum ou Suplemento [EDR Optimum+MDR]. Como resultado, são adicionadas duas chaves no computador: uma chave para o Kaspersky Endpoint Security e uma chave para o MDR ou EDR Optimum. A chave do Kaspersky Endpoint Security tem de ser a primeira a ser adicionada.

O Kaspersky Endpoint Security permite adicionar apenas uma *chave ativa* para o licenciamento MDR e EDR Optimum. Por conseguinte, se precisar de ativar estas duas soluções, tem de adicionar uma chave de [EDR Optimum+MDR] Add-on, em vez de uma chave separada para cada solução. Poderá também adicionar uma *chave de reserva*.

Se usou um ficheiro BLOB ao implementar o MDR, não precisa de uma chave separada para ativar o MDR. O ficheiro BLOB já contém informações de licença.

Licenciamento inicial de soluções

Ao implementar pela primeira vez o MDR e o EDR Optimum, as soluções são ativadas da mesma forma que a aplicação Kaspersky Endpoint Security. Pode adicionar uma chave através da tarefa *Adicionar chave* ou usar a funcionalidade de distribuição automática de chaves. A chave da licença é adicionada à aplicação como uma segunda chave ativa ou como uma chave de reserva, se selecionar a caixa de verificação relevante.

Mudar de uma licença para outra

Se a sua organização já tiver uma destas soluções implementadas e a chave correspondente tiver sido adicionada à aplicação, existem algumas considerações especiais envolvidas no licenciamento da nova configuração. Ao mudar para uma licença diferente, a aplicação não adiciona a nova chave à aplicação, mas substitui a chave atual pela nova chave. Isto deve-se à restrição que permite à aplicação adicionar apenas uma chave para ativar o MDR e o EDR Optimum.

Por exemplo, vamos supor que a sua organização tem a solução [EDR Optimum+MDR] implementada e que decidiu mudar para a configuração do Suplemento MDR. Para mudar para a nova configuração, tem de substituir a chave do [EDR Optimum+MDR] Add-on pela chave do Suplemento MDR.

Já não está disponível uma licença separada para o EDR Optimum e o MDR (Suplemento [EDR Optimum+MDR]). Se pretender utilizar estas duas soluções, tem de ativar o MDR utilizando um ficheiro BLOB e o EDR Optimum com uma chave de licença.

Com a funcionalidade de distribuição automática de chaves, a aplicação rejeita chaves de licença que abrangem o mesmo número de soluções. Ou seja, se tiver uma chave do Suplemento EDR Optimum adicionada, não pode substituir esta chave por uma chave do Suplemento MDR. No entanto, pode substituir a chave do Suplemento EDR Optimum por uma chave do Suplemento [EDR Optimum+MDR]. A aplicação também rejeita chaves se tentar substituir uma chave do Suplemento MDR por uma chave do Suplemento EDR. Para substituir uma chave, pode executar a tarefa *Adicionar chave*. A tarefa *Adicionar chave* permite substituir as chaves de licença por qualquer número de soluções.

Se tiver uma chave de reserva do [EDR Optimum+MDR] Add-on adicionada, para adicionar corretamente uma chave ativa para o Suplemento EDR Optimum ou o Suplemento MDR, primeiro tem de substituir a chave de reserva por uma chave do Suplemento EDR Optimum ou do Suplemento MDR ou, em alternativa, remover a chave de reserva e, em seguida, substituir a chave ativa.

Compatibilidade com soluções da EDR de terceiros

Pode utilizar o Kaspersky Endpoint Security para proteger estações de trabalho e servidores em conjunto com soluções EDR de outros fornecedores. Para eliminar falsos positivos, recomendamos que adicione os ficheiros executáveis do Kaspersky Endpoint Security e do Network Agent à zona fiável da sua solução EDR de terceiros.

Zona fiável 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`

Ficheiros 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 suporta a interação entre a aplicação e outras soluções da Kaspersky para detetar ameaças avançadas (por exemplo Kaspersky Sandbox). As soluções Kaspersky são compatíveis com versões específicas do Kaspersky Endpoint Agent.

Para utilizar o Kaspersky Endpoint Agent como parte das soluções da Kaspersky, tem de ativar essas soluções com uma chave de licença correspondente.

Para obter informações completas sobre o Kaspersky Endpoint Agent incluído na solução de software que está a utilizar e sobre a solução autónoma, 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. Pode selecionar o Kaspersky Endpoint Agent ao instalar o Kaspersky Endpoint Security for Windows. Como resultado, serão instaladas duas aplicações no seu computador: KEA e KES. No Kaspersky Endpoint Security 11.9.0, o pacote de distribuição do Kaspersky Endpoint Agent já não faz parte do kit de distribuição do Kaspersky Endpoint Security.

Correspondência das 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 a trocar todo o Detection and Response para trabalhar com o agente integrado do Kaspersky Endpoint Security, em vez do Kaspersky Endpoint Agent. A Kaspersky está gradualmente a suportar estas soluções e a eliminar gradualmente o Kaspersky Endpoint Agent (consulte a tabela abaixo). A partir da versão 12.1, a aplicação suporta todas as soluções de Detection and Response. Além disso, a partir da versão 12.1, a aplicação já não é compatível com o Kaspersky Endpoint Agent e já não é possível instalar as duas aplicações lado a lado 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 Endpoint Detection and Response)	Kaspersky Anti Targeted Attack Platform (componente 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**

Migrar a configuração [KES+KEA] para a configuração [KES+agente incorporado]

O Kaspersky Endpoint Security inclui agentes integrados para trabalhar com as soluções Detection and Response. Já não precisa de uma aplicação Kaspersky Endpoint Agent em separado para trabalhar com estas soluções. Quando implementa o Kaspersky Endpoint Security em computadores com o Kaspersky Endpoint Agent instalado, as soluções Detection and Response irão continuar a funcionar 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. Pode selecionar o Kaspersky Endpoint Agent ao instalar o Kaspersky Endpoint Security for Windows. Como resultado, serão instaladas duas aplicações no seu computador: KEA e KES. No Kaspersky Endpoint Security 11.9.0, o pacote de distribuição do Kaspersky Endpoint Agent já não faz parte do kit de distribuição do Kaspersky Endpoint Security.

A migração da configuração [KES+KEA] para [KES+agente incorporado] envolve os passos seguintes:

1. **Atualização do Kaspersky Security Center**

   Atualize todos os componentes do Kaspersky Security Center para a versão 13.2 ou superior, incluindo o Agente de Rede nos computadores dos utilizadores e na Consola Web.

2. **Atualização do plug-in da Web do Kaspersky Endpoint Security**

Na Consola Web do Kaspersky Security Center, atualize o plug-in da Web do Kaspersky Endpoint Security para a versão 11.7.0 ou superior. Para gerir os componentes EDR Optimum e Kaspersky Sandbox, tem de utilizar a Consola Web.

Para usar a Kaspersky Anti Targeted Attack Platform (EDR), irá precisar de um plug-in da Web para o Kaspersky Endpoint Security versão 12.1 ou posterior.

Para usar a Kaspersky Anti Targeted Attack Platform (NDR), irá precisar de um plug-in da Web para o Kaspersky Endpoint Security versão 12.7 ou posterior.

3. **Migração da política e das tarefas**

   Utilize a Política do Kaspersky Endpoint Agent e o Assistente de Migração de Políticas e Tarefas para migrar as definições do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows.

   Esta ação cria uma nova política do Kaspersky Endpoint Security. A nova política tem o estado *Inactive*. Para aplicar a política, abra as propriedades da política, aceite a Declaração da Kaspersky Security Network e defina o estado para *Active*.

4. **Funcionalidade do licenciamento**

   Se utilizar uma licença comum do Kaspersky Endpoint Detection and Response Optimum ou do Kaspersky Optimum Security para ativar o Kaspersky Endpoint Security for Windows e o Kaspersky Endpoint Agent, a funcionalidade EDR Optimum será ativada automaticamente após a atualização da aplicação para a versão 11.7.0. Não precisa de fazer mais nada.

   Se utilizar uma licença autónoma do Suplemento do Kaspersky Endpoint Detection and Response Optimum para ativar a funcionalidade EDR Optimum, deve certificar-se de que a chave do Suplemento EDR Optimum é adicionada ao repositório do Kaspersky Security Center e de que a funcionalidade de distribuição automática da chave de licença está ativada. Depois de atualizar a aplicação para a versão 11.7.0, a funcionalidade EDR Optimum é ativada automaticamente.

   Se utilizar 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, tem de substituir a chave do Kaspersky Endpoint Security for Windows pela chave comum do Kaspersky Endpoint Detection and Response Optimum ou do Kaspersky Optimum Security. Pode substituir a chave através da tarefa *Add key*.

   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.

   Apenas a licença da Kaspersky Anti Targeted Attack Platform pode ser usada para ativar o Kaspersky Endpoint Security como parte da solução da Kaspersky Anti Targeted Attack Platform. Depois de atualizar a aplicação para a versão 12.1, a funcionalidade EDR (KATA) é ativada automaticamente. Não precisa de fazer mais nada.

5. **Atualização da aplicação Kaspersky Endpoint Security**

   Para atualizar a aplicação e migrar a funcionalidade EDR Optimum e Kaspersky Sandbox, é recomendada uma tarefa de instalação remota.

   Para atualizar a aplicação usando uma tarefa de instalação remota, tem de editar as seguintes definições:

   - Selecione os componentes para as soluções Detection and Response nas definições do pacote de instalação.
   - Exclua o componente Kaspersky Endpoint Agent nas definições do pacote de instalação (para o Kaspersky Endpoint Security for Windows versões 11.2.0 – 11.8.0).
   - Se a Proteção por password estiver ativada para restringir o acesso ao Kaspersky Endpoint Agent, introduza a password de desinstalação da aplicação nas definições da tarefa *Install application remotely*. Pode inserir a password de desinstalação a partir do Kaspersky Security Center Linux 15.1.

Também pode atualizar a aplicação utilizando os seguintes métodos:

- Utilizando o serviço de atualização da Kaspersky (Seamless Update - SMU).
- Localmente, usando o Assistente de Configuração.

O Kaspersky Endpoint Security suporta a seleção automática de componentes ao atualizar a aplicação num computador com a aplicação Kaspersky Endpoint Agent instalada. A seleção automática dos componentes depende das permissões da conta do utilizador que está a atualizar a aplicação.

Se estiver a atualizar o Kaspersky Endpoint Security utilizando o ficheiro EXE ou MSI na conta do sistema (SYSTEM), o Kaspersky Endpoint Security ganha acesso a licenças atuais de soluções da Kaspersky. Portanto, se o computador tiver, por exemplo, o Kaspersky Endpoint Agent instalado e a solução EDR Optimum ativada, o instalador Kaspersky Endpoint Security configura automaticamente o conjunto de componentes e seleciona o componente EDR Optimum. Isto faz com que o Kaspersky Endpoint Security troque para a utilização do agente incorporado e remove o Kaspersky Endpoint Agent. A execução do instalador MSI na conta do sistema (SYSTEM) é normalmente realizada ao atualizra através do serviço de atualização da Kaspersky (SMU) ou ao implementar um pacote de instalação através do Kaspersky Security Center.

Se estiver a atualizar o Kaspersky Endpoint Security utilizando um ficheiro MSI numa conta de utilizador sem privilégios, o Kaspersky Endpoint Security não tem acesso às licenças atuais das soluções da Kaspersky. Neste caso, o Kaspersky Endpoint Security seleciona automaticamente os componentes com base na configuração do Kaspersky Endpoint Agent. Depois disso, o Kaspersky Endpoint Security troca para a utilização do agente incorporado e remove o Kaspersky Endpoint Agent.

6. **Reinício do computador**

   Reinicie o seu computador para terminar a atualização da aplicação com o agente integrado. Ao atualizar a aplicação, o instalador remove o Kaspersky Endpoint Agent antes de o computador ser reiniciado. Depois de o computador ser reiniciado, o instalador adiciona o agente integrado. Isto significa que o Kaspersky Endpoint Security não executa as funções do EDR e do Kaspersky Sandbox até o computador ser reiniciado.

7. **Verificação do estado de funcionamento do Kaspersky Endpoint Detection and Response Optimum e do Kaspersky Sandbox**

   Se, após a atualização, o computador tiver o estado *Critical* na consola do Kaspersky Security Center:

   - Certifique-se de que o computador tem o Agente de Rede versão 13.2 ou superior instalado.
   - Verifique o estado de funcionamento do agente integrado ao consultar o *Report on status of application components*. Se um componente tiver o estado *Not installed*, instale o componente com a tarefa *Change application components*.
   - Certifique-se de que aceita a Declaração da Kaspersky Security Network na nova política do Kaspersky Endpoint Security for Windows.
   - Certifique-se de que a funcionalidade EDR Optimum é ativada usando o *Report on status of application components*. Se um componente tiver o estado *Não abrangido pela licença*, certifique-se de que a funcionalidade de distribuição automática da chave de licença do EDR Optimum está ativada.

Migração de Política e Tarefa para o Kaspersky Endpoint Agent

O Kaspersky Endpoint Security for Windows inclui um assistente para migrar do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security. Pode migrar definições de tarefas e políticas para as seguintes soluções:

- Kaspersky Sandbox
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)
- Kaspersky Anti Targeted Attack Platform

Um assistente para migrar do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security funciona apenas na Consola Web e na Cloud Console. Na Consola de Administração (MMC), apenas é possível migrar as definições para a solução Kaspersky Anti Targeted Attack Platform (EDR) utilizando o Kaspersky Security Center Policy e o assistente de migração de tarefas.

Recomenda-se começar a migração do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security num único computador, de seguida num grupo de computadores e, por último, concluir a migração em todos os computadores da organização.

Para migrar as definições de tarefas e políticas do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security,

na janela principal da Consola Web, selecione **Operations → Migration from Kaspersky Endpoint Agent**.

Esta ação executa o assistente de migração de políticas e tarefas. Siga as instruções do Assistente.

Passo 1. Migração de políticas

O assistente de migração cria uma nova política que combina as definições das políticas do Kaspersky Endpoint Security e do Kaspersky Endpoint Agent. Na lista de políticas, selecione as políticas do Kaspersky Endpoint Agent cujas definições pretende combinar com a política do Kaspersky Endpoint Security. Clique na política do Kaspersky Endpoint Agent para selecionar a política do Kaspersky Endpoint Security com a qual pretende combinar definições. Certifique-se de que seleciona as políticas corretas e avance para o passo seguinte.

Passo 2. Migração de tarefas

O Assistente de Migração cria novas tarefas para o Kaspersky Endpoint Security. Na lista de tarefas, selecione as tarefas do Kaspersky Endpoint Agent que pretende criar para a política do Kaspersky Endpoint Security. O Assistente suporta tarefas para o Kaspersky Endpoint Detection and Response e o Kaspersky Sandbox. Avance para o passo seguinte.

Passo 3. Conclusão do assistente

Conclua o assistente. Como resultado, o assistente faz o seguinte:

- Cria uma nova política do Kaspersky Endpoint Security.

  A política combina as definições do Kaspersky Endpoint Security e Kaspersky Endpoint Agent A política é denominada *<Kaspersky Endpoint Security policy name> e <Kaspersky Endpoint Agent policy name>*. A nova política tem o estado *Inactive*. Para continuar, altere os estatutos das políticas do Kaspersky Endpoint Agent e Kaspersky Endpoint Security para *Inactive* e ative a nova política combinada.

  Depois de migrar do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows, certifique-se de que a nova política tem a funcionalidade para transferência de dados para o Servidor de Administração (dados de ficheiros de quarentena e dados de cadeia de desenvolvimento de ameaças) configurada. Os valores dos parâmetros de transferência de dados não são migrados a partir de uma política do Kaspersky Endpoint Agent.

  Ao migrar do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security para a solução do Kaspersky Anti Targeted Attack Platform (EDR), pode encontrar erros ao ligar o computador aos servidores do Central Node. O motivo é que o assistente de migração na Consola Web salta as seguintes definições de política e não as migra:

  - Proibição de modificação de definições **Connection to KATA servers** ("cadeado").

    Por defeito, as definições podem ser modificadas (o "cadeado" está aberto). Por conseguinte, as definições não são aplicadas no computador. Tem de proibir a modificação das definições e fechar o "cadeado".

  - Cripto-contentor.

    Se estiver a utilizar autenticação bidirecional para ligar aos servidores do Central Node, tem de voltar a adicionar o cripto-contentor. O assistente de migração migra corretamente o certificado TLS do servidor.

  O Assistente de Política e Migração de Tarefas na Consola de Administração (MMC) migra todas as definições para a solução do Kaspersky Anti Targeted Attack Platform (EDR).

- Cria novas tarefas do Kaspersky Endpoint Security.

  As novas tarefas são cópias das tarefas do Kaspersky Endpoint Agent para o Kaspersky Endpoint Detection and Response e o Kaspersky Sandbox. Simultaneamente, o Assistente deixa as tarefas do Kaspersky Endpoint Agent inalteradas.

Como migrar as definições de tarefas e políticas do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security na Consola de Administração (MMC) (apenas para KATA (EDR))

1. Na Consola de administração, selecione o Servidor de Administração e clique com o botão direito do rato para abrir o menu de contexto.

2. Selecione **All tasks → Policies and tasks batch conversion wizard**.

O Assistente de Conversão de Políticas e Tarefas em Lote vai iniciar. Siga as instruções do Assistente.

Passo 1. Selecionar a aplicação para o qual necessita de converter políticas e tarefas

Neste passo, tem de selecionar o Kaspersky Endpoint Security for Windows. Avance para o passo seguinte.

Passo 2. Conversão de políticas

O Assistente de Migração cria uma nova política do Kaspersky Endpoint Security para a qual as definições da política do Kaspersky Endpoint Agent serão migradas. Na lista de políticas, selecione as políticas do Kaspersky Endpoint Agent cujas definições pretende transferir para a política do Kaspersky Endpoint Security. Avance para o passo seguinte.

O Assistente de Migração irá começar a converter as políticas. Durante a conversão da política, o Assistente de Migração solicita que aceite a Declaração da Kaspersky Security Network. As novas políticas serão nomeadas *<Nome da política> (convertida)*.

Passo 3. Conversão de tarefas

Ignorar este passo. O Assistente suporta tarefas apenas para o Kaspersky Endpoint Detection and Response Optimum e o Kaspersky Sandbox. A gestão destes componentes está disponível apenas na Consola Web. Avance para o passo seguinte.

Passo 4. Conclusão do assistente

Conclua o assistente. Como resultado do assistente, será criada uma nova política do Kaspersky Endpoint Security.

Endpoint Detection and Response Agent (EDR Agent)

A partir do Kaspersky Endpoint Security 12.3 for Windows, a aplicação inclui a configuração do Endpoint Detection and Response Agent (EDR Agent). O *Endpoint Detection and Response Agent* é uma aplicação instalada em estações de trabalho e servidores individuais na infraestrutura de TI da organização para dar suporte as 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 suporta a integração com a solução Kaspersky Endpoint Detection and Response Expert (cloud).

O EDR Agent monitoriza continuamente os processos em execução nesses computadores, ligações de rede abertas e os ficheiro que são modificados. Os componentes de proteção e controlo da aplicação não estão disponíveis para o EDR Agent.

O EDR Agent é compatível com aplicações EPP de terceiros. Isso permite que use ferramentas de segurança de infraestrutura de terceiros em conjunto com o Detection and Response da Kaspersky.

Para implementar o EDR Agent, o computador deve ter o Agente de Rede instalado e o computador deve ser adicionado à consola do Kaspersky Security Center. Para ativar a interação do EDR Agent com o Kaspersky Security Center, deve instalar o plug-in de gestão do Kaspersky Endpoint Security for Windows. Pode especificar as definições do EDR Agent utilizando uma política de grupo. Para integrar o EDR Agent, deve configurar a integração nas secções de política apropriadas.

As seguintes aplicações Kaspersky têm de ser instaladas na infraestrutura para suportar as soluções Kaspersky Detection and Response:

	• Agente de Rede • EDR Agent
Endpoint	
	Plug-in de gestão do Kaspersky Endpoint Security for Windows
Kaspersky Security Center	
	
Soluções Detection and Response: MDR, KATA (EDR), KATA (NDR), KUMA, EDR Expert (on-premises)	

Instalar o EDR Agent

O Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent (EDR Agent) para as soluções Kaspersky Detection and Response são instaladas da mesma forma.

O EDR Agent pode ser instalado no computador de uma das seguintes formas:

- Remotamente, utilizando o Kaspersky Security Center.
- Localmente, utilizando o Assistente de Instalação.
- Localmente na linha de comando (apenas para KATA (EDR) e EDR Expert (on-premises)).

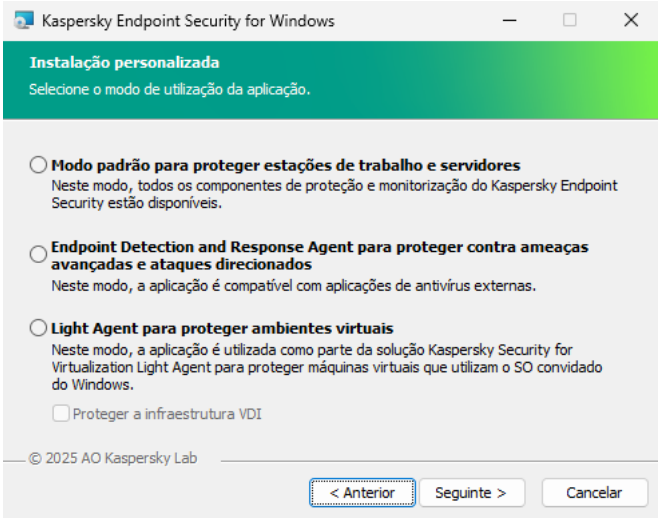
Para instalar o EDR Agent, deve selecionar a configuração apropriada em definições do pacote de instalação ou no Assistente de Instalação.

Como instalar o EDR Agent utilizando o Assistente de Instalação

1. Copie a pasta do kit de distribuição para o computador do utilizador.
2. Execute o ficheiro setup_kes.exe.

O Assistente de configuração é iniciado.

Configuração do Kaspersky Endpoint Security



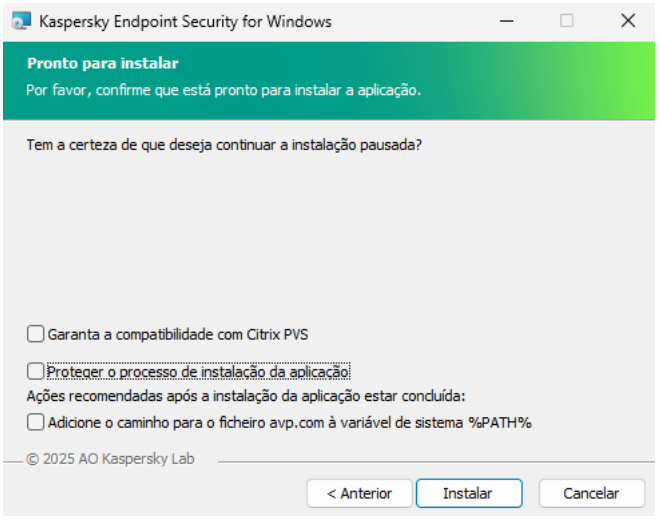
Escolher a configuração da aplicação

Selecione a configuração **Endpoint Detection and Response Agent**. Nesta configuração, só é possível instalar os componentes que fornecem suporte para soluções Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) e KUMA. Esta configuração será necessária se uma Endpoint Protection Platform (EPP) de terceiros for implementada na sua organização em conjunto com uma solução de Detection and Response da Kaspersky. Isso torna o Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent compatível com aplicações EPP de terceiros.

Componentes do Kaspersky Endpoint Security

Selecione os componentes que pretende instalar. Pode alterar os componentes da aplicação disponíveis após instalar a aplicação. Para o fazer, deve executar o Assistente de Instalação novamente e selecionar a alteração dos componentes disponíveis.

Definições avançadas



Definições avançadas de instalação da aplicação

Proteger o processo de instalação da aplicação. A proteção de instalação inclui a proteção contra a substituição do pacote de distribuição com aplicações maliciosas, bloqueando o acesso à pasta de instalação do Kaspersky Endpoint Security, e bloqueando o acesso à secção do registo do sistema contendo as chaves da aplicação. Contudo, se não for possível instalar a aplicação (por exemplo, ao executar uma instalação remota com a ajuda do Windows Remote Desktop), recomendamos que desative a proteção do processo de instalação.

Garanta a compatibilidade com Citrix PVS. Pode ativar o suporte dos Citrix Provisioning Services para instalar o Kaspersky Endpoint Security numa máquina virtual.

Adicione o caminho para o ficheiro avp.com à variável de sistema %PATH%. Pode adicionar o caminho de instalação à variável %PATH% para utilização conveniente da interface da linha de comando.

Como instalar o EDR Agent na linha de comando (apenas para KATA (EDR) e EDR Expert (on-premises))

1. Execute o interpretador de linha de comando (cmd.exe) como administrador.
2. Vá para 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, a aplicação EDR Agent para integração com o Kaspersky Anti Targeted Attack Platform (EDR) o Kaspersky Endpoint Detection and Response Expert (on-premises) é instalada no computador. Pode confirmar que a aplicação está instalada e verificar as definições da aplicação ao emitir o comando `status`.

Como instalar o EDR Agent utilizando a Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione a pasta **Remote installation** → **Advanced** → **Installation packages**.

   Isto abre uma lista de pacotes de instalação que foram transferidos para o Kaspersky Security Center.
3. Abra as propriedades do pacote de instalação.

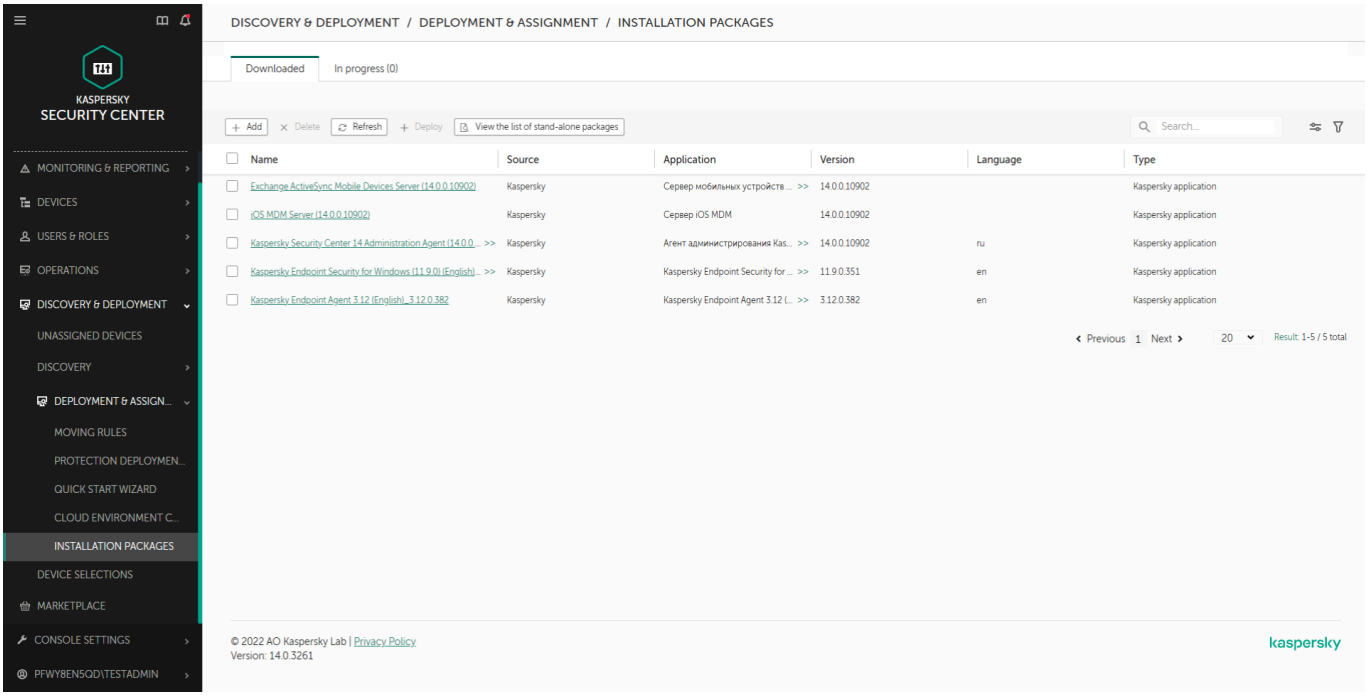
   Se necessário, crie um novo pacote de instalação.
4. Aceda à secção **Protection components**.
5. Selecione a configuração **Endpoint Detection and Response Agent para proteger contra ameaças avançadas e ataques direcionados**. Nesta configuração, só é possível instalar os componentes que fornecem suporte para soluções Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) e KUMA. Esta configuração será necessária se uma Endpoint Protection Platform (EPP) de terceiros for implementada na sua organização em conjunto com uma solução de Detection and Response da Kaspersky. Isso torna o Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent compatível com aplicações EPP de terceiros.
6. Selecione os componentes que pretende instalar.

   Pode alterar os componentes da aplicação disponíveis após instalar a aplicação.
7. Guarde as suas alterações.
8. Criar uma tarefa de instalação remota. Nas propriedades da tarefa, selecione o pacote de instalação que criou.

Como instalar o EDR Agent utilizando a Consola Web

1. Na janela principal da Consola Web, selecione **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.

   Isto abre uma lista de pacotes de instalação que foram transferidos para o Kaspersky Security Center.



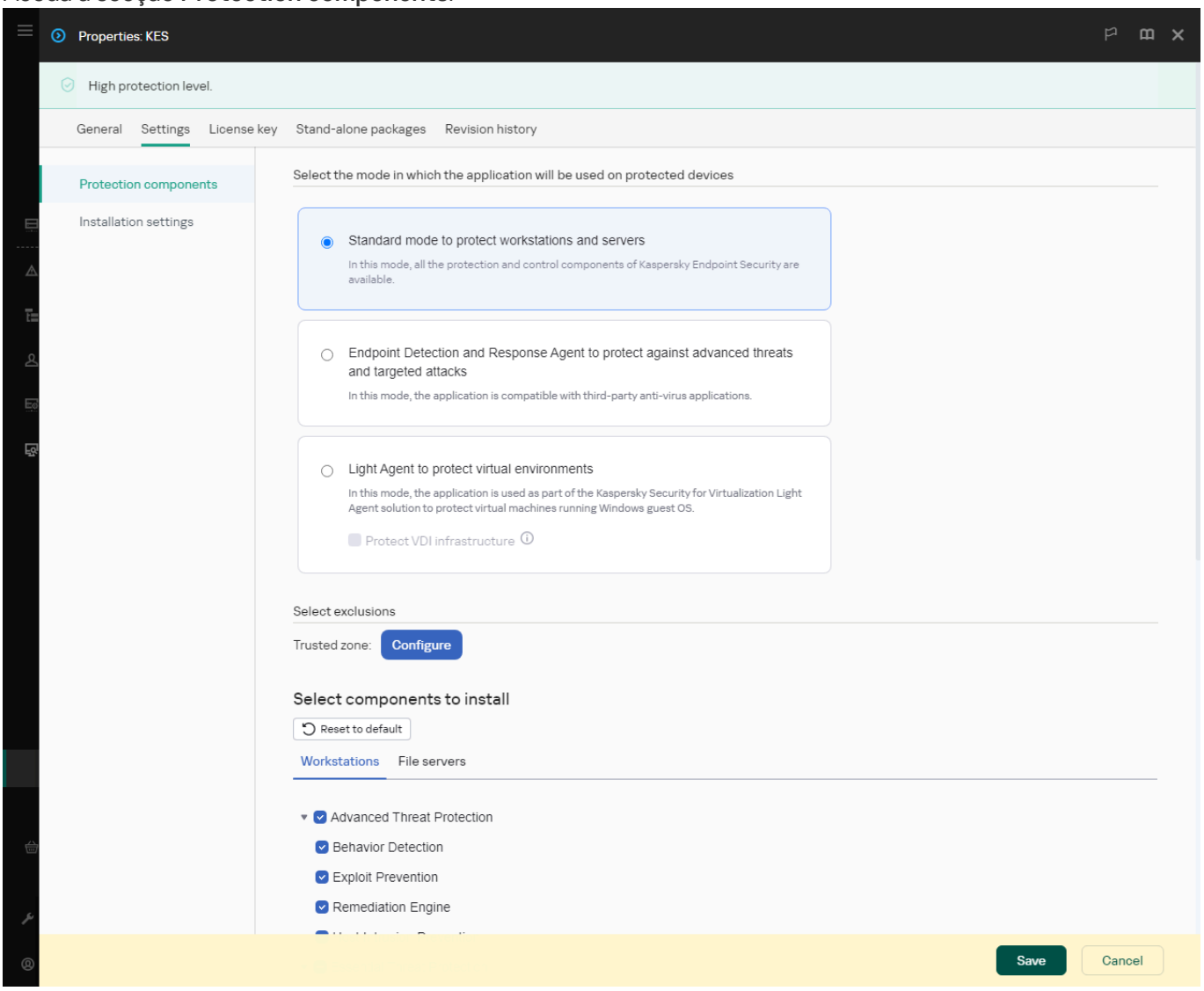
Lista de pacotes de instalação

2. Abra as propriedades do pacote de instalação.

   Se necessário, crie um novo pacote de instalação.

3. Selecione o separador **Settings**.

4. Aceda à secção **Protection components**.



Componentes incluídos no pacote de instalação

5. Selecione a configuração **Endpoint Detection and Response Agent**. Nesta configuração, só é possível instalar os componentes que fornecem suporte para soluções Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) e KUMA. Esta configuração será necessária se uma Endpoint Protection Platform (EPP) de terceiros for implementada na sua organização em conjunto com uma solução de Detection and Response da Kaspersky. Isso torna o Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent compatível com aplicações EPP de terceiros.

6. Selecione os componentes que pretende instalar.

   Pode alterar os componentes da aplicação disponíveis após instalar a aplicação.

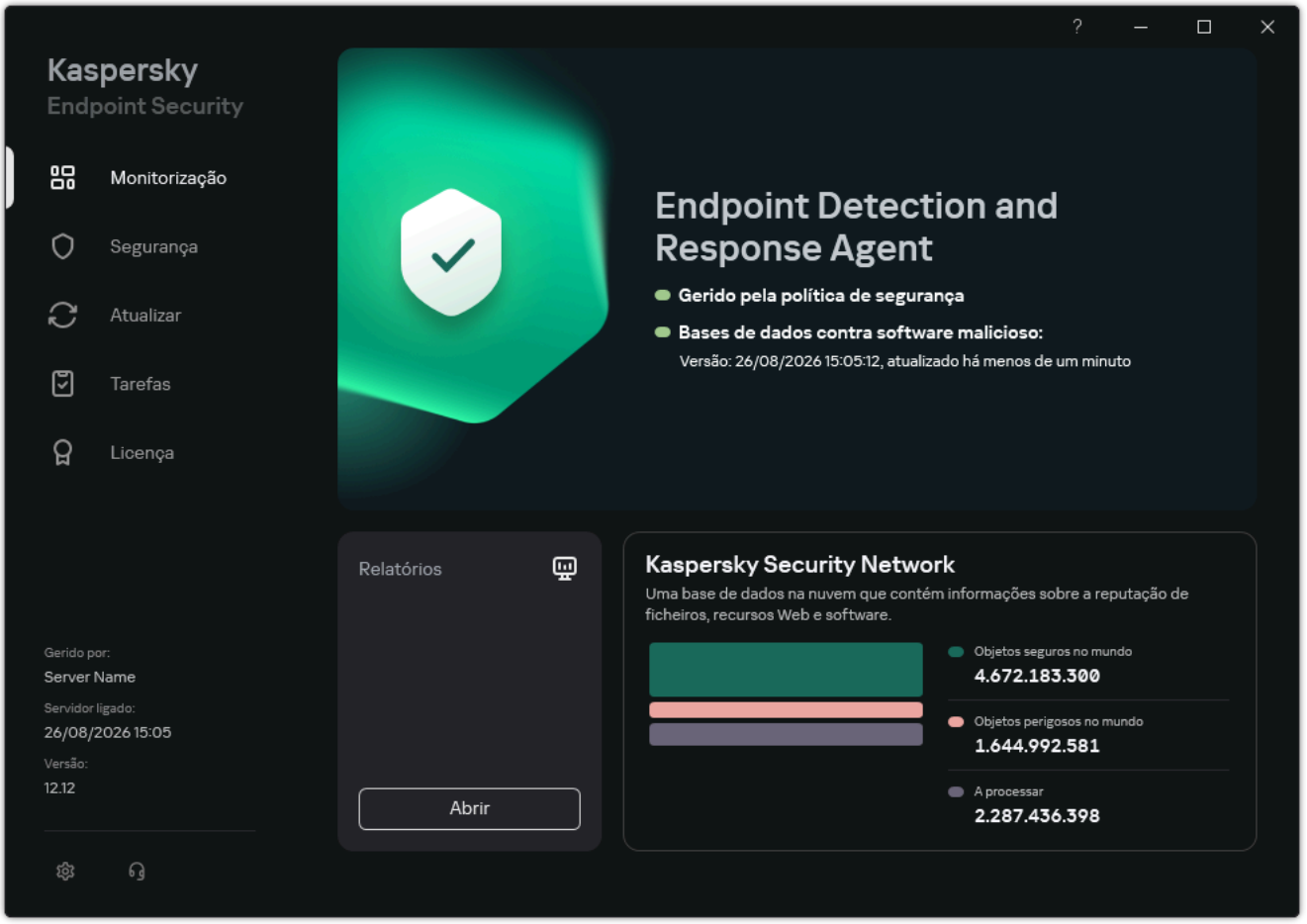
7. Guarde as suas alterações.

8. Criar uma tarefa de instalação remota. Nas propriedades da tarefa, selecione o pacote de instalação que criou.

Como resultado, o EDR Agent será instalado no computador do utilizador. Pode usar a interface da aplicação e será apresentado um ícone da aplicação na área de notificação .

No Kaspersky Security Center, o computador com a aplicação instalada na configuração do EDR Agent tem o estado *Critical* – . O computador tem este estado porque o componente Proteção contra ameaças de ficheiros está em falta. Não é necessário efetuar nenhuma ação.

Se não conseguiu instalar o EDR Agent num computador com uma aplicação EPP de terceiros porque o instalador encontrou software incompatível no computador, pode ignorar a verificação de software incompatível.



Janela principal do EDR Agent

Agora deve configurar a integração com a solução Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack (EDR) ou Kaspersky Anti Targeted Attack (NDR). Pode também especificar definições avançadas da aplicação e, por exemplo, criar uma zona fiável ou ocultar a interface da aplicação. Estão disponíveis as definições nas seguintes secções:

- Kaspersky Security Network
- Definições da aplicação
- Definições de Rede
- Exclusões
- Relatórios

- Interface
- Gerir definições

Integrar o EDR Agent com MDR

O EDR Agent é instalado em estações de trabalho e servidores na infraestrutura de TI da organização. O EDR Agent processa dados e os envia-os através da Kaspersky Security Network para o Kaspersky Managed Detection and Response.

Para o Kaspersky Managed Detection and Response funcionar com o Administration Server através do Consola Web do Kaspersky Security Center, deve estabelecer uma nova ligação segura, uma *ligação de fundo*. O Kaspersky Managed Detection and Response solicita que estabeleça uma ligação de fundo ao implementar a solução. Certifique-se de que a ligação de fundo é estabelecida.

Estabelecer uma ligação de fundo na Consola Web

1. Na janela principal da Consola Web, selecione **Settings** → **Integration**.
2. Aceda à secção **Integration**.
3. Ative o botão de alternar **Background connection for integration Enabled**.
4. Guarde as suas alterações.

A integração com o Kaspersky Managed Detection and Response consiste nos seguintes passos:

1. **Instalar o componente Managed Detection and Response**

   Pode selecionar o componente MDR durante a instalação ou atualização, bem como através da tarefa *Alterar componentes da aplicação*.

   > Para instalar o componente Managed Detection and Response sem reiniciar o computador utilizando a tarefa *Alterar componentes da aplicação*, precisa de desativar a opção **Verificar a existência de aplicações de terceiros incompatíveis** nas definições da tarefa.

2. **Configurar o Kaspersky Private Security Network**

   > Ignore este passo se estiver a utilizar o Kaspersky Security Center Cloud Console. O Kaspersky Security Center Cloud Console configura automaticamente o Kaspersky Private Security Network ao instalar o plug-in MDR.

   Kaspersky Private Security Network (KPSN) é uma solução que permite que utilizadores de computadores que alojam o Kaspersky Endpoint Security ou outras aplicações da Kaspersky tenham acesso às bases de dados de reputação do Kaspersky Security Network e a outros dados estatísticos sem enviar dados para o KSN a partir de seus próprios computadores.

   Carregue o ficheiro de configuração do Kaspersky Security Network nas propriedades do Servidor de administração. O ficheiro de configuração do Kaspersky Security Network está localizado no arquivo ZIP do ficheiro de configuração do MDR. Pode obter o arquivo ZIP na Consola do Kaspersky Managed Detection and Response. Para obter mais informações sobre a configuração da Kaspersky Private Security Network, consulte a Ajuda do Kaspersky Security Center. Pode também carregar um ficheiro de configuração do Kaspersky Security Network para o computador a partir da command line (consulte as instruções abaixo).

Como configurar o Kaspersky Private Security Network a partir da linha de comandos

1. Execute o interpretador de linha de comando (cmd.exe) como administrador.
2. Vá para a pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.
3. Execute o seguinte comando:

   ```
   avp.com KSN /private <file name>
   ```

   quando `<file name>` é o nome do ficheiro de configuração que contém as definições do Kaspersky Private Security Network (formato de ficheiro PKCS7 ou PEM).

   Exemplo:
   `avp.com KSN /private C:\kpsn_config.pkcs7`

Deste modo, o Kaspersky Endpoint Security utilizará o Kaspersky Private Security Network para determinar a reputação dos ficheiros, das aplicações e dos sites. A secção **Kaspersky Security Network** das definições de política irá exibir o seguinte estado operacional: *Infraestrutura:* Kaspersky Private Security Network.

Deve ativar o modo KSN alargado para que a Managed Detection and Response funcione.

3 Ativar o Kaspersky Managed Detection and Response

A partir do Kaspersky Endpoint Security for Windows 12.10, para ativar a funcionalidade Managed Detection and Response, como alternativa a um código de ativação, também pode utilizar um ficheiro-chave.

Comprar uma licença separada para o MDR (Suplemento do Kaspersky Managed Detection and Response).

A funcionalidade estará disponível após adicionar uma chave individual para o Suplemento do Kaspersky Managed Detection and Response. A licença para a funcionalidade Managed Detection and Response autónoma é a mesma que a licença do Kaspersky Endpoint Security.

Certifique-se de que a funcionalidade MDR é incluída na licença e está a funcionar na interface local da aplicação.

4 Ativação do componente Managed Detection and Response

Carregue o ficheiro de configuração BLOB na política do Kaspersky Endpoint Security (consulte as instruções abaixo). O ficheiro BLOB contém a ID do cliente e informações sobre a licença do Kaspersky Managed Detection and Response. O ficheiro BLOB está localizado dentro do arquivo ZIP do ficheiro de configuração do MDR. Pode obter o arquivo ZIP na Consola do Kaspersky Managed Detection and Response. Para obter mais informações sobre ficheiros BLOB, consulte a Ajuda do Kaspersky Managed Detection and Response.

A partir do Kaspersky Endpoint Security 12.6 for Windows, adicionar um ficheiro BLOB é opcional para o Kaspersky Managed Detection and Response sem inquilinos se tiver uma licença atual.

Como ativar o componente Managed Detection and Response na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**.
4. Selecione a caixa de verificação **Managed Detection and Response (Industrial CyberSecurity)**.

5. No bloco **Definições**, clique em **Carregar** e selecione o ficheiro BLOB recebido na Consola do Kaspersky Managed Detection and Response. O ficheiro possui a extensão P7.

   Por defeito, o utilizador tem permissão para gerir as definições da aplicação (o "cadeado" está aberto). Para aplicar a política em computadores, feche os cadeados .

6. Guarde as suas alterações.

Como ativar o componente Managed Detection and Response na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration** → **Managed Detection and Response**.
5. Ative o botão de alternar **Managed Detection and Response ENABLED**.
6. Clique em **Upload** e selecione o ficheiro BLOB que foi obtido na Consola do Kaspersky Managed Detection and Response. O ficheiro possui a extensão P7.

   Por defeito, o utilizador tem permissão para gerir as definições da política (o "cadeado" está aberto). Para aplicar a política em computadores, feche os cadeados .

7. Guarde as suas alterações.

Como ativar o componente Managed Detection and Response a partir da command line

1. Execute o interpretador de linha de comando (cmd.exe) como administrador.
2. Vá para a pasta onde o ficheiro 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 password deve estar ativada. O utilizador deve ter a permissão para **Configurar as definições da aplicação**.

Deste modo, o Kaspersky Endpoint Security verificará o ficheiro BLOB. A verificação do ficheiro BLOB inclui a verificação da assinatura digital e da validade da licença. Se o ficheiro BLOB for verificado com êxito, o Kaspersky Endpoint Security descarregará o ficheiro e enviá-lo-á para o computador durante a próxima sincronização com o Kaspersky Security Center. Verifique o estado de funcionamento do componente, ao consultar o *Report on status of application components*. Pode também ver o estado de funcionamento de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente **Managed Detection and Response** será adicionado à lista de componentes do Kaspersky Endpoint Security.

5 **Configurar outros componentes da aplicação para receber telemetria**

Deve ativar os componentes seguintes para que a Managed Detection and Response funcione:

- Kaspersky Security Network (modo ampliado).
- Deteção de comportamento.
- Prevenção de explorações.
- Proteção contra ameaças da Web.
- Proteção contra ameaças de correio.
- Proteção contra ameaças de ficheiros.
- Proteção contra ameaças de Rede.
- Firewall.
- Proteção AMSI.
- Verificação de fundo.

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration** → **Managed Detection and Response**.
5. Ative o botão de alternar **Managed Detection and Response ENABLED**.
6. Guarde as suas alterações.

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
4. Selecione a caixa de verificação **Managed Detection and Response (Industrial CyberSecurity)**.
5. Guarde as suas alterações.

Integrar o EDR Agent com EDR (KATA)

O EDR Agent é instalado em estações de trabalho e servidores na infraestrutura de TI da organização. Nestes computadores, o EDR Agent monitoriza continuamente processos, ligações de rede abertas e ficheiros que são modificados, e envia os dados de monitorização para o servidor com o componente Central Node.

Para integrar com o EDR (KATA), tem de ativar o componente Endpoint Detection and Response (KATA) e configurar o EDR Agent.

Para o Endpoint Detection and Response (KATA) funcionar, tem de cumprir as seguintes condições:

- Kaspersky Anti Targeted Attack Platform versões 5.0–7.1.
- Kaspersky Security Center versão 14.2 ou superior. Nas versões anteriores do Kaspersky Security Center, é impossível ativar a funcionalidade Endpoint Detection and Response (KATA).

https://www.youtube.com/watch?v=cZzgtBoeC7k

A integração com o Kaspersky Endpoint Detection and Response (KATA) implica os seguintes passos:

1. **Ativar o Endpoint Detection and Response (KATA)**

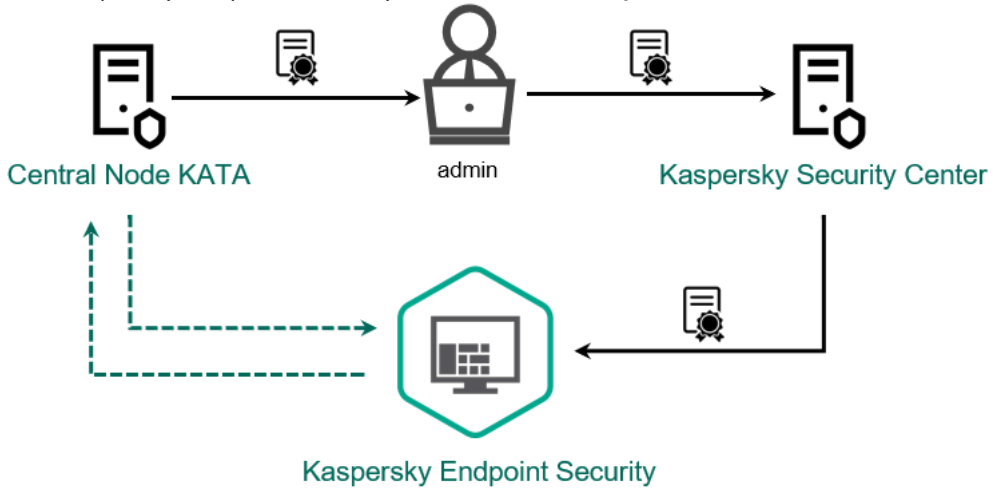
   Comprar uma licença separada para o EDR (KATA) (Suplemento do Kaspersky Endpoint Detection and Response (KATA)).

   A funcionalidade estará disponível após adicionar uma chave individual para o Kaspersky Endpoint Detection and Response (KATA). A licença para a funcionalidade Endpoint Detection and Response (KATA) autónoma é a mesma que a licença do Kaspersky Endpoint Security.

   Certifique-se de que a funcionalidade EDR (KATA) é incluída na licença e é executada na interface local da aplicação.

2. **Ligar ao Central Node**

   A Kaspersky Anti Targeted Attack Platform requer o estabelecimento de uma ligação fiável entre o Kaspersky Endpoint Security e o componente Central Node. Para configurar uma ligação fiável, tem de utilizar um certificado TLS. Pode obter um certificado TLS na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform). Em seguida, tem de adicionar o certificado TLS ao Kaspersky Endpoint Security (consulte as instruções abaixo).



Adicionar um certificado TLS ao Kaspersky Endpoint Security

Por padrão, o Kaspersky Endpoint Security verifica apenas o certificado TLS do Central Node. Para tornar a ligação mais segura, também pode ativar a verificação do computador no Central Node (autenticação bidirecional). Para ativar esta verificação, tem de ativar a autenticação bidirecional nas definições do Central Node e do Kaspersky Endpoint Security. Para usar a autenticação bidirecional, também irá precisar de um cripto-contentor. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform).

Como ligar um computador do Kaspersky Endpoint Security ao Central Node usando a Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Detection and Response → Endpoint Detection and Response Expert (on-premises)**.
5. Selecione a caixa de verificação **Endpoint Detection and Response Expert (on-premises)**.
6. Clique em **Definições de ligação do servidor**.
7. Configure a ligação do servidor:
   - **Tempo limite (seg)**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor de Central Node diferente.
   - **Certificado TLS do servidor**. Certificado TLS para estabelecer uma ligação fiável com o servidor do Central Node. Pode obter um certificado TLS na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform).
   - **Usar a autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma ligação segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para utilizar a autenticação bidirecional, é necessário ativar a autenticação bidirecional nas definições do servidor do Central Node e, em seguida, obter um contentor criptográfico e definir uma password para proteger o contentor criptográfico. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform). Após configurar as definições do Central Node, é também necessário ativar a autenticação bidirecional nas definições do Kaspersky Endpoint Security e carregar um contentor criptográfico protegido por password.

     O cripto-contentor deve ser protegido por password. Não é possível adicionar um cripto-contentor com uma password em branco.
8. Clique em **OK**.
9. Adicionar servidores de Central Node. Para o fazer, especifique o endereço do servidor (IPv4, IPv6) e a porta para se ligar ao servidor.

   Pode adicionar vários endereços do servidor do Nó Central. O Kaspersky Endpoint Security tenta ligar-se ao servidor utilizando o primeiro endereço IP. Se não for possível estabelecer uma ligação, o Kaspersky Endpoint Security tenta ligar-se utilizando o segundo endereço IP da lista e assim sucessivamente.

10. Se necessário, configure a telemetria.

11. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ligar um computador do Kaspersky Endpoint Security ao Central Node usando a Consola Web

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.

5. Ative o botão de alternar **Endpoint Detection and Response Expert (on-premises) ENABLED**.

6. Para configurar o EDR (KATA), selecione **Endpoint Detection and Response Expert (version 7.1 or earlier)** da lista de soluções.

7. Clique em **Connection settings**.

8. Configure a ligação do servidor:

   - **Timeout (sec)**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor de Central Node diferente.

   - **Server certificate**. Certificado TLS para estabelecer uma ligação fiável com o servidor do Central Node. Pode obter um certificado TLS na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform).

   - **Use two-way authentication**. Autenticação bidirecional ao estabelecer uma ligação segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para utilizar a autenticação bidirecional, é necessário ativar a autenticação bidirecional nas definições do servidor do Central Node e, em seguida, obter um contentor criptográfico e definir uma password para proteger o contentor criptográfico. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform). Após configurar as definições do Central Node, é também necessário ativar a autenticação bidirecional nas definições do Kaspersky Endpoint Security e carregar um contentor criptográfico protegido por password.

     O cripto-contentor deve ser protegido por password. Não é possível adicionar um cripto-contentor com uma password em branco.

9. Clique em **OK**.

10. Adicionar servidores de Central Node. Para o fazer, especifique o endereço do servidor (IPv4, IPv6) e a porta para se ligar ao servidor.

    Pode adicionar vários endereços do servidor do Nó Central. O Kaspersky Endpoint Security tenta ligar-se ao servidor utilizando o primeiro endereço IP. Se não for possível estabelecer uma ligação, o Kaspersky Endpoint Security tenta ligar-se utilizando o segundo endereço IP da lista e assim sucessivamente.

11. Se necessário, configure a telemetria.

12. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como resultado, o computador é adicionado à consola da Kaspersky Anti Targeted Attack Platform. Verifique o estado de funcionamento do componente, ao consultar o *Report on status of application components*. Pode também ver o estado de funcionamento de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente **Endpoint Detection and Response Expert (on-premises)** será adicionado à lista de componentes do Kaspersky Endpoint Security.

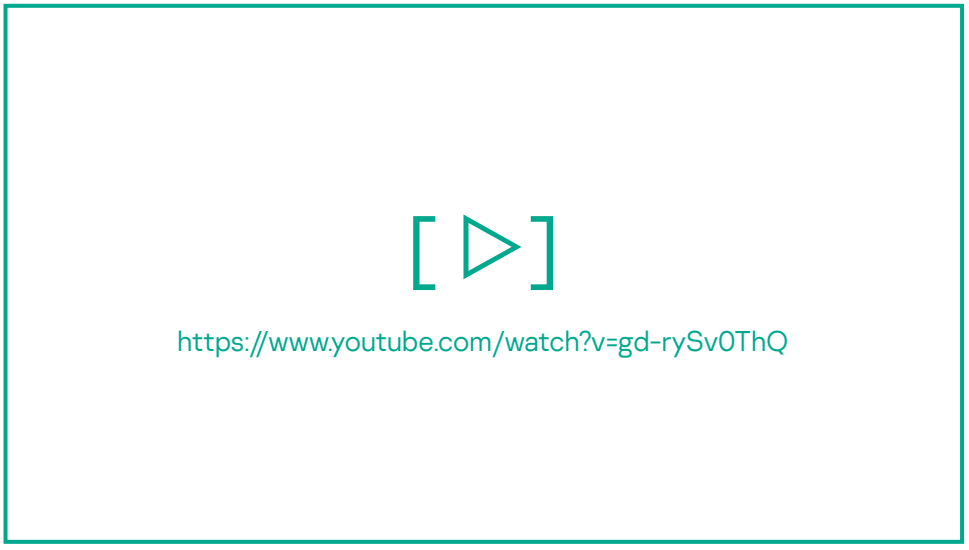
Integrar o EDR Agent com NDR (KATA)

O EDR Agent é instalado em estações de trabalho e servidores na infraestrutura de TI da organização. Nestes computadores, o EDR Agent monitoriza continuamente processos, ligações de rede abertas e ficheiros que são modificados, e envia os dados de monitorização para o servidor com o componente Central Node.

Para integrar com o NDR (KATA), tem de ativar o componente Network Detection and Response (KATA) e configurar o EDR Agent.

Para o Network Detection and Response (KATA) funcionar, tem de cumprir as seguintes condições:

- Kaspersky Anti Targeted Attack Platform versão 7.0 ou posterior.
- Kaspersky Security Center versão 14.2 ou superior. Nas versões anteriores do Kaspersky Security Center, é impossível ativar a funcionalidade Network Detection and Response (KATA).



https://www.youtube.com/watch?v=gd-rySv0ThQ

A integração com o Kaspersky Network Detection and Response (KATA) implica os seguintes passos:

1. **Ativar o Network Detection and Response (KATA)**

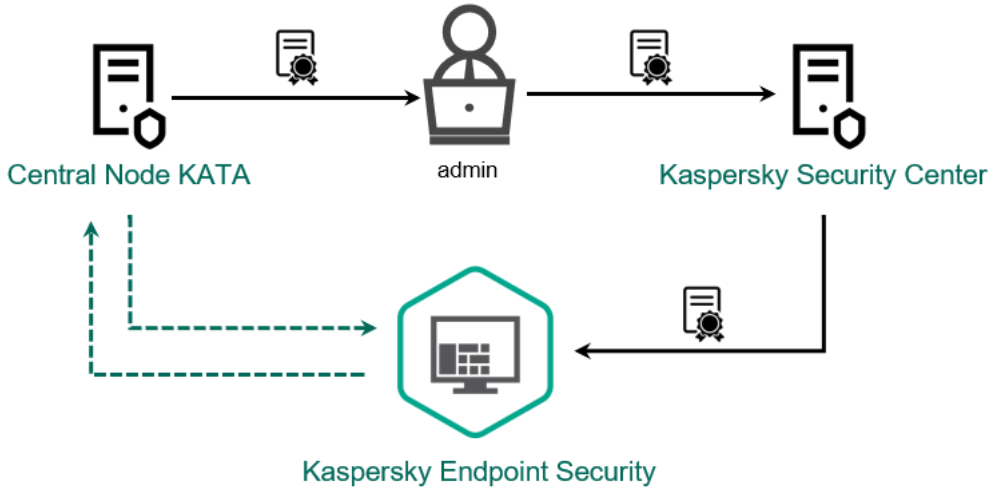
   Comprar uma licença separada para o NDR (KATA) (Suplemento do Kaspersky Network Detection and Response (KATA)).

   A funcionalidade estará disponível após adicionar uma chave separada para o Kaspersky Network Detection and Response (KATA). A licença para a funcionalidade Network Detection and Response (KATA) autónoma é a mesma que a licença do Kaspersky Endpoint Security.

   Certifique-se de que a funcionalidade NDR (KATA) é incluída na licença e é executada na interface local da aplicação.

2. **Ligar ao Central Node**

A Kaspersky Anti Targeted Attack Platform requer o estabelecimento de uma ligação fiável entre o Kaspersky Endpoint Security e o componente Central Node. Para configurar uma ligação fiável, tem de utilizar um certificado TLS. Pode obter um certificado TLS na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform). Em seguida, tem de adicionar o certificado TLS ao Kaspersky Endpoint Security (consulte as instruções abaixo).



Adicionar um certificado TLS ao Kaspersky Endpoint Security

Por padrão, o Kaspersky Endpoint Security verifica apenas o certificado TLS do Central Node. Para tornar a ligação mais segura, também pode ativar a verificação do computador no Central Node (autenticação bidirecional). Para ativar esta verificação, tem de ativar a autenticação bidirecional nas definições do Central Node e do Kaspersky Endpoint Security. Para usar a autenticação bidirecional, também irá precisar de um cripto-contentor. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform).

Como ligar um computador do Kaspersky Endpoint Security ao Central Node usando a Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Detection and Response → Network Detection and Response (KATA)**.
4. Selecione a caixa de verificação **Network Detection and Response (KATA)**.
5. Clique em **Connection settings**.
6. Configure a ligação do servidor:
   - **Timeout (sec)**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor de Central Node diferente.
   - **Server certificate**. Certificado TLS para estabelecer uma ligação fiável com o servidor do Central Node. Pode obter um certificado TLS na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform).

- **Use two-way authentication**. Autenticação bidirecional ao estabelecer uma ligação segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para utilizar a autenticação bidirecional, é necessário ativar a autenticação bidirecional nas definições do servidor do Central Node e, em seguida, obter um contentor criptográfico e definir uma password para proteger o contentor criptográfico. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform). Após configurar as definições do Central Node, é também necessário ativar a autenticação bidirecional nas definições do Kaspersky Endpoint Security e carregar um contentor criptográfico protegido por password.

  O cripto-contentor deve ser protegido por password. Não é possível adicionar um cripto-contentor com uma password em branco.

7. Clique em **OK**.
8. Adicionar servidores de Central Node. Para o fazer, especifique o endereço do servidor (IPv4, IPv6) e a porta para se ligar ao servidor.
9. Pode adicionar vários endereços do servidor do Nó Central. O Kaspersky Endpoint Security tenta ligar-se ao servidor utilizando o primeiro endereço IP. Se não for possível estabelecer uma ligação, o Kaspersky Endpoint Security tenta ligar-se utilizando o segundo endereço IP da lista e assim sucessivamente.
10. Se necessário, configure a telemetria.
11. Guarde as suas alterações.

Como ligar um computador do Kaspersky Endpoint Security ao Central Node usando a Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration** → **Network Detection and Response (KATA)**.
5. Ative o botão de alternar **Network Detection and Response (KATA) ENABLED**.
6. Clique em **Connection settings**.
7. Configure a ligação do servidor:

   - **Timeout (sec)**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor de Central Node diferente.
   - **Server certificate**. Certificado TLS para estabelecer uma ligação fiável com o servidor do Central Node. Pode obter um certificado TLS na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform).

- **Use two-way authentication**. Autenticação bidirecional ao estabelecer uma ligação segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para utilizar a autenticação bidirecional, é necessário ativar a autenticação bidirecional nas definições do servidor do Central Node e, em seguida, obter um contentor criptográfico e definir uma password para proteger o contentor criptográfico. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform). Após configurar as definições do Central Node, é também necessário ativar a autenticação bidirecional nas definições do Kaspersky Endpoint Security e carregar um contentor criptográfico protegido por password.

  O cripto-contentor deve ser protegido por password. Não é possível adicionar um cripto-contentor com uma password em branco.

8. Clique em **OK**.
9. Adicionar servidores de Central Node. Para o fazer, especifique o endereço do servidor (IPv4, IPv6) e a porta para se ligar ao servidor.
10. Pode adicionar vários endereços do servidor do Nó Central. O Kaspersky Endpoint Security tenta ligar-se ao servidor utilizando o primeiro endereço IP. Se não for possível estabelecer uma ligação, o Kaspersky Endpoint Security tenta ligar-se utilizando o segundo endereço IP da lista e assim sucessivamente.
11. Se necessário, configure a telemetria.
12. Guarde as suas alterações.

Como resultado, o computador é adicionado à consola da Kaspersky Anti Targeted Attack Platform. Verifique o estado de funcionamento do componente, ao consultar o *Report on status of application components*. Pode também ver o estado de funcionamento de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente **Network Detection and Response (KATA)** será adicionado à lista de componentes do Kaspersky Endpoint Security.

Integrar o EDR Agent com EDR Expert (on-premises)

O EDR Agent é instalado em estações de trabalho e servidores na infraestrutura de TI da organização. Nestes computadores, o EDR Agent monitoriza continuamente processos, ligações de rede abertas e ficheiros que são modificados, e envia os dados de monitorização para o servidor EDR Expert (on-premises).

Para integrar com o EDR Expert (on-premises), tem de ativar o componente Endpoint Detection and Response Expert (on-premises) e configurar o EDR Agent.

A integração com o Kaspersky Endpoint Detection and Response Expert (on-premises) implica os seguintes passos:

1. **Ativar o Kaspersky Endpoint Detection and Response Expert (on-premises)**

   Comprar uma licença separada para o EDR Expert (on-premises) (Suplemento do Kaspersky Endpoint Detection and Response Expert (on-premises)).

   A funcionalidade estará disponível após adicionar uma chave individual para o Kaspersky Endpoint Detection and Response Expert (on-premises). A licença para a funcionalidade Endpoint Detection and Response Expert (on-premises) autónoma é a mesma que a licença do Kaspersky Endpoint Security.

   Certifique-se de que a funcionalidade EDR Expert (on-premises) é incluída na licença e é executada na interface local da aplicação.

2 **Ligar ao servidor de recolha de telemetria e ao servidor de resposta**

O Kaspersky Endpoint Detection and Response Expert (on-premises) requer uma conexão fiável entre o Kaspersky Endpoint Security e dois servidores:

- Um *servidor de recolha de telemetria* é um servidor que faz parte de uma solução SIEM e que recolhe, normaliza, correlaciona, analisa e armazena informações sobre eventos que ocorrem no computador.
- Um *servidor de resposta* é um servidor para receber e analisar dados, estudar o comportamento de objetos e publicar os resultados desses estudos.

Para configurar uma ligação fiável, tem de utilizar um certificado TLS. Pode 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, tem de adicionar o certificado TLS ao Kaspersky Endpoint Security (consulte as instruções abaixo).

Por padrão, o Kaspersky Endpoint Security verifica apenas o certificado dos servidores. Para tornar a ligação mais segura, também pode ativar a verificação do computador no servidor (autenticação bidirecional). Para ativar esta verificação, tem de ativar a autenticação bidirecional nas definições do servidor e do Kaspersky Endpoint Security. Para usar a autenticação bidirecional, também irá precisar de um cripto-contentor. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)).

Como ligar um computador do Kaspersky Endpoint Security ao EDR Expert (on-premises) usando a Consola Web

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.
5. Ative o botão de alternar **Endpoint Detection and Response Expert (on-premises) ENABLED**.
6. Para configurar o EDR Expert (on-premises), selecione **Endpoint Detection and Response Expert (version 8.0 or later)** da lista de soluções.
7. Configure a ligação dos *servidores de recolha de telemetria*:

   a. No bloco **Connection to telemetry collection servers**, clique na ligação **Connection settings**.

   b. Configure a ligação dos servidores de recolha de telemetria:

   - **Timeout (sec)**. Tempo limite máximo de resposta do servidor. Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor diferente.
   - **Server certificate**. Certificado TLS para estabelecer uma ligação fiável com o servidor. Pode obter um certificado TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Use two-way authentication**. Autenticação bidirecional ao estabelecer uma ligação segura entre o Kaspersky Endpoint Security e o servidor. Para utilizar a autenticação bidirecional, é necessário ativar a autenticação bidirecional nas definições do servidor e, em seguida, obter um contentor criptográfico e definir uma password para proteger o contentor criptográfico. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). Após configurar as definições do servidor, é também necessário ativar a autenticação bidirecional nas definições do Kaspersky Endpoint Security e carregar um contentor criptográfico protegido por password.

  O cripto-contentor deve ser protegido por password. Não é possível adicionar um cripto-contentor com uma password em branco.

c. Clique em **OK**.

d. Adicione servidores de recolha de telemetria. Para o fazer, especifique o endereço do servidor (IPv4, IPv6) e a porta para se ligar ao servidor.

   Pode adicionar vários endereços do servidor de recolha de telemetria. O Kaspersky Endpoint Security tenta ligar-se ao servidor utilizando o primeiro endereço IP. Se não for possível estabelecer uma ligação, o Kaspersky Endpoint Security tenta ligar-se utilizando o segundo endereço IP da lista e assim sucessivamente.

e. Se necessário, configure a telemetria.

8. Configure a ligação dos *servidores de resposta*:

a. No bloco **Connection to response servers**, configure a definição **Send sync request to server every (min)**. Frequência de pedidos de sincronização enviados ao servidor. Durante a sincronização, o Kaspersky Endpoint Security recebe tarefas de resposta a ameaças e envia os resultados dessas tarefas.

b. Clique na hiperligação **Connection settings**.

c. Configure a ligação dos servidores de resposta:

- **Timeout (sec)**. Tempo limite máximo de resposta do servidor. Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor diferente.

- **Server certificate**. Certificado TLS para estabelecer uma ligação fiável com o servidor. Pode obter um certificado TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Use two-way authentication**. Autenticação bidirecional ao estabelecer uma ligação segura entre o Kaspersky Endpoint Security e o servidor. Para utilizar a autenticação bidirecional, é necessário ativar a autenticação bidirecional nas definições do servidor e, em seguida, obter um contentor criptográfico e definir uma password para proteger o contentor criptográfico. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). Após configurar as definições do servidor, é também necessário ativar a autenticação bidirecional nas definições do Kaspersky Endpoint Security e carregar um contentor criptográfico protegido por password.

  O cripto-contentor deve ser protegido por password. Não é possível adicionar um cripto-contentor com uma password em branco.

d. Clique em **OK**.

e. Adicione servidores de resposta. Para o fazer, especifique o endereço do servidor (IPv4, IPv6) e a porta para se ligar ao servidor.

   Pode adicionar vários endereços do servidor de resposta. O Kaspersky Endpoint Security tenta ligar-se ao servidor utilizando o primeiro endereço IP. Se não for possível estabelecer uma ligação, o Kaspersky Endpoint Security tenta ligar-se utilizando o segundo endereço IP da lista e assim sucessivamente.

9. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como resultado, o computador é adicionado à Open Single Management Platform (OSMP). Verifique o estado de funcionamento do componente, ao consultar o *Report on status of application components*. Pode também ver o estado de funcionamento de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente **Endpoint Detection and Response Expert (on-premises)** será adicionado à lista de componentes do Kaspersky Endpoint Security.

Compatibilidade com aplicações da EPP de terceiros

O EDR Agent oferece suporte à funcionalidade das soluções Kaspersky Detection and Response. Os componentes de proteção e controlo não estão disponíveis para o EDR Agent. Esta configuração permite instalar aplicações EPP de terceiros e implementar soluções Kaspersky Detection and Response na infraestrutura da organização.

O EDR Agent é compatível com aplicações EPP dos seguintes fornecedores:

- **Dr.Web**

  O EDR Agent é compatível com o Dr.Web Agent para Windows versão 13 e o Dr.Web Server (x64) 13.0.0.10200.

- **Dallas Lock**

  O EDR Agent é compatível com Dallas Lock 8.0-C versão 843.2.

  Para que o EDR Agent seja executado num computador que tenha o software Dallas Lock instalado, tem de permitir que a ligação aos serviços externos da Kaspersky nas definições do módulo da Firewall.

- **Secret Net Studio**

  O EDR Agent é compatível com Secret Net Studio versão 8.11 (20851).

A aplicação não pode ser instalada num computador onde o Secret Net Studio é implementado com o componente Antivírus. Para possibilitar a interoperabilidade, tem de remover o componente Antivírus do Secret Net Studio.

- **Trend Micro**

  O EDR Agent é compatível com Trend Micro Vision One (incluindo Security Agent versão 14.0.20731).

  O EDR Agent é compatível com Trend Micro Deep Security versão 20.0.3-18160 (incluindo Security Agent).

- **Windows Defender**

- **Sophos**

  O EDR Agent é compatível com Sophos Intercept X versão 2024.1.2 (incluindo Endpoint Agent) e Sophos Core Agent versão 2026.2.1.3.

- **Bitdefender**

  O EDR Agent é compatível com Bitdefender Endpoint Security Tools versão 8.26.7.647.

- **ESET**

  O EDR Agent é compatível com ESET Endpoint Security versão 13.0.2044.0 e ESET Management Agent versão 13.2.1189.0.

Em computadores com Windows 11 para Arm64, o Agente EDR não é compatível com Bitdefender Endpoint Security Tools.

As aplicações devem ser instaladas na seguinte ordem: primeiro, instale a aplicação EPP, depois o Agente de Rede do Kaspersky Security Center e, em seguida, o EDR Agent. É necessário instalar por esta ordem porque o instalador da aplicação EPP pode detetar o EDR Agent e o Agente de Rede como software incompatível e removê-los. Deve verificar o funcionamento do EDR Agent e do Agente de Rede após a atualização da aplicação EPP de terceiros, porque o seu instalador pode verificar novamente o computador em busca de software incompatível e remover as aplicações.

Se não conseguiu instalar o EDR Agent num computador com uma aplicação EPP de terceiros porque o instalador encontrou software incompatível no computador, pode ignorar a verificação de software incompatível.

Managed Detection and Response



O Kaspersky Endpoint Security for Windows suporta a integração com a solução Managed Detection and Response. A solução *Kaspersky Managed Detection and Response (MDR)* deteta e analisa automaticamente os incidentes de segurança na sua infraestrutura. Para tal, o MDR utiliza dados de telemetria recebidos de terminais e aprendizagem automática. O MDR envia os dados de incidentes aos especialistas da Kaspersky. Os especialistas podem então processar o incidente e, por exemplo, adicionar uma nova entrada às bases de dados de antivírus. Em alternativa, os especialistas podem emitir recomendações sobre o processamento do incidente e, por exemplo, sugerir que o computador seja isolado da rede. Para obter mais informações sobre a utilização da solução, 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 funcionar com MDR:

- **[KES+agente integrado]**. Nesta configuração, o Kaspersky Endpoint Security atua como a aplicação que garante a segurança do computador e como aplicação para trabalhar 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 Endpoint Detection and Response Agent (EDR Agent). Nesta configuração, o EDR Agent é compatível com aplicações de EPP de terceiros.

Integração do agente integrado com MDR

Para configurar a integração com o Kaspersky Managed Detection and Response, deve ativar o componente Managed Detection and Response e configurar o Kaspersky Endpoint Security.

Para o Kaspersky Managed Detection and Response funcionar com o Administration Server através do Consola Web do Kaspersky Security Center, deve estabelecer uma nova ligação segura, uma *ligação de fundo*. O Kaspersky Managed Detection and Response solicita que estabeleça uma ligação de fundo ao implementar a solução. Certifique-se de que a ligação de fundo é estabelecida.

Estabelecer uma ligação de fundo na Consola Web

1. Na janela principal da Consola Web, selecione **Settings** → **Integration**.
2. Aceda à secção **Integration**.
3. Ative o botão de alternar **Background connection for integration Enabled**.
4. Guarde as suas alterações.

A integração com o Kaspersky Managed Detection and Response consiste nos seguintes passos:

1. **Instalar o componente Managed Detection and Response**

   Pode selecionar o componente MDR durante a instalação ou atualização, bem como através da tarefa *Alterar componentes da aplicação*.

   > Para instalar o componente Managed Detection and Response sem reiniciar o computador utilizando a tarefa *Alterar componentes da aplicação*, precisa de desativar a opção **Verificar a existência de aplicações de terceiros incompatíveis** nas definições da tarefa.

2. **Configurar o Kaspersky Private Security Network**

   > Ignore este passo se estiver a utilizar o Kaspersky Security Center Cloud Console. O Kaspersky Security Center Cloud Console configura automaticamente o Kaspersky Private Security Network ao instalar o plug-in MDR.

Kaspersky Private Security Network (KPSN) é uma solução que permite que utilizadores de computadores que alojam o Kaspersky Endpoint Security ou outras aplicações da Kaspersky tenham acesso às bases de dados de reputação do Kaspersky Security Network e a outros dados estatísticos sem enviar dados para o KSN a partir de seus próprios computadores.

Carregue o ficheiro de configuração do Kaspersky Security Network nas propriedades do Servidor de administração. O ficheiro de configuração do Kaspersky Security Network está localizado no arquivo ZIP do ficheiro de configuração do MDR. Pode obter o arquivo ZIP na Consola do Kaspersky Managed Detection and Response. Para obter mais informações sobre a configuração da Kaspersky Private Security Network, consulte a Ajuda do Kaspersky Security Center. Pode também carregar um ficheiro de configuração do Kaspersky Security Network para o computador a partir da command line (consulte as instruções abaixo).

Como configurar o Kaspersky Private Security Network a partir da linha de comandos

1. Execute o interpretador de linha de comando (cmd.exe) como administrador.
2. Vá para a pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.
3. Execute o seguinte comando:

   ```
   avp.com KSN /private <file name>
   ```

   quando `<file name>` é o nome do ficheiro de configuração que contém as definições do Kaspersky Private Security Network (formato de ficheiro PKCS7 ou PEM).

   Exemplo:
   `avp.com KSN /private C:\kpsn_config.pkcs7`

Deste modo, o Kaspersky Endpoint Security utilizará o Kaspersky Private Security Network para determinar a reputação dos ficheiros, das aplicações e dos sites. A secção **Kaspersky Security Network** das definições de política irá exibir o seguinte estado operacional: *Infraestrutura:* Kaspersky Private Security Network.

Deve ativar o modo KSN alargado para que a Managed Detection and Response funcione.

3 Ativar o Kaspersky Managed Detection and Response

A partir do Kaspersky Endpoint Security for Windows 12.10, para ativar a funcionalidade Managed Detection and Response, como alternativa a um código de ativação, também pode utilizar um ficheiro-chave.

O Kaspersky Managed Detection and Response suporta os seguintes métodos de licenciamento:

- A funcionalidade Managed Detection and Response é abrangida pela licença Kaspersky Endpoint Security for Windows.

  A funcionalidade está imediatamente disponível após a ativação do Kaspersky Endpoint Security for Windows.

- É utilizada uma licença separada para MDR (Suplemento do Kaspersky Managed Detection and Response).

  A funcionalidade estará disponível após adicionar uma chave individual para o Suplemento do Kaspersky Managed Detection and Response. Como resultado, são adicionadas duas chaves no computador: uma chave para o Kaspersky Endpoint Security e uma chave para o Kaspersky Managed Detection and Response.

  A licença para a funcionalidade Managed Detection and Response autónoma é a mesma que a licença do Kaspersky Endpoint Security.

Certifique-se de que a funcionalidade MDR é incluída na licença e está a funcionar na interface local da aplicação.

4 Ativação do componente Managed Detection and Response

Carregue o ficheiro de configuração BLOB na política do Kaspersky Endpoint Security (consulte as instruções abaixo). O ficheiro BLOB contém a ID do cliente e informações sobre a licença do Kaspersky Managed Detection and Response. O ficheiro BLOB está localizado dentro do arquivo ZIP do ficheiro de configuração do MDR. Pode obter o arquivo ZIP na Consola do Kaspersky Managed Detection and Response. Para obter mais informações sobre ficheiros BLOB, consulte a Ajuda do Kaspersky Managed Detection and Response.

A partir do Kaspersky Endpoint Security 12.6 for Windows, adicionar um ficheiro BLOB é opcional para o Kaspersky Managed Detection and Response sem inquilinos se tiver uma licença atual.

Como ativar o componente Managed Detection and Response na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
4. Selecione a caixa de verificação **Managed Detection and Response (Industrial CyberSecurity)**.
5. No bloco **Definições**, clique em **Carregar** e selecione o ficheiro BLOB recebido na Consola do Kaspersky Managed Detection and Response. O ficheiro possui a extensão P7.

   Por defeito, o utilizador tem permissão para gerir as definições da aplicação (o "cadeado" está aberto). Para aplicar a política em computadores, feche os cadeados .

6. Guarde as suas alterações.

Como ativar o componente Managed Detection and Response na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration** → **Managed Detection and Response**.
5. Ative o botão de alternar **Managed Detection and Response ENABLED**.
6. Clique em **Upload** e selecione o ficheiro BLOB que foi obtido na Consola do Kaspersky Managed Detection and Response. O ficheiro possui a extensão P7.

   Por defeito, o utilizador tem permissão para gerir as definições da política (o "cadeado" está aberto). Para aplicar a política em computadores, feche os cadeados .

7. Guarde as suas alterações.

Como ativar o componente Managed Detection and Response a partir da command line

1. Execute o interpretador de linha de comando (cmd.exe) como administrador.
2. Vá para a pasta onde o ficheiro 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 password deve estar ativada. O utilizador deve ter a permissão para **Configurar as definições da aplicação**.

Deste modo, o Kaspersky Endpoint Security verificará o ficheiro BLOB. A verificação do ficheiro BLOB inclui a verificação da assinatura digital e da validade da licença. Se o ficheiro BLOB for verificado com êxito, o Kaspersky Endpoint Security descarregará o ficheiro e enviá-lo-á para o computador durante a próxima sincronização com o Kaspersky Security Center. Verifique o estado de funcionamento do componente, ao consultar o *Report on status of application components*. Pode também ver o estado de funcionamento de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente **Managed Detection and Response** será adicionado à lista de componentes do Kaspersky Endpoint Security.

5. **Configurar outros componentes da aplicação para receber telemetria**

Deve ativar os componentes seguintes para que a Managed Detection and Response funcione:

- Kaspersky Security Network (modo ampliado).
- Deteção de comportamento.
- Prevenção de explorações.
- Proteção contra ameaças da Web.
- Proteção contra ameaças de correio.
- Proteção contra ameaças de ficheiros.
- Proteção contra ameaças de Rede.
- Firewall.
- Proteção AMSI.
- Verificação de fundo.

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration** → **Managed Detection and Response**.

5. Ative o botão de alternar **Managed Detection and Response ENABLED**.

6. Guarde as suas alterações.

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**.

4. Selecione a caixa de verificação **Managed Detection and Response (Industrial CyberSecurity)**.

5. Guarde as suas alterações.

Guia de migração de KEA para o KES para MDR

O Kaspersky Endpoint Security for Windows inclui um agente integrado para a solução Kaspersky Managed Detection and Response. Já não precisa de uma aplicação Kaspersky Endpoint Agent em separado para trabalhar com MDR. Todas as funções do Kaspersky Endpoint Agent serão executadas pelo Kaspersky Endpoint Security.

Quando implementa o Kaspersky Endpoint Security em computadores com o Kaspersky Endpoint Agent instalado, as soluções Kaspersky Managed Detection and Response irão continuar a funcionar com o Kaspersky Endpoint Security. Além disso, o Kaspersky Endpoint Agent será removido do computador. Ocorrerá o mesmo comportamento no sistema quando 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 pode instalar estas aplicações no mesmo computador.

Devem ser cumpridas as seguintes condições para que o Kaspersky Endpoint Security funcione como parte do Kaspersky Managed Detection and Response:

- Versão 13.2 ou superior do Kaspersky Security Center (incluindo Agente de Rede). Nas versões anteriores do Kaspersky Security Center, é impossível ativar a funcionalidade Managed Detection and Response.
- Uma ligação de fundo entre a Consola Web do Kaspersky Security Center e o Administration Server é estabelecida. Para o MDR funcionar com o Servidor de Administração através da Consola Web do Kaspersky Security Center, deve estabelecer uma nova ligação segura, uma *ligação de fundo*.

Etapas para migrar a configuração [KES+KEA] para [KES+built-in agent] para MDR

1. **Atualização do Plug-in de gestão do Kaspersky Endpoint Security**

   O componente MDR pode ser gerido com a versão 11.6 ou superior do Plug-in de gestão do Kaspersky Endpoint Security. Dependendo do tipo de consola do Kaspersky Security Center que está a usar, atualize o plug-in de gestão na consola de administração (MMC) ou o plug-in da Web no consola Web.

2. **Migração da política e das tarefas**

Transfira as definições do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows. Estão disponíveis as seguintes opções:

- O assistente para a migração do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security. O assistente para a migração do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security funciona apenas na Consola Web

  Como migrar as definições de tarefas e políticas do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security na Consola Web

  Na janela principal da Consola Web, selecione **Operations** → **Migration from Kaspersky Endpoint Agent**.

  Esta ação executa o assistente de migração de políticas e tarefas. Siga as instruções do Assistente.

  Passo 1. Migração de políticas

  O assistente de migração cria uma nova política que combina as definições das políticas do Kaspersky Endpoint Security e do Kaspersky Endpoint Agent. Na lista de políticas, selecione as políticas do Kaspersky Endpoint Agent cujas definições pretende combinar com a política do Kaspersky Endpoint Security. Clique na política do Kaspersky Endpoint Agent para selecionar a política do Kaspersky Endpoint Security com a qual pretende combinar definições. Certifique-se de que seleciona as políticas corretas e avance para o passo seguinte.

  Passo 2. Migração de tarefas

  O Assistente de Migração não suporta tarefas MDR. Ignorar este passo.

  Passo 3. Conclusão do assistente

  Conclua o assistente. Como resultado do assistente, será criada uma nova política do Kaspersky Endpoint Security. A política combina as definições do Kaspersky Endpoint Security e Kaspersky Endpoint Agent A política é denominada *<Kaspersky Endpoint Security policy name> e <Kaspersky Endpoint Agent policy name>*. A nova política tem o estado *Inactive*. Para continuar, altere os estatutos das políticas do Kaspersky Endpoint Agent e Kaspersky Endpoint Security para *Inactive* e ative a nova política combinada.

- Um assistente de conversão de políticas e tarefas em lote padrão. O Assistente de conversão de políticas e tarefas em lote está disponível apenas na Consola de Administração (MMC). Para obter mais informações detalhadas sobre o Assistente de conversão de políticas e tarefas em lote, consulte a Ajuda do Kaspersky Security Center.

3. **Licenciamento da funcionalidade MDR**

   Para ativar o Kaspersky Endpoint Security como parte da solução da Kaspersky Managed Detection and Response, precisa de uma licença em separado para o suplemento Kaspersky Managed Detection and Response. Pode adicionar a chave através da tarefa *Add key*. Como resultado, serão adicionadas à aplicação duas chaves: *Kaspersky Endpoint Security* e *Kaspersky Managed Detection and Response*.

4. **Instalação/atualização da aplicação Kaspersky Endpoint Security**

Para migrar a funcionalidade MDR durante a instalação ou atualização de uma aplicação, é recomendável usar a tarefa de instalação remota. Ao criar uma tarefa de instalação remota, tem de selecionar o componente MDR nas definições do pacote de instalação.

Também pode atualizar a aplicação utilizando os seguintes métodos:

- Usar o serviço de atualização do Kaspersky.
- Localmente, usando o Assistente de Configuração.

O Kaspersky Endpoint Security suporta a seleção automática de componentes ao atualizar a aplicação num computador com a aplicação Kaspersky Endpoint Agent instalada. A seleção automática dos componentes depende das permissões da conta do utilizador que está a atualizar a aplicação.

Se estiver a atualizar o Kaspersky Endpoint Security utilizando o ficheiro EXE ou MSI na conta do sistema (SYSTEM), o Kaspersky Endpoint Security ganha acesso a licenças atuais de soluções da Kaspersky. Portanto, se o computador tiver o Kaspersky Endpoint Agent instalado e a solução MDR ativada, o instalador Kaspersky Endpoint Security configura automaticamente o conjunto de componentes e seleciona o componente MDR. Isto faz com que o Kaspersky Endpoint Security troque para a utilização do agente incorporado e remove o Kaspersky Endpoint Agent. A execução do instalador MSI na conta do sistema (SYSTEM) é normalmente realizada ao atualizar através do serviço de atualização da Kaspersky ou ao implementar um pacote de instalação através do Kaspersky Security Center.

Se estiver a atualizar o Kaspersky Endpoint Security utilizando um ficheiro MSI numa conta de utilizador sem privilégios, o Kaspersky Endpoint Security não tem acesso às licenças atuais das soluções da Kaspersky. Nesse caso, o Kaspersky Endpoint Security seleciona automaticamente os componentes com base num conjunto de componentes do Kaspersky Endpoint Agent. Depois disso, o Kaspersky Endpoint Security troca para a utilização do agente incorporado e remove o Kaspersky Endpoint Agent.

O Kaspersky Endpoint Security suporta a atualização sem reiniciar o computador. Pode selecionar o modo de atualização da aplicação nas propriedades da política.

5. **A verificar o funcionamento da aplicação**

Se, após a instalação da aplicação, o computador tiver o estado *Critical* na consola do Kaspersky Security Center:

- Certifique-se de que o computador tem o Agente de Rede versão 13.2 ou superior instalado.
- Verifique o estado de funcionamento do agente integrado ao consultar o *Report on status of application components*. Se um componente tiver o estado *Not installed*, instale o componente com a tarefa *Change application components*. Se um componente tiver o estado *Não abrangido pela licença*, certifique-se de que ativou a funcionalidade do agente integrado.
- Certifique-se de que aceita 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 tem um agente integrado para a solução Kaspersky Endpoint Detection and Response Optimum (doravante também referida como "EDR Optimum"). A partir da versão 11.8.0, o Kaspersky Endpoint Security for Windows tem um agente integrado para a solução Kaspersky Endpoint Detection and Response Expert (doravante também referida como "EDR Expert"). O *Kaspersky Endpoint Detection and Response* é uma gama de soluções para proteger a infraestrutura de TI corporativa contra ciberameaças avançadas. A funcionalidade das soluções combina a deteção automática de ameaças com a capacidade de reagir a tais ameaças para neutralizar ataques avançados, incluindo novas explorações, ransomware, ataques sem ficheiros, bem como métodos que utilizam ferramentas legítimas do sistema. O EDR Expert oferece mais funcionalidades de monitorização de ameaças e de resposta do que o EDR Optimum. Para conhecer os detalhes das soluções, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

Ferramentas de Informações sobre Ameaças

O Kaspersky Endpoint Detection and Response utiliza as seguintes ferramentas de Threat Intelligence:

- A integração com o Kaspersky Threat Intelligence Portal, que contém e apresenta informações sobre a reputação de ficheiros e endereços da Internet.
- A base de dados de Ameaças da Kaspersky.
- A infraestrutura dos serviços em nuvem da Kaspersky Security Network (doravante também chamada de "KSN"), que fornece acesso a ficheiros em tempo real, websites e informações de reputação de software da base de conhecimento da Kaspersky. A utilização de dados da Kaspersky Security Network permite uma resposta mais rápida das aplicações da Kaspersky a ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos diagnósticos positivos.
- A tecnologia Cloud Sandbox que lhe permite executar ficheiros detetados num ambiente isolado e verificar a sua reputação.

Princípio do funcionamento da solução

O Kaspersky Endpoint Detection and Response verifica e analisa o desenvolvimento de ameaças e disponibiliza ao *pessoal de segurança* ou *Administrador* informações sobre o possível ataque que são necessárias para uma resposta atempada. O Kaspersky Endpoint Detection and Response apresenta as informações da deteção numa janela separada. Um *alerta* é um evento na infraestrutura de TI corporativa que a aplicação identificou como incomum ou suspeito e que pode representar uma ameaça à segurança da infraestrutura de TI corporativa. As *informações da deteção* é uma ferramenta para visualizar todas as informações recolhidas sobre uma ameaça detetada. As informações da deteção incluem, por exemplo, o histórico dos ficheiros que aparecem no computador. Para conhecer os detalhes sobre a gestão de deteção, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

Suporte para versões anteriores do Kaspersky Endpoint Security

Se estiver a utilizar o Kaspersky Endpoint Security 11.2.0–11.6.0 para interoperabilidade com o Kaspersky Endpoint Detection and Response Optimum, a aplicação inclui o Kaspersky Endpoint Agent. Pode instalar o Kaspersky Endpoint Agent lado a lado com o Kaspersky Endpoint Security. No Kaspersky Endpoint Security 11.9.0, o pacote de distribuição do Kaspersky Endpoint Agent já não faz parte do kit de distribuição do Kaspersky Endpoint Security.

A solução Kaspersky Endpoint Detection and Response Expert não suporta a interoperabilidade com o Kaspersky Endpoint Agent. A solução Kaspersky Endpoint Detection and Response Expert utiliza o Kaspersky Endpoint Security com o agente integrado (versão 11.8.0 e posterior).

Integração do agente integrado com EDR Optimum / EDR Expert

Para configurar a integração com o Kaspersky Endpoint Detection and Response, tem de 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.

Para o Endpoint Detection and Response funcionar, tem de cumprir as seguintes condições:

- Kaspersky Security Center versão 13.2 ou superior. Nas versões anteriores do Kaspersky Security Center, é impossível ativar a funcionalidade Endpoint Detection and Response.
- Plug-in de gestão do Kaspersky Endpoint Detection and Response.

  A partir do Kaspersky Endpoint Security versão 12.6, a apresentação dos detalhes de alertas foi movida do plug-in de gestão do Kaspersky Endpoint Security para o plug-in de gestão do EDR. O plug-in de gestão do EDR é um plug-in único para trabalhar com agentes nos sistemas operativos Windows, Mac e Linux. Agora, ao trabalhar com o EDR Optimum, irá precisar do plug-in de gestão do Kaspersky Endpoint Security para criar tarefas de resposta a ameaças e do plug-in de gestão EDR para ver detalhes de alertas.
- O componente Endpoint Detection and Response Optimum, como parte do Kaspersky Endpoint Security, suporta a interação com a solução Kaspersky Endpoint Detection and Response Optimum 2.0. A interação com Kaspersky Endpoint Detection and Response Optimum versão 1.0 não é suportada.
- O EDR Optimum pode ser gerido na Consola Web do Kaspersky Security Center e na Cloud Console do Kaspersky Security Center.

  O EDR Expert só pode ser gerido utilizando a Cloud Console do Kaspersky Security Center. Não pode gerir esta funcionalidade utilizando a Consola de Administração (MMC).
- A aplicação é ativada e a funcionalidade é abrangida pela licença.
- O componente Endpoint Detection and Response está ativado.
- Os componentes da aplicação dos quais o Endpoint Detection and Response depende estão ativados e em funcionamento. O Endpoint Detection and Response depende dos seguintes componentes:
  - Proteção contra ameaças de ficheiros.
  - Proteção contra ameaças da Web.
  - Proteção contra ameaças de correio.
  - Prevenção de explorações.
  - Deteção de comportamento.
  - Prevenção contra invasões.

- Motor de remediação.
- Controlo de Anomalias Adaptativo.

A integração com o Kaspersky Endpoint Detection and Response implica os seguintes passos:

1. **Instale os componentes Endpoint Detection and Response**

   Pode selecionar o componente Endpoint Detection and Response Optimum ou o componente Endpoint Detection and Response Expert (cloud) durante a instalação ou a atualização, bem como através da tarefa *Alterar componentes da aplicação*.

   Tem de reiniciar o computador para terminar a atualização da aplicação com os novos componentes.

2. **Ativar o Kaspersky Endpoint Detection and Response**

   Pode obter uma licença para utilizar o Kaspersky Endpoint Detection and Response dos seguintes modos:

   - A funcionalidade Endpoint Detection and Response está incluída na licença Kaspersky Endpoint Security for Windows.

     A funcionalidade está imediatamente disponível após a ativação do Kaspersky Endpoint Security for Windows.

   - Comprar uma licença separada para o EDR Optimum ou o EDR Expert (Suplemento do Kaspersky Endpoint Detection and Response).

     A funcionalidade estará disponível após adicionar uma chave individual para o Kaspersky Endpoint Detection and Response. Como resultado, são adicionadas duas chaves no computador: uma chave para o Kaspersky Endpoint Security e uma chave para o Kaspersky Endpoint Detection and Response.

     A licença para a funcionalidade Endpoint Detection and Response autónoma é a mesma que a licença do Kaspersky Endpoint Security.

   Certifique-se de que a funcionalidade EDR Optimum ou EDR Expert é incluída na licença e é executada na interface local da aplicação.

   Para obter mais informações sobre o Contrato de Licença do Utilizador Final do EDR Optimum, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum.

3. **Ativação dos componentes Endpoint Detection and Response**

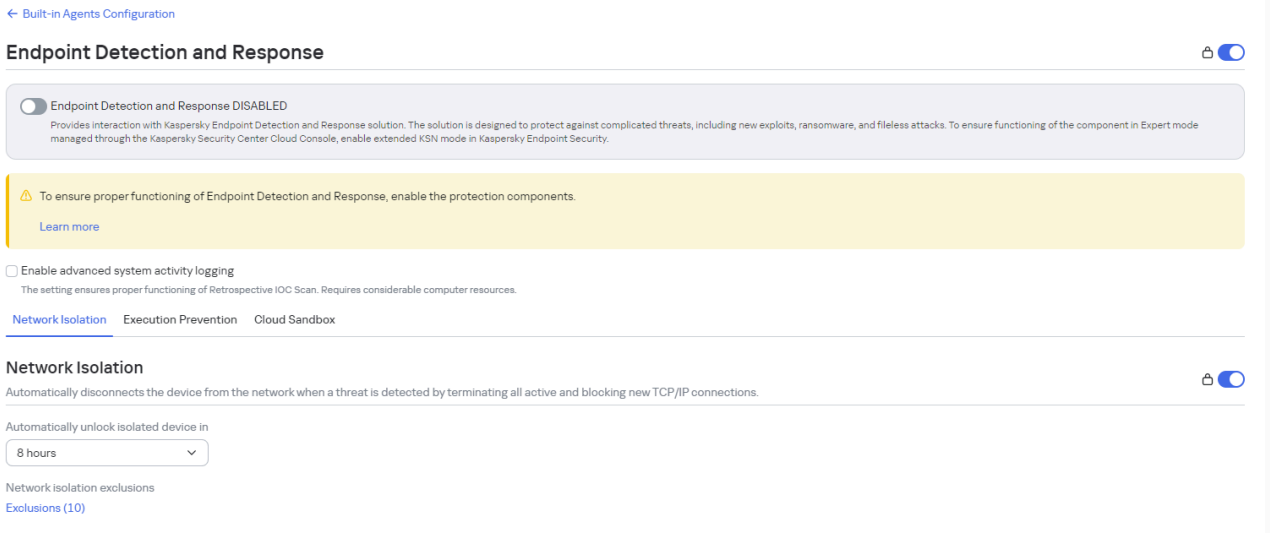
   Pode ativar ou desativar o componente nas definições de políticas do Kaspersky Endpoint Security for Windows.

   Como ativar ou desativar o componente Endpoint Detection and Response na Web Console

   1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
   2. Clique no nome da política do Kaspersky Endpoint Security.

      É apresentada a janela de propriedades da política.
   3. Selecione o separador **Application settings**.
   4. Aceda a **Built-in Agents Configuration** → **Endpoint Detection and Response**.
   5. Ative o botão de alternar **Endpoint Detection and Response ENABLED**.

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



Definições de integração EDR

O componente Kaspersky Endpoint Detection and Response está ativado. Verifique o estado de funcionamento do componente, ao consultar o *Report on status of application components*. Pode também ver o estado de funcionamento 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)** é adicionado à lista de componentes do Kaspersky Endpoint Security.

4 Ativar a transferência de dados para o Servidor de administração

Para ativar todas as funcionalidades do Endpoint Detection and Response, a transferência de dados tem de ser ativada para os seguintes tipos de dados:

- Dados de ficheiros de quarentena.

  Os dados são necessários para obter informações sobre ficheiros colocados em quarentena num computador através da Consola Web. Por exemplo, pode descarregar um ficheiro da quarentena para análise na Consola Web.

- Dados de cadeia de desenvolvimento de ameaças.

  Os dados são necessários para obter informações sobre ameaças detetadas num computador na Web Console. Pode ver os detalhes de alerta e tomar medidas de resposta na Web Console.

Como ativar a transferência de dados para o Servidor de Administração na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **KSC Integration**.
5. No bloco **Data transfer to Administration Server**, clique na ligação **Advanced settings**.

6. Na janela que abre, selecione as seguintes caixas de verificação:

   - **About Quarantine files**.
   - **About a threat development chain**.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Verificar os indicadores de compromisso (tarefa padrão)

Um *Indicador de comprometimento (IOC)* é um conjunto de dados relativos a um objeto ou atividade que indica acesso não autorizado ao computador (comprometimento de dados). Por exemplo, muitas tentativas falhadas de iniciar sessão no sistema podem constituir um Indicador de Comprometimento. A tarefa *IOC Scan* permite localizar indicadores de comprometimento no computador e adotar medidas de resposta a ameaças.

O Kaspersky Endpoint Security procura indicadores de comprometimento utilizando IOC files. Os *IOC files* são ficheiros que contêm os conjuntos de indicadores que a aplicação tenta corresponder para contar uma deteção. Os IOC files devem estar em conformidade com o padrão OpenIOC.

Modo de execução da tarefa IOC Scan

O Kaspersky Endpoint Detection and Response permite-lhe criar tarefas de Verificação IOC padrão para detetar dados comprometidos. A *tarefa verificação IOC padrão* é uma tarefa local ou de grupo que é criada e configurada manualmente na Consola Web. As tarefas são executadas utilizando IOC files preparados pelo utilizador. Se quiser adicionar manualmente um indicador de compromisso, leia os requisitos para os ficheiros do IOC.

O ficheiro que transfere através da ligação abaixo contém uma tabela com a lista completa dos termos IOC do padrão OpenIOC.

TRANSFERIR O FICHEIRO IOC_TERMS.XLSX

O Kaspersky Endpoint Security também suporta tarefas de verificação IOC independentes quando a aplicação é utilizada como parte da solução do Kaspersky Sandbox.

Criar ficheiro IOC

A partir do Kaspersky Endpoint Security 12.10 for Windows, pode criar ficheiros IOC diretamente nas definições da tarefa. Para criar um ficheiro IOC, deve preparar um ficheiro TXT com uma lista de indicadores de comprometimento. Pode adicionar listas dos seguintes objetos como indicadores de comprometimento:

- Hashes do ficheiro (MD5 / SHA256).

  A aplicação prepara um ficheiro IOC com um âmbito de verificação FileItem/Md5sum ou FileItem/Sha256sum.

- Endereços IP (IPv4, IPv6).

  A aplicação prepara um ficheiro IOC com um âmbito de verificação PortItem/RemoteIP.

- Nomes DNS.

  A aplicação prepara um ficheiro IOC com um âmbito de verificação DnsEntryItem/RecordName.

Como criar um ficheiro IOC na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Tasks**.

   A lista de tarefas é aberta.

2. Selecione a tarefa **IOC Scan**.

   É apresentada a janela de propriedades da tarefa. Se necessário, crie a tarefa **IOC Scan**.

3. Selecione o separador **Application settings**.

4. Aceda à secção **Threat Scan**.

5. Clique em **Redefine IOC files**.

6. Isto abre o formulário para criação de um ficheiro IOC:

   a. Em **IOC files source**, selecione **Generate from file**.

   b. Introduza o nome para o ficheiro IOC.

   c. Selecione um ficheiro TXT com uma lista de indicadores de comprometimento.

   d. Selecione o tipo de ficheiro IOC: **DNS names**, **File hashes**, **IP addresses**.

   e. Clique em **Upload**.

   O Kaspersky Endpoint Security adiciona ficheiros IOC à coleção IOC. Se necessário, pode excluir temporariamente os ficheiros IOC do âmbito da tarefa.

7. Guarde as suas alterações.

Criar uma tarefa IOC Scan

Pode criar tarefas *IOC Scan* manualmente:

- Nos detalhes do alerta (apenas para EDR Optimum).

  As *informações da deteção* é uma ferramenta para visualizar todas as informações recolhidas sobre uma ameaça detetada. As informações da deteção incluem, por exemplo, o histórico dos ficheiros que aparecem no computador. Para conhecer os detalhes sobre a gestão de deteção, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

- Utilizando o Assistente de Tarefas.

A tarefa de grupo *IOC Scan* não pode ser executada se a integração com o Kaspersky Endpoint Detection and Response Expert (on-premise) ou o Kaspersky Endpoint Detection and Response Expert (cloud) estiver configurada nos computadores que estão a ser verificados. Neste caso, recomendamos que utilize 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-premise).

Pode configurar a tarefa para o EDR Optimum na Consola Web e na Cloud Console. As definições da tarefa para o EDR Expert estão disponíveis apenas na Cloud Console.

Para criar uma tarefa IOC Scan:

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **IOC Scan**.

   c. No campo **Task name**, introduza uma breve descrição.

   d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Avance para o passo seguinte.

5. Introduza as credenciais da conta do utilizador cujos direitos deseja usar para executar a tarefa. Avance para o passo seguinte.

   Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com a conta de utilizador do sistema (SYSTEM).

A conta de sistema (SYSTEM) não tem a permissão para executar uma tarefa *IOC Scan* em unidades de rede. Se deseja executar a tarefa para uma unidade de rede, selecione a conta de utilizador que tem acesso a tal unidade.

Para tarefas de verificação IOC autónomas em unidades de rede, tem de selecionar manualmente a conta de utilizador que tem acesso a esta unidade nas propriedades da tarefa.

6. Conclua o assistente.

   Será apresentada uma nova tarefa na lista de tarefas.

7. Clique em nova tarefa.

   É apresentada a janela de propriedades da tarefa.

8. Selecione o separador **Application settings**.

9. Aceda à secção **Threat Scan**.

10. Carregue os ficheiros IOC para procurar indicadores de comprometimento.

    Após o carregamento dos ficheiros IOC, a aplicação apresenta informações resumidas sobre o ficheiro, incluindo a lista de indicadores que não passaram na verificação. Após carregar os ficheiros IOC, pode editá-los manualmente no editor integrado diretamente nas propriedades da tarefa. O Kaspersky Endpoint Security suporta a edição de ficheiros IOC compatíveis com o padrão OpenIOC 1.1. Não é possível modificar o conteúdo de ficheiros IOC compatíveis com a versão 1.0 do OpenIOC.

    O Kaspersky Endpoint Security adiciona ficheiros IOC à coleção IOC. Se necessário, pode excluir temporariamente os ficheiros IOC do âmbito da tarefa.

    Adicionar ou remover ficheiros IOC após a execução da tarefa não é recomendado. Isto pode originar uma apresentação incorreta dos resultados da verificação IOC relativos a execuções anteriores da tarefa. Para pesquisar indicadores de compromisso por novos ficheiros IOC, recomenda-se a adição de novas tarefas.

11. Se necessário, selecione a caixa de verificação **Retrospective IOC Scan**. A *Verificação retrospetiva dos IOC* é um modo da tarefa *IOC Scan* na qual o Kaspersky Endpoint Security verifica indicadores de comprometimento usando dados de um determinado período de tempo. Este modo destina-se à pesquisa de indicadores de comprometimento através dos dados de telemetria do computador protegido, tais como atividade de rede, processos, ficheiros e outros dados de telemetria. O Kaspersky Endpoint Security analisa os dados nos registos do sistema operativo e nos registos do navegador no computador. A Verificação retrospetiva dos IOC analisa os registos dos seguintes navegadores: Google Chrome, Mozilla Firefox, Microsoft Edge (versão 79 ou posterior).

12. Configure ações na deteção de IOC:

    - **Isolate device from the network**. Se esta opção for selecionada, o Kaspersky Endpoint Security isola o computador da rede para evitar que a ameaça se espalhe. Pode configurar a duração do isolamento em Definições do componente Endpoint Detection and Response.

      Se esta caixa de seleção estiver desmarcada, poderá isolar o computador da rede depois de executar a tarefa manualmente. Se a tarefa *IOC Scan* deteta um IOC, pode isolar o computador da rede diretamente do IOC (propriedades da tarefa *IOC Scan* → **Application settings** → **IOC Scan results**). O Kaspersky Endpoint Security também permite gerir imediatamente configurações adicionais: Período de desativação do isolamento da rede e Exclusões de isolamento da rede.

- **Move copy to Quarantine, delete object**. Se esta opção for selecionada, o Kaspersky Endpoint Security elimina o objeto malicioso encontrado no computador. Antes de eliminar o objeto, o Kaspersky Endpoint Security cria uma cópia de segurança, caso o objeto precise de ser posteriormente restaurado. O Kaspersky Endpoint Security move a cópia de segurança para a Quarentena.

  Se esta caixa de seleção estiver desmarcada, poderá colocar o ficheiro em quarentena manualmente após executar a tarefa manualmente. Se a tarefa *IOC Scan* deteta um ficheiro que pode comprometer os dados, pode colocar este ficheiro em quarentena diretamente dos resultados da verificação IOC (**Application settings → IOC Scan results**). Como resultado, o Kaspersky Endpoint Security inicia o assistente de criação de tarefas com dados predefinidos do ficheiro detetado. Só precisa gerir as configurações de tarefas adicionais, por exemplo, configurar o agendamento de tarefas.

  Se necessário, selecione a caixa de seleção **Apply to system critical objects**. Os System Critical Objects (SCO) incluem ficheiros necessários ao funcionamento do sistema operativo.

  Não recomendamos a aplicação de ações aos ficheiros SCO. Isto pode tornar o sistema operativo instável ou impedir o respetivo arranque.

- **Run Critical Areas Scan**. Se esta opção for selecionada, o Kaspersky Endpoint Security executa a tarefa *Critical Areas Scan*. Por predefinição, o Kaspersky Endpoint Security verifica a memória Kernel, os processos em execução e os setores de inicialização do disco.

13. Aceda à secção **Advanced**.

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 *IOC Scan* em conformidade com o conteúdo dos IOC files carregados. Não é recomendado remover a seleção de tipos de dados.

    Adicionalmente, pode configurar âmbitos de verificação para os seguintes tipos de dados:

    - **Files - FileItem**. Defina o âmbito de verificação IOC no computador utilizando âmbitos predefinidos.

      Por predefinição, o Kaspersky Endpoint Security verifica IOC apenas em áreas importantes do computador, tais como a pasta de transferências, o ambiente de trabalho, a pasta com ficheiros temporários do sistema operativo, etc. Pode também adicionar manualmente o âmbito de verificação.

    - **Windows Event Log - EventLogItem**. Introduza o período de tempo no qual os eventos foram registados. Também pode selecionar os registos de eventos do Windows que devem ser utilizados para a verificação IOC. Por defeito, são selecionados os seguintes registos de eventos: registo de eventos da aplicação, registo de eventos do sistema e registo de eventos de segurança.

      Para o termo IOC EventLogItem\source, utilize o valor **Nome do fornecedor** do esquema XML do evento.

    - **Windows Registry - RegistryItem**. Configure o âmbito de verificação IOC no registo.

      Por defeito, o Kaspersky Endpoint Security verifica um conjunto de chaves de registo.

15. Na janela de propriedades da tarefa, selecione o separador **Schedule**.

16. Configure o agendamento da tarefa.

> Wake-on-LAN não está disponível para esta tarefa. Certifique-se de que o computador está ligado para executar a tarefa.

17. Guarde as suas alterações.

18. Selecione a caixa de verificação junto à tarefa.

19. Clique em **Start**.

Deste modo, o Kaspersky Endpoint Security procura indicadores de comprometimento do computador. Pode visualizar os resultados da tarefa nas propriedades da tarefa na secção **Results**. Pode consultar a informação sobre os indicadores de comprometimento detetados nas propriedades da tarefa: **Application settings** → **IOC Scan results**. Nos resultados da verificação IOC, também pode colocar manualmente o ficheiro detetado em quarentena ou isolar o computador da rede.

O Kaspersky Endpoint Security procura duplicados entre os registos criados para o mesmo ficheiro IOC e mantém apenas registos únicos nos resultados da tarefa. Duplicados são registos do mesmo tipo que têm os mesmos valores em todos os campos comparados. A aplicação também pode não criar um registo se faltar um valor em um ou mais campos (consulte a tabela abaixo).

Tipo	Campos comparados	Condição para não criar um registo
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• Valor em falta dos campos FullPath, Md5sum, Sha256sum. • Valores em falta do campo FullPath e valores idênticos dos campos Md5sum, Sha256sum.
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	Valor em falta em, pelo menos, um dos seguintes campos: Hive, KeyPath, ValueName.
ProcessarItem	• startTime • PID	Valores em falta dos campos startTime ou PID.

> A janela **Alert Details** pode exibir registos RegistryItem com valores de campo idênticos. Esses registos não são duplicados porque têm valores diferentes no campo Texto, que não é apresentado na interface.

> Os resultados da verificação IOC são mantidos durante 30 dias. Após este período, o Kaspersky Endpoint Security elimina automaticamente as entradas mais antigas.

Telemetria estendida para Verificação IOC

Recomendamos ativar a telemetria estendida no computador para a verificação retrospetiva do IOC. A telemetria estendida melhora a precisão da deteção de IOC, mas utiliza mais recursos do computador.

A telemetria estendida inclui o suporte aos seguintes termos adicionais:

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

Se a telemetria estendida estiver desativada, o Kaspersky Endpoint Security poderá alternar as informações sobre os indicadores de comprometimento detetados.

Para ativar a telemetria estendida:

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Selecione a caixa de verificação **Enable advanced system activity logging**.
6. Guarde as suas alterações.

Mover ficheiro para Quarentena

Ao reagir a ameaças, o Kaspersky Endpoint Detection and Response pode criar tarefas *Move file to Quarantine*. Isto é necessário para minimizar as consequências da ameaça. *Quarentena* é um armazenamento local especial no computador. O utilizador pode colocar em quarentena ficheiros que considere perigosos para o computador. Os ficheiros na quarentena são armazenados num estado encriptado e não põem em risco a segurança do dispositivo. O Kaspersky Endpoint Security utiliza a Quarentena apenas quando integrado com as soluções Kaspersky Detection and Response. Em todos os outros casos, o Kaspersky Endpoint Security coloca o ficheiro pertinentes na Cópia de Segurança. Para obter mais informações sobre a gestão da Quarentena como parte das soluções, consulte Ajuda do Kaspersky Sandbox, Ajuda do Kaspersky Endpoint Detection and Response Optimum e Ajuda do Kaspersky Endpoint Detection and Response Expert, Ajuda do Kaspersky Anti Targeted Attack Platform e Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises).

Pode criar tarefas *Move file to Quarantine* dos seguintes modos:

- Nos detalhes do alerta (apenas para EDR Optimum).

  As *informações da deteção* é uma ferramenta para visualizar todas as informações recolhidas sobre uma ameaça detetada. As informações da deteção incluem, por exemplo, o histórico dos ficheiros que aparecem no computador. Para conhecer os detalhes sobre a gestão de deteção, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

- Utilizando o Assistente de Tarefas.

  Deve introduzir o hash (SHA256 ou MD5) ou caminho do ficheiro, ou o caminho do ficheiro e o hash do ficheiro.

- Nas definições da tarefa *IOC Scan*.

  Se a tarefa *IOC Scan* deteta um ficheiro que pode comprometer os dados, pode colocar este ficheiro em quarentena diretamente dos resultados da verificação IOC (**Application settings** → **IOC Scan results**). Como resultado, o Kaspersky Endpoint Security inicia o assistente de criação de tarefas com dados predefinidos do ficheiro detetado. Só precisa gerir as configurações de tarefas adicionais, por exemplo, configurar o agendamento de tarefas.

A tarefa *Move file to Quarantine* tem as seguintes limitações:

1. O tamanho do ficheiro não deve exceder 100 MB.
2. Não pode eliminar ficheiros necessários ao funcionamento do Kaspersky Endpoint Security for Windows:
   - Ficheiros abrangidos pela tecnologia de Autodefesa do Kaspersky Endpoint Security for Windows
   - Ficheiros assinados digitalmente pela Kaspersky
3. Pode configurar a tarefa para o EDR Optimum na Consola Web e na Cloud Console. As definições da tarefa para o EDR Expert estão disponíveis apenas na Cloud Console.
4. Não pode verificar um objeto colocado em quarentena como resultado da tarefa *Move file to Quarantine*.

Para criar uma tarefa Move file to Quarantine:

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **Move file to Quarantine**.

   c. No campo **Task name**, introduza uma breve descrição.

   d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Clique em **Next**.

5. Introduza as credenciais da conta do utilizador cujos direitos deseja usar para executar a tarefa. Clique em **Next**.

   Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com a conta de utilizador do sistema (SYSTEM).

6. Termine o assistente clicando no botão **Finish**.

   Será apresentada uma nova tarefa na lista de tarefas.

7. Clique em nova tarefa.

   É apresentada a janela de propriedades da tarefa.

8. Selecione o separador **Application settings**.

9. Se necessário, selecione a caixa de verificação **Apply to system critical objects**.

   Os System Critical Objects (SCO) incluem ficheiros necessários ao funcionamento do sistema operativo.

   Não recomendamos a aplicação de ações aos ficheiros SCO. Isto pode tornar o sistema operativo instável ou impedir o respetivo arranque.

10. Na lista de ficheiros, clique em **Add**.

    O assistente para adicionar ficheiros é iniciado.

11. Para adicionar o ficheiro, tem de introduzir o caminho completo para o ficheiro, ou o hash do ficheiro e o caminho.

    Se o ficheiro estiver localizado numa unidade de rede, introduza o caminho do ficheiro a partir dos caracteres `\\` e não da letra da unidade. Por exemplo, `\\server\shared_folder\file.exe`. Se o caminho do ficheiro contiver a letra da unidade de rede, pode ser apresentado um erro *Ficheiro não encontrado*.

12. Na janela de propriedades da tarefa, selecione o separador **Schedule**.

13. Configure o agendamento da tarefa.

    Wake-on-LAN não está disponível para esta tarefa. Certifique-se de que o computador está ligado para executar a tarefa.

14. Guarde as suas alterações.

15. Selecione a caixa de verificação junto à tarefa.

16. Clique em **Start**.

Deste modo, o Kaspersky Endpoint Security move o ficheiro para a Quarentena.

Se o ficheiro estiver bloqueado por um processo diferente, a tarefa será apresentada como Done, mas o próprio ficheiro só é movido para a Quarentena depois de o computador ser reiniciado. Após reiniciar o computador, confirme se o ficheiro foi eliminado.

Se o ficheiro estiver bloqueado por um processo diferente, a tarefa será apresentada como *Completed*, mas o próprio ficheiro só é movido para quarentena depois de o computador ser reiniciado. Após reiniciar o computador, confirme se o ficheiro foi eliminado.

A tarefa *Move file to Quarantine* pode terminar apresentando o erro *Acesso recusado* se estiver a tentar mover para quarentena um ficheiro executável que está em execução. Crie uma tarefa Terminação de Processo para o ficheiro e tente novamente.

A tarefa *Move file to Quarantine* pode terminar apresentando o erro *Espaço insuficiente no armazenamento da Quarentena* se estiver a tentar mover para quarentena um ficheiro demasiado grande. Esvazie a Quarentena ou aumente o espaço da Quarentena. E depois tente novamente.

Pode restaurar um ficheiro da Quarentena ou esvaziar a Quarentena utilizando a Consola Web. Pode restaurar objetos localmente no computador utilizando a Command line.

Obter ficheiro

Pode obter ficheiros dos computadores dos utilizadores. Por exemplo, pode configurar a obtenção de um ficheiro de registo de eventos criado por uma aplicação de terceiros. Como resultado da execução da tarefa, uma cópia do ficheiro é guardada na Quarentena. *Quarentena* é um armazenamento local especial no computador. Pode transferir este ficheiro da Quarentena para o seu computador utilizando a Consola Web (**Operations** → **Repositories** → **Quarantine**). No computador do utilizador, o ficheiro permanece na sua pasta original.

O tamanho do ficheiro não deve exceder 2 GB.

Pode configurar a tarefa para o EDR Optimum na Consola Web e na Cloud Console. As definições da tarefa para o EDR Expert estão disponíveis apenas na Cloud Console.

Para criar uma tarefa Obter ficheiro:

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **Get file**.

   c. No campo **Task name**, introduza uma breve descrição.

   d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Clique em **Next**.
5. Introduza as credenciais da conta do utilizador cujos direitos deseja usar para executar a tarefa. Clique em **Next**.

   Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com a conta de utilizador do sistema (SYSTEM).

6. Termine o assistente clicando no botão **Finish**.

   Será apresentada uma nova tarefa na lista de tarefas.

7. Clique em nova tarefa.

   É apresentada a janela de propriedades da tarefa.

8. Selecione o separador **Application settings**.
9. Na lista de ficheiros, clique em **Add**.

   O assistente para adicionar ficheiros é iniciado.

10. Para adicionar o ficheiro, tem de introduzir o caminho completo para o ficheiro, ou o hash do ficheiro e o caminho.

    Se o ficheiro estiver localizado numa unidade de rede, introduza o caminho do ficheiro a partir dos caracteres `\\` e não da letra da unidade. Por exemplo, `\\server\shared_folder\file.exe`. Se o caminho do ficheiro contiver a letra da unidade de rede, pode ser apresentado um erro *Ficheiro não encontrado*.

11. Na janela de propriedades da tarefa, selecione o separador **Schedule**.
12. Configure o agendamento da tarefa.

    Wake-on-LAN não está disponível para esta tarefa. Certifique-se de que o computador está ligado para executar a tarefa.

13. Guarde as suas alterações.
14. Selecione a caixa de verificação junto à tarefa.
15. Clique em **Start**.

    Deste modo, o Kaspersky Endpoint Security cria uma cópia do ficheiro e move tal cópia para a Quarentena. Pode transferir o ficheiro da Quarentena na Consola Web.

Delete file

Pode eliminar ficheiros remotamente utilizando a tarefa *Delete file*. Por exemplo, pode eliminar um ficheiro remotamente ao responder a ameaças.

Não pode eliminar ficheiros necessários ao funcionamento do Kaspersky Endpoint Security for Windows:

- Ficheiros abrangidos pela tecnologia de Autodefesa do Kaspersky Endpoint Security for Windows
- Ficheiros assinados digitalmente pela Kaspersky

Pode configurar a tarefa para o EDR Optimum na Consola Web e na Cloud Console. As definições da tarefa para o EDR Expert estão disponíveis apenas na Cloud Console.

Para criar uma tarefa Delete file:

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **Delete file**.

   c. No campo **Task name**, introduza uma breve descrição.

   d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Clique em **Next**.

5. Introduza as credenciais da conta do utilizador cujos direitos deseja usar para executar a tarefa. Clique em **Next**.

   Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com a conta de utilizador do sistema (SYSTEM).

6. Termine o assistente clicando no botão **Finish**.

   Será apresentada uma nova tarefa na lista de tarefas.

7. Clique em nova tarefa.

   É apresentada a janela de propriedades da tarefa.

8. Selecione o separador **Application settings**.

9. Para adicionar o ficheiro, tem de introduzir o caminho completo para o ficheiro, ou o hash do ficheiro e o caminho.

   Se o ficheiro estiver localizado numa unidade de rede, introduza o caminho do ficheiro a partir dos caracteres `\\` e não da letra da unidade. Por exemplo, `\\server\shared_folder\file.exe`. Se o caminho do ficheiro contiver a letra da unidade de rede, pode ser apresentado um erro *Ficheiro não encontrado*.

10. Se necessário, selecione a caixa de verificação **Apply to system critical objects**.

    Os System Critical Objects (SCO) incluem ficheiros necessários ao funcionamento do sistema operativo.

    Não recomendamos a aplicação de ações aos ficheiros SCO. Isto pode tornar o sistema operativo instável ou impedir o respetivo arranque.

11. Na janela de propriedades da tarefa, selecione o separador **Schedule**.

12. Configure o agendamento da tarefa.

    Wake-on-LAN não está disponível para esta tarefa. Certifique-se de que o computador está ligado para executar a tarefa.

13. Guarde as suas alterações.

14. Selecione a caixa de verificação junto à tarefa.

15. Clique em **Start**.

    Deste modo, o Kaspersky Endpoint Security elimina o ficheiro do computador. Se o ficheiro estiver bloqueado por um processo diferente, a tarefa será apresentada como *Done*, mas o próprio ficheiro só é eliminado depois de o computador ser reiniciado. Após reiniciar o computador, confirme se o ficheiro foi eliminado.

A tarefa *Delete file* pode terminar apresentando o erro *Access denied or file not found* se estiver a tentar eliminar um ficheiro executável que está em execução. Crie uma tarefa Terminação de Processo para o ficheiro e tente novamente.

Início do Processo

Pode executar ficheiros remotamente utilizando a tarefa *Process start*. Por exemplo, pode executar remotamente um utilitário que cria o ficheiro de configuração do computador. Em seguida, pode utilizar a tarefa *Get file* para receber o ficheiro criado na Consola Web do Kaspersky Security Center.

Pode configurar a tarefa para o EDR Optimum na Consola Web e na Cloud Console. As definições da tarefa para o EDR Expert estão disponíveis apenas na Cloud Console.

Para criar uma tarefa Process start:

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **Process start**.

   c. No campo **Task name**, introduza uma breve descrição.

   d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Clique em **Next**.

5. Introduza as credenciais da conta do utilizador cujos direitos deseja usar para executar a tarefa. Clique em **Next**.

   Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com a conta de utilizador do sistema (SYSTEM).

6. Termine o assistente clicando no botão **Finish**.

   Será apresentada uma nova tarefa na lista de tarefas.

7. Clique em nova tarefa.

8. É apresentada a janela de propriedades da tarefa.

9. Selecione o separador **Application settings**.

10. Introduza o comando de início do processo.

    Vamos supor que deseja executar um utilitário (`utility.exe`) que guarda as informações sobre a configuração do computador num ficheiro chamado `conf.txt` na pasta atual (por padrão). O utilitário está na pasta `C:\Users\admin\Diagnostic\`. Tem de guardar o ficheiro de configuração na pasta `C:\Users\admin\Documents\Configuration`. Insira os seguintes valores:

    - **Executable command** – `C:\Users\admin\Diagnostic\utility.exe`
    - **Command line arguments (optional)** – `/R conf.txt`
    - **Path to the working folder (optional)** – `C:\Users\admin\Documents\Configuration`

11. Na janela de propriedades da tarefa, selecione o separador **Schedule**.

12. Configure o agendamento da tarefa.

    Wake-on-LAN não está disponível para esta tarefa. Certifique-se de que o computador está ligado para executar a tarefa.

13. Guarde as suas alterações.

14. Selecione a caixa de verificação junto à tarefa.

15. Clique em **Start**.

Deste modo, o Kaspersky Endpoint Security executa o comando no modo silencioso e inicia o processo. Pode visualizar os resultados da tarefa nas propriedades da tarefa na secção **Execution results**.

Terminação de Processo

Pode terminar processos remotamente utilizando a tarefa *Terminate process*. Por exemplo, pode terminar remotamente um utilitário de teste de velocidade da Internet que foi iniciado utilizando a tarefa *Executar processo*.

Se pretende proibir a execução de um ficheiro, pode configurar o componente de prevenção da execução. Pode proibir a execução de ficheiros executáveis, scripts, ficheiros de formato do Office.

A tarefa *Terminate process* tem as seguintes limitações:

Não pode terminar processos de ficheiros necessários ao funcionamento do Kaspersky Endpoint Security for Windows:

- Ficheiros abrangidos pela tecnologia de Autodefesa do Kaspersky Endpoint Security for Windows
- Ficheiros assinados digitalmente pela Kaspersky

Pode configurar a tarefa para o EDR Optimum na Consola Web e na Cloud Console. As definições da tarefa para o EDR Expert estão disponíveis apenas na Cloud Console.

Para criar uma tarefa Terminate process:

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **Add**.

   O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

   a. Na lista pendente **Application**, selecione **Kaspersky Endpoint Security for Windows 14.2**.

   b. Na lista pendente **Task type**, selecione **Terminate process**.

   c. No campo **Task name**, introduza uma breve descrição.

   d. No bloco **Devices to which the task will be assigned**, selecione o âmbito de tarefa.

4. Selecione os dispositivos de acordo com a opção do âmbito da tarefa selecionada. Clique em **Next**.

5. Introduza as credenciais da conta do utilizador cujos direitos deseja usar para executar a tarefa. Clique em **Next**.

   Por predefinição, o Kaspersky Endpoint Security inicia a tarefa com a conta de utilizador do sistema (SYSTEM).

6. Termine o assistente clicando no botão **Finish**.

   Será apresentada uma nova tarefa na lista de tarefas.

7. Clique em nova tarefa.

   É apresentada a janela de propriedades da tarefa.

8. Selecione o separador **Application settings**.

9. Se necessário, selecione a caixa de verificação **Apply to system critical objects**.

   Os System Critical Objects (SCO) incluem ficheiros necessários ao funcionamento do sistema operativo.

   Não recomendamos a aplicação de ações aos ficheiros SCO. Isto pode tornar o sistema operativo instável ou impedir o respetivo arranque.

10. Para concluir o processo, tem de selecionar o ficheiro que deseja terminar. Pode selecionar um ficheiro através de uma das seguintes formas:

    - Introduza o nome completo do ficheiro.
    - Introduza o hash do ficheiro e o caminho para o ficheiro.
    - Introduza o PID do processo (apenas para tarefas locais).
    - Se o ficheiro estiver localizado numa unidade de rede, introduza o caminho do ficheiro a partir dos caracteres `\\` e não da letra da unidade. Por exemplo, `\\server\shared_folder\file.exe`. Se o caminho do ficheiro contiver a letra da unidade de rede, pode ser apresentado um erro *Ficheiro não encontrado*.

    Se o ficheiro estiver localizado numa unidade de rede, introduza o caminho do ficheiro a partir dos caracteres `\\` e não da letra da unidade. Por exemplo, `\\server\shared_folder\file.exe`. Se o caminho do ficheiro contiver a letra da unidade de rede, pode ser apresentado um erro *File not found*.

11. Na janela de propriedades da tarefa, selecione o separador **Schedule**.

12. Configure o agendamento da tarefa.

    Wake-on-LAN não está disponível para esta tarefa. Certifique-se de que o computador está ligado para executar a tarefa.

13. Clique em **Save**.

14. Selecione a caixa de verificação junto à tarefa.

15. Clique em **Start**.

Deste modo, o Kaspersky Endpoint Security termina o processo no computador. Por exemplo, se a aplicação GAME estiver a ser executada e terminar o processo game.exe, a aplicação é fechada sem guardar os dados. Pode visualizar os resultados da tarefa nas propriedades da tarefa na secção **Results**.

Prevenção da execução

A prevenção da execução permite gerir a execução de scripts e ficheiros executáveis, bem como a abertura de ficheiros do formato do Office. Deste modo, pode, por exemplo, prevenir a execução de aplicações que não considera seguras. Como resultado, a propagação da ameaça pode ser interrompida. A prevenção da execução suporta um conjunto de extensões de ficheiros Office e um conjunto de interpretadores de script.

Regra de bloqueio de execução

A prevenção da execução gere o acesso do utilizador a ficheiros com regras de bloqueio de execução. A *Regra de bloqueio de execução* é um conjunto de critérios que a aplicação tem em consideração ao reagir à execução de um objeto, por exemplo, ao bloquear a execução de um objeto. A aplicação identifica ficheiros pelos seus caminhos ou somas de verificação calculadas utilizando algoritmos hash MD5 e SHA256.

Pode criar regras de bloqueio de execução:

- Nos detalhes do alerta (apenas para EDR Optimum).

  As *informações da deteção* é uma ferramenta para visualizar todas as informações recolhidas sobre uma ameaça detetada. As informações da deteção incluem, por exemplo, o histórico dos ficheiros que aparecem no computador. Para conhecer os detalhes sobre a gestão de deteção, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

- Utilizando uma política de grupo ou definições de aplicações locais.

  Deve introduzir o caminho ou o hash do ficheiro (SHA256 ou MD5), ou o caminho da pasta e o hash do ficheiro.

Também pode gerir a prevenção da execução localmente utilizando a command line.

A prevenção de execução tem as seguintes limitações:

1. As regras de prevenção não abrangem os ficheiros em CD ou imagens ISO. A aplicação não bloqueia a execução ou abertura de tais ficheiros.
2. Não pode aplicar uma regra de prevenção a ficheiros necessários ao funcionamento do Kaspersky Endpoint Security for Windows:
   - Ficheiros abrangidos pela tecnologia de Autodefesa do Kaspersky Endpoint Security for Windows
   - Ficheiros assinados digitalmente pela Kaspersky
3. Não é recomendado criar mais de 5000 regras de prevenção de execução, uma vez que tal pode provocar instabilidade do sistema.

Modos da regra de bloqueio de execução

O componente de prevenção da execução tem dois modos de funcionamento:

- **Apenas estatísticas**

  Neste modo, o Kaspersky Endpoint Security publica um evento sobre tentativas de execução de objetos executáveis ou abrir documentos que correspondem aos critérios da regra de prevenção no Registo de Eventos do Windows e no Kaspersky Security Center, mas não bloqueia a tentativa de executar ou abrir o objeto ou documento. Esta modo está selecionado por predefinição.

- **Ativo**

  Neste modo, a aplicação bloqueia a execução de objetos ou a abertura de documentos que correspondam aos critérios da regra de prevenção. A aplicação também publica um evento sobre tentativas de execução de objetos ou documentos abertos no Registo de Eventos do Windows e no Registo de Eventos do Kaspersky Security Center.

Gestão de prevenção de execução

Apenas pode configurar as definições do componente na Consola Web.

Para prevenção da execução:

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Selecione o separador **Execution Prevention**.
6. Ative o botão de alternar **Execution Prevention ENABLED**.
7. No bloco **Action on execution or opening of forbidden object**, selecione o modo de operação do componente:

   - **Block and add to event log**. Neste modo, a aplicação bloqueia a execução de objetos ou a abertura de documentos que correspondam aos critérios da regra de prevenção. A aplicação também publica um evento sobre tentativas de execução de objetos ou documentos abertos no Registo de Eventos do Windows e no Registo de Eventos do Kaspersky Security Center.

     Se necessário, selecione a caixa de seleção **Apply to system critical objects**. Os System Critical Objects (SCO) incluem ficheiros necessários ao funcionamento do sistema operativo.

Não recomendamos a aplicação de ações aos ficheiros SCO. Isto pode tornar o sistema operativo instável ou impedir o respetivo arranque.

- **Add to event log**. Neste modo, o Kaspersky Endpoint Security publica um evento sobre tentativas de execução de objetos executáveis ou abrir documentos que correspondem aos critérios da regra de prevenção no Registo de Eventos do Windows e no Kaspersky Security Center, mas não bloqueia a tentativa de executar ou abrir o objeto ou documento. Esta modo está selecionado por predefinição.

8. Crie uma lista de regras de bloqueio de execução:

   a. Clique em **Add**.

   b. Esta ação abre uma janela; nesta janela, introduza o nome da regra de bloqueio de execução (por exemplo, *aplicação A*).

   c. Na lista pendente **Type**, selecione o objeto que pretende bloquear: **Executable file**, **Script**, **Microsoft Office document**.

   Se selecionar um tipo de objeto errado, o Kaspersky Endpoint Security não bloqueia o ficheiro ou script.

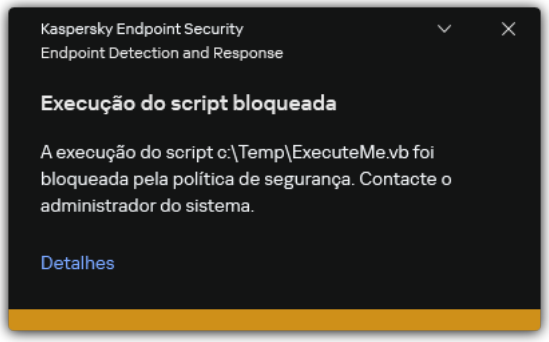
   d. Para adicionar o ficheiro, deve introduzir o hash do ficheiro (SHA256 ou MD5), o caminho completo para o ficheiro ou o hash e o caminho da pasta.

   Se o ficheiro estiver localizado numa unidade de rede, introduza o caminho do ficheiro a partir dos caracteres `\\` e não da letra da unidade. Por exemplo, `\\server\shared_folder\file.exe`. Se o caminho do ficheiro contiver uma letra da unidade de rede, o Kaspersky Endpoint Security não bloqueia o ficheiro ou script.

   A prevenção da execução suporta um conjunto de extensões de ficheiros Office e um conjunto de interpretadores de script.

9. Guarde as suas alterações.

Deste modo, o Kaspersky Endpoint Security bloqueia a execução de objetos: execução de scripts e ficheiros executáveis, abertura de ficheiros do formato do Office. No entanto, ainda que a execução do script esteja bloqueada, pode, por exemplo, abrir o ficheiro script file num editor de texto. Ao bloquear a execução de um objeto, o Kaspersky Endpoint Security apresenta uma notificação padrão (ver figura abaixo) se as notificações estiverem ativadas nas definições da aplicação.



Notificação de prevenção de execução

Isolamento da rede do computador

O isolamento da rede do computador permite isolar automaticamente um computador da rede em resposta à deteção de um indicador de comprometimento (IOC) – este é o *modo automático*. Pode ativar o Isolamento da rede manualmente enquanto investiga a ameaça detetada – este é o *modo manual*.

Quando o isolamento da rede é ativado, a aplicação interrompe todas as ligações ativas e bloqueia todas as novas ligações de rede TCP/IP no computador, exceto as seguintes:

- Ligações listadas em Network isolation exclusions.
- Ligações iniciadas pelos serviços do Kaspersky Endpoint Security.
- Ligações iniciadas pelo Kaspersky Security Center Network Agent.
- Ligações ao SVM e ao Servidor de Integração se a aplicação estiver a ser utilizada no modo Light Agent.
- Ligações ao KSN ao integrar a aplicação com o Kaspersky Managed Detection and Response.

Apenas pode configurar as definições do componente na Consola Web.

Modo de Isolamento da rede automático

Pode configurar a ativação automática do isolamento da rede em resposta a uma deteção de IOC. Pode configurar o modo de Isolamento da rede automático com uma política de grupo.

Como configurar a ativação automática do isolamento da rede em resposta a uma deteção de IOC

1. Na janela principal da Consola Web, selecione **Asset management** → **Tasks**.

   A lista de tarefas é aberta.

2. Clique na tarefa **IOC Scan** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

   Se necessário, crie a tarefa *IOC Scan*.

3. Selecione o separador **Application settings**.

4. Selecione a secção **Response settings**.

5. No bloco **Configure response actions on IOC detection**, selecione **Alert and response** e assinale a caixa de verificação **Isolate device from the network**.

6. Guarde as suas alterações.

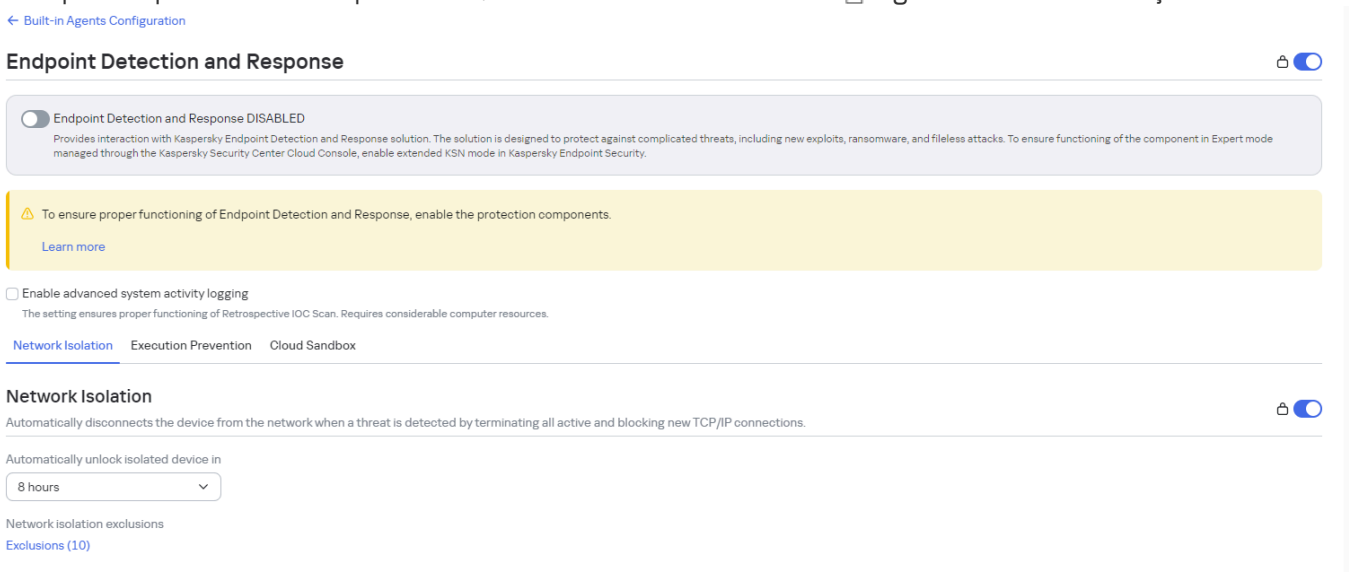
Deste modo, sempre que um IOC é detetado, a aplicação isola o computador da rede para prevenir que a ameaça se espalhe.

pode configurar o isolamento da rede automático para ser desativado após um determinado período de tempo. Por predefinição, a aplicação desativa o isolamento da rede 8 horas após este ter sido ativado. Também pode desativar manualmente o Isolamento da rede (consulte as instruções abaixo). Após desativar o isolamento da rede, o computador pode utilizar a rede sem restrições.

Como configurar o atraso da desativação do Isolamento da rede de um computador no modo automático

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Selecione o separador **Network Isolation**.
6. Selecione o atraso para desativar o isolamento de rede.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.



Definições de integração EDR

Modo de Isolamento da rede manual

Pode ativar e desativar manualmente o isolamento da rede. Pode configurar o modo de Isolamento da rede manual através das propriedades do computador na consola do Kaspersky Security Center.

Pode ativar o isolamento da rede:

- Nos detalhes do alerta (apenas para EDR Optimum).

  As *informações da deteção* é uma ferramenta para visualizar todas as informações recolhidas sobre uma ameaça detetada. As informações da deteção incluem, por exemplo, o histórico dos ficheiros que aparecem no computador. Para conhecer os detalhes sobre a gestão de deteção, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.
- Utilizando as definições da aplicação locais.

- Nas definições da tarefa *IOC Scan*.

  Se a tarefa *IOC Scan* deteta um IOC, pode isolar o computador da rede diretamente do IOC (propriedades da tarefa *IOC Scan* → **Application settings** → **IOC Scan results**). O Kaspersky Endpoint Security também permite gerir imediatamente configurações adicionais: Período de desativação do isolamento da rede e Exclusões de isolamento da rede.

Como ativar manualmente o isolamento da rede de um computador

1. Na janela principal da Consola Web, selecione **Asset management** → **Assets (Devices)**.
2. Selecione um computador para o qual quer configurar definições da aplicação locais.

   As propriedades do computador são apresentadas.
3. Selecione o separador **Applications**.
4. Clique em **Kaspersky Endpoint Security for Windows 14.2**.

   As definições da aplicação locais são apresentadas.
5. Selecione o separador **Application settings**.
6. Aceda a **Detection and Response** → **Endpoint Detection and Response**.
7. No bloco **Network isolation**, clique **Isolate computer from the network**.

pode configurar o isolamento da rede automático para ser desativado após um determinado período de tempo. Por predefinição, a aplicação desativa o isolamento da rede 8 horas após este ter sido ativado. Após desativar o isolamento da rede, o computador pode utilizar a rede sem restrições.

Como configurar o atraso da desativação do Isolamento da rede de um computador no modo manual

1. Na janela principal da Consola Web, selecione **Asset management** → **Assets (Devices)**.
2. Selecione um computador para o qual quer configurar definições da aplicação locais.

   As propriedades do computador são apresentadas.
3. Selecione o separador **Tasks**.

   Esta opção apresenta a lista de tarefas disponíveis no computador.
4. Selecione a tarefa **Network Isolation**.
5. Selecione o separador **Application settings**.
6. Isto abre uma janela; nesta janela, selecione o atraso para desativar o Isolamento da rede.
7. Guarde as suas alterações.

Como desativar manualmente o isolamento da rede de um computador

1. Na janela principal da Consola Web, selecione **Asset management** → **Assets (Devices)**.
2. Selecione um computador para o qual quer configurar definições da aplicação locais.

   As propriedades do computador são apresentadas.
3. Selecione o separador **Applications**.

4. Clique em **Kaspersky Endpoint Security for Windows 14.2**.

   As definições da aplicação locais são apresentadas.

5. Selecione o separador **Application settings**.

6. Aceda a **Built-in Agents Configuration** → **Endpoint Detection and Response**.

7. No bloco **Network Isolation**, clique **Unblock computer isolated from the network**.

Também pode desativar localmente o isolamento da rede utilizando a Command line.

A partir do Kaspersky Endpoint Security 12.10 for Windows, pode gerir o Isolamento da rede nos detalhes do alerta. Além disso, nos detalhes do alerta, pode especificar o período de isolamento da rede do computador. Para conhecer os detalhes sobre a gestão de deteção, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

Network isolation exclusions

Pode configurar as exclusões de isolamento da rede. Quando o isolamento da rede está ativado, as ligações de rede que correspondem às regras não são bloqueadas no computador.

Para configurar as exclusões de isolamento da rede, pode utilizar uma lista de *perfis de rede padrão*. Por predefinição, as exclusões incluem perfis de rede que contêm regras que garantem a operação ininterrupta de dispositivos com o servidor DNS/DHCP e funções de cliente DNS/DHCP. Também pode modificar as definições dos perfis de rede padrão ou definir exclusões manualmente (consulte as instruções abaixo).

As exclusões especificadas nas propriedades da política são aplicáveis apenas se o isolamento da rede for ativado automaticamente em resposta a uma ameaça detetada. As exclusões especificadas nas propriedades do computador são aplicáveis apenas se o isolamento da rede for ativado manualmente nas propriedades do computador na Consola do Kaspersky Security Center ou nos detalhes do alerta.

Uma política ativa não previne a aplicação de exclusões do isolamento da rede configuradas nas propriedades do computador, uma vez que tais parâmetros têm diferentes cenários de utilização.

Como adicionar uma exclusão de Isolamento da rede no modo automático

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Built-in Agents Configuration** → **Endpoint Detection and Response**.

5. Selecione o separador **Network Isolation**.

6. No bloco **Network isolation exclusions**, clique **Exclusions**.

7. Esta ação abre uma janela; nesta janela, clique em **Add** → **Add from profile** e selecione os perfis de rede padrão para configurar as exclusões.

   As exclusões de isolamento da rede do perfil são adicionadas à lista de exclusões de isolamento da rede. Pode ver as propriedades das ligações de rede. Se necessário, pode modificar as definições da ligação de rede.

8. Se necessário, pode adicionar uma exclusão de isolamento da rede manualmente. Para tal, na janela da lista de exclusões, clique em **Add** → **Add** e edite manualmente as definições da ligação de rede.

9. Guarde as suas alterações.

Como adicionar uma exclusão de Isolamento da rede no modo manual

1. Na janela principal da Consola Web, selecione **Asset management** → **Assets (Devices)**.

2. Selecione um computador para o qual quer configurar definições da aplicação locais.

   As propriedades do computador são apresentadas.

3. Selecione o separador **Tasks**.

   Esta opção apresenta a lista de tarefas disponíveis no computador.

4. Selecione a tarefa **Network isolation**.

5. Selecione o separador **Application settings**.

6. Isto abre uma janela; nesta janela, clique em **Exclusions**.

7. Esta ação abre uma janela; nesta janela, clique em **Add from profile** e selecione os perfis de rede padrão para configurar as exclusões.

   As exclusões de isolamento da rede do perfil são adicionadas à lista de exclusões de isolamento da rede. Pode ver as propriedades das ligações de rede. Se necessário, pode modificar as definições da ligação de rede.

8. Se necessário, pode adicionar uma exclusão de isolamento da rede manualmente. Para tal, na janela da lista de exclusões, clique em **Add** e edite manualmente as definições da ligação de rede.

9. Guarde as suas alterações.

Também pode ver a lista de exclusões de isolamento da rede localmente utilizando a Command line. Nesse caso, o computador tem de estar isolado.

A partir do Kaspersky Endpoint Security 12.10 for Windows, pode adicionar exclusões de isolamento da rede nos detalhes do alerta. Para conhecer os detalhes sobre a gestão de deteção, 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 lhe permite detetar ameaças avançadas num computador. O Kaspersky Endpoint Security encaminha automaticamente ficheiros detetados para o Cloud Sandbox para análise. O Cloud Sandbox gere estes ficheiros num ambiente isolado para identificar atividades maliciosas e decidir sobre a sua reputação. Os dados sobre estes ficheiros são então enviados para a Kaspersky Security Network. Portanto, se o Cloud Sandbox tiver detetado um ficheiro malicioso, o Kaspersky Endpoint Security irá realizar a ação apropriada para eliminar esta ameaça em todos os computadores onde este ficheiro for detetado.

Para o Cloud Sandbox funcionar, tem de ativar a utilização da Kaspersky Security Network.

Se estiver a utilizar a Kaspersky Private Security Network, a tecnologia Cloud Sandbox não está disponível.

A tecnologia Cloud Sandbox está permanentemente ativa e está disponível para todos os utilizadores da Kaspersky Security Network, independentemente do tipo de licença que estejam a utilizar. Se já tiver implementado a solução Endpoint Detection and Response Optimum, pode ativar um contador separado para as ameaças detetadas pelo Cloud Sandbox. Pode utilizar este contador para compilar estatísticas ao analisar as ameaças detetadas. O Kaspersky Endpoint Security indica a tecnologia de deteção de ameaças do Cloud Sandbox no *Report on threats* na consola do Kaspersky Security Center.



Contadores de ameaças

Para ativar o contador do Cloud Sandbox:

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Selecione o separador **Cloud Sandbox**.
6. Ative o botão de alternar **Cloud Sandbox ENABLED**.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Quando houver uma ameaça, o Kaspersky Endpoint Security ativa o contador de ameaças detetadas utilizando o Cloud Sandbox na janela principal da aplicação sob **Tecnologias de deteção de ameaças**. O Kaspersky Endpoint Security também irá indicar a tecnologia de deteção de ameaças do Cloud Sandbox no *Report on threats* na consola do Kaspersky Security Center.

Secção de política do Endpoint Detection and Response

Guia de migração de KEA para o KES para EDR Optimum

O Kaspersky Endpoint Security for Windows inclui um agente integrado para a solução Kaspersky Endpoint Detection and Response Optimum. Já não precisa de uma aplicação Kaspersky Endpoint Agent em separado para trabalhar com EDR Optimum. Todas as funções do Kaspersky Endpoint Agent serão executadas pelo Kaspersky Endpoint Security.

Quando implementa o Kaspersky Endpoint Security em computadores com o Kaspersky Endpoint Agent instalado, as soluções Kaspersky Endpoint Detection and Response Optimum irão continuar a funcionar com o Kaspersky Endpoint Security. Além disso, o Kaspersky Endpoint Agent será removido do computador. Ocorrerá o mesmo comportamento no sistema quando 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 pode instalar estas aplicações no mesmo computador.

Devem ser cumpridas as seguintes condições para que o Kaspersky Endpoint Security funcione como parte do Kaspersky Endpoint Detection and Response Optimum:

- Versão 2.0 ou superior do Kaspersky Endpoint Detection and Response Optimum.
- Versão 13.2 ou superior do Kaspersky Security Center (incluindo Agente de Rede). Nas versões anteriores do Kaspersky Security Center, é impossível ativar a funcionalidade EDR Optimum.
- O EDR Optimum só pode ser gerido utilizando a Consola Web do Kaspersky Security Center.

- A transferência de dados para o Servidor de Administração está ativada. Os dados são necessários para obter informações sobre ficheiros colocados em quarentena num computador através da Consola Web.
- Uma ligação de fundo entre a Consola Web do Kaspersky Security Center e o Administration Server é estabelecida. Para o EDR Optimum funcionar com o Administration Server através do Consola Web do Kaspersky Security Center, deve estabelecer uma nova ligação segura, uma *ligação de fundo*.

Etapas para migrar a configuração [KES+KEA] para [KES+built-in agent] para EDR Optimum

1. **Atualização do plug-in da Web do Kaspersky Endpoint Security**

   O componente EDR Optimum pode ser gerido com a versão 11.7.0 ou superior do Plug-in Web do Kaspersky Endpoint Security.

2. **Migração da política e das tarefas**

   Transfira as definições do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows. Para o fazer, use o assistente para migrar a partir do Kaspersky Endpoint Agent na Consola Web.

   Como migrar as definições de tarefas e políticas do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security na Consola Web

   Na janela principal da Consola Web, selecione **Operations** → **Migration from Kaspersky Endpoint Agent**.

   Esta ação executa o assistente de migração de políticas e tarefas. Siga as instruções do Assistente.

   Passo 1. Migração de políticas

   O assistente de migração cria uma nova política que combina as definições das políticas do Kaspersky Endpoint Security e do Kaspersky Endpoint Agent. Na lista de políticas, selecione as políticas do Kaspersky Endpoint Agent cujas definições pretende combinar com a política do Kaspersky Endpoint Security. Clique na política do Kaspersky Endpoint Agent para selecionar a política do Kaspersky Endpoint Security com a qual pretende combinar definições. Certifique-se de que seleciona as políticas corretas e avance para o passo seguinte.

   Passo 2. Migração de tarefas

   O Assistente de Migração cria novas tarefas para o Kaspersky Endpoint Security. Na lista de tarefas, selecione as tarefas do Kaspersky Endpoint Agent que pretende criar para a política do Kaspersky Endpoint Security. Avance para o passo seguinte.

   Passo 3. Conclusão do assistente

   Conclua o assistente. Como resultado, o assistente faz o seguinte:

   - Cria uma nova política do Kaspersky Endpoint Security.

A política combina as definições do Kaspersky Endpoint Security e Kaspersky Endpoint Agent A política é denominada *<Kaspersky Endpoint Security policy name> e <Kaspersky Endpoint Agent policy name>*. A nova política tem o estado *Inactive*. Para continuar, altere os estatutos das políticas do Kaspersky Endpoint Agent e Kaspersky Endpoint Security para *Inactive* e ative a nova política combinada.

Depois de migrar do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows, certifique-se de que a nova política tem a funcionalidade para transferência de dados para o Servidor de Administração (dados de ficheiros de quarentena e dados de cadeia de desenvolvimento de ameaças) configurada. Os valores dos parâmetros 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. Simultaneamente, o Assistente deixa as tarefas do Kaspersky Endpoint Agent inalteradas.

3 Licenciamento da funcionalidade EDR Optimum

Se utilizar uma licença comum do Kaspersky Endpoint Detection and Response Optimum ou do Kaspersky Optimum Security para ativar o Kaspersky Endpoint Security for Windows e o Kaspersky Endpoint Agent, a funcionalidade EDR Optimum será ativada automaticamente após a atualização da aplicação para a versão 11.7.0 ou superior. Não precisa de fazer mais nada.

Se utilizar uma licença autónoma do Suplemento do Kaspersky Endpoint Detection and Response Optimum para ativar a funcionalidade EDR Optimum, deve certificar-se de que a chave EDR Optimum é adicionada ao repositório do Kaspersky Security Center e de que a funcionalidade de distribuição automática da chave de licença está ativada. Depois de atualizar a aplicação para a versão 11.7.0 ou superior, a funcionalidade EDR Optimum é ativada automaticamente.

Se utilizar 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, tem de substituir a chave do Kaspersky Endpoint Security for Windows pela chave comum do Kaspersky Endpoint Detection and Response Optimum ou do Kaspersky Optimum Security. Pode substituir a chave através da tarefa *Add key*.

4 Instalação/atualização da aplicação Kaspersky Endpoint Security

Para migrar a funcionalidade EDR Optimum durante a instalação ou atualização de uma aplicação, é recomendável usar a tarefa de instalação remota. Ao criar uma tarefa de instalação remota, tem de selecionar o componente EDR Optimum nas definições do pacote de instalação.

Também pode atualizar a aplicação utilizando os seguintes métodos:

- Usar o serviço de atualização do Kaspersky.
- Localmente, usando o Assistente de Configuração.

O Kaspersky Endpoint Security suporta a seleção automática de componentes ao atualizar a aplicação num computador com a aplicação Kaspersky Endpoint Agent instalada. A seleção automática dos componentes depende das permissões da conta do utilizador que está a atualizar a aplicação.

Se estiver a atualizar o Kaspersky Endpoint Security utilizando o ficheiro EXE ou MSI na conta do sistema (SYSTEM), o Kaspersky Endpoint Security ganha acesso a licenças atuais de soluções da Kaspersky. Portanto, se o computador tiver, por exemplo, o Kaspersky Endpoint Agent instalado e a solução EDR Optimum ativada, o instalador Kaspersky Endpoint Security configura automaticamente o conjunto de componentes e seleciona o componente EDR Optimum. Isto faz com que o Kaspersky Endpoint Security troque para a utilização do agente incorporado e remove o Kaspersky Endpoint Agent. A execução do instalador MSI na conta do sistema (SYSTEM) é normalmente realizada ao atualizar através do serviço de atualização da Kaspersky ou ao implementar um pacote de instalação através do Kaspersky Security Center.

Se estiver a atualizar o Kaspersky Endpoint Security utilizando um ficheiro MSI numa conta de utilizador sem privilégios, o Kaspersky Endpoint Security não tem acesso às licenças atuais das soluções da Kaspersky. Neste caso, o Kaspersky Endpoint Security seleciona automaticamente os componentes com base na configuração do Kaspersky Endpoint Agent. Depois disso, o Kaspersky Endpoint Security troca para a utilização do agente incorporado e remove o Kaspersky Endpoint Agent.

O Kaspersky Endpoint Security suporta a atualização sem reiniciar o computador. Pode selecionar o modo de atualização da aplicação nas propriedades da política.

5. **A verificar o funcionamento da aplicação**

   Se, após a instalação da aplicação, o computador tiver o estado *Critical* na consola do Kaspersky Security Center:

   - Certifique-se de que o computador tem o Agente de Rede versão 13.2 ou superior instalado.
   - Verifique o estado de funcionamento do agente integrado ao consultar o *Report on status of application components*. Se um componente tiver o estado *Not installed*, instale o componente com a tarefa *Change application components*. Se um componente tiver o estado *Não abrangido pela licença*, certifique-se de que ativou a funcionalidade do agente integrado.
   - Certifique-se de que aceita 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 integrado para integração com a solução Kaspersky Sandbox. O componente *Sandbox* deteta e bloqueia automaticamente ameaças avançadas em computadores. O Sandbox analisa o comportamento do objeto para detetar atividades maliciosas e atividades características de ataques direcionados à infraestrutura de TI da organização. O Sandbox analisa e verifica objetos em servidores especiais com imagens virtuais implementadas de sistemas operativos Microsoft Windows (servidores do Sandbox). Para obter mais informações 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

É necessário adicionar o componente Sandbox para a integração com o Kaspersky Sandbox. Pode selecionar o componente Sandbox durante a instalação ou atualização, bem como através da tarefa *Alterar componentes da aplicação*.

Para utilizar o componente, devem ser cumpridas as seguintes condições:

- Kaspersky Security Center 13.2. As versões anteriores do Kaspersky Security Center não permitem a criação de tarefas de verificação IOC autónomas para resposta à ameaça.
- O componente só pode ser gerido através da Consola Web. Não pode gerir este componente utilizando a Consola de Administração (MMC).
- A aplicação é ativada e a funcionalidade é abrangida pela licença.
- A transferência de dados para o Servidor de Administração está ativada.

Para utilizar todas as funcionalidades do Kaspersky Sandbox, certifique-se de que a transferência de dados do ficheiro de quarentena está ativada. Os dados são necessários para obter informações sobre ficheiros colocados em quarentena num computador através da Consola Web. Por exemplo, pode descarregar um ficheiro da quarentena para análise na Consola Web.

Como ativar a transferência de dados para o Servidor de Administração na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **KSC Integration**.
5. No bloco **Data transfer to Administration Server**, selecione a caixa de verificação **About Quarantine files**.
6. Guarde as suas alterações.

- Uma ligação de fundo entre a Consola Web do Kaspersky Security Center e o Administration Server é estabelecida

  Para o Kaspersky Sandbox funcionar com o Administration Server através do Consola Web do Kaspersky Security Center, deve estabelecer uma nova ligação segura, uma *ligação de fundo*. Para informações sobre a integração do Kaspersky Security Center com outras soluções da Kaspersky, consulte a Ajuda do Kaspersky Security Center.

  Estabelecer uma ligação de fundo na Consola Web

  1. Na janela principal da Consola Web, selecione **Settings** → **Integration**.
  2. Aceda à secção **Integration**.
  3. Ative o botão de alternar **Background connection for integration Enabled**.
  4. Guarde as suas alterações.

  Se não for estabelecida uma ligação de fundo entre a Consola Web do Kaspersky Security Center e o Administration Server, não é possível criar tarefas de verificação IOC autónomas como parte da resposta à ameaça.

- Para configurar uma ligação fiável com o servidor do Sandbox, tem de preparar um certificado TLS. De seguida, tem de adicionar o certificado ao computador utilizando uma política. Também tem de adicionar o certificado ao servidor do Sandbox.

  > A autenticação bidirecional utilizando um cripto-contentor não está disponível para o Kaspersky Sandbox.

  Pode adicionar um Certificado TLS na Consola Web ou localmente utilizando a Linha de comandos.

- O componente Kaspersky Sandbox está ativado.

- Os componentes da aplicação que asseguram o funcionamento do Sandbox estão ativados e operacionais. Os seguintes componentes asseguram o funcionamento do Sandbox:
  - Proteção contra ameaças de ficheiros.
  - Prevenção contra invasões.
  - Firewall.
  - Proteção AMSI.
  - Verificação de fundo.

Para ativar ou desativar a integração com o Kaspersky Sandbox:

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration** → **Sandbox**.
5. Use o botão de alternar da **Integration with Sandbox ENABLED** para ativar ou desativar o componente.
6. No bloco **Integration mode**, selecione o modo de operação do componente: **Kaspersky Sandbox**.
7. Clique na hiperligação **Connection settings**.

   Tal abre a janela de definições de ligação do servidor do Sandbox.
8. No bloco **Server TLS certificate**, clique em **Upload** e selecione o ficheiro de certificado TLS.

   O Kaspersky Endpoint Security só pode ter um certificado TLS para um servidor do Sandbox. Se tiver previamente adicionado um certificado TLS, o certificado em causa será revogado. Apenas o último certificado adicionado é utilizado.
9. Estabeleça as definições avançadas de ligações para servidores do Sandbox:
   - **Timeout (msec)**. Tempo limite de ligação para o servidor Sandbox. Depois de decorrido o tempo limite definido, o Kaspersky Endpoint Security envia um pedido ao próximo servidor. Pode aumentar o tempo limite de ligação do servidor se a velocidade da sua ligação for baixa ou instável. O tempo limite recomendado do pedido é de 0.5 segundos ou menos.
   - **Request queue**. Tamanho da pasta da fila de pedidos. Ao enviar vários objetos para verificação no Sandbox, o Kaspersky Endpoint Security cria uma fila de pedidos. Por predefinição, o tamanho da pasta da fila de pedidos é limitado a 100 MB. Quando o tamanho máximo é atingido, o Sandbox para de adicionar novos pedidos à fila e envia o evento correspondente ao Kaspersky Security Center. Pode definir o tamanho da pasta da fila de pedidos consoante a configuração do seu servidor.
10. No bloco **Connection to Sandbox servers**, clique no botão **Add**.

11. Esta ação abre uma janela; naquela janela, introduza a porta e o endereço do servidor do Sandbox (IPv4, IPv6, DNS).

    Para obter mais informações sobre como implementar imagens virtuais e configurar servidores do Sandbox, consulte a Ajuda do Kaspersky Sandbox.

12. Guarde as suas alterações.

Deste modo, o Kaspersky Endpoint Security verifica o certificado TLS. Se o certificado for verificado com êxito, o Kaspersky Endpoint Security carrega e envia o ficheiro de certificado para o computador durante a próxima sincronização com o Kaspersky Security Center. Se tiver adicionado dois certificados TLS, o Kaspersky Sandbox irá utilizar o certificado mais recente para estabelecer uma ligação de confiança. Verifique o estado de funcionamento do componente, ao consultar o *Report on status of application components*. Pode também ver o estado de funcionamento de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente **Sandbox** será adicionado à lista de componentes do Kaspersky Endpoint Security.

Pode ativar ou desativar a integração com o Kaspersky Sandbox na Consola Web ou localmente usando a linha de comandos.

O Kaspersky Endpoint Security guarda informações sobre o funcionamento do componente Kaspersky Sandbox num relatório. O relatório também contém informações sobre erros. Se receber um erro com uma descrição que corresponda ao `Error code: XXX` formato (por exemplo, `0xa67b01f4`), contacte o Suporte técnico.

Verifique se há indicadores de compromisso (tarefa autónoma)

Um *Indicador de comprometimento (IOC)* é um conjunto de dados relativos a um objeto ou atividade que indica acesso não autorizado ao computador (comprometimento de dados). Por exemplo, muitas tentativas falhadas de iniciar sessão no sistema podem constituir um Indicador de Comprometimento. A tarefa *IOC Scan* permite localizar indicadores de comprometimento no computador e adotar medidas de resposta a ameaças.

O Kaspersky Endpoint Security procura indicadores de comprometimento utilizando IOC files. Os *IOC files* são ficheiros que contêm os conjuntos de indicadores que a aplicação tenta corresponder para contar uma deteção. Os IOC files devem estar em conformidade com o padrão OpenIOC. O Kaspersky Endpoint Security gera automaticamente ficheiros IOC para o Kaspersky Sandbox.

Modo de execução da tarefa IOC Scan

A aplicação cria tarefas de verificação IOC autónomas para o Kaspersky Sandbox. A *Tarefa de verificação IOC autónoma* é uma tarefa de grupo que é criada automaticamente ao reagir a uma ameaça detetada pelo Kaspersky Sandbox. O Kaspersky Endpoint Security gera automaticamente o ficheiro IOC. Os IOC files personalizados não são suportados. As tarefas são eliminadas automaticamente 30 dias após a hora de criação. Para obter mais informações sobre tarefas de Verificação IOC autónoma, consulte a Ajuda do Kaspersky Sandbox.

Definições de tarefa IOC Scan

O Kaspersky Sandbox pode criar e executar tarefas de *IOC Scan* automaticamente ao reagir a ameaças.

Apenas pode configurar as definições na Consola Web.

Precisa do Kaspersky Security Center 13.2 para que todas as tarefas de Verificação IOC autónomas do Kaspersky Sandbox funcionem.

Para alterar as definições da tarefa de IOC Scan:

1. Na janela principal da Consola Web, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique na tarefa **IOC Scan** do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da tarefa.

3. Selecione o separador **Application settings**.

4. Aceda à secção **IOC Scan settings**.

5. Configure ações na deteção de IOC:

   - **Move copy to Quarantine, delete object**. Se esta opção for selecionada, o Kaspersky Endpoint Security elimina o objeto malicioso encontrado no computador. Antes de eliminar o objeto, o Kaspersky Endpoint Security cria uma cópia de segurança, caso o objeto precise de ser posteriormente restaurado. O Kaspersky Endpoint Security move a cópia de segurança para a Quarentena.

   - **Run Critical Areas Scan**. Se esta opção for selecionada, o Kaspersky Endpoint Security executa a tarefa *Critical Areas Scan*. Por predefinição, o Kaspersky Endpoint Security verifica a memória Kernel, os processos em execução e os setores de inicialização do disco.

   - **Run only when the computer is idle**. 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 ecrã estiver ativada. Se interrompeu a execução da tarefa (por exemplo, ao desbloquear o computador), o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que foi interrompido. Esta opção de agendamento permite-lhe conservar os recursos do computador quando o computador está a ser utilizado.

6. Guarde as suas alterações.

Pode visualizar os resultados da tarefa nas propriedades da tarefa na secção **Results**. Pode consultar a informação sobre os indicadores de comprometimento detetados nas propriedades da tarefa: **Application settings** → **IOC Scan results**.

Os resultados da verificação IOC são mantidos durante 30 dias. Após este período, o Kaspersky Endpoint Security elimina automaticamente as entradas mais antigas.

Guia de migração de KEA para o KES para Kaspersky Sandbox

O Kaspersky Endpoint Security for Windows inclui um agente integrado com a solução Kaspersky Sandbox. Já não precisa de uma aplicação Kaspersky Endpoint Agent em separado para trabalhar com Kaspersky Sandbox. Todas as funções do Kaspersky Endpoint Agent serão executadas pelo Kaspersky Endpoint Security.

Quando implementa o Kaspersky Endpoint Security em computadores com o Kaspersky Endpoint Agent instalado, as soluções Kaspersky Sandbox irão continuar a funcionar com o Kaspersky Endpoint Security. Além disso, o Kaspersky Endpoint Agent será removido do computador. Ocorrerá o mesmo comportamento no sistema quando 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 pode instalar estas aplicações no mesmo computador.

Devem ser cumpridas as seguintes condições para que o Kaspersky Endpoint Security funcione como parte do Kaspersky Sandbox:

- Kaspersky Sandbox versão 2.0 ou posterior.
- Versão 13.2 ou superior do Kaspersky Security Center (incluindo Agente de Rede). Nas versões anteriores do Kaspersky Security Center, é impossível ativar a funcionalidade Kaspersky Sandbox.
- O Kaspersky Sandbox pode ser gerido através da Consola Web do Kaspersky Security Center.
- A transferência de dados para o Servidor de Administração está ativada. Os dados são necessários para obter informações sobre ficheiros colocados em quarentena num computador através da Consola Web.
- Uma ligação de fundo entre a Consola Web do Kaspersky Security Center e o Administration Server é estabelecida. Para o Kaspersky Sandbox funcionar com o Administration Server através do Consola Web do Kaspersky Security Center, deve estabelecer uma nova ligação segura, uma *ligação de fundo*.

Etapas para migrar a configuração [KES+KEA] para [KES+built-in agent] para Kaspersky Sandbox

1. **Atualização do plug-in da Web do Kaspersky Endpoint Security**

   O componente Kaspersky Sandbox pode ser gerido com a versão 11.7.0 ou posterior do Plug-in Web do Kaspersky Endpoint Security.

2. **Migração da política e das tarefas**

   Transfira as definições do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows. Para o fazer, use o assistente para migrar a partir do Kaspersky Endpoint Agent na Consola Web.

   Como migrar as definições de tarefas e políticas do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security na Consola Web

   Na janela principal da Consola Web, selecione **Operations** → **Migration from Kaspersky Endpoint Agent**.

   Esta ação executa o assistente de migração de políticas e tarefas. Siga as instruções do Assistente.

Passo 1. Migração de políticas

O assistente de migração cria uma nova política que combina as definições das políticas do Kaspersky Endpoint Security e do Kaspersky Endpoint Agent. Na lista de políticas, selecione as políticas do Kaspersky Endpoint Agent cujas definições pretende combinar com a política do Kaspersky Endpoint Security. Clique na política do Kaspersky Endpoint Agent para selecionar a política do Kaspersky Endpoint Security com a qual pretende combinar definições. Certifique-se de que seleciona as políticas corretas e avance para o passo seguinte.

Passo 2. Migração de tarefas

O Assistente de Migração cria novas tarefas para o Kaspersky Endpoint Security. Na lista de tarefas, selecione as tarefas do Kaspersky Endpoint Agent que pretende criar para a política do Kaspersky Endpoint Security. Avance para o passo seguinte.

Passo 3. Conclusão do assistente

Conclua o assistente. Como resultado, o assistente faz o seguinte:

- Cria uma nova política do Kaspersky Endpoint Security.

  A política combina as definições do Kaspersky Endpoint Security e Kaspersky Endpoint Agent A política é denominada *<Kaspersky Endpoint Security policy name> e <Kaspersky Endpoint Agent policy name>*. A nova política tem o estado *Inactive*. Para continuar, altere os estatutos das políticas do Kaspersky Endpoint Agent e Kaspersky Endpoint Security para *Inactive* e ative a nova política combinada.

  Depois de migrar do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows, certifique-se de que a nova política tem a funcionalidade para transferência de dados para o Servidor de Administração (dados de ficheiros de quarentena e dados de cadeia de desenvolvimento de ameaças) configurada. Os valores dos parâmetros 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. Simultaneamente, o Assistente deixa as tarefas do Kaspersky Endpoint Agent inalteradas.

3. **Licenciamento da funcionalidade Kaspersky Sandbox**

   Para ativar o Kaspersky Endpoint Security como parte da solução do Kaspersky Sandbox, precisa de uma licença em separado para o suplemento Kaspersky Sandbox. Pode adicionar a chave através da tarefa *Add key*. Como resultado, serão adicionadas à aplicação duas chaves: *Kaspersky Endpoint Security* e *Kaspersky Sandbox*.

4. **Instalação/atualização da aplicação Kaspersky Endpoint Security**

   Para migrar a funcionalidade Kaspersky Sandbox durante a instalação ou atualização de uma aplicação, é recomendável usar a tarefa de instalação remota. Ao criar uma tarefa de instalação remota, tem de selecionar o componente Kaspersky Sandbox nas definições do pacote de instalação.

Também pode atualizar a aplicação utilizando os seguintes métodos:

- Usar o serviço de atualização do Kaspersky.
- Localmente, usando o Assistente de Configuração.

O Kaspersky Endpoint Security suporta a seleção automática de componentes ao atualizar a aplicação num computador com a aplicação Kaspersky Endpoint Agent instalada. A seleção automática dos componentes depende das permissões da conta do utilizador que está a atualizar a aplicação.

Se estiver a atualizar o Kaspersky Endpoint Security utilizando o ficheiro EXE ou MSI na conta do sistema (SYSTEM), o Kaspersky Endpoint Security ganha acesso a licenças atuais de soluções da Kaspersky. Portanto, se o computador tiver, por exemplo, o Kaspersky Endpoint Agent instalado e a solução Kaspersky Sandbox ativada, o instalador Kaspersky Endpoint Security configura automaticamente o conjunto de componentes e seleciona o componente Kaspersky Sandbox. Isto faz com que o Kaspersky Endpoint Security troque para a utilização do agente incorporado e remove o Kaspersky Endpoint Agent. A execução do instalador MSI na conta do sistema (SYSTEM) é normalmente realizada ao atualizar através do serviço de atualização da Kaspersky ou ao implementar um pacote de instalação através do Kaspersky Security Center.

Se estiver a atualizar o Kaspersky Endpoint Security utilizando um ficheiro MSI numa conta de utilizador sem privilégios, o Kaspersky Endpoint Security não tem acesso às licenças atuais das soluções da Kaspersky. Neste caso, o Kaspersky Endpoint Security seleciona automaticamente os componentes com base na configuração do Kaspersky Endpoint Agent. Depois disso, o Kaspersky Endpoint Security troca para a utilização do agente incorporado e remove o Kaspersky Endpoint Agent.

O Kaspersky Endpoint Security suporta a atualização sem reiniciar o computador. Pode selecionar o modo de atualização da aplicação nas propriedades da política.

5 A verificar o funcionamento da aplicação

Se, após a instalação da aplicação, o computador tiver o estado *Critical* na consola do Kaspersky Security Center:

- Certifique-se de que o computador tem o Agente de Rede versão 13.2 ou superior instalado.
- Verifique o estado de funcionamento do agente integrado ao consultar o *Report on status of application components*. Se um componente tiver o estado *Not installed*, instale o componente com a tarefa *Change application components*. Se um componente tiver o estado *Não abrangido pela licença*, certifique-se de que ativou a funcionalidade do agente integrado.
- Certifique-se de que aceita 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 suporta o funcionamento com a solução Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* é uma solução criada para a deteção atempada de ameaças sofisticadas, como ataques direcionados, ameaças persistentes avançadas (APT), ataques de dia zero e outras. 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)*)

Pode adquirir todas as unidades funcionais ou unidades funcionais individuais separadamente. Para obter mais informações sobre a solução, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform. A aplicação inclui agentes integrados para componentes EDR e NDR. A aplicação também permite trabalhar com o componente Sandbox que faz parte do KATA.

Ferramentas de Informações sobre Ameaças

O Kaspersky Endpoint Detection and Response utiliza as seguintes ferramentas de Threat Intelligence:

- A integração com o Kaspersky Threat Intelligence Portal, que contém e apresenta informações sobre a reputação de ficheiros e endereços da Internet.
- A base de dados de Ameaças da Kaspersky.
- A infraestrutura dos serviços em nuvem da Kaspersky Security Network (doravante também chamada de "KSN"), que fornece acesso a ficheiros em tempo real, websites e informações de reputação de software da base de conhecimento da Kaspersky. A utilização de dados da Kaspersky Security Network permite uma resposta mais rápida das aplicações da Kaspersky a ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos diagnósticos positivos.

Princípio do funcionamento da solução

A Kaspersky Endpoint Security é instalada em computadores individuais na infraestrutura de TI corporativa e monitoriza continuamente os processos, as ligações de rede abertas e os ficheiros que estão a ser modificados. As informações sobre eventos no computador (dados de telemetria) são enviadas para o servidor Kaspersky Anti Targeted Attack Platform. Neste caso, o Kaspersky Endpoint Security também envia informações para o servidor Kaspersky Anti Targeted Attack Platform sobre ameaças detetadas pela aplicação, bem como informações sobre os resultados de processamento destas ameaças.

A integração do EDR (KATA) e NDR (KATA) é configurada na consola do Kaspersky Security Center. O agente integrado é então gerido usando a consola da Kaspersky Anti Targeted Attack Platform, incluindo a execução de tarefas, a gestão de objetos em quarentena, a exibição de relatórios e outras ações.

Configurações do Kaspersky Endpoint Security para funcionar com EDR/NDR (KATA)

As seguintes configurações podem ser utilizadas para funcionar com EDR/NDR (KATA):

- **[KES+agente integrado]**. Nesta configuração, o Kaspersky Endpoint Security atua como a aplicação que garante a segurança do computador e como a aplicação para funcionar 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 EDR/NDR (KATA) é fornecida pelo Kaspersky Endpoint Security na configuração de Endpoint Detection and Response Agent (EDR Agent). Nesta configuração, o EDR Agent é compatível com aplicações de 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.

Suporte para versões anteriores do Kaspersky Endpoint Security

Se estiver a utilizar o Kaspersky Endpoint Security 11.2.0–11.8.0 para interoperabilidade com o Kaspersky Anti Targeted Attack Platform (EDR), a aplicação inclui o Kaspersky Endpoint Agent. Pode instalar o Kaspersky Endpoint Agent lado a lado com o Kaspersky Endpoint Security.

Se estiver a utilizar o Kaspersky Endpoint Security 11.9.0 – 12.0, precisará de instalar o Kaspersky Endpoint Agent separadamente, porque a partir do Kaspersky Endpoint Security 11.9.0, o pacote de distribuição do Kaspersky Endpoint Agent deixou de fazer parte do kit de distribuição do Kaspersky Endpoint Security.

Integração do agente integrado com EDR/NDR (KATA)

Para integração com o EDR/NDR (KATA), tem de adicionar o componente relevante: Endpoint Detection and Response (KATA) ou Network Detection and Response (KATA). Pode selecionar os componentes para integração com EDR / NDR (KATA) durante a instalação ou atualização da aplicação, bem como através da tarefa *Alterar componentes da aplicação*.

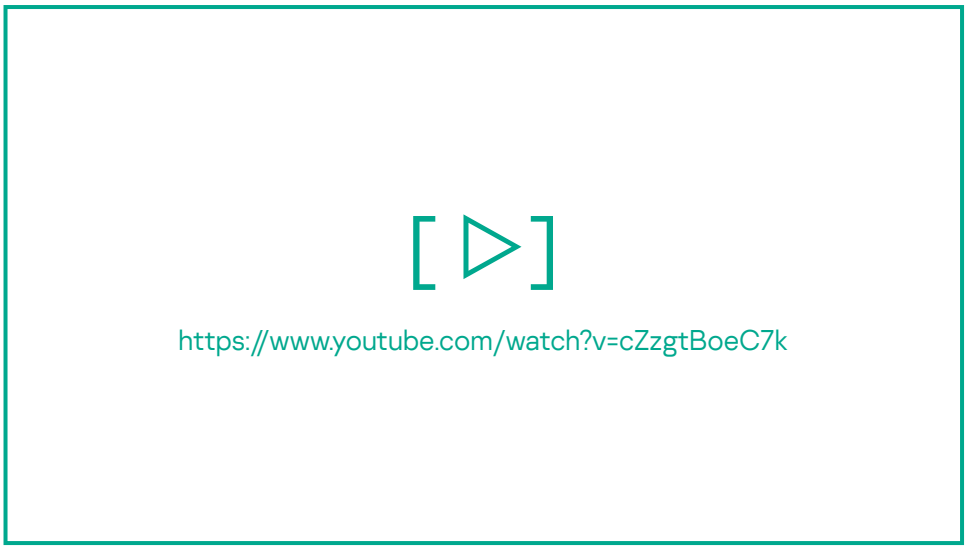
A partir da versão 12.11 do Kaspersky Endpoint Security for Windows, o componente EDR (KATA) foi renomeado para **Endpoint Detection and Response Expert (version 8.0 or later)**. Nesta versão da aplicação, o componente é compatível com o Kaspersky Anti Targeted Attack Platform 7.1 e versões anteriores, bem como com o Kaspersky Endpoint Detection and Response Expert (on-premises).

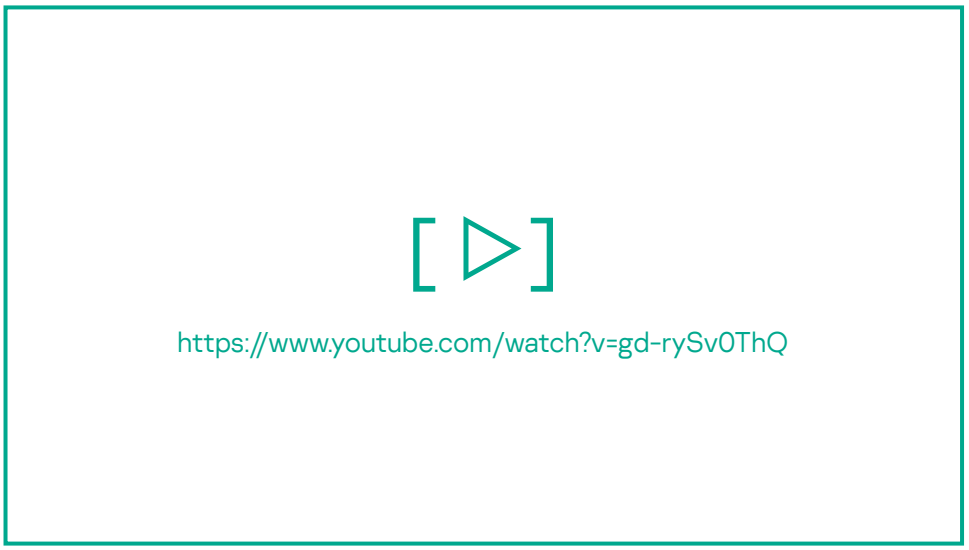
Os componentes Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) e Endpoint Detection and Response Expert (on-premises) não são compatíveis entre si.

Para utilizar o EDR/NDR (KATA), têm de ser cumpridas as seguintes condições:

- 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 superior. Nas versões anteriores do Kaspersky Security Center, é impossível ativar a funcionalidade EDR/NDR (KATA).
- A aplicação é ativada e a funcionalidade é abrangida pela licença.
- Os componentes Endpoint Detection and Response (KATA) e Network Detection and Response (KATA) estão ativados.
- Os componentes da aplicação que asseguram o funcionamento do EDR/NDR (KATA) estão ativados e operacionais. Os seguintes componentes asseguram o funcionamento do EDR/NDR (KATA):
  - Proteção contra ameaças de ficheiros.
  - Proteção contra ameaças da Web.
  - Proteção contra ameaças de correio.
  - Prevenção de explorações.
  - Deteção de comportamento.
  - Prevenção contra invasões.
  - Proteção AMSI.

- Verificação de fundo.
- Kaspersky Security Network.





A integração com o Kaspersky Endpoint Detection and Response (KATA) implica os seguintes passos:

1. **Instalar os componentes Endpoint Detection and Response (KATA) e Network Detection and Response (KATA)**

   Pode selecionar os componentes EDR (KATA) e NDR (KATA) durante a instalação ou atualização, bem como através da tarefa *Alterar componentes da aplicação*.

   > Tem de reiniciar o computador para terminar a atualização da aplicação com os novos componentes.

2. **Ativar os componentes Endpoint Detection and Response (KATA) e Network Detection and Response (KATA)**

   Tem de comprar uma licença separada para o EDR (KATA) e NDR (KATA) (por exemplo, Suplemento do Kaspersky Endpoint Detection and Response (KATA)).

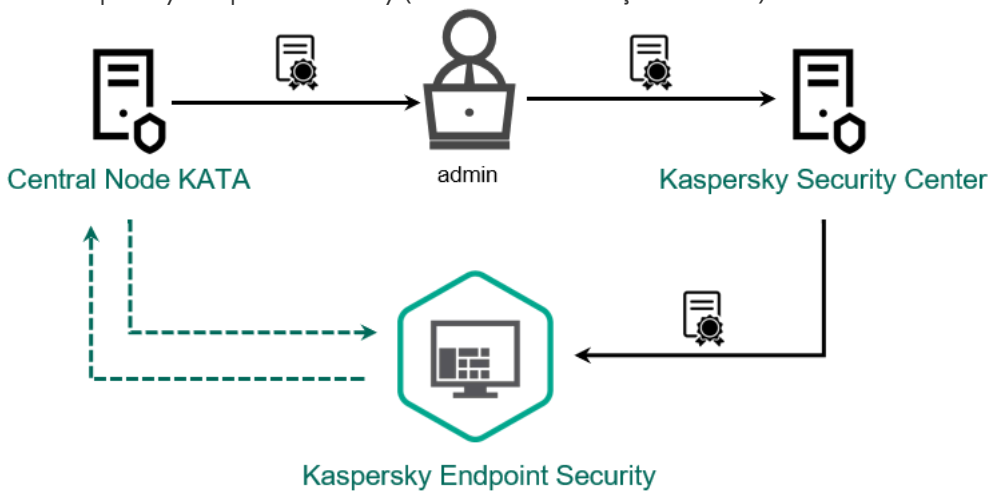
   A funcionalidade fica disponível após a adição de uma chave separada que abrange a funcionalidade EDR (KATA) e NDR (KATA). Como resultado, são adicionadas várias chaves no computador: uma chave para o Kaspersky Endpoint Security e chaves para o Kaspersky Endpoint Detection and Response (KATA) e o Network Detection and Response (KATA).

   A licença para a funcionalidade EDR (KATA) e NDR (KATA) autónoma é a mesma que a licença do Kaspersky Endpoint Security.

Certifique-se de que ambas as funcionalidades EDR (KATA) e NDR (KATA) estão incluídas na licença e são executadas na interface local da aplicação.

3 Ligar ao Central Node

A Kaspersky Anti Targeted Attack Platform requer o estabelecimento de uma ligação fiável entre o Kaspersky Endpoint Security e o componente Central Node. Para configurar uma ligação fiável, tem de utilizar um certificado TLS. Pode obter um certificado TLS na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform). Em seguida, tem de adicionar o certificado TLS ao Kaspersky Endpoint Security (consulte as instruções abaixo).



Adicionar um certificado TLS ao Kaspersky Endpoint Security

Por padrão, o Kaspersky Endpoint Security verifica apenas o certificado TLS do Central Node. Para tornar a ligação mais segura, também pode ativar a verificação do computador no Central Node (autenticação bidirecional). Para ativar esta verificação, tem de ativar a autenticação bidirecional nas definições do Central Node e do Kaspersky Endpoint Security. Para usar a autenticação bidirecional, também irá precisar de um cripto-contentor. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform).

Como ligar um computador do Kaspersky Endpoint Security ao Central Node usando a Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Detection and Response** e selecione o componente que pretende configurar: **Endpoint Detection and Response Expert (on-premises)** ou **Network Detection and Response (KATA)**.
5. Selecione a caixa de verificação correspondente: **Endpoint Detection and Response Expert (versão 7.1 ou posterior)** ou **Network Detection and Response (KATA)**.
6. Clique em **Definições de ligação do servidor**.

7. Configure a ligação do servidor:

   - **Tempo limite (seg)**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor de Central Node diferente.

   - **Certificado TLS do servidor**. Certificado TLS para estabelecer uma ligação fiável com o servidor do Central Node. Pode obter um certificado TLS na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform).

   - **Usar a autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma ligação segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para utilizar a autenticação bidirecional, é necessário ativar a autenticação bidirecional nas definições do servidor do Central Node e, em seguida, obter um contentor criptográfico e definir uma password para proteger o contentor criptográfico. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform). Após configurar as definições do Central Node, é também necessário ativar a autenticação bidirecional nas definições do Kaspersky Endpoint Security e carregar um contentor criptográfico protegido por password.

     O cripto-contentor deve ser protegido por password. Não é possível adicionar um cripto-contentor com uma password em branco.

8. Clique em **OK**.

9. Adicionar servidores de Central Node. Para o fazer, especifique o endereço do servidor (IPv4, IPv6) e a porta para se ligar ao servidor.

   Pode adicionar vários endereços do servidor do Nó Central. O Kaspersky Endpoint Security tenta ligar-se ao servidor utilizando o primeiro endereço IP. Se não for possível estabelecer uma ligação, o Kaspersky Endpoint Security tenta ligar-se utilizando o segundo endereço IP da lista e assim sucessivamente.

10. Se necessário, configure a telemetria.

11. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ligar um computador do Kaspersky Endpoint Security ao Central Node usando a Consola Web

1. Na janela principal da Consola Web, selecione o separador **Asset management → Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda à secção **Built-in Agents Configuration** e selecione o componente que pretende configurar: **Endpoint Detection and Response Expert (on-premises)** ou **Network Detection and Response (KATA)**.

5. Ative o botão de alternar correspondente: **Endpoint Detection and Response Expert (on-premises) ENABLED** ou **Network Detection and Response (KATA) ENABLED**.

6. Para configurar o EDR (KATA), selecione **Endpoint Detection and Response Expert (version 7.1 or earlier)** da lista de soluções.

7. Clique em **Connection settings**.

8. Configure a ligação do servidor:

   - **Timeout (sec)**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor de Central Node diferente.

   - **Server certificate**. Certificado TLS para estabelecer uma ligação fiável com o servidor do Central Node. Pode obter um certificado TLS na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform).

   - **Use two-way authentication**. Autenticação bidirecional ao estabelecer uma ligação segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para utilizar a autenticação bidirecional, é necessário ativar a autenticação bidirecional nas definições do servidor do Central Node e, em seguida, obter um contentor criptográfico e definir uma password para proteger o contentor criptográfico. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform). Após configurar as definições do Central Node, é também necessário ativar a autenticação bidirecional nas definições do Kaspersky Endpoint Security e carregar um contentor criptográfico protegido por password.

     O cripto-contentor deve ser protegido por password. Não é possível adicionar um cripto-contentor com uma password em branco.

9. Clique em **OK**.

10. Adicionar servidores de Central Node. Para o fazer, especifique o endereço do servidor (IPv4, IPv6) e a porta para se ligar ao servidor.

    Pode adicionar vários endereços do servidor do Nó Central. O Kaspersky Endpoint Security tenta ligar-se ao servidor utilizando o primeiro endereço IP. Se não for possível estabelecer uma ligação, o Kaspersky Endpoint Security tenta ligar-se utilizando o segundo endereço IP da lista e assim sucessivamente.

11. Se necessário, configure a telemetria.

12. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Pode adicionar um Certificado TLS localmente utilizando a Linha de comandos.

Como resultado, o computador é adicionado à consola da Kaspersky Anti Targeted Attack Platform. Verifique o estado de funcionamento dos componentes, ao consultar o *Report on status of application components*. Pode também ver o estado de funcionamento dos componentes em relatórios na interface local do Kaspersky Endpoint Security. Os componentes **Endpoint Detection and Response Expert (version 8.0 or later)** e **Network Detection and Response (KATA)** serão adicionados à lista de componentes do Kaspersky Endpoint Security.

Pode verificar o estado dos componentes na consola do Kaspersky Security Center nas propriedades do computador, na secção **Components**. Considere o seguinte ao verificar o estado do componente na consola. Se o componente não estiver instalado e a funcionalidade não estiver abrangida pela sua licença, a consola apresenta o estado **Not supported by license**, em vez de **Not installed**.

A partir do Kaspersky Endpoint Security 12.6 for Windows, pode monitorizar o estado do componente EDR (KATA) na Consola de Administração do Kaspersky Security Center (MMC). O estado atual do componente é exibido nas propriedades do computador na coluna **Endpoint Sensor status** (*Running*, *Starting*, *Stopped*, *Paused*, *Failed*, *Unknown*). A Consola Web não apresenta o estado do Endpoint Sensor.

Configurar a telemetria EDR (KATA)

Telemetria é uma lista de eventos que ocorreram no computador protegido. O Kaspersky Endpoint Security analisa os dados de telemetria e envia-os 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 é satisfeita:

- O intervalo de sincronização acaba.
- O número de eventos na memória intermédia excede o limite superior.

Portanto, por defeito, a aplicação sincroniza a cada 30 segundos ou sempre que a memória intermédia contém 1024 eventos. Pode configurar o comportamento de sincronização na política do Kaspersky Endpoint Security e selecionar os valores ideais para corresponder à sua carga de rede (consulte as instruções abaixo).

Se não houver ligação entre o Kaspersky Endpoint Security e o servidor, a aplicação coloca novos eventos na fila. Quando a ligação é restaurada, o Kaspersky Endpoint Security envia eventos da fila para o servidor na ordem correta. Para evitar sobrecarregar o servidor, o Kaspersky Endpoint Security pode ignorar alguns eventos. Para ativar esta opção, pode otimizar as definições de transmissão de eventos, por exemplo, para definir um valor máximo de eventos por hora (consulte as instruções abaixo).

Se estiver a utilizar a Kaspersky Anti Targeted Attack Platform juntamente com outra solução que também usa telemetria, pode desativar a telemetria para o KATA (EDR) (consulte as instruções abaixo). Isto permite otimizar a carga do servidor para estas soluções. Por exemplo, se tiver a solução Managed Detection and Response e o KATA (EDR) implementado, pode utilizar a telemetria MDR e criar tarefas de Resposta à Ameaça no KATA (EDR).

Como configurar a telemetria na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Detection and Response** e selecione o componente que pretende configurar: **Endpoint Detection and Response Expert (on-premises)** ou **Network Detection and Response (KATA)**.
5. Configure a definição **Enviar pedido de sincronização ao servidor KATA a cada (min)**. Frequência de pedidos de sincronização enviados ao servidor. Durante a sincronização, o Kaspersky Endpoint Security envia informações sobre as definições e tarefas modificadas da aplicação.
6. Certifique-se de que a caixa de verificação **Enviar telemetria ao KATA** está assinalada.
7. Se necessário, configure a sincronização com as definições do servidor no bloco **Definições de transmissão de dados**:
   - **Atraso máximo de transmissão de eventos (seg)**. A aplicação sincroniza com o servidor para enviar eventos após o término do intervalo de sincronização. A predefinição é 30 segundos.
   - **Número máximo de pacotes de eventos**. A aplicação é sincronizada com o servidor quando a memória intermédia está cheia de eventos. A predefinição é 1024 eventos.

8. Se for necessário, selecione a caixa de verificação **Ativar limitação de pedidos** no bloco **Limitação de pedidos**.

   Esta ação ajuda a otimizar a carga no servidor. Se esta funcionalidade estiver ativada, a aplicação restringe a transmissão de eventos. Se o número de eventos exceder os limites configurados, o Kaspersky Endpoint Security irá interromper o envio de eventos.

9. Configure as definições de otimização para enviar eventos ao servidor:

   - **Número máximo de eventos por hora**. A aplicação analisa o fluxo de dados de telemetria e restringe o envio de eventos se o fluxo de eventos exceder o limite de eventos por hora configurado. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. A predefinição é 3000 eventos por hora. Se a aplicação estiver instalada num servidor, o fluxo de dados de telemetria é mais elevado. Para os servidores, recomenda-se que o valor seja aumentado para 60 000 eventos por hora.

   - **Percentagem de excesso do limite de evento**. A aplicação ordena os eventos por tipo (por exemplo, eventos "alterações no registo") e restringe a transmissão de eventos se a proporção de eventos do mesmo tipo para o número total de eventos exceder o limite configurado em percentagem. O Kaspersky Endpoint Security retoma o envio de eventos quando a proporção de outros eventos para o número total de eventos se torna grande o suficiente novamente. A predefinição é 15%.

10. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como configurar a telemetria na consola Web

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.

5. Para configurar o EDR (KATA), selecione **Endpoint Detection and Response Expert (version 7.1 or earlier)** da lista de soluções.

6. Certifique-se de que a caixa de verificação **Send telemetry to KATA servers** está selecionada no bloco **Data transmission settings**.

7. Configure a definição **Send sync request to server every (min)**. Frequência de pedidos de sincronização enviados ao servidor. Durante a sincronização, o Kaspersky Endpoint Security envia informações sobre as definições e tarefas modificadas da aplicação.

8. Certifique-se de que a caixa de verificação **Send telemetry to KATA servers** está assinalada.

9. Se necessário, configure a sincronização com as definições do servidor no bloco **Data transmission settings**:

   - **Maximum event transmission delay (sec)**. A aplicação sincroniza com o servidor para enviar eventos após o término do intervalo de sincronização. A predefinição é 30 segundos.

   - **Maximum number of event packages**. A aplicação é sincronizada com o servidor quando a memória intermédia está cheia de eventos. A predefinição é 1024 eventos.

10. Se for necessário, selecione a caixa de verificação **Enable request throttling** no bloco **Request throttling**.

    Esta ação ajuda a otimizar a carga no servidor. Se esta funcionalidade estiver ativada, a aplicação restringe a transmissão de eventos. Se o número de eventos exceder os limites configurados, o Kaspersky Endpoint Security irá interromper o envio de eventos.

11. Configure as definições de otimização para enviar eventos ao servidor:

    - **Maximum number of events per hour**. A aplicação analisa o fluxo de dados de telemetria e restringe o envio de eventos se o fluxo de eventos exceder o limite de eventos por hora configurado. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. A predefinição é 3000 eventos por hora. Se a aplicação estiver instalada num servidor, o fluxo de dados de telemetria é mais elevado. Para os servidores, recomenda-se que o valor seja aumentado para 60 000 eventos por hora.

    - **Percentage of event limit excess**. A aplicação ordena os eventos por tipo (por exemplo, eventos "alterações no registo") e restringe a transmissão de eventos se a proporção de eventos do mesmo tipo para o número total de eventos exceder o limite configurado em percentagem. O Kaspersky Endpoint Security retoma o envio de eventos quando a proporção de outros eventos para o número total de eventos se torna grande o suficiente novamente. A predefinição é 15%.

12. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda à secção **Integração KATA** → **Exclusões de telemetria**.

5. Em **Definições de transmissão de dados**, selecione a caixa de verificação **Utilizar exclusões**.

6. Clique em **Adicionar** e configure as exclusões:

   Os critérios são combinados com a lógica *E*.

   - **Caminho**. Caminho completo para o ficheiro, incluindo o seu nome e extensão. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara. Para que a exclusão funcione, o caminho para o ficheiro tem de ser especificado.

   - **Linha de comandos**. Comando utilizado para executar o objeto.

   - **Descrição**. Valor do parâmetro FileDescription de um recurso RT_VERSION (VersionInfo).

     Para obter mais informações sobre o recurso VersionInfo, visite o site da Microsoft.

   - **Nome do ficheiro original**. Valor do parâmetro OriginalFilename de um recurso RT_VERSION (VersionInfo).

   - **Versão**. Valor do parâmetro FileVersion de um recurso RT_VERSION (VersionInfo).

   - **MD5**. Hash MD5 do ficheiro.

- **SHA256**. Hash SHA256 do ficheiro.
- **Tipos de eventos**. Para que a exclusão funcione, tem de selecionar, pelo menos, um tipo de evento.

7. Guarde as suas alterações.

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Tasks**.

   A lista de tarefas é aberta.

2. Clique em **New task**.

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

Passo 1. Selecionar o tipo de tarefa

1. Selecione **Kaspersky Endpoint Security for Windows (14.2)** → **Reverter atualização**.

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

Selecione os computadores nos quais a tarefa será executada. Estão disponíveis as seguintes opções:

- Atribua a tarefa a um grupo de administração. Neste caso, a tarefa é atribuída a computadores incluídos num grupo de administração criado anteriormente.
- Selecione os computadores detetados pelo Servidor de administração na rede: *unassigned devices*. Os dispositivos específicos podem incluir dispositivos em grupos de administração bem como dispositivos não atribuídos.
- Especifique os endereços do dispositivo manualmente ou importe endereços da lista. Pode especificar nomes de NetBIOS, endereços IP e sub-redes de IP de dispositivos aos quais quer atribuir a tarefa.

Passo 3. Configurar um agendamento de início de uma tarefa

Configure o agendamento de tarefas, por exemplo, manualmente.

Passo 4. Definir o nome da tarefa

Insira um nome para a tarefa.

Passo 7. Completar a criação da tarefa

Conclua o assistente. Se necessário, selecione a caixa de verificação **Run the task after the wizard finishes**. Pode controlar o progresso 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, pode configurar exclusões de telemetria. Por exemplo, pode optar por não enviar dados de comunicações de rede para aplicações individuais.

Como criar uma exclusão de telemetria na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais → Exclusões e tipos de objetos**.
4. No bloco **Definições de telemetria → Telemetria do EDR (KATA)/NDR (KATA)**, clique no botão **Definições**.
5. Na janela que se abre, configure as exclusões de telemetria (consulte a tabela abaixo).

   A aplicação combina condições de exclusão com a lógica AND. Para criar uma regra, tem de especificar um valor no campo **Caminho completo** e selecionar, pelo menos, um tipo de evento na lista **Utilizar para os seguintes tipos de eventos**.
6. Guarde as suas alterações.

Como criar uma exclusão de telemetria na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings → Telemetry Settings**.
5. Selecione o separador **EDR (KATA) / NDR (KATA) telemetry**.
6. Na janela que se abre, configure as exclusões de telemetria (consulte a tabela abaixo).

   A aplicação combina condições de exclusão com a lógica AND. Para criar uma regra, tem de especificar um valor no campo **Full path** e selecionar, pelo menos, um tipo de evento.
7. Guarde as suas alterações.

Parâmetro	Descrição
Processos excluídos	**Otimizar o tamanho da telemetria a enviar**. 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 Microsoft SMB, o serviço WinRM e o processo klnagent.exe do Agente de Rede, bem como informação alargada sobre os tipos de pacotes de rede para todos os tipos de protocolos de rede. O Kaspersky Endpoint Security combina critérios de acionamento de regras com um AND (E) lógico. **Process** e **Parent process**: • **Full path**. Caminho completo para o ficheiro, incluindo o seu nome e extensão. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara. • **Command line text**. Comando utilizado para executar o ficheiro. • **Description**. Valor do parâmetro FileDescription de um recurso RT_VERSION (VersionInfo). • **Original file name**. Valor do parâmetro OriginalFilename de um recurso RT_VERSION (VersionInfo). • **Version**. Valor do parâmetro FileVersion de um recurso RT_VERSION (VersionInfo). • **File checksums**. MD5 e SHA256. Também pode selecionar um ficheiro manualmente e a aplicação irá preencher automaticamente os campos do ficheiro selecionado. Nos sistemas operativos de 64 bits, tem de introduzir manualmente os parâmetros da versão de 64 bits do ficheiro executável de um processo da pasta `C:\windows\system32`, porque a aplicação preenche os campos de parâmetros do ficheiro executável com dados das propriedades da versão de 32 bits do mesmo ficheiro executável na pasta `C:\windows\syswow64`. Por exemplo, se selecionar `C:\windows\system32\cmd.exe`, o plug-in apresenta os parâmetros de `C:\windows\syswow64\cmd.exe`. Este comportamento é ditado por peculiaridades do sistema operativo. **Utilizar para os seguintes tipos de eventos**: • **Modificação do ficheiro**. • **Eventos de rede**. • **Processo: entrada interativa na consola**. • **Módulo carregado**. • **Registo modificado**. • **Registos DNS**. • **Acesso ao processo**. • **Injeção de código**. • **Consulta WMI**. • **Pipe**. • **LDAP**. • **AMSI**.
Comunicações em rede excluídas	**Nome da regra**. **Direção**. **Protocolo**. **Socket em 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 a excluir a telemetria do tráfego de rede. **Endereço remoto**. O endereço de rede do computador para o qual o Kaspersky Endpoint Security está a excluir a telemetria do tráfego de rede. Apenas o formato IPv4 é suportado para endereços IP. **Aplicações**. Lista de ficheiros executáveis de aplicações para as quais o Kaspersky Endpoint Security está a excluir a telemetria EDR do tráfego de rede.

Parâmetro	Descrição
Operações de ficheiros excluídas	**Nome da regra**. **Máscara ou nome de ficheiro**. Nome ou máscara de um ficheiro ou pasta; o Kaspersky Endpoint Security aplica a regra de exclusão quando este ficheiro ou pasta é acedido. O Kaspersky Endpoint Security suporta os caracteres `*` e `?` ao introduzir uma máscara. **Tipo de operação**. **Caminho anterior**. O Kaspersky Endpoint Security combina critérios de acionamento de regras com um AND (E) lógico. **Process** e **Parent process**: • **Full path**. Caminho completo para o ficheiro, incluindo o seu nome e extensão. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara. • **Command line text**. Comando utilizado para executar o ficheiro. • **Description**. Valor do parâmetro FileDescription de um recurso RT_VERSION (VersionInfo). • **Original file name**. Valor do parâmetro OriginalFilename de um recurso RT_VERSION (VersionInfo). • **Version**. Valor do parâmetro FileVersion de um recurso RT_VERSION (VersionInfo). • **File checksums**. MD5 e SHA256. Também pode selecionar um ficheiro manualmente e a aplicação irá preencher automaticamente os campos do ficheiro selecionado. Nos sistemas operativos de 64 bits, tem de introduzir manualmente os parâmetros da versão de 64 bits do ficheiro executável de um processo da pasta `C:\windows\system32`, porque a aplicação preenche os campos de parâmetros do ficheiro executável com dados das propriedades da versão de 32 bits do mesmo ficheiro executável na pasta `C:\windows\syswow64`. Por exemplo, se selecionar `C:\windows\system32\cmd.exe`, o plug-in apresenta os parâmetros de `C:\windows\syswow64\cmd.exe`. Este comportamento é ditado por peculiaridades do sistema operativo.
Operações de DNS excluídas	**Nome da regra**. O Kaspersky Endpoint Security combina critérios de acionamento de regras com um AND (E) lógico. **Process** e **Parent process**: • **Full path**. Caminho completo para o ficheiro, incluindo o seu nome e extensão. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara. • **Command line text**. Comando utilizado para executar o ficheiro. • **Description**. Valor do parâmetro FileDescription de um recurso RT_VERSION (VersionInfo). • **Original file name**. Valor do parâmetro OriginalFilename de um recurso RT_VERSION (VersionInfo). • **Version**. Valor do parâmetro FileVersion de um recurso RT_VERSION (VersionInfo). • **File checksums**. MD5 e SHA256. Também pode selecionar um ficheiro manualmente e a aplicação irá preencher automaticamente os campos do ficheiro selecionado. Nos sistemas operativos de 64 bits, tem de introduzir manualmente os parâmetros da versão de 64 bits do ficheiro executável de um processo da pasta `C:\windows\system32`, porque a aplicação preenche os campos de parâmetros do ficheiro executável com dados das propriedades da versão de 32 bits do mesmo ficheiro executável na pasta `C:\windows\syswow64`. Por exemplo, se selecionar `C:\windows\system32\cmd.exe`, o plug-in apresenta os parâmetros de `C:\windows\syswow64\cmd.exe`. Este comportamento é ditado por peculiaridades do sistema operativo. **DNS**: • **Endereço IP do servidor DNS**. • **Opções de consulta**. • **Estado**. • **Nome do domínio**. • **ID do tipo de definições**. • **Dados da resposta**.

Parâmetro	Descrição
Operações de LDAP excluídas	**Nome da regra**. **Âmbito de pesquisa LDAP**. **Filtro**. **Nome distinto para pesquisa de objetos LDAP**. **Atributos do objeto**. O Kaspersky Endpoint Security combina critérios de acionamento de regras com um AND (E) lógico. **Process** e **Parent process**: • **Full path**. Caminho completo para o ficheiro, incluindo o seu nome e extensão. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara. • **Command line text**. Comando utilizado para executar o ficheiro. • **Description**. Valor do parâmetro FileDescription de um recurso RT_VERSION (VersionInfo). • **Original file name**. Valor do parâmetro OriginalFilename de um recurso RT_VERSION (VersionInfo). • **Version**. Valor do parâmetro FileVersion de um recurso RT_VERSION (VersionInfo). • **File checksums**. MD5 e SHA256. Também pode selecionar um ficheiro manualmente e a aplicação irá preencher automaticamente os campos do ficheiro selecionado. Nos sistemas operativos de 64 bits, tem de introduzir manualmente os parâmetros da versão de 64 bits do ficheiro executável de um processo da pasta `C:\windows\system32`, porque a aplicação preenche os campos de parâmetros do ficheiro executável com dados das propriedades da versão de 32 bits do mesmo ficheiro executável na pasta `C:\windows\syswow64`. Por exemplo, se selecionar `C:\windows\system32\cmd.exe`, o plug-in apresenta os parâmetros de `C:\windows\syswow64\cmd.exe`. Este comportamento é ditado por peculiaridades do sistema operativo.
Consultas de acesso a processos excluídos	**Nome da regra**. **Tipo de operação**. **Acesso solicitado ao processo**. **Rastreio da pilha de chamadas**. O Kaspersky Endpoint Security combina critérios de acionamento de regras com um AND (E) lógico. **Process**, **Parent process**, **File of the target process**, **Handle to the source process** e **Handle to the target process**. • **Caminho completo**. Caminho completo para o ficheiro, incluindo o seu nome e extensão. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara. • **Texto da linha de comandos**. Comando utilizado para executar o ficheiro. • **Especifique os critérios de ativação da regra e os tipos de eventos para os quais esta regra deve ser utilizada**. Valor do parâmetro FileDescription de um recurso RT_VERSION (VersionInfo). • **Nome do ficheiro original**. Valor do parâmetro OriginalFilename de um recurso RT_VERSION (VersionInfo). • **Versão**. Valor do parâmetro FileVersion de um recurso RT_VERSION (VersionInfo). • **Somas de verificação de ficheiros**. MD5 e SHA256. Também pode selecionar um ficheiro manualmente e a aplicação irá preencher automaticamente os campos do ficheiro selecionado. Nos sistemas operativos de 64 bits, tem de introduzir manualmente os parâmetros da versão de 64 bits do ficheiro executável de um processo da pasta `C:\windows\system32`, porque a aplicação preenche os campos de parâmetros do ficheiro executável com dados das propriedades da versão de 32 bits do mesmo ficheiro executável na pasta `C:\windows\syswow64`. Por exemplo, se selecionar `C:\windows\system32\cmd.exe`, o plug-in apresenta os parâmetros de `C:\windows\syswow64\cmd.exe`. Este comportamento é ditado por peculiaridades do sistema operativo.

Parâmetro	Descrição
Injeções de códigos excluídos	**Nome da regra**. **Método de acesso**. **Pilha de chamadas**. **Linha de comandos modificada**. **Endereço de injeção**. **Nome de DLL injetado**. O Kaspersky Endpoint Security combina critérios de acionamento de regras com um AND (E) lógico. **Process** e **Parent process**: • **Full path**. Caminho completo para o ficheiro, incluindo o seu nome e extensão. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara. • **Command line text**. Comando utilizado para executar o ficheiro. • **Description**. Valor do parâmetro FileDescription de um recurso RT_VERSION (VersionInfo). • **Original file name**. Valor do parâmetro OriginalFilename de um recurso RT_VERSION (VersionInfo). • **Version**. Valor do parâmetro FileVersion de um recurso RT_VERSION (VersionInfo). • **File checksums**. MD5 e SHA256. Também pode selecionar um ficheiro manualmente e a aplicação irá preencher automaticamente os campos do ficheiro selecionado. Nos sistemas operativos de 64 bits, tem de introduzir manualmente os parâmetros da versão de 64 bits do ficheiro executável de um processo da pasta `C:\windows\system32`, porque a aplicação preenche os campos de parâmetros do ficheiro executável com dados das propriedades da versão de 32 bits do mesmo ficheiro executável na pasta `C:\windows\syswow64`. Por exemplo, se selecionar `C:\windows\system32\cmd.exe`, o plug-in apresenta os parâmetros de `C:\windows\syswow64\cmd.exe`. Este comportamento é ditado por peculiaridades do sistema operativo.
Consultas WMI eliminadas	**Nome da regra**. **Tipo de operação WMI**. **Consulta remota**. **Nome de um computador que executou um comando WMI**. **Conta de utilizador WMI**. **Comando WMI executado**. **Espaço de nomes WMI**. **Filtro do consumidor de eventos WMI**. **Nome do consumidor de eventos WMI criado**. **Código-fonte de um consumidor de eventos WMI**. O Kaspersky Endpoint Security combina critérios de acionamento de regras com um AND (E) lógico. **Process** e **Parent process**: • **Full path**. Caminho completo para o ficheiro, incluindo o seu nome e extensão. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara. • **Command line text**. Comando utilizado para executar o ficheiro. • **Description**. Valor do parâmetro FileDescription de um recurso RT_VERSION (VersionInfo). • **Original file name**. Valor do parâmetro OriginalFilename de um recurso RT_VERSION (VersionInfo). • **Version**. Valor do parâmetro FileVersion de um recurso RT_VERSION (VersionInfo). • **File checksums**. MD5 e SHA256. Também pode selecionar um ficheiro manualmente e a aplicação irá preencher automaticamente os campos do ficheiro selecionado. Nos sistemas operativos de 64 bits, tem de introduzir manualmente os parâmetros da versão de 64 bits do ficheiro executável de um processo da pasta `C:\windows\system32`, porque a aplicação preenche os campos de parâmetros do ficheiro executável com dados das propriedades da versão de 32 bits do mesmo ficheiro executável na pasta `C:\windows\syswow64`. Por exemplo, se selecionar `C:\windows\system32\cmd.exe`, o plug-in apresenta os parâmetros de `C:\windows\syswow64\cmd.exe`. Este comportamento é ditado por peculiaridades do sistema operativo.

Parâmetro	Descrição
Operações de pipe excluídas	**Nome da regra**. **Nome do pipe**. **Tipo de operação**. O Kaspersky Endpoint Security combina critérios de acionamento de regras com um AND (E) lógico. **Process** e **Parent process**: • **Full path**. Caminho completo para o ficheiro, incluindo o seu nome e extensão. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara. • **Command line text**. Comando utilizado para executar o ficheiro. • **Description**. Valor do parâmetro FileDescription de um recurso RT_VERSION (VersionInfo). • **Original file name**. Valor do parâmetro OriginalFilename de um recurso RT_VERSION (VersionInfo). • **Version**. Valor do parâmetro FileVersion de um recurso RT_VERSION (VersionInfo). • **File checksums**. MD5 e SHA256. Também pode selecionar um ficheiro manualmente e a aplicação irá preencher automaticamente os campos do ficheiro selecionado. Nos sistemas operativos de 64 bits, tem de introduzir manualmente os parâmetros da versão de 64 bits do ficheiro executável de um processo da pasta `C:\windows\system32`, porque a aplicação preenche os campos de parâmetros do ficheiro executável com dados das propriedades da versão de 32 bits do mesmo ficheiro executável na pasta `C:\windows\syswow64`. Por exemplo, se selecionar `C:\windows\system32\cmd.exe`, o plug-in apresenta os parâmetros de `C:\windows\syswow64\cmd.exe`. Este comportamento é ditado por peculiaridades do sistema operativo.
Alterações de registo excluídas	**Nome da regra**. **Tipo de operação**. **Caminho**. **Nome do valor**. **Valor**. **Nome completo de um ficheiro de registo**. O Kaspersky Endpoint Security combina critérios de acionamento de regras com um AND (E) lógico. **Process** e **Parent process**: • **Full path**. Caminho completo para o ficheiro, incluindo o seu nome e extensão. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara. • **Command line text**. Comando utilizado para executar o ficheiro. • **Description**. Valor do parâmetro FileDescription de um recurso RT_VERSION (VersionInfo). • **Original file name**. Valor do parâmetro OriginalFilename de um recurso RT_VERSION (VersionInfo). • **Version**. Valor do parâmetro FileVersion de um recurso RT_VERSION (VersionInfo). • **File checksums**. MD5 e SHA256. Também pode selecionar um ficheiro manualmente e a aplicação irá preencher automaticamente os campos do ficheiro selecionado. Nos sistemas operativos de 64 bits, tem de introduzir manualmente os parâmetros da versão de 64 bits do ficheiro executável de um processo da pasta `C:\windows\system32`, porque a aplicação preenche os campos de parâmetros do ficheiro executável com dados das propriedades da versão de 32 bits do mesmo ficheiro executável na pasta `C:\windows\syswow64`. Por exemplo, se selecionar `C:\windows\system32\cmd.exe`, o plug-in apresenta os parâmetros de `C:\windows\syswow64\cmd.exe`. Este comportamento é ditado por peculiaridades do sistema operativo.
Operações excluídas com dispositivos	**Nome da regra**. **Tipo de dispositivo**. **ID de dispositivo**. **Nome do dispositivo**.

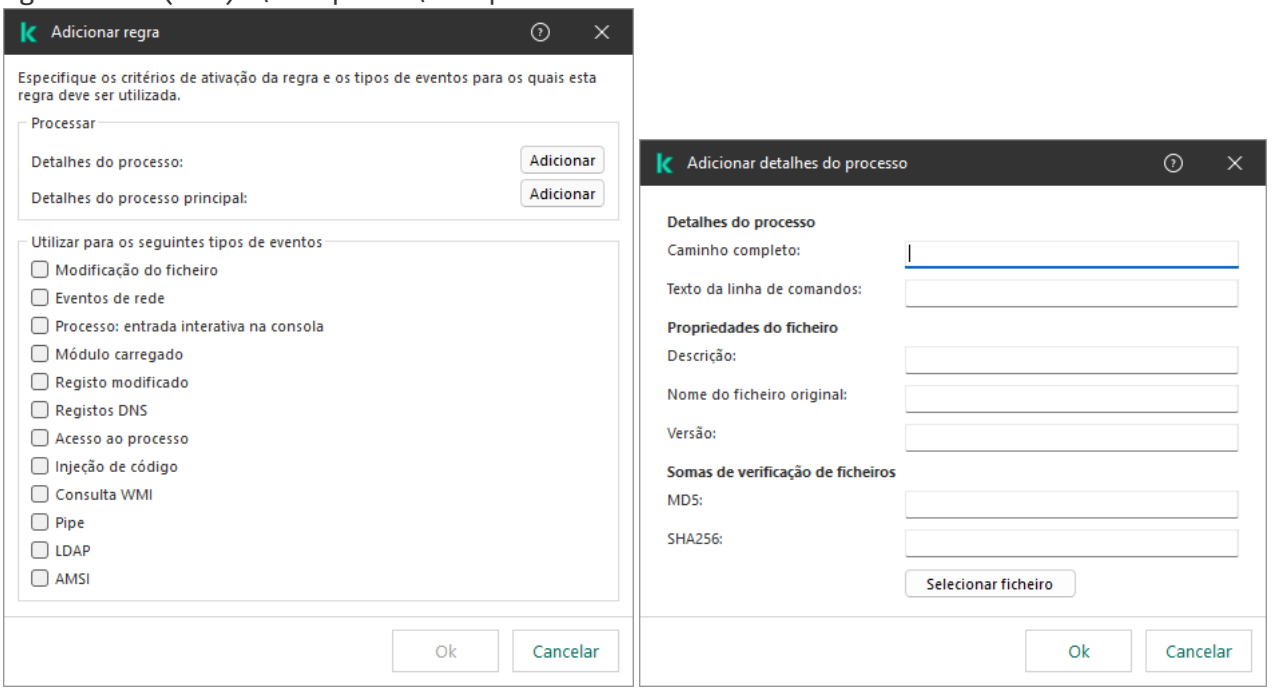
Exemplo 1. Processos excluídos

Para excluir eventos de aplicações (processos) de terceiros da telemetria, abra a janela de exclusões de telemetria EDR no separador **Processos excluídos** e adicione o ficheiro executável da aplicação.

O Kaspersky Endpoint Security combina critérios de acionamento de regras com um AND (E) lógico.

O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara. Por exemplo:

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`



Excluir um processo

Exemplo 1. Modificação de ficheiro

Se costuma editar scripts na aplicação Notepad++ e deseja excluir os eventos de modificação para os scripts correspondentes, adicione o ficheiro executável Notepad++ às exclusões de telemetria.

Especifique as definições da seguinte forma:

- **Caminho completo**: `C:\Program Files\Notepad++\notepad++.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.
- **Utilizar para os seguintes tipos de eventos**: Modificação do ficheiro.

Exemplo 2. Eventos de rede

Se usar a aplicação WinSCP para gerir ficheiros num servidor remoto e pretender excluir eventos de rede, adicione o ficheiro executável WinSCP às exclusões de telemetria.

Especifique as definições da seguinte forma:

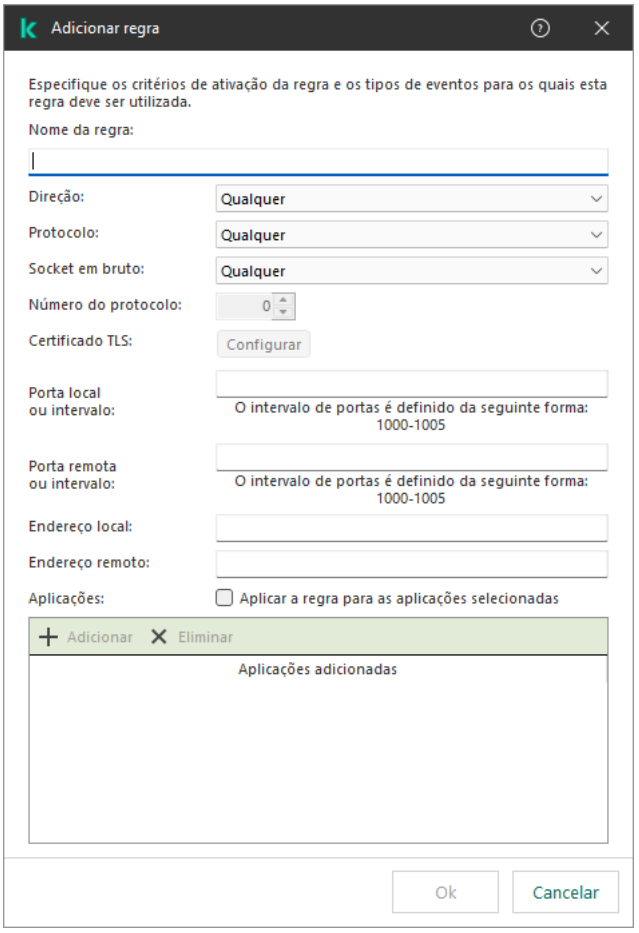
- **Caminho completo**: `C:\Program Files (x86)\WinSCP\WinSCP.exe`.
- **SHA256**: 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (opcional).
- **Utilizar para os seguintes tipos de eventos**: Eventos de rede.

Exemplo 2. Comunicações de rede excluídas

Para excluir eventos de ligação de serviço remoto da telemetria, abra a janela de exclusões de telemetria EDR no separador **Comunicações em rede excluídas** e adicione as definições de ligação: protocolo, porta, direção, endereço IP, certificado TLS e outros.

O Kaspersky Endpoint Security combina critérios de acionamento de regras com um AND (E) lógico.

Não pode especificar um endereço de sub-rede (por exemplo, 10.28.0.0/24). A aplicação apenas permite a especificação de um endereço IP (por exemplo, 10.28.0.105).



Exclusão de comunicação de rede

Se utilizar um servidor Web da empresa e pretender excluir eventos do navegador ao ligar a esse servidor Web, adicione o endereço IP do servidor e o ficheiro executável do navegador às exclusões de telemetria.

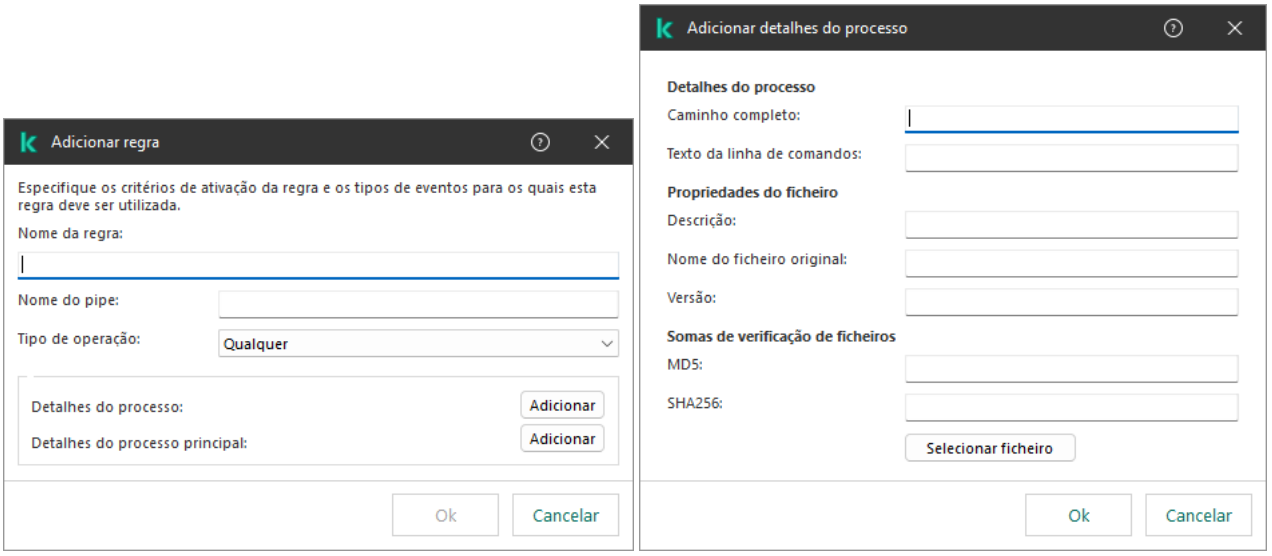
Especifique as definições da seguinte forma:

- **Protocolo**: TCP.
- **Porta remota ou intervalo**: 443.
- **Endereço remoto**: 10.28.0.105.
- **Aplicações**: `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`; `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`.

Exemplo 3. Operações de ficheiro excluídas

Para excluir eventos que envolvam operações com ficheiros fiáveis da telemetria, abra a janela de exclusões de telemetria EDR no separador **Operações de ficheiros excluídas** e adicione o ficheiro fiável.

O Kaspersky Endpoint Security combina critérios de acionamento de regras com um AND (E) lógico.



Excluir operações de ficheiro

Se uma aplicação escrever num registo e pretender excluir eventos de modificação do ficheiro de registo, adicione o ficheiro de registo e o ficheiro executável da aplicação à telemetria.

Especifique as definições da seguinte forma:

- **Máscara ou nome de ficheiro**: `C:\Apache24\logs\error.log`.
- **Tipo de operação**: Modificação do ficheiro.
- **Caminho completo**: `C:\Apache24\bin\httpd.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

Exemplo 4. Modificações de registo excluídas

Para excluir eventos de modificação de registo da telemetria, abra a janela de exclusões de telemetria EDR no separador **Alterações de registo excluídas** e adicione uma chave de registo.

O Kaspersky Endpoint Security combina critérios de acionamento de regras com um AND (E) lógico.

Se uma aplicação modificar frequentemente os seus valores do registo e pretender excluir estes eventos de modificação do registo da telemetria, adicione a chave do registo e o ficheiro executável da aplicação às exclusões de telemetria.

Especifique as definições 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 lhe permite detetar ameaças avançadas num computador. O Sandbox analisa o comportamento do objeto para detetar atividades maliciosas e atividades características de ataques direcionados à infraestrutura de TI da organização. O Sandbox analisa e verifica objetos em servidores especiais com imagens virtuais implementadas de sistemas operativos Microsoft Windows (servidores do Sandbox). Para obter mais informações sobre a solução, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform.

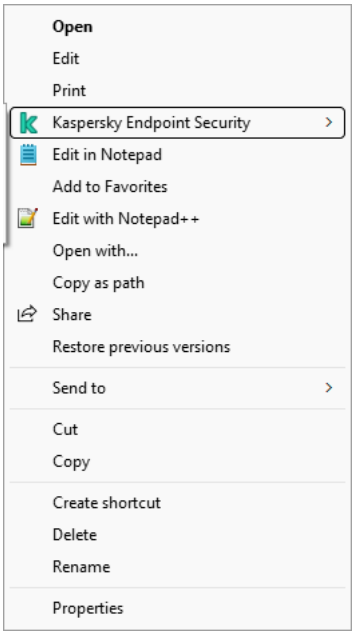
Para ativar o KATA Sandbox, precisa de uma chave de licença que inclua a funcionalidade KATA ou KEDR. Para obter mais informações sobre as funcionalidades disponíveis, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform.

O KATA Sandbox permite analisar ficheiros nos seguintes modos:

- *Manualmente*. O utilizador envia manualmente o ficheiro para verificação a partir do menu de contexto (**Enviar para Sandbox**). Ao enviar um ficheiro para o Sandbox, a aplicação verifica o ficheiro através de bases de dados de antivírus.
- *Automaticamente*. A aplicação deteta automaticamente os objetos e envia-os para o Sandbox para verificação.

Depois de o ficheiro ser enviado para o Sandbox, o ficheiro permanece acessível ao utilizador. O Kaspersky Endpoint Security regista o evento correspondente e envia-o para o Kaspersky Security Center e para a consola Kaspersky Anti Targeted Attack Platform. Se o Sandbox detetar atividade maliciosa, o Kaspersky Endpoint Security executa uma ação de Resposta a ameaças automaticamente (por exemplo, elimina o objeto e inicia uma Verificação de áreas críticas).

Para que o KATA Sandbox funcione no modo manual, o Kaspersky Anti Targeted Attack Platform 7.0 ou versão posterior tem de ser implementado. Para que o KATA Sandbox funcione no modo automático, o Kaspersky Anti Targeted Attack Platform 8.0 ou versão posterior tem de ser implementado.



Análise no KATA Sandbox a partir do menu de contexto

Integração do agente integrado com o KATA Sandbox

É necessário adicionar o componente Sandbox para a integração com o KATA Sandbox. Pode selecionar o componente Sandbox durante a instalação ou atualização, bem como através da tarefa *Alterar componentes da aplicação*.

Para enviar ficheiros para verificação, tem de ativar a integração com o KATA Sandbox e adicionar um servidor de Central Node que esteja implementado na solução. O componente só pode ser gerido através da Consola Web do Kaspersky Security Center. Não pode gerir este componente utilizando a Consola de Administração (MMC).

Para ativar ou desativar a integração com o KATA Sandbox:

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration** → **Sandbox**.
5. Use o botão de alternar da **Integration with Sandbox ENABLED** para ativar ou desativar o componente.

6. Selecione o modo de funcionamento do KATA Sandbox:

   - **Manually**. O utilizador envia manualmente o ficheiro para verificação a partir do menu de contexto (**Enviar para Sandbox**).
   - **Automatically**. A aplicação deteta automaticamente os objetos e envia-os para o Sandbox para verificação.
   - **Combined**.

7. Clique na hiperligação **Connection settings**.

8. Configurar as definições de ligação do servidor do Central Node:

   - **Timeout (msec)**. Tempo limite de ligação para o servidor do Central Node. Depois de decorrido o tempo limite definido, o Kaspersky Endpoint Security envia um pedido ao próximo servidor. Pode aumentar o tempo limite de ligação do servidor se a velocidade da sua ligação for baixa ou instável. O tempo limite recomendado do pedido é de 0.5 segundos ou menos.
   - **Request queue**. Tamanho da pasta da fila de pedidos. Ao enviar vários objetos para verificação no Sandbox, o Kaspersky Endpoint Security cria uma fila de pedidos. Por predefinição, o tamanho da pasta da fila de pedidos é limitado a 100 MB. Quando o tamanho máximo é atingido, o Sandbox para de adicionar novos pedidos à fila e envia o evento correspondente ao Kaspersky Security Center. Pode definir o tamanho da pasta da fila de pedidos consoante a configuração do seu servidor.
   - **Server TLS certificate**. Para configurar uma ligação fiável com o servidor do Central Node, tem de preparar um certificado TLS. De seguida, tem de adicionar o certificado ao computador utilizando uma política. Também tem de adicionar o certificado ao servidor do Central Node.
   - **Use two-way authentication**. Autenticação bidirecional ao estabelecer uma ligação segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para utilizar a autenticação bidirecional, é necessário ativar a autenticação bidirecional nas definições do servidor do Central Node e, em seguida, obter um contentor criptográfico e definir uma password para proteger o contentor criptográfico. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform). Após configurar as definições do Central Node, é também necessário ativar a autenticação bidirecional nas definições do Kaspersky Endpoint Security e carregar um contentor criptográfico protegido por password.

9. No bloco **Connection to Sandbox servers**, clique no botão **Add**.

10. Esta ação abre uma janela; naquela janela, introduza a porta e o endereço do servidor do Central Node (IPv4, IPv6, DNS).

    Para obter mais informações sobre como implementar imagens virtuais e configurar servidores do Central Node, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform.

11. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Deste modo, o componente Sandbox está ativado. Verifique o estado de funcionamento do componente, ao consultar o *Report on status of application components*. Pode também ver o estado de funcionamento de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente **Sandbox** será adicionado à lista de componentes do Kaspersky Endpoint Security.

Configuração de ações de Resposta a ameaças

Se o Sandbox detetar atividade maliciosa, o Kaspersky Endpoint Security executa uma ação de Resposta a ameaças automaticamente (por exemplo, elimina o objeto e inicia uma Verificação de áreas críticas).

Para configurar as ações de Resposta a ameaças:

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration** → **Sandbox**.
5. Selecione a ação relevante no bloco **Action on threat detection**:

   - **Move copy to Quarantine, delete object**. Se esta opção for selecionada, o Kaspersky Endpoint Security elimina o objeto malicioso encontrado no computador. Antes de eliminar o objeto, o Kaspersky Endpoint Security cria uma cópia de segurança, caso o objeto precise de ser posteriormente restaurado. O Kaspersky Endpoint Security move a cópia de segurança para a Quarentena.
   - **Run Critical Areas Scan**. Se esta opção for selecionada, o Kaspersky Endpoint Security executa a tarefa *Critical Areas Scan*. Por predefinição, o Kaspersky Endpoint Security verifica a memória Kernel, os processos em execução e os setores de inicialização do disco.
   - **Create IOC Scan task**. Se esta opção for selecionada, o Kaspersky Endpoint Security cria automaticamente uma tarefa *IOC Scan (tarefa de verificação IOC autónoma)*. Para esta tarefa, pode configurar o modo de execução, âmbito de verificação e ação na deteção de IOC (*Move copy to Quarantine, delete object* ou *Run Critical Areas Scan*). Para modificar outras definições da tarefa *IOC Scan*, aceda às definições da tarefa.
6. Se necessário, configure as definições de tarefa *Verificação IOC* no bloco **IOC Scan scope**.

   - **Critical file areas**. Se esta opção for selecionada, o Kaspersky Endpoint Security fará uma verificação IOC apenas em áreas críticas do ficheiro do computador: memória kernel e setores de arranque.
   - **File areas on system drive of the computer**. Se esta opção for selecionada, o Kaspersky Endpoint Security fará uma verificação IOC na unidade de sistema do computador.
7. Se necessário, configure as definições de tarefa *Verificação IOC* no bloco **Run IOC Scan task**.

   - **Manually**. Modo de execução, no qual pode iniciar a tarefa *IOC Scan* manualmente quando for conveniente para si.
   - **Automatically**. Modo de execução no qual o Kaspersky Endpoint Security executa a tarefa *IOC Scan* automaticamente assim que uma ameaça é detetada.
   - **Run only when the computer is idle**. Modo de execução no qual o Kaspersky Endpoint Security executa a tarefa *Verificação IOC* se a proteção de ecrã estiver ativa ou se o ecrã estiver bloqueado. Se o utilizador desbloquear o computador, o Kaspersky Endpoint Security pausa a tarefa. Tal significa que a tarefa pode demorar vários dias até ser concluída.

8. Configurar definições de tarefa avançadas para *Verificação IOC*.

9. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Guia de migração de KEA para o KES para EDR (KATA)

A partir da versão 12.1, o Kaspersky Endpoint Security for Windows inclui um agente integrado para gerir o componente Kaspersky Endpoint Detection and Response como parte da solução Kaspersky Anti Targeted Attack Platform. Já não precisa de uma aplicação Kaspersky Endpoint Agent em separado para trabalhar com EDR (KATA). Todas as funções do Kaspersky Endpoint Agent serão executadas pelo Kaspersky Endpoint Security. A carga nos servidores Kaspersky Anti Targeted Attack Platform permanecerá a mesma.

Quando implementar o Kaspersky Endpoint Security em computadores com o Kaspersky Endpoint Agent instalado, a solução do Kaspersky Anti Targeted Attack Platform (EDR) continuará a funcionar com o Kaspersky Endpoint Security. Além disso, o Kaspersky Endpoint Agent será removido do computador. Ocorrerá o mesmo comportamento no sistema quando atualizar o Kaspersky Endpoint Security para a versão 12.1 ou superior.

O Kaspersky Endpoint Security não é compatível com o Kaspersky Endpoint Agent. Não pode instalar estas aplicações no mesmo computador.

Devem ser cumpridas as seguintes condições 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.
- Versão 14.2 ou superior do Kaspersky Security Center (incluindo Agente de Rede). Nas versões anteriores do Kaspersky Security Center, é impossível ativar a funcionalidade Endpoint Detection and Response (KATA).

Etapas para migrar a configuração [KES KEA] para [KES built-in agent] para EDR (KATA)

1. **Atualização do Plug-in de gestão do Kaspersky Endpoint Security**

   O componente EDR (KATA) pode ser gerido com a versão 12.1 ou superior do Plug-in de gestão do Kaspersky Endpoint Security. Dependendo do tipo de consola do Kaspersky Security Center que está a usar, atualize o plug-in de gestão na consola de administração (MMC) ou o plug-in da Web no consola Web.

2. **Migração da política e das tarefas**

   Transfira as definições do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows. Estão disponíveis as seguintes opções:

   - O assistente para a migração do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security. O assistente para a migração do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security funciona apenas na Consola Web

     Como migrar as definições de tarefas e políticas do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security na Consola Web

     Na janela principal da Consola Web, selecione **Operations** → **Migration from Kaspersky Endpoint Agent**.

     Esta ação executa o assistente de migração de políticas e tarefas. Siga as instruções do Assistente.

Passo 1. Migração de políticas

O assistente de migração cria uma nova política que combina as definições das políticas do Kaspersky Endpoint Security e do Kaspersky Endpoint Agent. Na lista de políticas, selecione as políticas do Kaspersky Endpoint Agent cujas definições pretende combinar com a política do Kaspersky Endpoint Security. Clique na política do Kaspersky Endpoint Agent para selecionar a política do Kaspersky Endpoint Security com a qual pretende combinar definições. Certifique-se de que seleciona as políticas corretas e avance para o passo seguinte.

Passo 2. Migração de tarefas

O Assistente de Migração não suporta tarefas EDR (KATA). Ignorar este passo.

Passo 3. Conclusão do assistente

Conclua o assistente. Como resultado do assistente, será criada uma nova política do Kaspersky Endpoint Security. A política combina as definições do Kaspersky Endpoint Security e Kaspersky Endpoint Agent A política é denominada *<Kaspersky Endpoint Security policy name> e <Kaspersky Endpoint Agent policy name>*. A nova política tem o estado *Inactive*. Para continuar, altere os estatutos das políticas do Kaspersky Endpoint Agent e Kaspersky Endpoint Security para *Inactive* e ative a nova política combinada.

O assistente de migração na Consola Web ignora as seguintes definições de política e não as migra:

- Proibição de modificação de definições **Connection settings** ("cadeado").

  Por defeito, as definições podem ser modificadas (o "cadeado" está aberto). Por conseguinte, as definições não são aplicadas no computador. Tem de proibir a modificação das definições e fechar o "cadeado".

- Cripto-contentor.

  Se estiver a utilizar autenticação bidirecional para ligar aos servidores do Central Node, tem de voltar a adicionar o cripto-contentor.

Como o Assistente de Migração não migra essas definições, podem ocorrer erros ao ligar o computador aos servidores do Central Node. Para corrigir os erros, tem de aceder às propriedades da política e configurar as definições de ligação.

- Um assistente de conversão de políticas e tarefas em lote padrão. O Assistente de conversão de políticas e tarefas em lote está disponível apenas na Consola de Administração (MMC). Para obter mais informações detalhadas sobre o Assistente de conversão de políticas e tarefas em lote, consulte a Ajuda do Kaspersky Security Center.

Para garantir que o Kaspersky Endpoint Security funciona corretamente nos servidores, é recomendável adicionar ficheiros importantes para o funcionamento do servidor à zona fiável. Para servidores SQL, tem de adicionar ficheiros base de dados MDF e LDF. Para servidores Microsoft Exchange, tem de adicionar ficheiros CHK, EDB, JRS, LOG e JSL. Pode utilizar máscaras, por exemplo, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

A partir do Kaspersky Endpoint Security 12.6 para Windows, as exclusões de verificação e as aplicações fiáveis são adicionadas à zona fiável. Exclusões de verificação predefinidas e aplicações fiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e System Center Configuration Manager. Isto significa que não é necessário configurar manualmente uma zona fiável para a aplicação nos servidores.

As exclusões de telemetria EDR não migram da política do Kaspersky Endpoint Agent para a política do Kaspersky Endpoint Security. O Kaspersky Endpoint Security tem as suas próprias ferramentas de exclusão - aplicações fiáveis. A operação do Kaspersky Endpoint Security é otimizada de modo a que a ausência de exclusões individuais de telemetria EDR não provoque qualquer carga adicional ao seu computador em comparação com o Kaspersky Endpoint Agent. O Kaspersky Endpoint Security usa a telemetria não só para o EDR (KATA), mas também para a operação de componentes de proteção de aplicações. Portanto, não precisa de transferir exclusões individuais de telemetria de EDR. Se detetar uma diminuição do desempenho do computador, verifique a operação da aplicação (consulte o passo 7 Verificar o desempenho).

3. **Licenciamento da funcionalidade EDR (KATA)**

   Para ativar o Kaspersky Endpoint Security como parte da solução da Kaspersky Anti Targeted Attack Platform, precisa de uma licença em separado para o suplemento Kaspersky Endpoint Detection and Response (KATA). Pode adicionar a chave através da tarefa *Add key*. Como resultado, serão adicionadas à aplicação duas chaves: *Kaspersky Endpoint Security* e *Kaspersky Endpoint Detection and Response (KATA)*.

   Licenciamento do suplemento Kaspersky Endpoint Detection and Response (KATA) em computadores com as funcionalidades EDR Optimum ou EDR Expert ativadas anteriormente envolve as seguintes considerações especiais:

   - Se estiver a utilizar um *key file* para licenciar o Kaspersky Endpoint Security com as funcionalidades EDR Optimum ou EDR Expert, não pode adicionar uma chave separada para o suplemento Kaspersky Endpoint Detection and Response (KATA). Pode utilizar um código de ativação para licenciamento ou entrar em contacto com seu fornecedor de serviços para obter um novo key file para ativar as funcionalidades Kaspersky Endpoint Security e EDR. O fornecedor de serviços fornecerá um ou mais key files para licenciamento.

   - Se estiver a utilizar um *key file* para licenciar o Kaspersky Endpoint Security sem as funcionalidades EDR Optimum ou EDR Expert, pode adicionar uma chave separada para o suplemento Kaspersky Endpoint Detection and Response (KATA) sem emitir novamente key files.

   - Se estiver a utilizar um *código de ativação* para licenciamento, o servidor de ativação Kaspersky voltará a emitir automaticamente as chaves e as funcionalidades EDR (KATA) ficarão disponíveis automaticamente. Neste caso, as funcionalidades EDR Optimum e EDR Expert serão desativadas.

   - O Kaspersky Endpoint Security permite adicionar até duas chaves de licença ativas: chave do Kaspersky Endpoint Security e chave de suplemento. Poderá também adicionar até duas chaves de reserva. Uma chave de licença de reserva do Kaspersky Endpoint Security e uma chave de suplemento de reserva.

4. **Instalação/atualização da aplicação Kaspersky Endpoint Security**

   Para migrar a funcionalidade EDR (KATA) durante a instalação ou atualização de uma aplicação, é recomendável usar a tarefa de instalação remota. Ao criar uma tarefa de instalação remota, tem de selecionar o componente EDR (KATA) nas definições do pacote de instalação.

   Também pode atualizar a aplicação utilizando os seguintes métodos:

   - Usar o serviço de atualização do Kaspersky.

   - Localmente, usando o Assistente de Configuração.

O Kaspersky Endpoint Security suporta a seleção automática de componentes ao atualizar a aplicação num computador com a aplicação Kaspersky Endpoint Agent instalada. A seleção automática dos componentes depende das permissões da conta do utilizador que está a atualizar a aplicação.

Se estiver a atualizar o Kaspersky Endpoint Security utilizando o ficheiro EXE ou MSI na conta do sistema (SYSTEM), o Kaspersky Endpoint Security ganha acesso a licenças atuais de soluções da Kaspersky. Portanto, se o computador tiver o Kaspersky Endpoint Agent instalado e a solução EDR (KATA) ativada, o instalador Kaspersky Endpoint Security configura automaticamente o conjunto de componentes e seleciona o componente EDR (KATA). Isto faz com que o Kaspersky Endpoint Security troque para a utilização do agente incorporado e remove o Kaspersky Endpoint Agent. A execução do instalador MSI na conta do sistema (SYSTEM) é normalmente realizada ao atualizar através do serviço de atualização da Kaspersky ou ao implementar um pacote de instalação através do Kaspersky Security Center.

Se estiver a atualizar o Kaspersky Endpoint Security utilizando um ficheiro MSI numa conta de utilizador sem privilégios, o Kaspersky Endpoint Security não tem acesso às licenças atuais das soluções da Kaspersky. Nesse caso, o Kaspersky Endpoint Security seleciona automaticamente os componentes com base num conjunto de componentes do Kaspersky Endpoint Agent. Depois disso, o Kaspersky Endpoint Security troca para a utilização do agente incorporado e remove o Kaspersky Endpoint Agent.

O Kaspersky Endpoint Security suporta a atualização sem reiniciar o computador. Pode selecionar o modo de atualização da aplicação nas propriedades da política.

5 A verificar o funcionamento da aplicação

Se, após a instalação da aplicação, o computador tiver o estado *Critical* na consola do Kaspersky Security Center:

- Certifique-se de que o computador tem o Agente de Rede versão 13.2 ou superior instalado.
- Verifique o estado de funcionamento do agente integrado ao consultar o *Report on status of application components*. Se um componente tiver o estado *Not installed*, instale o componente com a tarefa *Change application components*. Se um componente tiver o estado *Não abrangido pela licença*, certifique-se de que ativou a funcionalidade do agente integrado.
- Certifique-se de que aceita a Declaração da Kaspersky Security Network na nova política do Kaspersky Endpoint Security for Windows.

6 A verificar a ligação com o servidor do Kaspersky Anti Targeted Attack Platform

Verifique a ligação com o servidor da Kaspersky Anti Targeted Attack Platform. Para tal:

1. Verifique se tem um certificado válido.
2. Verifique as definições de ligação do servidor.
3. Verifique o registo de eventos.

   Se for estabelecida uma ligação ao servidor, a aplicação envia o evento *Successful connection to the EDR Expert server*. Se não ocorrer nenhum evento de ligação com êxito e não ocorrerem eventos com erros de ligação, verifique as definições do registo de eventos e ative o envio de eventos para o Endpoint Detection and Response (KATA).

O estado da ligação ao servidor não afeta o estado do computador na consola do Kaspersky Security Center. Portanto, se não existir ligação com o servidor, o computador ainda pode ter o estado *OK*. Verifique o registo de eventos para verificar a ligação ao servidor.

7 A verificar o desempenho

Se o desempenho do seu computador diminuiu após a instalação ou atualização de uma aplicação, pode otimizar a transferência de dados. Para tal:

1. Desative o componente EDR (KATA) e verifique se a degradação do desempenho é devido ao EDR (KATA).
2. Para aplicações fiáveis, desative a recolha de telemetria nas operações de entrada na consola (ativado por predefinição).
3. Adicione aplicações que reduzem o desempenho do computador à lista de aplicações fiáveis.
4. Entre em contacto com o Suporte Técnico da Kaspersky. Especialistas do suporte irão ajudá-lo a configurar a filtragem de telemetria no Kaspersky Anti Targeted Attack Platform. Esta ação reduzirá o volume de tráfego. Se o desempenho do seu computador for afetado por uma determinada aplicação, anexe o pacote de distribuição dessa aplicação à solicitação.

Endpoint Detection and Response Expert (on-premises)



O Kaspersky Endpoint Security for Windows suporta a integração com a solução Kaspersky Endpoint Detection and Response Expert (on-premises). O *Kaspersky Endpoint Detection and Response Expert (on-premises)* é uma solução de cibersegurança empresarial que inclui aplicações da Kaspersky que permitem a uma organização defender-se contra a maioria dos tipos de riscos cibernéticos e cobrir 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 numa única interface e permite integrar aplicações da Kaspersky com aplicações de terceiros num sistema de segurança abrangente.

Um dos elementos centrais da solução é o *SIEM*. O SIEM rastreia eventos provenientes de todos os componentes e correlaciona esses eventos entre si usando regras definidas pelo fornecedor e pelo utilizador. O EDR Expert (on-premises) analisa os registos e a telemetria recebidos da infraestrutura corporativa para detetar automaticamente ataques e permite investigar incidentes usando um gráfico de investigação unificado que combina todos os eventos recolhidos no EDR Expert (on-premises), incluindo eventos de aplicações da Kaspersky e produtos de segurança da informação de terceiros.

Para responder a incidentes avançados, o EDR Expert (on-premises) utiliza cenários predefinidos e definidos pelo utilizador. Também pode usar ações de resposta de aplicações de terceiros e cenários de resposta que envolvem várias aplicações.

Ferramentas de Informações sobre Ameaças

O Kaspersky Endpoint Detection and Response utiliza as seguintes ferramentas de Threat Intelligence:

- A integração com o Kaspersky Threat Intelligence Portal, que contém e apresenta informações sobre a reputação de ficheiros e endereços da Internet.
- A base de dados de Ameaças da Kaspersky.
- A infraestrutura dos serviços em nuvem da Kaspersky Security Network (doravante também chamada de "KSN"), que fornece acesso a ficheiros em tempo real, websites e informações de reputação de software da base de conhecimento da Kaspersky. A utilização de dados da Kaspersky Security Network permite uma resposta mais rápida das aplicações da Kaspersky a ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos diagnósticos positivos.

Princípio do funcionamento da solução

A Kaspersky Endpoint Security é instalada em computadores individuais na infraestrutura de TI corporativa e monitoriza continuamente os processos, as ligações de rede abertas e os ficheiros que estão a ser modificados.

Quando instalado no modo padrão na infraestrutura VDI, o Kaspersky Endpoint Security suporta a integração com o EDR Expert (on-premises). No entanto, não é garantido o funcionamento das restantes funcionalidades da aplicação. Para proteger as máquinas virtuais na infraestrutura VDI, recomendamos a utilização do Kaspersky Endpoint Security no modo Light Agent.

As informações sobre eventos no computador (telemetria) são enviadas para o servidor EDR Expert (on-premises). Neste caso, o Kaspersky Endpoint Security também envia informações sobre ameaças detetadas pela aplicação, bem como informações sobre os resultados de processamento destas ameaças para os servidores de recolha de telemetria.

A integração do EDR Expert (on-premises) é configurada na consola do Kaspersky Security Center. O agente integrado é então gerido usando a Open Single Management Platform (OSMP), incluindo a execução de tarefas, a gestão de objetos em quarentena, a exibição de relatórios e outras ações.

Configurações do Kaspersky Endpoint Security para funcionar com EDR Expert (on-premises)

As seguintes configurações podem ser utilizadas para funcionar com EDR Expert (on-premises):

- **[KES+agente integrado]**. Nesta configuração, o Kaspersky Endpoint Security atua como a aplicação que garante a segurança do computador e como a aplicação para funcionar com o EDR Expert (on-premises). O agente integrado para 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 Endpoint Detection and Response Agent (EDR Agent). Nesta configuração, o EDR Agent é compatível com aplicações de 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 EDR Expert (on-premises)

Para integrar com a solução Kaspersky Endpoint Detection and Response Expert (on-premises), tem de 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.

Para o Endpoint Detection and Response Expert (on-premises) funcionar, tem de cumprir as seguintes condições:

- O OSMP (Open Single Management Platform) está instalado.
- A aplicação é ativada e a funcionalidade é abrangida pela licença.
- O componente Endpoint Detection and Response Expert (on-premises) está ativado.
- Os componentes da aplicação que asseguram o funcionamento do EDR Expert (on-premises) estão ativados e operacionais. Os seguintes componentes asseguram o funcionamento do EDR Expert (on-premises):
  - Proteção contra ameaças de ficheiros.
  - Proteção contra ameaças da Web.
  - Proteção contra ameaças de correio.
  - Prevenção de explorações.
  - Deteção de comportamento.
  - Prevenção contra invasões.
  - Motor de remediação.
  - Controlo de Anomalias Adaptativo.

A configuração da integração do EDR Expert (on-premises) envolve os seguintes passos:

1. **Instalar o componente EDR Expert (on-premises)**

   Pode selecionar o componente EDR Expert (on-premises) durante a instalação ou atualização, bem como através da tarefa *Alterar componentes da aplicação*.

   > Tem de reiniciar o computador para terminar a atualização da aplicação com o novo componente.

2. **Ativar o Kaspersky Endpoint Detection and Response Expert (on-premises)**

   Comprar uma licença separada para o EDR Expert (on-premises) (Suplemento do Kaspersky Endpoint Detection and Response Expert (on-premises)).

   A funcionalidade estará disponível após adicionar uma chave individual para o Kaspersky Endpoint Detection and Response Expert (on-premises). Como resultado, são adicionadas duas chaves no computador: uma chave para o Kaspersky Endpoint Security e uma chave para o Kaspersky Endpoint Detection and Response Expert (on-premises).

   A licença para a funcionalidade Endpoint Detection and Response Expert (on-premises) autónoma é a mesma que a licença do Kaspersky Endpoint Security.

   Certifique-se de que a funcionalidade EDR Expert (on-premises) é incluída na licença e é executada na interface local da aplicação.

3. **Ligar ao servidor de recolha de telemetria e ao servidor de resposta**

O Kaspersky Endpoint Detection and Response Expert (on-premises) requer uma conexão fiável entre o Kaspersky Endpoint Security e dois servidores:

- Um *servidor de recolha de telemetria* é um servidor que faz parte de uma solução SIEM e que recolhe, normaliza, correlaciona, analisa e armazena informações sobre eventos que ocorrem no computador.
- Um *servidor de resposta* é um servidor para receber e analisar dados, estudar o comportamento de objetos e publicar os resultados desses estudos.

Para configurar uma ligação fiável, tem de utilizar um certificado TLS. Pode 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, tem de adicionar o certificado TLS ao Kaspersky Endpoint Security (consulte as instruções abaixo).

Por padrão, o Kaspersky Endpoint Security verifica apenas o certificado dos servidores. Para tornar a ligação mais segura, também pode ativar a verificação do computador no servidor (autenticação bidirecional). Para ativar esta verificação, tem de ativar a autenticação bidirecional nas definições do servidor e do Kaspersky Endpoint Security. Para usar a autenticação bidirecional, também irá precisar de um cripto-contentor. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)).

Como ligar um computador do Kaspersky Endpoint Security ao EDR Expert (on-premises) usando a Consola Web

1. Na janela principal da Consola Web, selecione o separador **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration → Endpoint Detection and Response Expert (on-premises)**.
5. Ative o botão de alternar **Endpoint Detection and Response Expert (on-premises) ENABLED**.
6. Para configurar o EDR Expert (on-premises), selecione **Endpoint Detection and Response Expert (version 8.0 or later)** da lista de soluções.
7. Configure a ligação dos *servidores de recolha de telemetria*:

   a. No bloco **Connection to telemetry collection servers**, clique na ligação **Connection settings**.

   b. Configure a ligação dos servidores de recolha de telemetria:

   - **Timeout (sec)**. Tempo limite máximo de resposta do servidor. Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor diferente.
   - **Server certificate**. Certificado TLS para estabelecer uma ligação fiável com o servidor. Pode obter um certificado TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Use two-way authentication**. Autenticação bidirecional ao estabelecer uma ligação segura entre o Kaspersky Endpoint Security e o servidor. Para utilizar a autenticação bidirecional, é necessário ativar a autenticação bidirecional nas definições do servidor e, em seguida, obter um contentor criptográfico e definir uma password para proteger o contentor criptográfico. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). Após configurar as definições do servidor, é também necessário ativar a autenticação bidirecional nas definições do Kaspersky Endpoint Security e carregar um contentor criptográfico protegido por password.

  O cripto-contentor deve ser protegido por password. Não é possível adicionar um cripto-contentor com uma password em branco.

c. Clique em **OK**.

d. Adicione servidores de recolha de telemetria. Para o fazer, especifique o endereço do servidor (IPv4, IPv6) e a porta para se ligar ao servidor.

   Pode adicionar vários endereços do servidor de recolha de telemetria. O Kaspersky Endpoint Security tenta ligar-se ao servidor utilizando o primeiro endereço IP. Se não for possível estabelecer uma ligação, o Kaspersky Endpoint Security tenta ligar-se utilizando o segundo endereço IP da lista e assim sucessivamente.

e. Se necessário, configure a telemetria.

8. Configure a ligação dos *servidores de resposta*:

   a. No bloco **Connection to response servers**, configure a definição **Send sync request to server every (min)**. Frequência de pedidos de sincronização enviados ao servidor. Durante a sincronização, o Kaspersky Endpoint Security recebe tarefas de resposta a ameaças e envia os resultados dessas tarefas.

   b. Clique na hiperligação **Connection settings**.

   c. Configure a ligação dos servidores de resposta:

   - **Timeout (sec)**. Tempo limite máximo de resposta do servidor. Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor diferente.

   - **Server certificate**. Certificado TLS para estabelecer uma ligação fiável com o servidor. Pode obter um certificado TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Use two-way authentication**. Autenticação bidirecional ao estabelecer uma ligação segura entre o Kaspersky Endpoint Security e o servidor. Para utilizar a autenticação bidirecional, é necessário ativar a autenticação bidirecional nas definições do servidor e, em seguida, obter um contentor criptográfico e definir uma password para proteger o contentor criptográfico. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). Após configurar as definições do servidor, é também necessário ativar a autenticação bidirecional nas definições do Kaspersky Endpoint Security e carregar um contentor criptográfico protegido por password.

  O cripto-contentor deve ser protegido por password. Não é possível adicionar um cripto-contentor com uma password em branco.

d. Clique em **OK**.

e. Adicione servidores de resposta. Para o fazer, especifique o endereço do servidor (IPv4, IPv6) e a porta para se ligar ao servidor.

   Pode adicionar vários endereços do servidor de resposta. O Kaspersky Endpoint Security tenta ligar-se ao servidor utilizando o primeiro endereço IP. Se não for possível estabelecer uma ligação, o Kaspersky Endpoint Security tenta ligar-se utilizando o segundo endereço IP da lista e assim sucessivamente.

9. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Pode verificar o estado do componente utilizando o *Report on status of application components*. Pode também ver o estado de funcionamento de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente **Endpoint Detection and Response Expert (on-premises)** será adicionado à lista de componentes do Kaspersky Endpoint Security.

Configurar as definições 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 e envia-os para os servidores de recolha de telemetria 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 é satisfeita:

- O intervalo de sincronização acaba.
- O número de eventos na memória intermédia excede o limite superior.

Portanto, por defeito, a aplicação sincroniza a cada 30 segundos ou sempre que a memória intermédia contém 1024 eventos. Pode configurar o comportamento de sincronização na política do Kaspersky Endpoint Security e selecionar os valores ideais para corresponder à sua carga de rede (consulte as instruções abaixo).

Se não houver ligação entre o Kaspersky Endpoint Security e o servidor, a aplicação coloca novos eventos na fila. Quando a ligação é restaurada, o Kaspersky Endpoint Security envia eventos da fila para o servidor na ordem correta. Para evitar sobrecarregar o servidor, o Kaspersky Endpoint Security pode ignorar alguns eventos. Para ativar esta opção, pode otimizar as definições de transmissão de eventos, por exemplo, para definir um valor máximo de eventos por hora (consulte as instruções abaixo).

Para configurar as definições de telemetria, siga os seguintes passos:

1. Na janela principal da Consola Web, selecione o separador **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration → Endpoint Detection and Response Expert (on-premises)**.
5. Para configurar o EDR Expert (on-premises), selecione **Endpoint Detection and Response Expert (version 8.0 or later)** da lista de soluções.
6. Certifique-se de que a caixa de verificação **Send telemetry to telemetry collection servers** está selecionada no bloco **Data transmission settings**.
7. Se necessário, selecione a caixa de verificação **Send telemetry with IOA only**. *Indicador de Ataque (IOA)* é uma regra que contém uma descrição do comportamento suspeito no sistema que pode indicar um ataque direcionado. A aplicação compara o comportamento contínuo no sistema com essas regras e regista eventos que indicam um ataque direcionado. A aplicação utiliza a tecnologia de *análise em tempo real*, que permite o acompanhamento em tempo real desses eventos.
8. Se necessário, configure a sincronização com as definições do servidor no bloco **Data transmission settings**:

   - **Maximum event transmission delay (sec)**. A aplicação sincroniza com o servidor para enviar eventos após o término do intervalo de sincronização. A predefinição é 30 segundos.
   - **Maximum number of event packages**. A aplicação é sincronizada com o servidor quando a memória intermédia está cheia de eventos. A predefinição é 1024 eventos.
9. Se for necessário, desmarque a caixa de verificação **Enable request throttling** no bloco **Request throttling**.

   Esta ação ajuda a otimizar a carga no servidor. Se esta funcionalidade estiver ativada, a aplicação restringe a transmissão de eventos. Se o número de eventos exceder os limites configurados, o Kaspersky Endpoint Security irá interromper o envio de eventos. Esta opção está ativada por predefinição.
10. Configure as definições de otimização para enviar eventos ao servidor:

    - **Maximum number of events per hour**. A aplicação analisa o fluxo de dados de telemetria e restringe o envio de eventos se o fluxo de eventos exceder o limite de eventos por hora configurado. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. A predefinição é 3000 eventos por hora. Se a aplicação estiver instalada num servidor, o fluxo de dados de telemetria é mais elevado. Para os servidores, recomenda-se que o valor seja aumentado para 60.000 eventos por hora.
    - **Percentage of event limit excess**. A aplicação ordena os eventos por tipo (por exemplo, eventos "alterações no registo") e restringe a transmissão de eventos se a proporção de eventos do mesmo tipo para o número total de eventos exceder o limite configurado em percentagem. O Kaspersky Endpoint Security retoma o envio de eventos quando a proporção de outros eventos para o número total de eventos se torna grande o suficiente novamente. A predefinição é 15%.
11. No bloco **Connection to response servers**, insira um valor para o parâmetro **Send sync request to server every (min)**.

12. Frequência de pedidos de sincronização enviados ao servidor. Durante a sincronização, o Kaspersky Endpoint Security envia informações sobre as definições e tarefas modificadas da aplicação.

13. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Exclusões de telemetria do EDR Expert (on-premises)

Para melhorar o desempenho e otimizar a transmissão de dados para o servidor de recolha de telemetria, pode adicionar exclusões de telemetria. Por exemplo, pode optar por não enviar dados de comunicações de rede para aplicações individuais.

> Usar demasiadas regras pode aumentar a carga no servidor de recolha de telemetria e reduzir o desempenho do computador. Recomendamos que adicione apenas as regras necessárias.

Para criar uma exclusão de telemetria na Consola Web e na Cloud Console:

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **General Settings** → **Telemetry Settings**.

5. Selecione o separador **EDR Expert (on-premises) telemetry**.

6. No bloco **General exclusions**, clique no botão **Add**.

   Abre-se a janela **Add exclusion rule**.

7. Se necessário, altere o estado da regra. Por predefinição, a regra está ativada.

8. Insira um nome para a regra.

9. Selecione a ação a ser realizada quando a regra for acionada:

   - **Do not collect**. O evento filtrado será excluído da telemetria enviada.

   - **Exclude IOA**. O evento que aciona a regra da IOA será excluído da telemetria enviada.

10. Se a opção **Exclude IOA** estiver selecionada, especifique as regras da IOA a serem adicionadas às exclusões:

    - **Exclude all**. Quando a condição especificada for atendida, a aplicação excluirá da telemetria os eventos gerados com base em todas as regras de IOA.

    - **Exclude by GUID**. Especifique o GUID da regra da IOA. Pode especificar vários GUID ao utilizar `,`. Para obter mais detalhes sobre as regras da 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 o valor do campo do evento será comparado.

Lista de operadores condicionais

Operador	Descrição
<	Se o valor do campo for inferior ao valor especificado na condição, o evento será excluído.
≤	Se o valor do campo for inferior ou igual ao valor especificado na condição, o evento será excluído.
=	Se o valor do campo for igual ao valor especificado na condição, o evento será excluído.
≥	Se o valor do campo for maior ou igual ao valor especificado na condição, o evento será excluído.
>	Se o valor do campo for superior ao valor especificado na condição, o evento será excluído.
≠	Se o valor do campo não for igual ao valor especificado na condição, o evento será excluído.
is like	Se o valor do campo corresponder à máscara especificada na condição, o evento será excluído. A aplicação suporta os caracteres `*` e `?` ao introduzir uma máscara:
is not like	Se o valor do campo não corresponder à máscara especificada na condição, o evento será excluído. A aplicação suporta os caracteres `*` e `?` ao introduzir uma máscara:
one of	Se o valor do campo corresponder a um dos valores da lista especificada na condição, o evento é considerado filtrado.
none of	Se o valor do campo não corresponder a nenhum dos valores da lista especificada na condição, o evento é considerado filtrado.
is like one of	Se o valor do campo corresponder a uma das máscaras especificadas na condição, o evento será excluído. A aplicação suporta os caracteres * e ? ao introduzir uma máscara.
is not like one of	Se o valor do campo não corresponder a nenhuma das máscaras especificadas na condição, o evento será excluído. A aplicação suporta os caracteres * e ? ao introduzir uma máscara.
exists	Se o campo especificado na condição estiver presente no evento, este será excluído.
not exists	Se o campo especificado na condição não estiver presente no evento, este será excluído.
contains	Se o valor especificado na condição estiver presente no valor do campo, o evento será excluído.
is equal to	Se o valor do campo for igual ao valor especificado na condição, o evento será excluído. A verificação não distingue maiúsculas de minúsculas.
bitwise AND	Se o resultado da operação AND (&) bit a bit entre o valor do campo e o valor especificado na condição for 1, o evento será excluído.

12. Se necessário, pode criar critérios de filtragem complexos, adicionando várias condições de filtragem e grupos de condições. Também pode adicionar condições aninhadas e grupos de condições a um grupo de condições. Pode utilizar os seguintes operadores:

    - **AND** significa que o filtro seleciona eventos que atendem a todas as condições especificadas.
    - **OR** significa que o filtro seleciona os eventos que cumprem uma das condições especificadas.
    - **NOT** (para usar este operador, selecione a opção **Add NOT before**) 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. Se o seu computador estiver a executar a Open Single Management Platform (OSMP), pode verificar a regra de filtragem que criou. Para executar a verificação, clique no botão **Check rule**.

    Na janela que se abre, será exibida uma tabela de eventos filtrados pela regra criada. Para obter mais detalhes, consulte a Ajuda do EDR Expert (on-premises).

14. Se necessário, em **All event types**, adicione exclusões de telemetria por tipo de evento.

    a. Clique no nome do tipo de evento.

    b. Na janela que abre, clique no botão **Set up manually**.

    c. Se necessário, configure a transmissão de telemetria para o tipo de evento selecionado ao utilizar o botão **Send event**. Por padrão, a transmissão de telemetria está ativada para todos os tipos de eventos.

    d. No bloco **Exclusion rules**, clique no botão **Add**.

    Abre-se a janela **Add exclusion rule**.

    e. Execute as ações descritas nos passos 7 a 13 para cada regra que adicionar.

15. Para alguns tipos de eventos, também é possível adicionar regras de inclusão para ampliar a telemetria recolhida:

    a. No bloco **Inclusion rules**, clique no botão **Add**.

    Abre-se a janela **Add inclusion rules**.

    b. Insira um nome para a regra.

    c. Em **Condition**, introduza os valores nos campos apresentados. 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 guarde as suas alterações.

Exportar e importar filtros de eventos do EDR Expert (on-premises)

Pode exportar a lista de exclusões para um ficheiro JSON. Em seguida, pode modificar o ficheiro para, por exemplo, adicionar um grande número de ID de eventos. Também pode utilizar a função de exportação/importação para fazer uma cópia de segurança de filtros de eventos ou para migrar a lista para um servidor diferente.

> Usar demasiadas regras pode aumentar a carga no servidor de recolha de telemetria e reduzir o desempenho do computador. Recomendamos que adicione apenas as regras necessárias.

Como exportar e importar filtros de eventos na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Definições gerais → Exclusões e tipos de objetos**.

5. No bloco **Definições de telemetria → Telemetria do EDR Expert (on-premises)**, clique no botão **Definições**.

6. Para exportar os filtros de eventos:

   a. Clique em **Exportar**.

   Na janela que se abre, especifique o nome do ficheiro JSON para o qual pretende exportar os filtros de eventos e selecione a pasta onde pretende guardar este ficheiro.

   b. Guardar o ficheiro.

   O Kaspersky Endpoint Security exporta os filtros de eventos para o ficheiro JSON.

7. Para importar os filtros de eventos:

   a. Clique em **Importar**.

   b. Na janela que se abre, selecione o ficheiro JSON a partir do qual pretende importar os filtros de eventos.

   c. Abrir o ficheiro.

   Se as regras de filtragem de eventos já existirem no computador, o Kaspersky Endpoint Security irá substitui-las durante a importação.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como exportar e importar filtros de eventos na Consola Web

1. Na janela principal da Consola Web, selecione o separador **Asset management → Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **General Settings → Telemetry Settings**.

5. Selecione o separador **EDR Expert (on-premises) telemetry**.

6. Para exportar os filtros de eventos:

   a. Clique em **Export**.

   b. Na janela que se abre, especifique o nome do ficheiro JSON para o qual pretende exportar os filtros de eventos e selecione a pasta onde pretende guardar este ficheiro.

   c. Guardar o ficheiro.

   O Kaspersky Endpoint Security exporta os filtros de eventos para o ficheiro JSON.

7. Para importar os filtros de eventos:

   a. Clique em **Import**.

   b. Na janela que se abre, selecione o ficheiro JSON a partir do qual pretende importar os filtros de eventos.

c. Selecione como deseja que as regras de filtragem de eventos sejam importadas: adicionando-as às regras existentes ou descartando as regras existentes e substituindo-as por novas.

d. Abrir o ficheiro.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Também pode exportar ou importar filtros de eventos na linha de comandos.

Considerações especiais ao usar perfis de política para configurar a integração com o EDR Expert (on-premises) e o EDR (KATA)

Para configurar a integração com o EDR (KATA) para determinados grupos administrativos e com o EDR Expert (on-premises) para outros, como parte de uma única política, terá de usar perfis de política. Tem de configurar as definições de integração do EDR (KATA) nas propriedades da política, e a integração do EDR Expert (on-premises) para os grupos de administração selecionados deve ser configurada nas propriedades do perfil da política.

A utilização de perfis de política para configurar a integração com o EDR Expert (on-premises) apresenta as seguintes limitações:

- Se configurar a integração com o EDR Expert (on-premises) nas propriedades da política, estas definições serão aplicadas a todos os grupos de administração; as definições de integração dos perfis de política não serão aplicadas.

- Ao utilizar perfis de política para configurar a integração com o EDR Expert (on-premises), não é possível utilizar a Consola de Administração (MMC) para gerir as políticas. Quando abrir as propriedades da política na Consola de Administração, as definições de integração do EDR Expert (on-premises) nos perfis da política serão substituídas pelas definições da própria política, o que fará com que o componente funcione incorretamente. Terá de repor as definições do componente Endpoint Detection and Response Expert (on-premises) de acordo com as instruções abaixo.

- Ao utilizar perfis de política para configurar a integração com o EDR Expert (on-premises), não é possível utilizar políticas secundárias.

Se já tiver uma política configurada numa versão anterior do plug-in web, deve redefinir as definições para o componente Endpoint Detection and Response Expert (on-premises) para aplicar as definições de integração do EDR Expert (on-premises) aos dispositivos geridos a partir dos perfis de política.

Para repor as definições do componente:

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.

5. Altere o modo de funcionamento de **Endpoint Detection and Response Expert (version 7.1 or earlier)** para **Modo Endpoint Detection and Response Expert (versão 8.0 ou posterior)**.

6. Troque para **Endpoint Detection and Response Expert (version 7.1 or earlier)**.

7. Guarde as suas 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. A previsão é que esta funcionalidade seja disponibilizada até ao final de 2026. Acompanhe as nossas Notas de Versão para ficar a par das atualizações da aplicação e das novas funcionalidades.



O Kaspersky Endpoint Security suporta a integração com a solução Kaspersky Endpoint Detection and Response Expert (cloud). O *Kaspersky Endpoint Detection and Response Expert (cloud)* é uma solução de cibersegurança empresarial baseada na nuvem que inclui aplicações da Kaspersky que permitem a uma organização defender-se contra a maioria dos tipos de riscos cibernéticos e cobrir os cenários mais importantes de propagação de ameaças. Os componentes do EDR Expert (cloud) são implementados no Open Single Management Platform (OSMP). Esta plataforma executa cenários multiplataforma numa única interface e permite integrar aplicações da Kaspersky com aplicações de terceiros num sistema de segurança abrangente.

Um dos elementos centrais da solução é o *SIEM*. O SIEM rastreia eventos provenientes de todos os componentes e correlaciona esses eventos entre si usando regras definidas pelo fornecedor e pelo utilizador. O EDR Expert (cloud) analisa os registos e a telemetria recebidos da infraestrutura corporativa para detetar automaticamente ataques e permite investigar incidentes usando um gráfico de investigação unificado que combina todos os eventos recolhidos no EDR Expert (cloud), incluindo eventos de aplicações da Kaspersky e produtos de segurança da informação de terceiros.

Para responder a incidentes avançados, o EDR Expert (cloud) utiliza cenários predefinidos e definidos pelo utilizador. Também pode usar ações de resposta de aplicações de terceiros e cenários de resposta que envolvem várias aplicações.

Ferramentas de Informações sobre Ameaças

O Kaspersky Endpoint Detection and Response utiliza as seguintes ferramentas de Threat Intelligence:

- A integração com o Kaspersky Threat Intelligence Portal, que contém e apresenta informações sobre a reputação de ficheiros e endereços da Internet.
- A base de dados de Ameaças da Kaspersky.
- A infraestrutura dos serviços em nuvem da Kaspersky Security Network (doravante também chamada de "KSN"), que fornece acesso a ficheiros em tempo real, websites e informações de reputação de software da base de conhecimento da Kaspersky. A utilização de dados da Kaspersky Security Network permite uma resposta mais rápida das aplicações da Kaspersky a ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos diagnósticos positivos.

Princípio do funcionamento da solução

A Kaspersky Endpoint Security é instalada em computadores individuais na infraestrutura de TI corporativa e monitoriza continuamente os processos, as ligações de rede abertas e os ficheiros que estão a ser modificados.

As informações sobre eventos no computador (telemetria) são enviadas para o servidor EDR Expert (cloud). Neste caso, o Kaspersky Endpoint Security também envia informações sobre ameaças detetadas pela aplicação, bem como informações sobre os resultados de processamento destas ameaças para os servidores de recolha de telemetria.

A integração do EDR Expert (cloud) é configurada na consola do Kaspersky Security Center. O agente integrado é então gerido usando a Open Single Management Platform (OSMP), incluindo a execução de tarefas, a gestão de objetos em quarentena, a exibição de relatórios e outras ações.

Integração do agente integrado com EDR Expert (cloud)

Para configurar a integração com a solução Kaspersky Endpoint Detection and Response (cloud), tem de 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 funcionamento do EDR Expert (cloud)

Para que o EDR Expert (cloud) funcione, é necessário que as seguintes condições sejam cumpridas:

- A infraestrutura do Kaspersky Endpoint Detection and Response Expert (cloud) está disponível na sua região. Para obter informações sobre a disponibilidade da infraestrutura do EDR Expert (cloud) na sua região, contacte o Suporte Técnico.
- O OSMP (Open Single Management Platform) está instalado.
- Kaspersky Endpoint Security instalado no modo padrão.
- A aplicação do Kaspersky Endpoint Security é ativada e a funcionalidade é abrangida pela licença.
- Aceitou os termos do Contrato de Tratamento de Dados do Kaspersky Endpoint Detection and Response Expert (cloud).
- O componente Endpoint Detection and Response Expert (cloud) está ativado.
- Os componentes da aplicação que asseguram o funcionamento do EDR Expert (cloud) estão ativados e operacionais:
  - Proteção contra ameaças de ficheiros.
  - Proteção contra ameaças da Web.
  - Proteção contra ameaças de correio.
  - Prevenção de explorações.
  - Deteção de comportamento.
  - Prevenção contra invasões.

- Motor de remediação.
- Controlo de Anomalias Adaptativo.

Passos para integração com o EDR Expert (cloud)

A configuração da integração do EDR Expert (cloud) envolve os seguintes passos:

1. **Instalar o componente Endpoint Detection and Response Expert (cloud)**

   Pode selecionar o componente Endpoint Detection and Response Expert (cloud) durante a instalação ou atualização, bem como através da tarefa *Alterar componentes da aplicação*.

   > Tem de reiniciar o computador para terminar a atualização da aplicação com o novo componente.

2. **Ativar o Kaspersky Endpoint Detection and Response Expert (cloud)**

   Tem de comprar uma licença separada para o Kaspersky Endpoint Detection and Response Expert (cloud).

   A funcionalidade estará disponível após adicionar uma chave individual para o Kaspersky Endpoint Detection and Response Expert (cloud). Como resultado, são adicionadas duas chaves no computador: uma chave para o Kaspersky Endpoint Security e uma chave para o Kaspersky Endpoint Detection and Response Expert (cloud).

   A licença para a funcionalidade Endpoint Detection and Response Expert (cloud) autónoma é a mesma que a licença do Kaspersky Endpoint Security.

   Certifique-se de que a funcionalidade EDR Expert (cloud) é incluída na licença e é executada na interface local da aplicação.

3. **Ligar ao servidor de recolha de telemetria e ao servidor de resposta**

   O Kaspersky Endpoint Detection and Response Expert (cloud) requer uma conexão fiável entre o Kaspersky Endpoint Security e dois servidores:

   - Um *servidor de recolha de telemetria* é um servidor que faz parte de uma solução SIEM e que recolhe, normaliza, correlaciona, analisa e armazena informações sobre eventos que ocorrem no computador.
   - Um *servidor de resposta* é um servidor para receber e analisar dados, estudar o comportamento de objetos e publicar os resultados desses estudos.

   Como ligar um computador do Kaspersky Endpoint Security ao EDR Expert (cloud) usando a Consola Web

   1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
   2. Clique no nome da política do Kaspersky Endpoint Security.

      É apresentada a janela de propriedades da política.
   3. Selecione o separador **Application settings**.
   4. Aceda a **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (cloud)**.
   5. Ative o componente ao utilizar o botão **Endpoint Detection and Response Expert (cloud) DISABLED**.

6. Se a política atual for uma política secundária e a política principal proibir alterações nas definições de integração do EDR Expert (cloud) ("cadeado" fechado), pode configurar a herança de definições na secção **Inheritance**:

   - **Inherit connection settings from the policy** (valor padrão). As definições de ligação serão herdadas da política principal. Não poderá editar as definições.

   - **Use custom connection settings**. Pode configurar as definições de ligação manualmente.

7. O separador **Response server** apresenta o nome de domínio completo e a porta do servidor de resposta, que são obtidos automaticamente. Se a política de segurança da sua infraestrutura não permitir que se ligue diretamente aos servidores do EDR Expert (cloud), pode configurar uma ligação através de um túnel TCP:

   a. Selecione a caixa de verificação **Use a TCP tunnel for response**.

   b. Especifique o endereço do servidor (IPv4, IPv6) e a porta para se ligar ao túnel.

8. Se necessário, defina a frequência de envio de pedidos de sincronização para o servidor no campo **Send sync request to server every (min)**. Durante a sincronização, o Kaspersky Endpoint Security recebe tarefas de resposta a ameaças e envia os resultados dessas tarefas.

9. Aceda ao separador **Telemetry collection server**.

10. Configure as definições de ligação dos servidores de recolha de telemetria:

    a. Clique na hiperligação **Edit**.

    b. Na janela que se abre, selecione o servidor de recolha de telemetria da lista. O coletor KUMA funciona como servidor de recolha de telemetria no EDR Expert (cloud). Para mais detalhes, consulte a Ajuda do Kaspersky Unified Monitoring and Analysis Platform.

    Se ocorrer um erro durante a ligação ao servidor de recolha de telemetria, selecione um servidor diferente. Se não conseguir estabelecer a ligação ao servidor de recolha de telemetria, contacte o Suporte Técnico.

    c. Se necessário, pode configurar uma ligação ao servidor de recolha de telemetria através de um túnel TCP, tal como faria para o servidor de resposta.

11. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Pode verificar o estado do componente utilizando o *Report on status of application components*. Pode também ver o estado de funcionamento de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente **Endpoint Detection and Response Expert (cloud)** será adicionado à lista de componentes do Kaspersky Endpoint Security.

Configurar as definições 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 e envia-os para os servidores de recolha de telemetria 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 é satisfeita:

- O intervalo de sincronização acaba.
- O número de eventos na memória intermédia excede o limite superior.

Portanto, por defeito, a aplicação sincroniza a cada 30 segundos ou sempre que a memória intermédia contém 1024 eventos. Pode configurar o comportamento de sincronização na política do Kaspersky Endpoint Security e selecionar os valores ideais para corresponder à sua carga de rede (consulte as instruções abaixo).

Se não houver ligação entre o Kaspersky Endpoint Security e o servidor, a aplicação coloca novos eventos na fila. Quando a ligação é restaurada, o Kaspersky Endpoint Security envia eventos da fila para o servidor na ordem correta. Para evitar sobrecarregar o servidor, o Kaspersky Endpoint Security pode ignorar alguns eventos. Para ativar esta opção, pode otimizar as definições de transmissão de eventos, por exemplo, para definir um valor máximo de eventos por hora (consulte as instruções abaixo).

Para configurar as definições de telemetria, siga os seguintes passos:

1. Na janela principal da Consola Web, selecione o separador **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration → Endpoint Detection and Response Expert (cloud)**.
5. Na janela que abre, selecione o separador **Data transmission settings**.
6. Certifique-se de que a caixa de verificação **Sending telemetry ENABLED** está assinalada.
7. Se necessário, ative a funcionalidade **Send telemetry with IOA only**. *Indicador de Ataque (IOA)* é uma regra que contém uma descrição do comportamento suspeito no sistema que pode indicar um ataque direcionado. A aplicação compara o comportamento contínuo no sistema com essas regras e regista eventos que indicam um ataque direcionado. A aplicação utiliza a tecnologia de *análise em tempo real*, que permite o acompanhamento em tempo real desses eventos. Por predefinição, a funcionalidade está desativada.
8. Se necessário, configure as definições de sincronização do servidor:
   - **Maximum event transmission delay (sec)**. A aplicação sincroniza com o servidor para enviar eventos após o término do intervalo de sincronização. A predefinição é 30 segundos.
   - **Maximum number of event packages**. A aplicação é sincronizada com o servidor quando a memória intermédia está cheia de eventos. A predefinição é 1024 eventos.
9. Aceda ao separador **Request throttling**.

10. Se necessário, desative a limitação de pedidos utilizando o botão **Request throttling ENABLED**.

    Esta ação ajuda a otimizar a carga no servidor. Se esta funcionalidade estiver ativada, a aplicação restringe a transmissão de eventos. Se o número de eventos exceder os limites configurados, o Kaspersky Endpoint Security irá interromper o envio de eventos. Esta opção está ativada por predefinição.

11. Configure as definições de otimização para enviar eventos ao servidor:

    - **Maximum number of events per hour**. A aplicação analisa o fluxo de dados de telemetria e restringe o envio de eventos se o fluxo de eventos exceder o limite de eventos por hora configurado. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. A predefinição é 3000 eventos por hora. Se a aplicação estiver instalada num servidor, o fluxo de dados de telemetria é mais elevado. Para os servidores, recomenda-se que o valor seja aumentado para 60 000 eventos por hora.

    - **Percentage of event limit excess (%)**. A aplicação ordena os eventos por tipo (por exemplo, eventos "alterações no registo") e restringe a transmissão de eventos se a proporção de eventos do mesmo tipo para o número total de eventos exceder o limite configurado em percentagem. O Kaspersky Endpoint Security retoma o envio de eventos quando a proporção de outros eventos para o número total de eventos se torna grande o suficiente novamente. A predefinição é 15%.

12. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Exclusões de telemetria do EDR Expert (cloud)

Para melhorar o desempenho e otimizar a transmissão de dados para o servidor de recolha de telemetria, pode adicionar exclusões de telemetria. Por exemplo, pode optar por não enviar dados de comunicações de rede para aplicações individuais.

Usar demasiadas regras pode aumentar a carga no servidor de recolha de telemetria e reduzir o desempenho do computador. Recomendamos que adicione apenas as regras necessárias.

Para criar uma exclusão de telemetria na Consola Web e na Cloud Console:

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **General Settings** → **Telemetry Settings**.

5. Selecione o separador **EDR Expert (cloud) telemetry**.

6. No bloco **General exclusions**, clique no botão **Add**.

   Abre-se a janela **Add exclusion rule**.

7. Se necessário, altere o estado da regra. Por predefinição, a regra está ativada.

8. Insira um nome para a regra.

9. Selecione a ação a ser realizada quando a regra for acionada:

   - **Do not collect**. O evento filtrado será excluído da telemetria enviada.
   - **Exclude IOA**. O evento que aciona a regra da IOA será excluído da telemetria enviada.

10. Se a opção **Exclude IOA** estiver selecionada, especifique as regras da IOA a serem adicionadas às exclusões:

    - **Exclude all**. Quando a condição especificada for atendida, a aplicação excluirá da telemetria os eventos gerados com base em todas as regras de IOA.
    - **Exclude by GUID**. Especifique o GUID da regra da IOA. Pode especificar vários GUID ao utilizar `,`. Para obter mais detalhes sobre as regras da IOA, consulte a Ajuda do 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 o valor do campo do evento será comparado.

Lista de operadores condicionais

Operador	Descrição
<	Se o valor do campo for inferior ao valor especificado na condição, o evento será excluído.
≤	Se o valor do campo for inferior ou igual ao valor especificado na condição, o evento será excluído.
=	Se o valor do campo for igual ao valor especificado na condição, o evento será excluído.
≥	Se o valor do campo for maior ou igual ao valor especificado na condição, o evento será excluído.
>	Se o valor do campo for superior ao valor especificado na condição, o evento será excluído.
≠	Se o valor do campo não for igual ao valor especificado na condição, o evento será excluído.
is like	Se o valor do campo corresponder à máscara especificada na condição, o evento será excluído. A aplicação suporta os caracteres `*` e `?` ao introduzir uma máscara:
is not like	Se o valor do campo não corresponder à máscara especificada na condição, o evento será excluído. A aplicação suporta os caracteres `*` e `?` ao introduzir uma máscara:
one of	Se o valor do campo corresponder a um dos valores da lista especificada na condição, o evento é considerado filtrado.
none of	Se o valor do campo não corresponder a nenhum dos valores da lista especificada na condição, o evento é considerado filtrado.
is like one of	Se o valor do campo corresponder a uma das máscaras especificadas na condição, o evento será excluído. A aplicação suporta os caracteres * e ? ao introduzir uma máscara.
is not like one of	Se o valor do campo não corresponder a nenhuma das máscaras especificadas na condição, o evento será excluído. A aplicação suporta os caracteres * e ? ao introduzir uma máscara.
exists	Se o campo especificado na condição estiver presente no evento, este será excluído.
not exists	Se o campo especificado na condição não estiver presente no evento, este será excluído.
contains	Se o valor especificado na condição estiver presente no valor do campo, o evento será excluído.
is equal to	Se o valor do campo for igual ao valor especificado na condição, o evento será excluído. A verificação não distingue maiúsculas de minúsculas.
bitwise AND	Se o resultado da operação AND (&) bit a bit entre o valor do campo e o valor especificado na condição for 1, o evento será excluído.

12. Se necessário, pode criar critérios de filtragem complexos, adicionando várias condições de filtragem e grupos de condições. Também pode adicionar condições aninhadas e grupos de condições a um grupo de condições. Pode utilizar os seguintes operadores:

    - **AND** significa que o filtro seleciona eventos que atendem a todas as condições especificadas.
    - **OR** significa que o filtro seleciona os eventos que cumprem uma das condições especificadas.
    - **NOT** (para usar este operador, selecione a opção **Add NOT before**) 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 analisar a regra de filtragem que criou, clique no botão **Check rule**.

    Na janela que se abre, será exibida uma tabela de eventos filtrados pela regra criada. Para obter mais detalhes, consulte a Ajuda do EDR Expert (cloud).

14. Se necessário, em **All event types**, adicione exclusões de telemetria por tipo de evento.

    a. Clique no nome do tipo de evento.

    b. Na janela que abre, clique no botão **Set up manually**.

    c. Se necessário, configure a transmissão de telemetria para o tipo de evento selecionado ao utilizar o botão **Send event**. Por padrão, a transmissão de telemetria está ativada para todos os tipos de eventos.

    d. No bloco **Exclusion rules**, clique no botão **Add**.

    Abre-se a janela **Add exclusion rule**.

    e. Execute as ações descritas nos passos 7 a 13 para cada regra que adicionar.

15. Para alguns tipos de eventos, também é possível adicionar regras de inclusão para ampliar a telemetria recolhida:

    a. No bloco **Inclusion rules**, clique no botão **Add**.

    Abre-se a janela **Add inclusion rules**.

    b. Insira um nome para a regra.

    c. Em **Condition**, introduza os valores nos campos apresentados. 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 estão fechados (🔒) e guarde as suas alterações.

Como exportar ou importar filtros de eventos do EDR Expert (cloud)

Pode exportar a lista de exclusões para um ficheiro JSON. Em seguida, pode modificar o ficheiro para, por exemplo, adicionar um grande número de ID de eventos. Também pode utilizar a função de exportação/importação para fazer uma cópia de segurança de filtros de eventos ou para migrar a lista para um servidor diferente.

Usar demasiadas regras pode aumentar a carga no servidor de recolha de telemetria e reduzir o desempenho do computador. Recomendamos que adicione apenas as regras necessárias.

Para exportar ou importar filtros de eventos na Consola Web:

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **Telemetry Settings**.
5. Selecione o separador **EDR Expert (cloud) telemetry**.
6. Para exportar os filtros de eventos:
   a. Clique em **Export**.
   b. Na janela que se abre, especifique o nome do ficheiro JSON para o qual pretende exportar os filtros de eventos e selecione a pasta onde pretende guardar este ficheiro.
   c. Guardar o ficheiro.

      O Kaspersky Endpoint Security exporta os filtros de eventos para o ficheiro JSON.
7. Para importar os filtros de eventos:
   a. Clique em **Import**.
   b. Na janela que se abre, selecione o ficheiro JSON a partir do qual pretende importar os filtros de eventos.
   c. Selecione como deseja que as regras de filtragem de eventos sejam importadas: adicionando-as às regras existentes ou descartando as regras existentes e substituindo-as por novas.
   d. Abrir o ficheiro.

8. Para aplicar a política aos computadores, certifique-se de que os cadeados estão fechados (🔒) e guarde as suas alterações.

    1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
    2. Clique no nome da política do Kaspersky Endpoint Security.

       É apresentada a janela de propriedades da política.
    3. Selecione o separador **Application settings**.
    4. Aceda a **General Settings** → **Telemetry Settings**.
    5. Selecione o separador **EDR Expert (cloud) telemetry**.
    6. Para exportar os filtros de eventos:

        a. Clique em **Export**.

        b. Na janela que se abre, especifique o nome do ficheiro JSON para o qual pretende exportar os filtros de eventos e selecione a pasta onde pretende guardar este ficheiro.

        c. Guardar o ficheiro.

           O Kaspersky Endpoint Security exporta os filtros de eventos para o ficheiro JSON.
    7. Para importar os filtros de eventos:

        a. Clique em **Import**.

        b. Na janela que se abre, selecione o ficheiro JSON a partir do qual pretende importar os filtros de eventos.

        c. Selecione como deseja que as regras de filtragem de eventos sejam importadas: adicionando-as às regras existentes ou descartando as regras existentes e substituindo-as por novas.

        d. Abrir o ficheiro.
    8. Para aplicar a política aos computadores, certifique-se de que os cadeados estão fechados (🔒) e guarde as suas alterações.

Gerir a Quarentena

Quarentena é um armazenamento local especial no computador. O utilizador pode colocar em quarentena ficheiros que considere perigosos para o computador. Os ficheiros na quarentena são armazenados num estado encriptado e não põem em risco a segurança do dispositivo. O Kaspersky Endpoint Security utiliza a Quarentena apenas quando integrado com as soluções Kaspersky Detection and Response. Em todos os outros casos, o Kaspersky Endpoint Security coloca o ficheiro pertinentes na Cópia de Segurança. Para obter mais informações sobre a gestão da Quarentena como parte das soluções, consulte Ajuda do Kaspersky Sandbox, Ajuda do Kaspersky Endpoint Detection and Response Optimum e Ajuda do Kaspersky Endpoint Detection and Response Expert, Ajuda do Kaspersky Anti Targeted Attack Platform e Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises).

O Kaspersky Endpoint Security utiliza a conta de sistema (SYSTEM) para colocar os ficheiros na quarentena.

Só pode configurar as definições de quarentena na Consola do Kaspersky Security Center. Também pode utilizar a Consola do Kaspersky Security Center para gerir objetos na quarentena (restaurar, eliminar, adicionar, etc). Localmente, no computador, só pode restaurar o objeto usando a linha de comandos.

Configurar o tamanho máximo da Quarentena

Por defeito, o tamanho da Quarentena é limitado a 1024 MB. Quando a Quarentena atinge o tamanho máximo, o Kaspersky Endpoint Security interrompe o envio dos ficheiros e gera o evento *Espaço insuficiente no armazenamento da Quarentena*. Para evitar que a quarentena fique sem espaço no disco, pode definir um limite no qual o Kaspersky Endpoint Security gera um evento *O armazenamento da Quarentena está quase sem espaço disponível*. Não pode configurar um período de retenção para ficheiros em quarentena para que eles sejam removidos automaticamente.

Se a solução Kaspersky Anti Targeted Attack Platform (EDR) for implementada na sua organização, recomendamos que aumente o tamanho da Quarentena. Ao realizar uma verificação YARA, a aplicação pode encontrar uma grande descarga de memória. Se o tamanho da descarga de memória exceder o tamanho da Quarentena, a verificação YARA será concluída com um erro e a descarga de memória não será colocada em quarentena. Recomendamos que o tamanho da Quarentena seja 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 de quarentena na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais → Relatórios e armazenamento**.
4. No bloco **Quarentena** configure o tamanho da Quarentena:
   - **Limitar o tamanho da Quarentena a N MB**. Se a caixa de verificação estiver selecionada, o tamanho máximo da Quarentena será limitado ao valor definido. Por predefinição, o tamanho máximo é de 1024 MB. Quando a Quarentena atinge o tamanho máximo, o Kaspersky Endpoint Security envia o evento *Espaço insuficiente no armazenamento da Quarentena* para o Kaspersky Security Center e publica-o no Registo de Eventos do Windows. Entretanto, a aplicação deixa de colocar novos objetos na quarentena. Tem de esvaziar manualmente a Quarentena.

     Se a caixa de seleção estiver desmarcada, o tamanho da Quarentena será limitado pelo espaço livre no disco disponível.

   - **Notificar quando o armazenamento de quarentena atingir N percentagens**. Valor limite da Quarentena. Por exemplo, pode definir o limite da quarentena para 50 %. Quando a Quarentena atinge o valor limite, o Kaspersky Endpoint Security envia o evento correspondente ao Kaspersky Security Center e publica-o no Registo de Eventos do Windows. Entretanto, a aplicação continua a colocar novos objetos na quarentena.

     Se esta caixa de seleção estiver desmarcada, a aplicação não irá gerar eventos quando o limite da quarentena for atingido.
5. Guarde as suas alterações.

Como configurar o tamanho máximo da Quarentena na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **Reports and Storage**.
5. No bloco **Quarantine** configure o tamanho da Quarentena:

   - **Limit the size of Quarantine**. Se a caixa de verificação estiver selecionada, o tamanho da Quarentena será limitado ao valor especificado. Se a caixa de seleção estiver desmarcada, o tamanho da Quarentena será limitado pelo espaço livre no disco disponível. Isto pode ser necessário para a verificação YARA porque a aplicação pode guardar um ficheiro de despejo de memória de grande dimensão.
   - **Maximum size of Quarantine (MB)**. Se a caixa de verificação estiver selecionada, o tamanho máximo da Quarentena será limitado ao valor definido. Por predefinição, o tamanho máximo é de 1024 MB. Quando a Quarentena atinge o tamanho máximo, o Kaspersky Endpoint Security envia o evento *Espaço insuficiente no armazenamento da Quarentena* para o Kaspersky Security Center e publica-o no Registo de Eventos do Windows. Entretanto, a aplicação deixa de colocar novos objetos na quarentena. Tem de esvaziar manualmente a Quarentena.

     Se a caixa de seleção estiver desmarcada, o tamanho da Quarentena será limitado pelo espaço livre no disco disponível.
   - **Notify when the Quarantine storage reaches (%)**. Valor limite da Quarentena. Por exemplo, pode definir o limite da quarentena para 50 %. Quando a Quarentena atinge o valor limite, o Kaspersky Endpoint Security envia o evento correspondente ao Kaspersky Security Center e publica-o no Registo de Eventos do Windows. Entretanto, a aplicação continua a colocar novos objetos na quarentena.
6. Guarde as suas alterações.

Enviar dados sobre ficheiros da Quarentena para o Kaspersky Security Center

Para realizar ações com objetos em quarentena na Consola Web, deve ativar o envio de dados de ficheiros em quarentena para o Servidor de Administração. Por exemplo, pode descarregar um ficheiro da quarentena para análise na Consola Web. O envio de dados de ficheiros em quarentena deve ser ativado para todas as funcionalidades do Kaspersky Sandbox e Kaspersky Endpoint Detection and Response trabalharem.

Como ativar a transferência de dados de ficheiros em quarentena na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais** → **Relatórios e armazenamento**.
4. No bloco **Transferência de dados para o Servidor de administração**, clique no botão **Definições**.

5. Na janela que abre, selecione a caixa de verificação **Ficheiros da Quarentena**.

6. Guarde as suas alterações.

Como ativar a transferência de dados de ficheiros em quarentena na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **General Settings** → **KSC Integration**.

5. No bloco **Data transfer to Administration Server**, selecione a caixa de verificação **About Quarantine files**.

6. Guarde as suas alterações.

Como resultado, pode ver uma lista de ficheiros colocados em quarentena no seu computador, na Consola do Kaspersky Security Center. Pode utilizar a Consola do Kaspersky Security Center para gerir objetos na quarentena (restaurar, eliminar, adicionar, etc). Para obter mais informação detalhada sobre como utilizar a Quarentena, consulte a Ajuda do Kaspersky Security Center.

Restaurar ficheiros a partir da Quarentena

Por defeito, o Kaspersky Endpoint Security restaura os ficheiros na sua pasta original. Se a pasta de destino foi eliminada ou o utilizador não possui direitos de acesso a essa pasta, a aplicação coloca o ficheiro na pasta `%DataRoot%\QB\Restored`. Depois tem de mover manualmente o ficheiro para a pasta de destino.

Para restaurar ficheiros a partir da Quarentena:

1. Na janela principal da Consola Web, selecione **Operations** → **Repositories** → **Quarantine**.

2. Esta ação abre a lista de ficheiros na Quarentena; nessa lista, selecione os ficheiros que deseja restaurar e clique em **Restore**.

   O Kaspersky Endpoint Security restaura o ficheiro. Caso a pasta de destino já possua um ficheiro com o mesmo nome, a aplicação cancela a restauração do ficheiro. A aplicação guarda uma cópia do ficheiro na Quarentena depois de restaurar o ficheiro. Para eliminar o ficheiro, tem de limpar manualmente a Quarentena.

Monitorização de ações de EDR

O Kaspersky Endpoint Security for Windows 12.9 apresenta o centro de monitorização de ações EDR. O *Centro de monitorização de ações EDR* é uma consola na qual pode visualizar o histórico de Resposta a Ameaças para todas as soluções do Kaspersky Detection and Response. Se a sua organização tiver vários sistemas de Deteção e Resposta implementados (por exemplo, EDR Optimum e MDR), o Kaspersky Endpoint Security apresenta o histórico de Resposta a Ameaças para todas as soluções. Isto permite analisar o desempenho das soluções de Deteção e Resposta num computador separado e otimizar as definições destas soluções.

O centro de monitorização fornece as seguintes informações:

- Informações sobre tarefas de Resposta a Ameaças (por exemplo, a tarefa *Terminar processo*)
- Alterações nas regras de Isolamento de rede e Prevenção de execução

Se a resposta a ameaças encontrar um erro relacionado com o acesso a uma partilha de rede, esse erro será omitido do histórico de Resposta a Ameaças apresentado.

Para navegar até o centro de monitorização de ações do EDR:

1. Na janela principal da Consola Web, selecione **Asset management** → **Assets (Devices)**.
2. Selecione um computador para o qual quer configurar definições da aplicação locais.

   As propriedades do computador são apresentadas.
3. Selecione o separador **Applications**.
4. Clique em **Kaspersky Endpoint Security for Windows 14.2**.

   As definições da aplicação locais são apresentadas.
5. Selecione o separador **Application settings**.
6. Aceda a **Detection and Response** → **Response history**.

Isto abre a consola do centro de monitorização de ações do EDR. Pode utilizar a consola para visualizar o estado das tarefas de Resposta a Ameaças, a duração das tarefas, as alterações de regras e os detalhes do iniciador.

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



O Kaspersky Endpoint Security for Windows suporta a solução Kaspersky Unified Monitoring and Analysis Platform. O *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* é uma solução de gestão de eventos e informações de segurança (SIEM) para a infraestrutura informática das organizações. O KUMA permite detetar, analisar e atenuar as ameaças à segurança, antes que estas possam causar danos.

A Kaspersky Endpoint Security é instalada em computadores individuais na infraestrutura de TI corporativa e monitoriza continuamente os processos, as ligações de rede abertas e os ficheiros que estão a ser modificados. As informações sobre eventos no computador (telemetria) são enviadas para o servidor Kaspersky Unified Monitoring and Analysis Platform (KUMA). Na sua consola, o KUMA apresenta os eventos como uma lista sem marcação, semelhante ao registo de eventos do Windows.

O Kaspersky Endpoint Security não fornece todas as funcionalidades de um agente para o KUMA. A aplicação apenas envia eventos para o KUMA sem marcação. Para aceder a todas as funcionalidades do KUMA, é necessário adquirir uma licença e implementar a solução de acordo com o Guia de administrador do KUMA.

Integração do Kaspersky Endpoint Security com o KUMA

A configuração da integração do KES com o KUMA envolve os seguintes passos:

1. Na consola do KUMA, adicione um coletor.
2. Na consola do KUMA, configure um conector para que o coletor receba eventos do KES.
3. Na consola do KUMA, ative a autenticação bidirecional (opcional).
4. Na política do Kaspersky Endpoint Security for Windows, configure as definições de ligação do KES ao KUMA.
5. Na consola do KUMA, certifique-se de que os eventos do KES são encaminhados para o tenant correto e processados pelas regras de correlação corretas.

Preparação para a integração do KES com o KUMA

Para utilizar o KUMA, devem ser cumpridas as seguintes condições:

- Kaspersky Security Center versão 14.2 ou superior. Nas versões anteriores do Kaspersky Security Center, é impossível ativar a funcionalidade de integração do KUMA.
- A aplicação é ativada e a funcionalidade é abrangida pela licença.
- O componente de integração do KUMA está ativado.

A preparação para a integração do KES com o KUMA envolve os seguintes passos:

1. **Instalação do componente de integração do KUMA**

   Pode selecionar o componente de integração KUMA durante a instalação ou atualização da aplicação, bem como através da tarefa *Alterar componentes da aplicação*.

   Tem de reiniciar o computador para terminar a atualização da aplicação com o novo componente.

2. **Ativação KUMA**

   Para além de uma licença de aplicação do Kaspersky Endpoint Security (por exemplo, Kaspersky Endpoint Security for Business Standard), precisa de uma licença separada para a integração do Kaspersky Endpoint Security com o KUMA (Suplemento de Integração do KUMA no Kaspersky Endpoint Security for Windows).

   Se estiver a instalar a aplicação no modo EDR Agent, precisa de uma licença para integrar o Kaspersky Endpoint Security com o KUMA e uma licença da Kaspersky Anti Targeted Attack Platform (KATA) ou uma licença do Kaspersky Managed Detection and Response (MDR). Não pode implementar o EDR Agent apenas para o KUMA.

   A funcionalidade fica disponível depois de adicionar a 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 autónoma é a mesma que a licença do Kaspersky Endpoint Security.

   Certifique-se de que a funcionalidade KUMA é incluída na licença e está a funcionar na interface local da aplicação.

Ligação do KES ao KUMA

Para ligar o computador com a aplicação do Kaspersky Endpoint Security à solução KUMA:

1. Na consola do KUMA, adicione um coletor com conectores do tipo **tcp**, **udp** ou **http** e especifique as definições básicas de rede da ligação. Para obter detalhes sobre a gestão de conectores, consulte a Ajuda do Kaspersky Unified Monitoring and Analysis Platform.

2. Na política do Kaspersky Endpoint Security, adicione endereços de coletores KUMA e especifique as definições de rede da ligação.

Como ligar um computador do Kaspersky Endpoint Security ao KUMA usando a Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.

2. Na árvore da consola, selecione **Policies**.

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

4. Na janela de política, selecione **Integração KUMA**.

5. Selecione a caixa de verificação **Integração KUMA**.

6. No bloco **Definições de Integração**, selecione a caixa de verificação **$IsKUMATelemetry ? "Ativar a transmissão de eventos do Windows para um servidor KUMA": "Ativar a transmissão de eventos do Windows para um servidor SIEM**.

7. Adicione servidores KUMA:

   a. Clique em **Adicionar**.

   Isto abre o formulário no qual pode adicionar servidores KUMA.

   b. Selecione o protocolo de ligação ao servidor KUMA: **HTTP / HTTPS**, **TCP**, **UDP**.

   O protocolo de ligação ao coletor no Kaspersky Endpoint Security tem de corresponder ao tipo de conector no KUMA: **http**, **tcp** ou **udp**.

   > Ao utilizar o protocolo UDP, poderão perder-se dados devido à perda de tráfego inerente ao protocolo.

   c. Introduza o endereço do servidor (IPv4, IPv6, FQDN) e a porta para estabelecer ligação ao servidor (por predefinição, é especificada a porta 443).

   Ao introduzir o endereço do servidor, tenha em conta o seguinte:

   - **TCP**:
     - **Sem TLS**. Pode especificar o endereço IP ou o FQDN do servidor.
     - **Com TLS**. Tem de especificar apenas o FQDN do servidor.
   - **HTTP / HTTPS**:
     - **Sem TLS**. Tem de especificar explicitamente o protocolo HTTP no endereço do servidor (por exemplo, `http://server.com` ou `http://10.10.10.100`).
     - **Com TLS**. Não tem de especificar o protocolo (por exemplo, `https://server.com` ou `server.com`).
   - **UDP**. O protocolo UDP não suporta encriptação TLS. Pode especificar o endereço IP ou o FQDN do servidor.

   Pode ver o endereço do servidor nas propriedades do conector na consola do KUMA. Para obter mais informações sobre os conectores KUMA, consulte a Ajuda do Kaspersky Unified Monitoring and Analysis Platform.

   d. Clique em **OK**.

   O Kaspersky Endpoint Security liga-se ao primeiro servidor KUMA da lista. Se a ligação falhar, o Kaspersky Endpoint Security liga-se ao segundo servidor KUMA da lista e assim por diante.

8. Se necessário, configure a definição **Atraso máximo de transmissão de eventos (seg)** no bloco **Definições de transmissão de dados**. Quando o tempo especificado termina, o Kaspersky Endpoint Security tenta ligar-se ao mesmo coletor ou liga-se ao coletor seguinte da lista, se existirem vários coletores. A predefinição é 30 segundos.

9. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ligar um computador do Kaspersky Endpoint Security ao KUMA usando a Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Built-in Agents Configuration** → **KUMA Integration**.
5. Ative o botão de alternar **KUMA Integration ENABLED**.
6. Adicione servidores KUMA:

   a. Clique em **Add**.

   Isto abre o formulário no qual pode adicionar servidores KUMA.

   b. Selecione o protocolo de ligação ao servidor KUMA: **HTTP/HTTPS**, **TCP**, **UDP**.

   O protocolo de ligação ao coletor no Kaspersky Endpoint Security tem de corresponder ao tipo de conector no KUMA: **http**, **tcp** ou **udp**.

   > Ao utilizar o protocolo UDP, poderão perder-se dados devido à perda de tráfego inerente ao protocolo.

   c. Introduza o endereço do servidor (IPv4, IPv6, FQDN) e a porta para estabelecer ligação ao servidor (por predefinição, é especificada a porta 443).

   Ao introduzir o endereço do servidor, tenha em conta o seguinte:

   - **TCP**:
     - **Sem TLS**. Pode especificar o endereço IP ou o FQDN do servidor.
     - **Com TLS**. Tem de especificar apenas o FQDN do servidor.
   - **HTTP/HTTPS**:
     - **Sem TLS**. Tem de especificar explicitamente o protocolo HTTP no endereço do servidor (por exemplo, `http://server.com` ou `http://10.10.10.100`).
     - **Com TLS**. Não tem de especificar o protocolo (por exemplo, `https://server.com` ou `server.com`).
   - **UDP**. O protocolo UDP não suporta encriptação TLS. Pode especificar o endereço IP ou o FQDN do servidor.

   Pode ver o endereço do servidor nas propriedades do conector na consola do KUMA. Para obter mais informações sobre os conectores KUMA, consulte a Ajuda do Kaspersky Unified Monitoring and Analysis Platform.

   d. Clique em **OK**.

O Kaspersky Endpoint Security liga-se ao primeiro servidor KUMA da lista. Se a ligação falhar, o Kaspersky Endpoint Security liga-se ao segundo servidor KUMA da lista e assim por diante.

7. Se necessário, configure a definição **Maximum delay when sending events (sec)** no bloco **Server connection settings**. Quando o tempo especificado termina, o Kaspersky Endpoint Security tenta ligar-se ao mesmo coletor ou liga-se ao coletor seguinte da lista, se existirem vários coletores. A predefinição é 30 segundos.

8. Guarde as suas alterações.

Pode verificar se a integração do KUMA está corretamente configurada na consola KUMA (para mais informações, consulte Ajuda da Kaspersky Unified Monitoring and Analysis Platform). Verifique o estado de funcionamento do componente ao visualizar o *Report on status of application components* na consola do Kaspersky Security Center. Pode também ver o estado de funcionamento de um componente em relatórios na interface local do Kaspersky Endpoint Security. O componente **Integração KUMA** será adicionado à lista de componentes do Kaspersky Endpoint Security.

Estabelecer uma ligação de confiança entre o KES e o KUMA

Pode estabelecer uma ligação de confiança entre o Kaspersky Endpoint Security e um coletor KUMA com um conector do tipo tcp ou http. Não é possível estabelecer uma ligação fidedigna com um conector do tipo udp.

Para estabelecer uma ligação fidedigna, tem de configurar um modo TLS nas definições do conector. Estão disponíveis os seguintes modos TLS:

- **Disabled**: Não utilizar encriptação TLS. Esta opção está selecionada por predefinição.
- **Enabled**: Utilizar encriptação TLS, mas sem verificação do certificado.
- **Custom PFX with client authentication**: Utilizar encriptação TLS com um segredo PFX. Neste modo, o cliente é autenticado com um certificado.

O Kaspersky Endpoint Security não suporta o modo TLS **Custom PFX**. Ao integrar o KES com o KUMA através de PFX, é necessária a autenticação do utilizador com uma palavra-passe.

Para configurar uma ligação de confiança, é necessário um certificado TLS — o *certificado da AC para o microsserviço*. Pode obter um certificado TLS na consola do KUMA. Para obter detalhes sobre a transferência de certificados TLS, consulte a Ajuda do Kaspersky Unified Monitoring and Analysis Platform. Em seguida, tem de adicionar o certificado TLS ao Kaspersky Endpoint Security (consulte as instruções abaixo).

Para tornar a ligação mais segura, pode ativar a autenticação adicional do computador no KUMA (autenticação bidirecional). Para ativar este tipo de autenticação, tem de criar um cripto-contentor numa autoridade de certificação externa. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada no formato PKCS#12. Em seguida, tem de ativar a autenticação bidirecional nas definições do KUMA (modo TLS **Custom PFX with client authentication**), ativar a autenticação bidirecional no Kaspersky Endpoint Security e adicionar um arquivo PFX à consola do KUMA e ao Kaspersky Endpoint Security.

Como configurar uma ligação de confiança entre o KES e o KUMA na Administration Console (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.

2. Na árvore da consola, selecione **Policies**.

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

4. Na janela de política, selecione **Integração KUMA**.

5. Selecione a caixa de verificação **Integração KUMA**.

6. No bloco **Definições para ligar aos servidores da KUMA**, selecione a caixa de verificação **Utilizar encriptação TLS**.

7. Configure a ligação fiável:

   a. Clique em **Definições para ligar aos servidores da KUMA**.

   b. Configure a ligação do servidor:

   - **Tempo limite (seg)**. Tempo máximo de espera por uma resposta do servidor KUMA (por predefinição, o valor é de 5 segundos). Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor KUMA diferente.

   - **Certificado TLS do servidor**. Certificado TLS para estabelecer uma ligação fiável com o servidor KUMA. Pode obter um certificado TLS na consola do Kaspersky Unified Monitoring and Analysis Platform (consulte as instruções na Ajuda do Kaspersky Unified Monitoring and Analysis Platform).

     Para estabelecer uma ligação de confiança, tem de selecionar o modo TLS **Enabled** na consola do KUMA.

   - **Usar a autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma ligação segura entre o KES e o KUMA. Para utilizar a autenticação bidirecional, na consola KUMA, nas definições do conetor, tem de selecionar o modo TLS **Custom PFX with client authentication** (consulte as definições do conetor na Ajuda do Kaspersky Unified Monitoring and Analysis Platform). Em seguida, tem de transferir um certificado de servidor e definir uma password para proteger o contentor criptográfico.

     > O cripto-contentor deve ser protegido por password. Não é possível adicionar um cripto-contentor com uma password em branco.

   c. Clique em **OK**.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como configurar uma ligação de confiança entre o KES e o KUMA na Web Console

1. Na janela principal da Consola Web, selecione o separador **Asset management → Policies**.

2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

4. Aceda a **Built-in Agents Configuration → KUMA Integration**.

5. Ative o botão de alternar **KUMA Integration ENABLED**.

6. Sob **Server connection settings**, ative a opção **Use TLS encryption**.

7. Configure a ligação fiável:

   a. Clique em **Connection settings**.

   b. Configure a ligação do servidor:

   - **Timeout (sec)**. Tempo máximo de espera por uma resposta do servidor KUMA (por predefinição, o valor é de 5 segundos). Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor KUMA diferente.
   - **Server TLS certificate**. Certificado TLS para estabelecer uma ligação fiável com o servidor KUMA. Pode obter um certificado TLS na consola do Kaspersky Unified Monitoring and Analysis Platform (consulte as instruções na Ajuda do Kaspersky Unified Monitoring and Analysis Platform).

     Para estabelecer uma ligação de confiança, tem de selecionar o modo TLS **Enabled** na consola do KUMA.
   - **Use two-way authentication**. Autenticação bidirecional ao estabelecer uma ligação segura entre o KES e o KUMA. Para utilizar a autenticação bidirecional, na consola KUMA, nas definições do conetor, tem de selecionar o modo TLS **Custom PFX with client authentication** (consulte as definições do conetor na Ajuda do Kaspersky Unified Monitoring and Analysis Platform). Em seguida, tem de transferir um certificado de servidor e definir uma password para proteger o contentor criptográfico.

     > O cripto-contentor deve ser protegido por password. Não é possível adicionar um cripto-contentor com uma password em branco.

   c. Clique em **OK**.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Ativar o envio de dados de telemetria para o servidor KUMA

Por predefinição, o envio de eventos para o servidor KUMA está desativado. Para garantir que o KUMA funcione corretamente, tem de ativar o envio de dados de telemetria. Pode selecionar uma fonte do evento entre os registos padrão: *Application*, *Security* ou *System*.

Como ativar o envio de telemetria para o KUMA na Administration Console (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Definições gerais → Exclusões e tipos de objetos**.
5. No bloco **Definições de telemetria → Telemetria KUMA**, clique no botão **Definições**.
6. Selecione os registos de eventos que pretende utilizar como fontes de eventos: *Application*, *Security* ou *System*.

   Para além dos registos padrão, pode especificar um registo de uma aplicação de terceiros.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como ativar o envio de telemetria para o KUMA na Web Console

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **Telemetry Settings**.
5. Selecione o separador **KUMA telemetry**.
6. Selecione os registos de eventos que pretende utilizar como fontes de eventos: *Application*, *Security* ou *System*.

   Para além dos registos padrão, pode especificar um registo de uma aplicação de terceiros.
7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Filtrar eventos a serem enviados para o KUMA

Por predefinição, o envio de eventos para o servidor KUMA está desativado. Para garantir que o KUMA funcione corretamente, tem de ativar o envio de dados de telemetria. Pode selecionar uma fonte do evento entre os registos padrão: *Application*, *Security* ou *System*. Para melhorar o desempenho e otimizar a transmissão de dados para o servidor KUMA, pode adicionar ou excluir manualmente eventos individuais da telemetria. Por exemplo, pode excluir eventos Sysmon.

Como criar uma lista de eventos a serem enviados ao KUMA na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Definições gerais** → **Exclusões e tipos de objetos**.
5. No bloco **Definições de telemetria** → **Telemetria KUMA**, clique no botão **Definições**.
6. Na janela exibida, configure os filtros de eventos a serem enviados ao KUMA.

   Pode configurar a filtragem de eventos para os registos padrão *Application*, *Security*, *System* ou adicionar manualmente outro registo:

   a. Abra as propriedades do registo ou clique no botão **Adicionar** e insira o nome do registo.

   b. Selecione um modo de envio de evento:

   - **Enviar todos os eventos**. Neste modo, a aplicação envia todos os eventos do registo do Windows, exceto os eventos adicionados às regras de exclusão.
   - **Enviar apenas eventos selecionados**. Neste modo, a aplicação envia apenas eventos adicionados nas regras de inclusão.

c. Crie listas de regras de exclusão ou regras de inclusão para o modo de envio de eventos relevante.

Para adicionar regras, tem de especificar o ID do evento no registo de eventos do Windows. Pode listar vários ID de eventos numa regra. Para especificar vários ID de eventos, use o carácter vírgula (,).

d. Se necessário, ative o registo de eventos utilizando a caixa de verificação junto ao nome do registo.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como criar uma lista de eventos a serem enviados ao KUMA na Consola Web

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **Telemetry Settings**.
5. Selecione o separador **KUMA telemetry**.
6. Na janela exibida, configure os filtros de eventos a serem enviados ao KUMA.

   Pode configurar a filtragem de eventos para os registos padrão *Application*, *Security*, *System* ou adicionar manualmente outro registo:

   a. Abra as propriedades do registo ou clique no botão **Add** e insira o nome do registo.

   b. Selecione um modo de envio de evento:

   - **Send all events**. Neste modo, a aplicação envia todos os eventos do registo do Windows, exceto os eventos adicionados às regras de exclusão.
   - **Send only selected events**. Neste modo, a aplicação envia apenas eventos adicionados nas regras de inclusão.

   c. Crie listas de regras de exclusão ou regras de inclusão para o modo de envio de eventos relevante.

   Para adicionar regras, tem de especificar o ID do evento no registo de eventos do Windows. Pode listar vários ID de eventos numa regra. Para especificar vários ID de eventos, use o carácter vírgula (,).

   d. Se necessário, ative o registo de eventos utilizando o botão junto ao nome do registo.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Exportar e importar filtros de eventos do KUMA

Pode exportar a lista de exclusões para um ficheiro JSON. Em seguida, pode modificar o ficheiro para, por exemplo, adicionar um grande número de ID de eventos. Também pode utilizar a função de exportação/importação para fazer uma cópia de segurança de 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 que adicione apenas as regras necessárias.

Como exportar e importar filtros de eventos na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Definições gerais** → **Exclusões e tipos de objetos**.
5. No bloco **Definições de telemetria** → **Telemetria KUMA**, clique no botão **Definições**.
6. Para exportar os filtros de eventos:
   a. Selecione os registos de eventos com os filtros que deseja exportar.
   b. Selecione o botão → **Exportar**.
   c. Na janela que se abre, especifique o nome do ficheiro JSON para o qual pretende exportar os filtros de eventos e selecione a pasta onde pretende guardar este ficheiro.
   d. Guardar o ficheiro.
      O Kaspersky Endpoint Security exporta os filtros de eventos para o ficheiro JSON.
7. Para importar os filtros de eventos:
   a. Selecione o botão → **Importar**.
   b. Na janela que se abre, selecione o ficheiro JSON a partir do qual pretende importar os filtros de eventos.
   c. Abrir o ficheiro.
      Se as regras de filtragem de eventos já existirem no computador, o Kaspersky Endpoint Security irá substitui-las durante a importação.
8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como exportar e importar filtros de eventos na Consola Web

1. Na janela principal da Consola Web, selecione o separador **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings** → **Telemetry Settings**.
5. Selecione o separador **KUMA telemetry**.
6. Para exportar os filtros de eventos:
   a. Selecione os registos de eventos com os filtros que deseja exportar.
   b. Selecione o botão → **Export**.

c. Na janela que se abre, especifique o nome do ficheiro JSON para o qual pretende exportar os filtros de eventos e selecione a pasta onde pretende guardar este ficheiro.

d. Guardar o ficheiro.

O Kaspersky Endpoint Security exporta os filtros de eventos para o ficheiro JSON.

7. Para importar os filtros de eventos:

a. Selecione o botão → **Import**.

b. Na janela que se abre, selecione o ficheiro JSON a partir do qual pretende importar os filtros de eventos.

c. Abrir o ficheiro.

Se as regras de filtragem de eventos já existirem no computador, o Kaspersky Endpoint Security irá substitui-las durante a importação.

8. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Também pode exportar ou importar filtros de eventos na linha de comandos.

Guia de Migração do KSWS para o KES

A partir da versão 11.8.0, o Kaspersky Endpoint Security for Windows oferece suporte à funcionalidade básica da solução Kaspersky Security for Windows Server (KSWS). *Kaspersky Security for Windows Server* protege servidores que executam sistemas operativos Microsoft Windows e armazenamentos anexados à rede contra vírus e outras ameaças à segurança do computador às quais os servidores e armazenamentos anexados à rede estão expostos durante a troca de ficheiros. Para obter mais informações sobre a utilização da solução, consulte a Ajuda do Kaspersky Security for Windows Server. A partir do Kaspersky Endpoint Security 11.8.0, pode migrar do Kaspersky Security for Windows Server para o Kaspersky Endpoint Security for Windows e utilizar uma única solução para proteger estações de trabalho e servidores.

Requisitos do software

Antes de iniciar a migração do KSWS para o KES, certifique-se de que o seu servidor cumpre os requisitos de hardware e software do Kaspersky Endpoint Security for Windows. As listas das versões do sistema operativo suportadas são diferentes para o KES e o KSWS. Por exemplo, o KES não suporta servidores que executam o Windows Server 2003.

Requisitos mínimos de software para migrar do KSWS para o KES:

- Kaspersky Endpoint Security for Windows 12.0.
- Kaspersky Security 11.0.1 for Windows Server.

  Se tiver uma versão anterior do Kaspersky Security for Windows Server instalada, recomendamos que atualize a aplicação para a versão mais recente. O Assistente de conversão de políticas e tarefas não suporta versões anteriores do Kaspersky Security for Windows Server.
- Kaspersky Security Center 14.2

  Se tiver uma versão anterior do Kaspersky Security Center instalada, atualize-a para a versão 14.2 ou uma mais recente. Nesta versão do Kaspersky Security Center, o Assistente de conversão de políticas e tarefas em lote permite migrar políticas para um perfil em vez de uma política. Nesta versão do Kaspersky Security Center, o Assistente de conversão de políticas e tarefas em lote também permite que migre uma gama mais ampla de definições de política.
- Kaspersky Endpoint Agent 3.10.

  Se tiver uma versão anterior do Kaspersky Endpoint Agent instalada, recomendamos que atualize a aplicação para a versão mais recente. O Kaspersky Endpoint Security suporta a migração de uma configuração [KSWS+KEA] para [KES+agente integrado] a partir do Kaspersky Endpoint Agent 3.10.

Recomendações de migração

Ao migrar do KSWS para o KES, observe as seguintes recomendações:

- Planeie o tempo de migração do KSWS para o KES com antecedência. Escolha um horário em que os servidores estejam a trabalhar com uma carga mais leve, por exemplo, durante o fim de semana.
- Após a migração, ative os componentes da aplicação gradualmente. Isto é, por exemplo, comece por ativar apenas o componente Proteção contra ameaças de ficheiros, depois ative outros componentes de proteção, ative o controlo dos componentes e assim por diante. Em cada passo, tem de verificar se a aplicação está a funcionar corretamente e monitorizar o desempenho do servidor. A arquitetura do KES difere do KSWS, portanto, o sistema operativo também se pode 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, por exemplo, primeiro migre os servidores de base de dados, depois os servidores de correio e assim por diante.
- A migração em servidores de alta carga envolve algumas considerações especiais.

Passos da migração

A migração do KSWS para o KES é realizada de forma semiautomática. Isto é necessário devido às diferentes arquiteturas das aplicações. Para migrar definições de política, tem de executar o Assistente de conversão de políticas e tarefas em lote (o assistente de migração). Depois de migrar as definições de política, tem de configurar manualmente as definições que o assistente de migração não pode migrar automaticamente (por exemplo, as definições de Proteção por password). Após a migração, também é recomendável verificar se o assistente de migração migrou corretamente todas as definições.

Migre do KSWS para o KES na seguinte ordem:

1. **Migrar tarefas e políticas do KSWS**

   Depois de migrar as políticas e tarefas, tem de executar passos de configuração adicionais. Também recomendamos que garanta que o Kaspersky Endpoint Security oferece o nível de segurança necessário após a migração do KSWS.

   > O Assistente de conversão de políticas e tarefas em lote do Kaspersky Security for Windows Server está disponível apenas na Consola de Administração (MMC). As definições de políticas e tarefas não podem ser migradas na Consola da Web e na Consola de Nuvem do Kaspersky Security Center.

2. **Instalar o Kaspersky Endpoint Security**

Pode instalar o Kaspersky Endpoint Security das seguintes formas:

- Instalar o KES após remover o KSWS (recomendado).

  O utilitário kavremover não suporta a gestão do KSWS.

- Instalar o KES sobre o KSWS.

3. Ativar o KES com uma chave KSWS

4. **Confirme se a aplicação está a funcionar corretamente após a migração**

   Depois de migrar do KSWS para o KES, certifique-se de que a aplicação está a funcionar corretamente. Verifique o estado do servidor na consola (deve ser *OK*). Certifique-se de que não é relatado nenhum erro para a aplicação, verifique também a hora da última ligação com o Servidor de Administração, a hora da última atualização da base de dados e o estado da proteção do servidor.

   Preste atenção especial à migração de listas de exclusão, aplicações fiáveis, endereços da Internet fiáveis, regras de Controlo das Aplicações.

Correspondência dos componentes KSWS e KES

Ao migrar do KSWS para o KES, o conjunto de componentes é migrado apenas quando a aplicação está a ser instalada 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 programa
Log Inspection	Inspeção de Registo
Device Control	Controlo de Dispositivos
Firewall Management	*(não suportado)* As funções da Firewall do KSWS são executadas pela Firewall ao nível do sistema. No KES, um componente separado é responsável pela funcionalidade da Firewall. Após a migração, pode configurar a Firewall do Kaspersky Endpoint Security.
File Integrity Monitor	Monitorização da integridade do sistema
Exploit Prevention	Prevenção de explorações
System Tray Icon	*(não suportado)* Pode configurar a interação do utilizador nas definições da interface da aplicação.
Integration with Kaspersky Security Center	Conector do Agente de Rede
Endpoint Agent	*(não suportado)* No Kaspersky Endpoint Security 11.9.0, o pacote de distribuição do Kaspersky Endpoint Agent já não faz parte do kit de distribuição do Kaspersky Endpoint Security. Tem de transferir o pacote de distribuição do Kaspersky Endpoint Agent em separado.
Network Threat Protection	Proteção contra ameaças de rede
Anti-Cryptor	Deteção de comportamento
Anti-Cryptor for NetApp	*(não suportado)*

Componente do Kaspersky Security for Windows Server	Componente do Kaspersky Endpoint Security for Windows
Traffic Security	Proteção contra ameaças da web Proteção contra ameaças de correio Controlo de Internet
On-Demand Scan	Kernel do programa
ICAP Network Storage Protection	*(não suportado)* O Kaspersky Endpoint Security não suporta componentes de Proteção de armazenamentos anexados à rede. Se precisar destes componentes, pode continuar a utilizar o Kaspersky Security for Windows Server.
RPC Network Storage Protection	*(não suportado)* O Kaspersky Endpoint Security não suporta componentes de Proteção de armazenamentos anexados à rede. Se precisar destes componentes, pode continuar a utilizar o Kaspersky Security for Windows Server.
Real-Time File Protection	Proteção contra ameaças de ficheiros
Script Monitoring	*(não suportado)* A Monitorização do Script é controlada por outros componentes, por exemplo, Proteção AMSI.
KSN Usage	Kaspersky Security Network
Applications Launch Control	Controlo das Aplicações
Performance counters	*(não suportado)*

Correspondência das definições KSWS e KES

Ao migrar políticas e tarefas, o KES é configurado de acordo com as definições do KSWS. As definições dos componentes da aplicação que o KSWS não possui são definidas com os valores predefinidos.

Application settings

Scalability, interface and scanning settings

As definições da aplicação não são suportadas no Kaspersky Endpoint Security for Windows.

Definições da aplicação

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Scalability settings	*(não migra)* O Kaspersky Endpoint Security gere todos os processos de trabalho.
Show System Tray Icon	*(não migra)* Num computador do cliente, a janela principal do Kaspersky Endpoint Security e o ícone na área de notificação do Windows estão disponíveis por defeito. No menu contextual do ícone, o utilizador pode realizar operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security apresenta também notificações acima do ícone da aplicação. Pode configurar a interação do utilizador nas definições da interface da aplicação.
Restore file attributes after scanning	*(não migra)* O Kaspersky Endpoint Security restaura automaticamente os atributos do ficheiro depois de verificar um ficheiro.
Limit CPU usage for scanning threads	*(não migra)* O Kaspersky Endpoint Security não limita a utilização da CPU ao verificar. Pode configurar a tarefa para ser executada quando o computador estiver a funcionar com carga mínima.

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Folder for temporary files created during scanning	*(não migra)* O Kaspersky Endpoint Security coloca os ficheiros temporários na pasta `C:\Windows\Temp`.
HSM system settings	*(não migra)* O Kaspersky Endpoint Security não suporta sistemas HSM.

Security and reliability

As definições de segurança do KSWS são migradas para a secção **Definições gerais**, Definições da aplicação e as subsecções Interface.

Definições de segurança da aplicação

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Protect application processes from external threats	**Ativar Autodefesa** (subsecção **Definições da aplicação**)
Apply password protection	*(não migra)* O Kaspersky Endpoint Security tem uma funcionalidade integrada de Proteção por password (consulte a subsecção **Interface**).
Perform task recovery	*(não migra)* O Kaspersky Endpoint Security restaura apenas automaticamente tarefas de *Verificação de software malicioso*. O Kaspersky Endpoint Security executa outras tarefas num agendamento.
Do not start scheduled scan tasks	**Adiar as tarefas agendadas quando o computador estiver ligado com bateria** (subsecção **Definições da aplicação**)
Stop current scan tasks	*(não migra)* Quando o computador é alimentado por uma UPS, o Kaspersky Endpoint Security não interrompe as tarefas de verificação que já estão em execução.

Connection settings

As definições de interação do Servidor de Administração são migradas para a secção **Definições gerais**, Definições de Rede e as subsecções Definições da aplicação.

Definições de interação do Servidor de Administração

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Proxy server settings	**Definições do servidor de proxy** (subsecção **Definições de Rede**)
Do not use proxy server for local addresses	**Ignorar um servidor de proxy nos endereços locais** (subsecção **Definições de Rede**)
Proxy server authentication settings	**Usar autenticação do servidor de proxy** (subsecção **Definições de Rede**) A password de autenticação do servidor proxy não é migrada. Após a migração de uma política, a password tem de ser introduzida manualmente.
Use Kaspersky Security Center as a proxy server when activating the application	**Utilizar o Kaspersky Security Center como servidor de proxy para ativação** (subsecção **Definições da aplicação**)

Run local system tasks

O Kaspersky Endpoint Security ignora as definições para executar tarefas do sistema local do Kaspersky Security for Windows Server. Pode configurar a utilização de tarefas locais do KES em **Tarefas locais**, Gestão de tarefas. Também pode configurar um horário para executar as tarefas *Verificação de software malicioso* e *Atualização das bases de dados e módulos da aplicação* nas propriedades destas tarefas.

Supplementary

Trusted zone

As definições de zona fiável do KSWS são migradas para a secção **Definições gerais**, subsecção **Exclusões**.

Definições da Zona fiável

Definições do Kaspersky Security for Windows Server	Definições 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 ficheiros individuais ou caminhos para o ficheiro/a pasta. Se o KSWS tiver exclusões configuradas como uma área predefinida ou um URL de script, tais exclusões não serão migradas. Após a migração, deve adicionar tais exclusões manualmente. As exclusões como áreas predefinidas têm de ser configuradas nas definições da tarefa *Verificação de software malicioso*. As exclusões como endereços da Internet de scripts têm de ser adicionadas aos endereços da Internet fiáveis para a Proteção contra ameaças da web.
Apply also to subfolders (Exclusions)	**Incluir subpastas** (Exclusões de verificação)
Objects to detect (Exclusions)	**Tipo de objeto detetado** (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 da aplicação.
Comment (Exclusions)	**Comentário** (Exclusões de verificação)
Trusted process (Trusted process)	**Aplicações fiáveis** Os métodos de seleção de processos/aplicações fiáveis diferem no KSWS e KES. Ao migrar, o KES oferece suporte a aplicações fiáveis configurados como um caminho para o ficheiro executável ou máscara. Se o KSWS tiver processos fiáveis configurados como um hash do ficheiro, tais processos fiáveis não serão migrados. Após a migração, deve adicionar esses processos fiáveis manualmente.
Do not check file backup operations (Trusted process)	**Não monitorizar a atividade da aplicação** (Aplicações fiáveis)

Removable drives scan

As definições de Verificação das unidades amovíveis são migradas para a secção **Tarefas locais**, subsecção **Verificação das unidades amovíveis**.

Definições de Verificação das unidades amovíveis

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Scan removable drives on connection via USB	**Ação ao ligar uma unidade amovível**
Scan removable drives if its stored data volume does not exceed (MB)	**Tamanho máximo da unidade amovível**

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Scan with security level: • **Maximum protection** • **Recommended** • **Maximum performance**	**Ação ao ligar uma unidade amovível**: • **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 à atribuição de permissões de acesso ao utilizador para gestão da aplicação e gestão de serviços da aplicação. Pode definir as definições de acesso para utilizadores e grupos de utilizadores para gerir a aplicação no Kaspersky Security Center.

User access permissions for Kaspersky Security Service management

O Kaspersky Endpoint Security não oferece suporte à atribuição de permissões de acesso ao utilizador para gestão da aplicação e gestão de serviços da aplicação. Pode definir as definições de acesso para utilizadores e grupos de utilizadores para gerir a aplicação no Kaspersky Security Center.

Storages

As definições de armazenamento do KSWS são migradas para a secção **Definições gerais**, subsecção **Relatórios e armazenamento** e para a secção **Proteção essencial contra ameaças**, subsecção **Proteção contra ameaças de rede**.

Definições de armazenamento

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Backup folder	*(não migra)* O Kaspersky Endpoint Security guarda cópias dos ficheiros da cópia de segurança na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.
Maximum Backup size (MB)	**Limitar o tamanho da Cópia de segurança a N MB** (secção **Definições gerais → Relatórios e armazenamento**)
Threshold value for space available (MB)	*(não migra)* O Kaspersky Endpoint Security regista o evento *O armazenamento da quarentena está quase sem espaço disponível* quando o limite de 50% é alcançado.
Target folder for restoring objects	*(não migra)* O Kaspersky Endpoint Security restaura os ficheiros na sua pasta original.
Quarantine folder	*(não migra)* O Kaspersky Endpoint Security guarda cópias dos ficheiros da cópia de segurança na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.
Maximum Quarantine size (MB)	*(não migra)* O Kaspersky Endpoint Security usa a Cópia de segurança para armazenar objetos provavelmente infetados. Durante a migração, o Kaspersky Endpoint Security ignora as definições da Quarentena.
Threshold value for space available (MB)	*(não migra)* O Kaspersky Endpoint Security usa a Cópia de segurança para armazenar objetos provavelmente infetados. Durante a migração, o Kaspersky Endpoint Security ignora as definições da Quarentena.
Target folder for restoring objects	*(não migra)* O Kaspersky Endpoint Security restaura os ficheiros na sua pasta original.
Unblock automatically in N	**Bloquear dispositivos de ataque durante N min** (secção **Proteção essencial contra ameaças → Proteção contra ameaças de rede**)

Real-time server protection

Real-Time File Protection

As definições de Proteção de ficheiros em tempo real são migradas para a secção **Proteção essencial contra ameaças**, subsecção **Proteção contra ameaças de ficheiros**.

Definições de Proteção de ficheiros em tempo real

Definições do Kaspersky Security for Windows Server	Definições 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 aceder**. • **Ao aceder e modificar**.
Deeper analysis of launching processes	*(não migra)* O Kaspersky Endpoint Security suporta apenas um modo de análise, o modo Optimal.
Heuristic analyzer: • **Light** • **Medium** • **Deep**	**Análise heurística**: • **Nível superficial**. • **Nível médio**. • **Nível aprofundado**.
Apply Trusted Zone	*(não migra)* O Kaspersky Endpoint Security aplica a zona fiável a todos os componentes. Pode configurar exclusões nas definições da zona fiável.
Use KSN for protection	*(não migra)* O Kaspersky Endpoint Security utiliza o KSN para todos os componentes da aplicação.
Block access to network shared resources for the hosts that show malicious activity	*(não migra)* Por defeito, o Kaspersky Endpoint Security bloqueia o acesso aos recursos partilhados da rede para anfitriões 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 é detetada uma infeção ativa.
Use Kaspersky Sandbox for protection	*(não migra)* Por defeito, o Kaspersky Endpoint Security envia objetos para verificação ao Kaspersky Sandbox.
Protection scope	**Âmbito de Proteção**
Schedule settings	*(não migra)* O Kaspersky Endpoint Security utiliza sua própria programação para pausar a Proteção contra ameaças de ficheiros.

KSN Usage

As definições do KSWS para a Kaspersky Security Network são migradas para a secção **Proteção avançada contra ameaças**, subsecção **Kaspersky Security Network**.

Definições da Kaspersky Security Network

Definições do Kaspersky Security for Windows Server	Definições 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 pede o consentimento com a Declaração da Kaspersky Security Network quando a aplicação é instalada, uma nova política é criada ou a utilização do Kaspersky Security Network é ativada.
Send data about scanned files	*(não migra)* O Kaspersky Endpoint Security envia dados sobre os ficheiros verificados automaticamente se o KSN estiver ativado.

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Send data about requested URLs	*(não migra)* O Kaspersky Endpoint Security envia dados sobre URLs solicitados automaticamente se o KSN estiver ativado.
Send Kaspersky Security Network statistics	**Ativar o modo KSN alargado**
Accept the terms of the Kaspersky Managed Protection Statement	*(não migra)* O Kaspersky Endpoint Security não inclui o serviço do KMP.
Action to perform on KSN untrusted objects	*(não migra)* Pode configurar a Ação após deteção de ameaças nas definições do componente de Proteção e nas definições da tarefa de Verificação.
Do not calculate checksum before sending to KSN if file size exceeds N MB	*(não migra)* Pode configurar restrições de verificação de ficheiros grandes nas definições do componente de Proteção e definições da tarefa de Verificação.
Use Kaspersky Security Center as KSN Proxy	**Usar um Servidor de administração como um servidor proxy 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 definições de Segurança de tráfego do KSWS são migradas para a secção **Proteção essencial contra ameaças**, subsecção **Proteção contra ameaças da web** e **Proteção contra ameaças de correio**, secção **Controlos de segurança**, subsecção **Controlo de Internet**, secção **Definições gerais**, subsecção **Definições de Rede**.

Definições de Segurança de tráfego

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Apply URL-based rules	**Controlo de Internet** (subsecção **Controlo de Internet**) 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 suporta regras baseadas em certificados:
Apply rules for web traffic category control	**Controlo de Internet** (subsecção **Controlo de Internet**) As regras de bloqueio para controlo da categoria de tráfego de Internet são migradas para uma única regra de bloqueio no Kaspersky Endpoint Security. O Kaspersky Endpoint Security ignora regras de permissão para controlo da categoria. A correspondência das categorias do KSWS e KES está listada abaixo.
Allow access if the web page can not be categorized	*(não migra)* O Kaspersky Endpoint Security permite o acesso se a página da Web não puder 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 da Web legítimos que podem ser utilizados para danificar o dispositivo protegido.
Allow access to legitimate advertisement	*(não migra)* Pode gerir o acesso a anúncios legítimos utilizando a categoria de recursos da Internet *Faixas* nas definições do Controlo de Internet.
Operation mode: • **Driver Interceptor** • **Redirector** • **External Proxy**	*(não migra)* O Kaspersky Endpoint Security suporta apenas o modo Driver Interceptor.
ICAP-service connection settings	*(não migra)* O Kaspersky Endpoint Security não suporta a Proteção do Armazenamento de Rede ICAP.
Check safe connections through the HTTPS protocol	**Verificar ligações encriptadas** / **Verificar sempre ligações encriptadas** modo (subsecção **Definições de Rede**)

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Use TLS protocol version	*(não migra)* O Kaspersky Endpoint Security verifica o tráfego de rede encriptada transmitido através dos seguintes protocolos: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Pode também bloquear ligações SSL 2.0 nas definições de Verificação de ligações encriptadas.
Do not trust web-servers with invalid certificate	**Endereço** (subsecção **Definições de Rede**)
Intercept ports (Interception area)	**Portas monitorizadas** (subsecção **Definições de Rede**) Durante a migração, o KES desmarca as caixas de verificação **Monitorizar todas as portas para as aplicações da lista recomendada pela Kaspersky** e **Monitorizar todas as portas das aplicações especificadas**.
Exclude ports (Interception area)	*(não migra)*
Exclude IP addresses (Interception area)	**Configurar endereços fiáveis** (subsecção **Definições de Rede**)
Exclude processes (Interception area)	**Configurar aplicações fiáveis** (subsecção **Definições de rede**) Durante a migração, o KES configura as seguintes definições para a aplicação fiável: • A caixa de verificação **Não verificar tráfego de rede** está selecionada. O KES não verifica o tráfego de rede em busca de endereços IP remotos e portas. • As outras caixas de verificação nas definições da aplicação fiável são desmarcadas.
Security port	*(não migra)*
Use malicious URL database to scan web links	**Verificar o endereço da Internet contra a base de dados de endereços da Internet maliciosos** (subsecção **Proteção contra ameaças da web**)
Use anti-phishing database to scan web pages	**Verificar o endereço da Internet contra a base de dados de endereços da Internet de phishing** (subsecção **Proteção contra ameaças da web**)
Use KSN for protection	*(não migra)* O Kaspersky Endpoint Security utiliza o KSN para todos os componentes da aplicação.
Use Trusted Zone	*(não migra)* O Kaspersky Endpoint Security aplica a zona fiável a todos os componentes. Pode configurar exclusões nas definições da zona fiável.
Use heuristic analyzer	**Utilizar análise heurística** (subsecções **Proteção contra ameaças da web** e **Proteção contra ameaças de 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 de correio. Por defeito, o Kaspersky Endpoint Security define o nível de segurança recomendado.
Enable mail threat protection	**Proteção contra ameaças de correio** (subsecção **Proteção contra ameaças de correio**) **Ligar a extensão do Microsoft Outlook** **Apenas mensagens de entrada** (Âmbito 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 definições da Prevenção de explorações do KSWS são migradas para a secção **Proteção avançada contra ameaças**, subsecção **Prevenção de explorações**.

Definições da Prevenção de explorações

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Prevent vulnerable processes exploit: • **Terminate on exploit** • **Notify only**	**Ao detetar exploração**: • **Bloquear**. • **Informar**.

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Notify about abused processes via Terminal Service	*(não migra)* O Kaspersky Endpoint Security não suporta as seguintes definições:
Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled	*(não migra)* O Kaspersky Endpoint Security impede constantemente explorações de processos vulneráveis.
Protected processes	**Ativar proteção da memória de processos do sistema** O Kaspersky Endpoint Security não suporta a seleção de processos protegidos. Só pode ativar a proteção da 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 explorações disponíveis.

Network Threat Protection

As definições de Proteção contra ameaças de Rede do KSWS são migradas para a secção **Proteção essencial contra ameaças**, subsecção **Proteção contra ameaças de rede**.

Definições da Proteção contra ameaças de Rede

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Operation mode: • **Pass-through** • **Only inform about network attacks** • **Block connections when attack is detected**	**Proteção contra ameaças de rede** Se o modo **Pass-through** estiver selecionado, a Proteção contra ameaças de Rede é desativada. Se o modo **Only inform about network attacks** ou o modo **Block connections when attack is detected** estiver selecionado, a Proteção contra ameaças de Rede é ativada. O Kaspersky Endpoint Security funciona sempre 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 suporta o componente Monitorização do Script. A Monitorização do Script é controlada por outros componentes, por exemplo, Proteção AMSI.

Website categories

O Kaspersky Endpoint Security não suporta 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 recurso da Web com categorias não suportadas não são migradas.

Categoria de sites

Categorias Kaspersky Security for Windows Server	Categorias Kaspersky Endpoint Security for Windows
Wargaming	Videojogos
Abortion	*(não migra)*
Lotteries (extended)	Jogo, lotarias, apostas
Alcohol	Álcool, tabaco, narcóticos
Anonymous proxy servers	Anonimizadores
Anorexia	*(não migra)*
Rentals for real estate	*(não migra)*

Categorias Kaspersky Security for Windows Server	Categorias Kaspersky Endpoint Security for Windows
Audio, video and software	Software, áudio, vídeo
Banks	Bancos
Blogs	Blogues
Military	Armas, explosivos, conteúdo militar
For children	*(não migra)*
Discrimination	Violência, intolerância
Home and family	*(não migra)*
Hosting and domain services	Comunicações de rede
Pets and animals	*(não migra)*
Law and politics	Proibido pelas leis regionais
Restricted by Roskomnadzor (RF)	Proibido pelas leis da Federação Russa
Restricted by Federal Law 436 (RF)	Proibido pelas leis da Federação Russa
Restricted by RF legislation	Proibido pelas leis da Federação Russa
Restricted by global legislation	Proibido pelas leis regionais
Adult dating	Conteúdo para adultos
Internet services	*(não migra)*
Sex shops	Conteúdo para adultos
Information technologies	*(não migra)*
Casinos, card games	Jogo, lotarias, apostas
Books and writing	*(não migra)*
Computer games	Videojogos
Health and beauty	*(não migra)*
Culture and society	*(não migra)*
LGBT	Conteúdo para adultos
Lotteries	Jogo, lotarias, apostas
Medicine	*(não migra)*
Fashion	*(não migra)*
Music	*(não migra)*
Drugs	Álcool, tabaco, narcóticos
Violence	Violência, intolerância
Discontent	*(não migra)*
Illegal drugs	Álcool, tabaco, narcóticos
Hate and discrimination	Violência, intolerância
Obscene vocabulary	Profanação, obscenidade
Lingerie	Conteúdo para adultos
News	Meios de comunicação social de notícias
Nudism	Conteúdo para adultos
Education	*(não migra)*
Online shopping	Lojas online
All communication media	Comunicações de rede
Payment by credit cards	Sistemas de pagamento

Categorias Kaspersky Security for Windows Server	Categorias Kaspersky Endpoint Security for Windows
Online shopping (own payment system)	Lojas online
Online encyclopedias	*(não migra)*
Online banking	Bancos
Weapons	Armas, explosivos, conteúdo militar
Fishing and hunting	*(não migra)*
Payment systems	Sistemas de pagamento
Job search	Procura de emprego
Search engines	*(não migra)*
Police decision (JP)	Proibido pela Polícia do Japão
Trusted by KPSN	*(não migra)*
Untrusted by KPSN	*(não migra)*
Porn	Conteúdo para adultos
Media hosting and streaming	Meios de comunicação social de notícias
Web Mail	E-mail baseado na Web
Traveling	*(não migra)*
TV and radio	Meios de comunicação social de notícias
Teasers and ads services	Faixas
Religion	Religiões, associações religiosas
Restaurants, cafe and food	*(não migra)*
Dating sites	Sites de encontros românticos
Sex education	Conteúdo para adultos
Social networks	Redes sociais
Sport	*(não migra)*
Betting	Jogo, lotarias, apostas
Suicide	Violência, intolerância
Tobacco	Álcool, tabaco, narcóticos
Torrents	Torrents
Mentioned in Federal list of extremists (RF)	Proibido pelas leis da Federação Russa
File sharing	Partilha de ficheiros
Pharmacy	*(não migra)*
Hobby and entertainment	*(não migra)*
Chats and forums	Salas de conversação, fóruns, mensagens instantâneas
Schools and universities pages	*(não migra)*
Astrology and esoterica	*(não migra)*
Extremism and racism	Violência, intolerância
E-commerce	Lojas online
Erotic	Conteúdo para adultos
Humor	*(não migra)*

Local activity control

Applications Launch Control

As definições do Controlo das Aplicações do KSWS são migradas para a secção **Controlos de segurança**, subsecção **Controlo das aplicações**.

Definições do Controlo de Execução de Aplicações

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Operation mode: • **Statistics only** • **Active**	**Ação** (Controlo das Aplicações): • **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 a aplicação sempre que tentar ser executada.
Deny the command interpreters launch with no command to execute	*(não migra)* O Kaspersky Endpoint Security permite a execução de intérpretes de comandos se não forem proibidos pela Controlo das Aplicações.
Rules	**Regras de controlo das aplicações** *(suportado com limitações)* O Kaspersky Endpoint Security 11.11.0 apresenta suporte para a migração de regras de Controlo da Inicialização de Aplicações. A funcionalidade de migração da regra Controlo da Inicialização de Aplicações tem algumas limitações. Por padrão, o Controlo da Inicialização de Aplicações do KSWS inclui duas regras: • **Allow scripts and MSI by OS-trusted certificate** • **Allow executable by OS-trusted certificate** Se, pelo menos, uma regra do KSWS de origem tiver o tipo **Allow**, durante a migração, o KES cria uma nova regra de permissão, **Applications with trusted root certificates**. Ou seja, o Controlo das Aplicações do KES utiliza uma única regra para permitir a execução de scripts fiáveis, pacotes MSI e ficheiros executáveis. Se ambas as regras do KSWS de origem tiverem o tipo **Deny**, o KES não adiciona regras para gerir aplicações com certificados de raiz fiável.
Apply rules to executable files	*(não migra)* O âmbito da aplicação da regra não pode ser configurado nas definições do Controlo das Aplicações do KES. O Controlo das Aplicações do KES aplica regras a todos os tipos de ficheiros: ficheiros executáveis, scripts e pacotes MSI. Se todos os tipos de ficheiro estiverem incluídos no âmbito da aplicação de regra no KSWS, durante a migração, o KES transporta as regras do KSWS. Se algum tipo de ficheiro for excluído do âmbito da aplicação de regra no KSWS, durante a migração, o KES também transporta as regras do KSWS, mas **Testar regras** é selecionado como a ação do Controlo das Aplicações.
Monitor loading of DLL modules	**Monitorizar a carga dos módulos DLL (aumenta significativamente a carga no sistema)**
Apply rules to scripts and MSI packages	*(não migra)* O âmbito da aplicação da regra não pode ser configurado nas definições do Controlo das Aplicações do KES. O Controlo das Aplicações do KES aplica regras a todos os tipos de ficheiros: ficheiros executáveis, scripts e pacotes MSI. Se todos os tipos de ficheiro estiverem incluídos no âmbito da aplicação de regra no KSWS, durante a migração, o KES transporta as regras do KSWS. Se algum tipo de ficheiro for excluído do âmbito da aplicação de regra no KSWS, durante a migração, o KES transporta as regras do KSWS, mas **Testar regras** é selecionado como a ação do Controlo das Aplicações.
Deny applications untrusted by KSN	*(não migra)* O Kaspersky Endpoint Security não considera a reputação das aplicações e permite ou nega a execução de aplicações de acordo com as regras.
Allow applications trusted by KSN	Durante a migração, o KES adiciona uma nova regra de permissão. A categoria do KL **Outro software\Aplicações e software 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	**Utilizadores e os seus direitos** numa regra de permissão do Controlo das Aplicações que inclui a categoria KL **Outro software\Aplicações e software confiável de acordo com a reputação no KSN**.

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Automatically allow software distribution via applications and packages listed	O Controlo de Distribuição de Software no KSWS e no KES funciona de forma diferente. Durante a migração, o KES adiciona novas regras de permissão para aplicações que têm a distribuição automática de software permitida. O hash do ficheiro é especificado como a condição de acionamento da regra.
Always allow software distribution via Windows Installer	O Controlo de Distribuição de Software no KSWS e no KES funciona de forma diferente. Durante a migração, o KES adiciona novas regras de permissão para aplicações que têm a distribuição automática de software permitida (**Software distribution applications and packages allowed**). O hash do ficheiro é especificado como a condição de acionamento da regra. Em propriedades da conta, a caixa de verificação **Atualizadores fiáveis** está marcada.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(não migra)*
Software distribution applications and packages allowed	O Controlo de Distribuição de Software no KSWS e no KES funciona de forma diferente. Durante a migração, o KES adiciona novas regras de permissão para aplicações que têm a distribuição automática de software permitida. O hash do ficheiro é especificado como a condição de acionamento da regra. Em propriedades da conta, a caixa de verificação **Atualizadores fiáveis** está marcada.
Schedule settings	*(não migra)* Se for configurado um agendamento para o componente nas definições do KSWS, o componente Controlo das Aplicações será ativado na migração. Se não for configurado um agendamento para o componente nas definições do KSWS, o Controlo das Aplicações será desativado 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 definições do Controlo de Dispositivos do KSWS são migradas para a secção **Controlos de segurança**, subsecção **Controlo de Dispositivos**.

Definições do Controlo de Dispositivos

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Operation mode: • **Active** • **Statistics only**	*(não migra)* O Controlo das Aplicações opera no modo *Active*. As estatísticas de ligação do dispositivo são fornecidas continuamente pela Auditoria.
Allow using all external devices when the Device Control task is not running	*(não migra)* O Controlo de Dispositivos está sempre ativado durante a execução do Kaspersky Endpoint Security.
Device Control rules	**Dispositivos fiáveis** Durante a migração, o Kaspersky Endpoint Security ignora as regras do KSWS desativadas.
Schedule settings	*(não migra)* O Kaspersky Endpoint Security utiliza o seu próprio agendamento para obter acesso a determinados tipos de dispositivos.

Network-Attached Storages Protection

RPC Network Storage Protection

O Kaspersky Endpoint Security não suporta componentes de Proteção de armazenamentos anexados à rede. Se precisar destes componentes, pode continuar a utilizar o Kaspersky Security for Windows Server.

ICAP Network Storage Protection

O Kaspersky Endpoint Security não suporta componentes de Proteção de armazenamentos anexados à rede. Se precisar destes componentes, pode continuar a utilizar o Kaspersky Security for Windows Server.

Anti-Cryptor for NetApp

O Kaspersky Endpoint Security não suporta o Anti-Cryptor for NetApp. A funcionalidade Anti-Cryptor é fornecida por outros componentes da aplicação, como Deteção de comportamento.

Network activity control

Firewall Management

O Kaspersky Endpoint Security não suporta a Gestão da Firewall do KSWS. As funções da Firewall do KSWS são executadas pela Firewall ao nível do sistema. Após a migração, pode configurar a Firewall do Kaspersky Endpoint Security.

Anti-Cryptor

As definições o Anti-Cryptor da Rede são migradas para a secção **Proteção avançada contra ameaças**, subsecção **Deteção de comportamento**.

Definições do Anti-Cryptor

Definições do KSWS	Definições do KES
Operation mode: • **Statistics only** • **Active**	**Ao detetar encriptação externa de pastas partilhadas**: • **Informar**. • **Bloquear**.
Heuristic analyzer	*(não migra)* O Kaspersky Endpoint Security não utiliza Análise heurística para Deteção 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 encriptação de todas as pastas de rede partilhadas do computador protegido.
Exclusions	*(não migra)* O Kaspersky Endpoint Security tem as suas próprias exclusões para o componente Deteção de comportamento. Pode adicionar 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 definições do Monitor de integridade de ficheiros do KSWS são migradas para a secção **Controlos de segurança**, subsecção **Monitorização da integridade do sistema**.

Definições do Monitor de integridade do ficheiro

Definições do KSWS	Definições do KES
Log information about file operations that appear during the monitor interruption period	*(não migra)* O Kaspersky Endpoint Security não regista eventos para operações de ficheiro 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 registo do USN.
Monitoring scope	**Âmbito da monitorização** → **Ficheiro** *(suportado com limitações)* Os registos de âmbito de monitorização desativados não são migrados para o KES. O Kaspersky Endpoint Security adiciona apenas registos permitidos no âmbito de monitorização.
Trusted users	**Utilizadores e/ou grupos de utilizadores fiáveis**
File operation markers	**Marcadores de operações de ficheiros**
Calculate checksum for the file if possible	**Hashing**
Exclusions	**Exclusões** → **Ficheiro**

Log Inspection

As definições da Inspeção de Registo do KSWS são migradas para a secção **Controlos de segurança**, subsecção **Inspeção de Registo**.

Definições da Inspeção de Registo

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Apply custom rules for log inspection	*(não migra)* O Kaspersky Endpoint Security aplica todas as regras personalizadas permitidas.
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 permitidas.
Predefined rules	**Regras predefinidas**
Password brute-force detection	**Deteção de ataque de força bruta**
Network logon detection	**Deteção de início de sessão de rede**
Exclusions (IP addresses)	**Exclusões** (Endereço IP)
Exclusions (users)	**Exclusões** (Utilizadores)
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 definições dos Registos do KSWS são migradas para a secção **Definições gerais**, **Interface** e as subsecções **Relatórios e armazenamento**.

Definições de registos

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Event logging	**Notificações** (subsecção **Interface**)
Logs folder	*(não migra)* O Kaspersky Endpoint Security guarda os relatórios na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\Report`.
Remove task logs older than N day(s)	*(não migra)* Pode configurar o período de armazenamento para relatórios do KES sob **Definições 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)* Pode configurar a integração do SIEM no Kaspersky Security Center.

Event notifications

As definições de Notificações do KSWS são migradas para a secção **Definições gerais**, subsecção **Interface**.

Definições de notificações

Definições do Kaspersky Security for Windows Server	Definições 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 suporta a modificação do texto da notificação. O Kaspersky Endpoint Security apresenta notificações padrão.
Notify administrators: • **By using Windows Messenger Service command** • **By running executable file** • **By sending email**	Apenas as definições de notificação por e-mail são migradas para o Kaspersky Endpoint Security – **Definições de notificações por e-mail** (grupo **Notificações**). Outros métodos de notificação de administradores não são suportados.
Application database is out of date	**Enviar a notificação "Bases de dados desatualizadas" caso as bases de dados não tenham sido atualizadas**
Application database is extremely out of date	**Enviar a notificação "Bases de dados muito desatualizadas" caso as bases de dados não tenham sido atualizadas**
Critical areas scan has not been performed for a long time	*(não migra)* O Kaspersky Endpoint Security gera um evento ignorado de Verificação de Áreas Críticas após três dias.

Interaction with Administration Server

As definições de interação do Servidor de Administração do KSWS são migradas para a secção **Definições gerais**, subsecção **Relatórios e armazenamento**.

Definições de interação do Servidor de Administração

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Quarantined files	**Ficheiros da Quarentena**
Backed up files	**Criar cópia de segurança do ficheiros**
Blocked hosts	*(não migra)* O Kaspersky Endpoint Security envia automaticamente dados sobre anfitriões bloqueados.

Tasks

Activating the application

O Kaspersky Endpoint Security não suporta a tarefa *Application activation* (KSWS). Pode criar uma tarefa *Adicionar chave* (KES), adicionar uma chave de licença ao Pacote de instalação ou ativar a distribuição automática de chaves de licença.

Copying Updates

As definições da tarefa *Copying Updates* (KSWS) são migradas para a tarefa *Atualização das bases de dados e módulos da aplicação* (KES).

Definições da tarefa Copiar atualizações

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Origem da atualização**: • **Kaspersky Security Center**. • **Servidores de atualização da Kaspersky**. • **Especificado pelo utilizador**.
Use Kaspersky update servers if specified servers are not available	*(não migra)* O Kaspersky Endpoint Security permite selecionar várias fontes de atualização, incluindo servidores de atualização da Kaspersky. Se a primeira origem de atualização não estiver disponível, o Kaspersky Endpoint Security permite que obtenha atualizações de outra origem na lista.
Use proxy server settings to connect to Kaspersky update servers	*(não migra)* O Kaspersky Endpoint Security utiliza o servidor de proxy para todos os componentes. Pode configurar a ligação do servidor de proxy nas opções de rede da aplicação.
Use proxy server settings to connect to other servers	*(não migra)* O Kaspersky Endpoint Security utiliza o servidor de proxy para todos os componentes. Pode configurar a ligação do servidor de proxy nas opções de rede da aplicação.
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 base de dados e atualizações críticas de módulos de aplicações como um único pacote.
Folder for local storage of copied updates	**Copiar atualizações para a pasta**

Baseline File Integrity Monitor

As definições da tarefa *Baseline File Integrity Monitor* (KSWS) são migradas para a tarefa *Verificação de integridade do sistema* e para a secção da política **Controlos de segurança**, subseção **Monitorização da integridade do sistema**.

Definições da tarefa Monitor de integridade do ficheiro de linha de base

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Hash calculation algorithm: • **MD5** • **SHA256**.	*(não migra)* O Kaspersky Endpoint Security usa o algoritmo SHA256 para cálculo de soma de verificação.
Scan scope	**Âmbito da monitorização** (subsecção **Monitorização da integridade do sistema**)

Database Update

As definições da tarefa *Database Update* (KSWS) são migradas para a tarefa *Atualização das bases de dados e módulos da aplicação* (KES).

Definições da tarefa Atualização da base de dados

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Origem da atualização**: • **Kaspersky Security Center**. • **Servidores de atualização da Kaspersky**. • **Especificado pelo utilizador**.
Use Kaspersky update servers if specified servers are not available	*(não migra)* O Kaspersky Endpoint Security permite selecionar várias fontes de atualização, incluindo servidores de atualização da Kaspersky. Se a primeira origem de atualização não estiver disponível, o Kaspersky Endpoint Security permite que obtenha atualizações de outra origem na lista.
Use proxy server settings to connect to Kaspersky update servers	*(não migra)* O Kaspersky Endpoint Security utiliza o servidor de proxy para todos os componentes. Pode configurar a ligação do servidor de proxy nas opções de rede da aplicação.
Use proxy server settings to connect to other servers	*(não migra)* O Kaspersky Endpoint Security utiliza o servidor de proxy para todos os componentes. Pode configurar a ligação do servidor de proxy nas opções de rede da aplicação.
Lower the load on the disk I/O	*(não migra)*

Software modules updates

As definições da tarefa *Software Modules Update* (KSWS) são migradas para a tarefa *Atualização das bases de dados e módulos da aplicação* (KES).

Definições da tarefa Atualização de Módulos de Software

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Origem da atualização**: • **Kaspersky Security Center**. • **Servidores de atualização da Kaspersky**. • **Especificado pelo utilizador**.
Use Kaspersky update servers if specified servers are not available	*(não migra)* O Kaspersky Endpoint Security permite selecionar várias fontes de atualização, incluindo servidores de atualização da Kaspersky. Se a primeira origem de atualização não estiver disponível, o Kaspersky Endpoint Security permite que obtenha atualizações de outra origem na lista.
Use proxy server settings to connect to Kaspersky update servers	*(não migra)* O Kaspersky Endpoint Security utiliza o servidor de proxy para todos os componentes. Pode configurar a ligação do servidor de proxy nas opções de rede da aplicação.
Use proxy server settings to connect to other servers	*(não migra)* O Kaspersky Endpoint Security utiliza o servidor de proxy para todos os componentes. Pode configurar a ligação do servidor de proxy nas opções de rede da aplicação.
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 módulos de aplicação.
Allow operating system restart	*(não migra)* O Kaspersky Endpoint Security pede ao utilizador permissão para reiniciar o computador.
Receive information about available scheduled software modules updates	*(não migra)* O Kaspersky Endpoint Security apresenta notificações sobre atualizações de módulos de software.

Rollback of Application Database Update

As definições da tarefa *Rollback of Application Database Update* (KSWS) são migradas para a tarefa *Reverter atualização* (KES). A nova tarefa *Reverter atualização* (KES) tem um calendário de início de tarefas – *Manually*.

On-Demand Scan

As definições da tarefa *On-Demand Scan* (KSWS) são migradas para a tarefa *Verificação de software malicioso* (KES).

Definições da tarefa Verificação de vírus

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Scan scope	Âmbito de verificação
Protection level: • Maximum protection • Recommended • Maximum performance	Nível de segurança: • Elevado. • Recomendado. • Baixo. As definições do nível de segurança são diferentes no KSWS e 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 ficheiros: • Todos os ficheiros. • Ficheiros verificados por formato. • Ficheiros verificados por extensão. O Kaspersky Endpoint Security não permite criar listas de extensões personalizadas. O Kaspersky Endpoint Security substitui o valor **Objects scanned by specified list of extensions** com o valor **Ficheiros 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 apenas os ficheiros novos e modificados
Scan of compound objects: • All archives • All SFX archives • All email databases • All packed objects • All plain email • All embedded OLE objects	Verificação de ficheiros compostos: • Verificar arquivos. • Verificar arquivos protegidos por password. • Verificar pacotes de distribuição. • Verificar ficheiros de formatos de e-mail. • Verificar ficheiros em formatos do Microsoft Office.
Action to perform on infected and other objects: • Disinfect • Disinfect. Remove if disinfection fails • Remove • Perform recommended action • Notify only	Ação após deteção de ameaças: • Desinfetar, eliminar se a desinfeção falhar. • Desinfetar, informar se a desinfeção 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 se for detetada alguma ameaça.
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 fiável a todos os componentes. Pode configurar exclusões nas definições da zona fiável.
Do not detect	*(não migra)*

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Stop scanning if it takes longer than N sec	**Ignorar ficheiros verificados durante mais de N seg**
Do not scan compound objects larger than N MB	**Não descompactar ficheiros compostos extensos**
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 ficheiros offline na sua totalidade.

Application Integrity Check

As definições da tarefa *Application Integrity Control* (KSWS) são migradas para a tarefa *Verificação de integridade da aplicação* (KES).

Rule Generator for Applications Launch Control

O Kaspersky Endpoint Security não suporta a tarefa *Applications Launch Control Generator*. Pode gerar regras nas definições do Controlo das Aplicações.

Rule Generator for Device Control

O Kaspersky Endpoint Security não suporta a tarefa *Rule Generator for Device Control*. Pode gerar regras nas definições do Controlo de Dispositivos.

Migrar componentes do KSWS

Antes da instalação local, o Kaspersky Endpoint Security verifica se existem outras aplicações da Kaspersky no computador. Se o Kaspersky Security for Windows Server estiver instalado no computador, o KES deteta o conjunto de componentes do KSWS que estão 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 contra invasões e o Motor de remediação são instalados com as definições predefinidas.
- Os componentes Prevenção de ataques BadUSB, Controlo de Anomalias Adaptativo, Encriptação de dados, Detection and Response são ignorados.

Quando instalada remotamente, a aplicação do KES ignora o conjunto de componentes do KSWS instalados. O instalador instala componentes que seleciona nas propriedades do pacote de instalação. Depois de instalar o Kaspersky Endpoint Security e migrar políticas e tarefas, as definições do KES são configuradas de acordo com as definições do KSWS.

Migrar tarefas e políticas do KSWS

Pode migrar definições de tarefas e políticas do KSWS das seguintes formas:

- Usando o Assistente de Conversão de Políticas e Tarefas em Lote (doravante também referido como o Assistente de Migração).

  > O Assistente de Migração do KSWS está disponível apenas na Consola de Administração (MMC). As definições de políticas e tarefas não podem ser migradas na Consola Web e na Cloud Console.

  O assistente de conversão em lote funciona de forma diferente para diferentes versões do Kaspersky Security Center. Recomendamos que atualize a solução para a versão 14.2 ou superior. Nesta versão do Kaspersky Security Center, o Assistente de conversão de políticas e tarefas em lote permite migrar políticas para um perfil em vez de uma política. Nesta versão do Kaspersky Security Center, o Assistente de conversão de políticas e tarefas em lote também permite que migre uma gama mais ampla de definições de política.

- Utilizar o Novo Assistente de Política para o Kaspersky Endpoint Security for Windows.

  O Novo Assistente de Política permite-lhe criar uma política do KES com base numa política do KSWS.

Os procedimentos de migração de política do KSWS são diferentes ao usar o Assistente de migração e o Novo Assistente de Política.

Assistente de conversão de políticas e tarefas em lote

O assistente de migração transfere as definições de política do KSWS para o perfil da política, em vez das definições de política do KES. O *perfil da política* é um conjunto de definições de política que é ativado num computador, se o computador atender às regras de ativação configuradas. A etiqueta do dispositivo `UpgradedFromKSWS` é selecionada como o critério de acionamento do perfil da política. O Kaspersky Security Center adiciona automaticamente a etiqueta `UpgradedFromKSWS` a todos os computadores nos quais instala o KES sobre o KSWS, utilizando a tarefa de instalação remota. Se escolheu um método de instalação diferente, pode atribuir a etiqueta aos dispositivos manualmente.

Para adicionar uma etiqueta a um dispositivo:

1. Crie uma nova etiqueta para servidores – `UpgradedFromKSWS`.

   Para obter mais informação detalhada sobre a criação de etiquetas para dispositivos, consulte a Ajuda do Kaspersky Security Center.

2. Crie um novo grupo de administração na consola do Kaspersky Security Center e adicione os servidores aos quais deseja atribuir a etiqueta a esse grupo.

   Pode agrupar servidores com a ferramenta de seleção. Para obter mais informação detalhada sobre como trabalhar com seleções, consulte a Ajuda do Kaspersky Security Center.

3. Selecione todos os servidores do grupo de administração na consola do Kaspersky Security Center, abra as propriedades dos servidores selecionados e atribua a etiqueta.

Se estiver a migrar várias políticas do KSWS, cada política será convertida num perfil dentro de uma política abrangente. Se a política do KSWS já tiver perfis, esses perfis também serão migrados como perfis. Como resultado, irá obter uma única política que inclui perfis correspondentes a todas as políticas do KSWS.

Como utilizar o Assistente de Conversão de Políticas e Tarefas em Lote para migrar as definições de políticas do KSWS

1. Na Consola de administração, selecione o Servidor de Administração e clique com o botão direito do rato para abrir o menu de contexto.

2. Selecione **All tasks** → **Policies and tasks batch conversion wizard**.

O Assistente de Conversão de Políticas e Tarefas em Lote vai iniciar. Siga as instruções do Assistente.

Passo 1. Selecionar a aplicação para o qual necessita de converter políticas e tarefas

Neste passo, tem de selecionar o Kaspersky Endpoint Security for Windows. Avance para o passo seguinte.

Passo 2. Conversão de políticas

O assistente de migração cria perfis de política do KSWS dentro de uma política do KES. Selecione as políticas do Kaspersky Security for Windows Server que deseja converter para perfis de política. Avance para o passo seguinte.

O Assistente de Migração irá começar a converter as políticas. Os nomes dos novos perfis de política irão corresponder às políticas do KSWS originais.

Passo 3. Relatório de migração de políticas

O assistente de migração cria um relatório de migração de políticas. O relatório de migração de políticas contém a data e a hora em que as políticas foram convertidas, o nome da política do KSWS original, o nome da política do KES de destino e o nome do novo perfil de política.

Passo 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 pretende criar para o Kaspersky Endpoint Security. As novas tarefas serão nomeadas *<Nome da tarefa do KSWS> (convertida).* Avance para o passo seguinte.

Passo 5. Conclusão do assistente

Conclua o assistente. Como resultado, o assistente faz o seguinte:

- São adicionados novos perfis de política à política do Kaspersky Endpoint Security.

  A política inclui perfis com as definições do Kaspersky Security for Windows Server. A nova política tem o estado *Active*. 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 de política com as definições do KSWS será nomeado *UpgradedFromKSWS <Nome da política do Kaspersky Security for Windows Server>*. Nas propriedades do perfil, o assistente de migração seleciona automaticamente a etiqueta do dispositivo `UpgradedFromKSWS` como critério de acionamento. Desta forma, as definições do perfil da política são aplicadas aos servidores automaticamente.

Assistente para criar uma política com base numa política do KSWS

Quando uma política do KES é criada com base numa política do KSWS, o assistente transfere as definições para a nova política respetivamente. Ou seja, uma política do KES irá corresponder a uma política do KSWS. O assistente não converte a política num perfil.

Como utilizar o Novo Assistente de Política para migrar as definições de política do KSWS

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Managed devices** da árvore na Consola de Administração, selecione a pasta com o nome do grupo de administração ao qual os computadores cliente em questão pertencem.
3. Na área de trabalho, selecione o separador **Policies**.
4. Clique em **New policy**.

   O Assistente de Política é iniciado.
5. Siga as instruções do Assistente de Política.

Passo 1. Selecionar a aplicação para criar política de grupo

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

Passo 2. Nomear a política de grupo

Insira um nome para a política de grupo, por exemplo, *Política para o escritório*.

Selecione a caixa de verificação **Use policy settings for an earlier version of the application**. Clique em **Browse** e selecione a política do KSWS.

Passo 3. Participar na Kaspersky Security Network

Leia e aceite os termos da Declaração da Kaspersky Security Network (KSN).

Passo 4. Selecionar o modo de utilização da aplicação em computadores

Selecione **Modo padrão para proteger anfitriões**. O Kaspersky Endpoint Security oferece uma política comum para todos os modos de aplicação e tipos de SO.

Recomendamos a utilização de diferentes políticas para diferentes modos e tipos de sistemas operativos.

Passo 5. Importar definições

Este passo está disponível se selecionar a configuração manual da política no passo 4.

Pode criar uma política com base nas definições do Kaspersky Endpoint Security a partir de um ficheiro de configuração CFG. O Assistente de Nova Política não suporta ficheiros de configuração encriptados. Ao exportar o ficheiro de configuração, ignore o passo de encriptação do ficheiro.

Ao importar um ficheiro de configuração CFG da aplicação, nem todas as definições de política estão disponíveis no assistente. Por exemplo, faltam perfis de política nas definições da aplicação. Se pretender transferir todas as definições e perfis para a política, pode importar outra política a partir de um ficheiro KLP.

Ao importar um ficheiro de configuração, o Kaspersky Endpoint Security não transfere as passwords dos cripto-contentores. Se utilizar a autenticação de dois fatores ao ligar-se aos servidores, terá de definir as passwords do cripto-contentor a partir do zero.

Passo 6 – 10. Configurar as definições de política

Este passo está disponível se selecionar a configuração manual da política no passo 4.

Siga os passos para gerir as definições da política.

Passo 11. Configurar a zona fiável

Configurar a zona fiável. Pode adicionar exclusões de verificação predefinidas e aplicações fiáveis. Exclusões de verificação predefinidas e aplicações fiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e System Center Configuration Manager. Isto significa que não é necessário configurar manualmente uma zona fiável para a aplicação nos servidores. As exclusões de verificação predefinidas e as aplicações fiáveis também podem ajudá-lo a configurar rapidamente o Kaspersky Endpoint Security no modo Light Agent em ambientes virtuais Citrix e VMware.

Passo 12. Selecionar o estado da política

- **Active**. Depois seguinte sincronização, a política será utilizada como a política ativa do computador.

  As definições de uma política ativa são guardadas nos computadores cliente durante a sincronização. Não é possível aplicar simultaneamente várias políticas a um computador, por isso apenas é possível ter uma política ativa em cada grupo.

- **Inactive**. Política de reserva. Se necessário, uma política inativa pode mudar para o estado ativo.

  Pode criar um número ilimitado de políticas inativas. Uma política inativa não afeta as definições da aplicação em computadores na rede. As políticas inativas destinam-se a preparações para situações de emergência, como um ataque de vírus. Se ocorrer um ataque através das unidades amovíveis, pode ativar uma política que bloqueia o acesso às unidades USB. Neste caso, a política ativa torna-se automaticamente inativa.

- **Out-of-office**. A política é ativada quando um computador abandona a rede da organização.

Conclua o assistente.

Configuração adicional de políticas e tarefas após a migração

O KSWS e o KES têm diferentes conjuntos de componentes e definições de política, portanto, após a migração, tem de verificar se as definições da política cumprem os seus requisitos de segurança corporativa.

Verifique as seguintes definições básicas de política:

- Proteção por password. As definições de Proteção por password do KSWS não são migradas. O Kaspersky Endpoint Security possui uma funcionalidade integrada da Proteção por password. Se necessário, ative a Proteção por password e defina uma password.

- Zona confiável. Os métodos utilizados pelo KSWS e KES para selecionar objetos são diferentes. Ao migrar, o KES oferece suporte a exclusões definidas como ficheiros individuais ou caminhos para o ficheiro/a pasta. Se o KSWS tiver exclusões configuradas como uma área predefinida ou um URL de script, tais exclusões não serão migradas. Após a migração, deve adicionar tais exclusões manualmente.

Para garantir que o Kaspersky Endpoint Security funciona corretamente nos servidores, é recomendável adicionar ficheiros importantes para o funcionamento do servidor à zona fiável. Para servidores SQL, tem de adicionar ficheiros base de dados MDF e LDF. Para servidores Microsoft Exchange, tem de adicionar ficheiros CHK, EDB, JRS, LOG e JSL. Pode utilizar máscaras, por exemplo, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

A partir do Kaspersky Endpoint Security 12.6 para Windows, as exclusões de verificação e as aplicações fiáveis são adicionadas à zona fiável. Exclusões de verificação predefinidas e aplicações fiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e System Center Configuration Manager. Isto significa que não é necessário configurar manualmente uma zona fiável para a aplicação nos servidores.

- Firewall. As funções da Firewall do KSWS são executadas pela Firewall ao nível do sistema. No KES, um componente separado é responsável pela funcionalidade da Firewall. Após a migração, pode configurar a Firewall do Kaspersky Endpoint Security.
- Kaspersky Security Network. O Kaspersky Endpoint Security não suporta a configuração do KSN para componentes individuais. O Kaspersky Endpoint Security utiliza o KSN para todos os componentes da aplicação. Para utilizar o KSN, tem de aceitar os novos termos e condições da Declaração da Kaspersky Security Network.
- Controlo de Internet. As regras de bloqueio para controlo da categoria de tráfego de Internet são migradas para uma única regra de bloqueio no Kaspersky Endpoint Security. O Kaspersky Endpoint Security ignora regras de permissão para controlo da categoria. O Kaspersky Endpoint Security não suporta 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 recurso da Web com categorias não suportadas não são migradas. Se for necessário, adicione regras de controlo de Internet.
- Servidor de proxy. A password de ligação do servidor proxy não é migrada. Introduza a password a ser usada para se ligar ao servidor de proxy manualmente.
- Agendamentos de componentes individuais. O Kaspersky Endpoint Security não suporta a configuração de agendamentos para componentes individuais. Os componentes estão sempre ativados enquanto o Kaspersky Endpoint Security está operacional.
- Conjunto de componentes. O conjunto de funcionalidades disponíveis no Kaspersky Endpoint Security depende do tipo de sistema operativo: estação de trabalho ou servidor. Por exemplo, fora das ferramentas de encriptação, apenas a Encriptação de Unidade BitLocker está disponível nos servidores.
- Atributo . O estado do atributo não é migrado. O atributo terá o valor predefinido. Por padrão, quase todas as definições na nova política têm uma proibição aplicada na modificação de definições nas políticas secundárias e na interface da aplicação local. O atributo tem o valor nas definições da política na secção **Managed Detection and Response (Industrial CyberSecurity)** e no grupo de definições **Suporte de utilizador** (secção **Interface**). Se for necessário, configure a herança de definições da política principal.
- Trabalhar com ameaças ativas. A Desinfeção avançada funciona de forma diferente para computadores e servidores. Pode configurar a desinfeção avançada nas definições de tarefa da *Verificação de software malicioso* e nas definições da aplicação.
- Atualizar a aplicação. Para instalar as principais atualizações e correções sem reiniciar, tem de alterar o modo de atualização da aplicação. Por padrão, a funcionalidade Instale atualizações da aplicação sem reiniciar está desativada.

- Kaspersky Endpoint Agent. O Kaspersky Endpoint Security tem um agente integrado para trabalhar com as soluções Detection and Response. Se for necessário, transfira as definições da política do Kaspersky Endpoint Agent para a política do Kaspersky Endpoint Security.

- Tarefas de *Atualização das bases de dados e módulos da aplicação*. Certifique-se de que as definições da tarefa *Atualização das bases de dados e módulos da aplicação* foram migradas corretamente. Em vez das três tarefas do KSWS, o KES usa uma única tarefa do KES. Pode otimizar as tarefas *Atualização das bases de dados e módulos da aplicação* e remover tarefas supérfluas.

- Outras tarefas. Os componentes Controlo das Aplicações, Controlo de Dispositivos e Monitor de integridade de ficheiros funcionam de maneira diferente no KSWS e no KES. O KES não utiliza as tarefas *Baseline File Integrity Monitor*, *Applications Launch Control Generator*, *Rule Generator for Device Control*. Portanto, estas tarefas não são migradas. Após a migração, pode configurar os componentes Monitor de integridade de ficheiros, Controlo das Aplicações, Controlo de Dispositivos.

Migrar a zona fiável do KSWS

Uma *zona fiável* consiste numa lista de objetos e aplicações, configurada pelo administrador do sistema, que o Kaspersky Endpoint Security não monitoriza quando está ativo. Pode migrar objetos de zona fiável do KSWS para o KES através do *Assistente de conversão de políticas e tarefas em lote* ou o *assistente para criar uma nova política KES baseada na política KSWS*. O KSWS e o KES têm diferentes conjuntos de componentes e funcionalidades, portanto, após a migração, tem de verificar se as exclusões cumprem os seus requisitos de segurança corporativa. Os métodos de adição de exclusões à zona fiável também são diferentes para o KES e o KSWS. O Assistente de Migração não possui ferramentas para migrar todas as exclusões do KSWS. Isto significa que, após a migração, tem de adicionar manualmente algumas das exclusões do KSWS.

Para garantir que o Kaspersky Endpoint Security funciona corretamente nos servidores, é recomendável adicionar ficheiros importantes para o funcionamento do servidor à zona fiável. Para servidores SQL, tem de adicionar ficheiros base de dados MDF e LDF. Para servidores Microsoft Exchange, tem de adicionar ficheiros CHK, EDB, JRS, LOG e JSL. Pode utilizar máscaras, por exemplo, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

A partir do Kaspersky Endpoint Security 12.6 para Windows, as exclusões de verificação e as aplicações fiáveis são adicionadas à zona fiável. Exclusões de verificação predefinidas e aplicações fiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e System Center Configuration Manager. Isto significa que não é necessário configurar manualmente uma zona fiável para a aplicação nos servidores.

Métodos de criação de zona fiável do KES e KSWS.

KSWS		KES
Object to scan		
• Predefined scope	*(não migra)*	
• Disk, folder or network location	→	**Ficheiro ou pasta**
• File	→	**Ficheiro ou pasta**
• Script file or web address	*(não migra)*	
Detected object	→	**Tipo de objeto detetado**
Trusted processes	→	**Aplicações fiáveis**

Migração de objetos analisados

As exclusões do KSWS que têm o método **Object to scan** selecionado nas suas propriedades são migrados para as exclusões do KES que têm o método **Ficheiro ou pasta** selecionado nas suas propriedades, com algumas limitações. A migração de uma exclusão depende do método de seleção de objetos:

- Predefined scope – *não migra*.

  Após a migração, deve adicionar tais exclusões manualmente. As exclusões como áreas predefinidas têm de ser configuradas nas definições da tarefa *Verificação de software malicioso*.

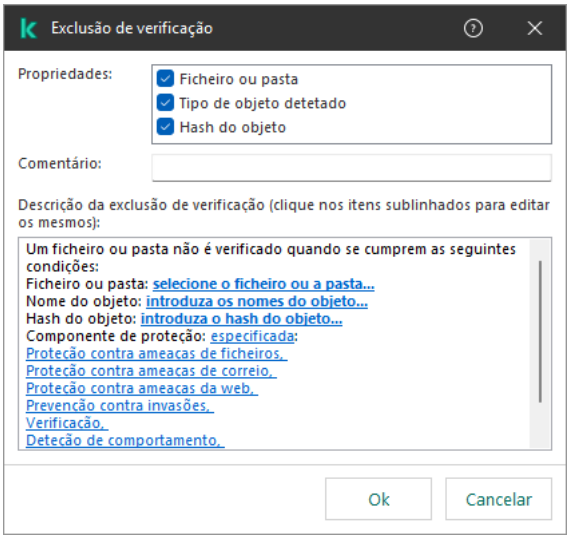
- Disk, folder or network location – migrar para as exclusões do KES que têm o método "Ficheiro ou pasta" selecionado nas propriedades.

- File – migrar para as exclusões do KES que têm o método "Ficheiro ou pasta" selecionado nas propriedades.

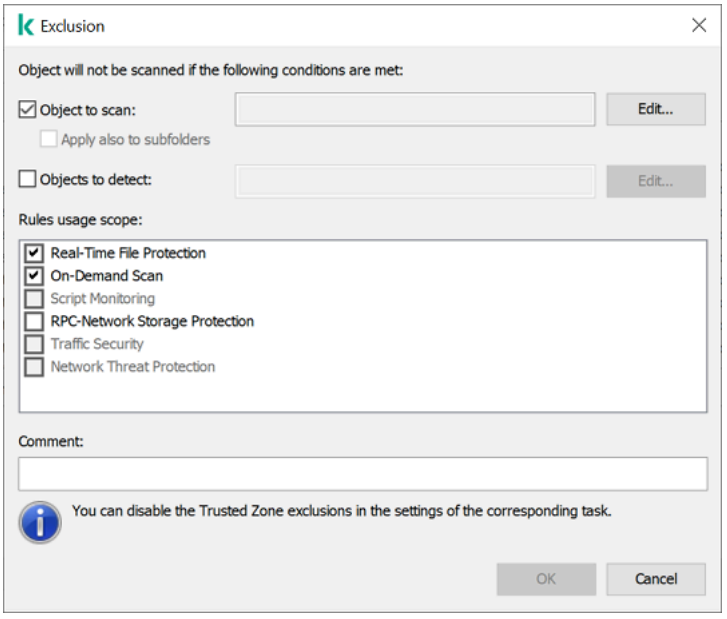
- Script file or web address – *não migra*.

  Após a migração, deve adicionar tais exclusões manualmente. As exclusões como endereços da Internet de scripts têm de ser adicionadas aos endereços da Internet fiáveis para a Proteção contra ameaças da web.

Se a caixa de verificação **Apply also to subfolders** estiver selecionada para o objeto analisado, esta definição é migrada para as exclusões do KES (a caixa de verificação **Incluir subpastas**).



Definições de exclusão do KES



Definições de exclusão do KSWS

Migração de objetos detetados

As exclusões do KSWS que têm o método **Detected object** selecionado nas suas propriedades são migrados para as exclusões do KES que têm o método **Tipo de objeto detetado** selecionado nas suas propriedades. O nome do objeto detetado corresponde à classificação da Enciclopédia Kaspersky (por exemplo, `Email-Worm`, `Rootkit` ou `RemoteAdmin`). O Kaspersky Endpoint Security suporta máscaras com o ponto de interrogação `?` (corresponde a qualquer carácter único) e o asterisco `*` (corresponde a qualquer sequência de caracteres).

Migração do âmbito de utilização da exclusão

O âmbito de utilização de uma exclusão é um conjunto de componentes aos quais a exclusão se aplica. O KES e o KSWS têm conjuntos de componentes diferentes, pelo que o Assistente de migração não pode migrar o âmbito de utilização da exclusão. Por conseguinte, se pelo menos um componente for selecionado no âmbito de utilização do KSWS, o KES aplicará a exclusão a todos os componentes da aplicação.

Pode configurar o âmbito de utilização do KSWS nas definições da zona fiável e também nas definições dos componentes de proteção do KSWS. Para tal, pode selecionar ou desmarcar a caixa de verificação **Apply Trusted Zone** na secção correspondente da política. As definições dos componentes de proteção do KES não incluem esta caixa de verificação. Isto significa que o estado da zona fiável nas definições do componente individual é perdido aquando da migração. Depois de concluir a migração, selecione os componentes aos quais a exclusão se aplica nas definições da zona fiável na política do KES.

Migração de comentários

Os comentários da zona fiável do KSWS são migrados para os comentários de exclusão do KES sem modificação.

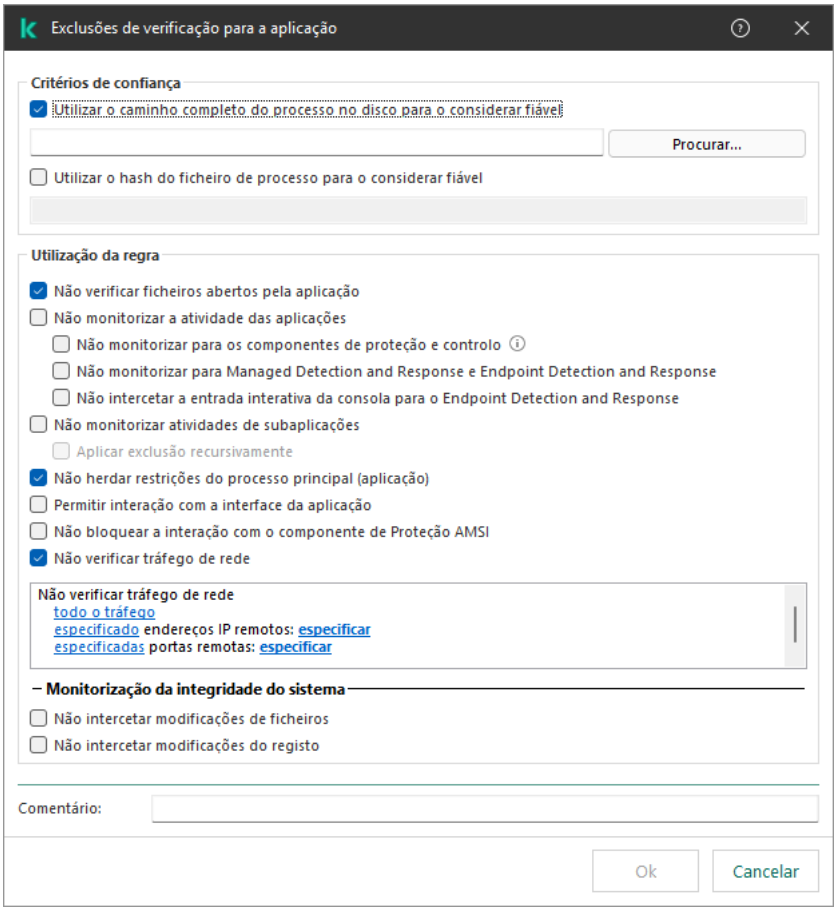
Migração dos processos fiáveis

Os processos fiáveis do KSWS são migrados para processos fiáveis do KES com algumas limitações. A migração de processos fiáveis depende do método de seleção do objeto:

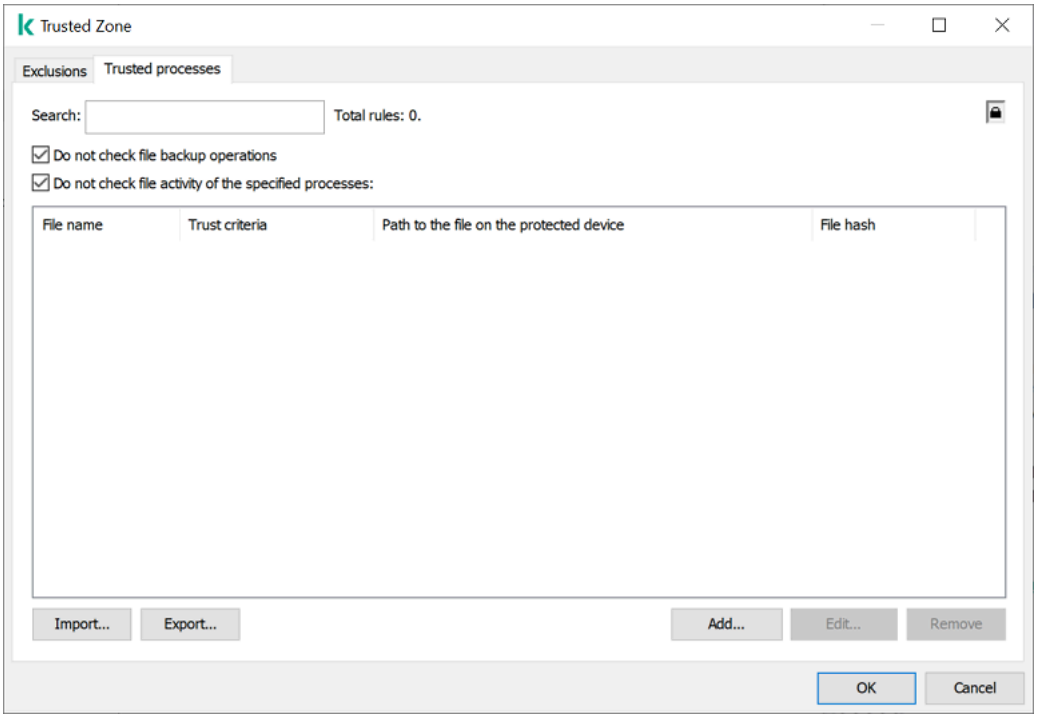
- Path to the file on the protected device – migra para aplicações fiáveis do KES.
- File hash – *não migra*.

Se o KSWS tiver processos fiáveis configurados como um hash do ficheiro, tais processos fiáveis não serão migrados. Após a migração, deve adicionar esses processos fiáveis manualmente.

Se a caixa de verificação **Do not check file backup operations** estiver selecionada nas definições do processo fiável, esta definição é migrada para as aplicações fiáveis do KES (a caixa de verificação **Não monitorizar a atividade da aplicação**).



Definições da aplicação fiável do KES



Definições do processo fiável do KSWS

Migrar regras do Controlo de Execução de Aplicações do KSWS

O Controlo de execução de aplicações do KSWS é bloqueado por padrão. Ou seja, o Controlo de execução de aplicações bloqueia automaticamente todas as aplicações que não estão especificadas nas regras como aplicações permitidas. Portanto, o assistente de migração para o Controlo de aplicações do KES define automaticamente o modo de controlo **Lista de permissão**, que corresponde ao princípio de bloqueio por padrão.

Pode migrar regras do KSWS para o KES através do *Assistente de conversão de políticas e tarefas em lote* ou o *assistente para criar uma nova política KES baseada na política KSWS*.

Migrar o modo do Controlo de execução de aplicações

O modo do Controlo de execução de aplicações do KSWS migra para o Controlo das Aplicações KES da seguinte forma:

- **Statistics only** → **Testar regras**;
- **Active** → **Aplicar regras**.

Migrar regras predefinidas do Controlo de execução de aplicações do KSWS

Por padrão, o Controlo da Inicialização de Aplicações 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 *ficheiros executáveis* assinado por um certificado de raiz fiável. Se, pelo menos, uma regra predefinida do KSWS tiver o tipo **Allow**, o assistente de migração cria uma nova regra de permissão, **Applications with trusted root certificates**. Ou seja, o Controlo das Aplicações do KES utiliza uma única regra para permitir a execução de scripts fiáveis, pacotes MSI e ficheiros executáveis.

Se ambas as regras predefinidas do KSWS tiverem o tipo **Deny**, o KES ignora as regras predefinidas.

Migrar regras personalizadas do Controlo de execução de aplicações KSWS

As regras do Controlo de execução de aplicações do KSWS regulam a execução de ficheiros de acordo com os seguintes critérios:

- assinatura com um certificado digital;
- hash SHA256;
- caminho do ficheiro.

As regras são criadas de forma diferente no KSWS e no KES, portanto, o assistente de migração cria *categorias da aplicação*, que inclui condições e exclusões das regras do KSWS e adiciona estas categorias da aplicação às regras do KES. O assistente utiliza as condições **Certificado**, **Caminho da pasta** e **Hash do ficheiro** em categorias da aplicação. As novas categorias de aplicações estão disponíveis na Consola de Administração do Kaspersky Security Center na secção **Application management → Application categories**.

O assistente de migração agrupa as regras KSWS por tipo e por utilizador. Em seguida, o assistente cria categorias de aplicação que incluem condições e exclusões das regras do KSWS e adiciona as categorias da aplicação às novas regras do KES. O assistente especifica os nomes das regras do KSWS no campo **Descrição** das regras KES.

Migrar as definições avançadas do Controlo de execução de aplicações do KSWS

O princípio de funcionamento do Controlo de execução de aplicações do KSWS e do Controlo das Aplicações do KES é diferente, pelo que o assistente de migração pode migrar um subconjunto de definições.

Definições do Controlo de Execução de Aplicações

Definições do Kaspersky Security for Windows Server	Definições 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 a aplicação sempre que tentar ser executada.
Deny the command interpreters launch with no command to execute	*(não migra)* O Kaspersky Endpoint Security permite a execução de intérpretes de comandos se não forem proibidos pela Controlo das Aplicações.
Apply rules to executable files	*(não migra)* O âmbito da aplicação da regra não pode ser configurado nas definições do Controlo das Aplicações do KES. O Controlo das Aplicações do KES aplica regras a todos os tipos de ficheiros: ficheiros executáveis, scripts e pacotes MSI. Se todos os tipos de ficheiro estiverem incluídos no âmbito da aplicação de regra no KSWS, durante a migração, o KES transporta as regras do KSWS. Se algum tipo de ficheiro for excluído do âmbito da aplicação de regra no KSWS, durante a migração, o KES também transporta as regras do KSWS, mas **Testar regras** é selecionado como a ação do Controlo das Aplicações.
Monitor loading of DLL modules	**Monitorizar a carga dos módulos DLL (aumenta significativamente a carga no sistema)**
Apply rules to scripts and MSI packages	*(não migra)* O âmbito da aplicação da regra não pode ser configurado nas definições do Controlo das Aplicações do KES. O Controlo das Aplicações do KES aplica regras a todos os tipos de ficheiros: ficheiros executáveis, scripts e pacotes MSI. Se todos os tipos de ficheiro estiverem incluídos no âmbito da aplicação de regra no KSWS, durante a migração, o KES transporta as regras do KSWS. Se algum tipo de ficheiro for excluído do âmbito da aplicação de regra no KSWS, durante a migração, o KES transporta as regras do KSWS, mas **Testar regras** é selecionado como a ação do Controlo das Aplicações.

Definições do Kaspersky Security for Windows Server	Definições do Kaspersky Endpoint Security for Windows
Deny applications untrusted by KSN	*(não migra)* O Kaspersky Endpoint Security não considera a reputação das aplicações e permite ou nega a execução de aplicações de acordo com as regras.
Allow applications trusted by KSN	Durante a migração, o KES adiciona uma nova regra de permissão. A categoria do KL **Outro software\Aplicações e software 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	**Utilizadores e os seus direitos** numa regra de permissão do Controlo das Aplicações que inclui a categoria KL **Outro software\Aplicações e software confiável de acordo com a reputação no KSN**.
Automatically allow software distribution via applications and packages listed	O Controlo de Distribuição de Software no KSWS e no KES funciona de forma diferente. Durante a migração, o KES adiciona novas regras de permissão para aplicações que têm a distribuição automática de software permitida. O hash do ficheiro é especificado como a condição de acionamento da regra.
Always allow software distribution via Windows Installer	O Controlo de Distribuição de Software no KSWS e no KES funciona de forma diferente. Durante a migração, o KES adiciona novas regras de permissão para aplicações que têm a distribuição automática de software permitida (**Software distribution applications and packages allowed**). O hash do ficheiro é especificado como a condição de acionamento da regra. Em propriedades da conta, a caixa de verificação **Atualizadores fiáveis** está marcada.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(não migra)*
Software distribution applications and packages allowed	O Controlo de Distribuição de Software no KSWS e no KES funciona de forma diferente. Durante a migração, o KES adiciona novas regras de permissão para aplicações que têm a distribuição automática de software permitida. O hash do ficheiro é especificado como a condição de acionamento da regra. Em propriedades da conta, a caixa de verificação **Atualizadores fiáveis** está marcada.
Schedule settings	*(não migra)* Se for configurado um agendamento para o componente nas definições do KSWS, o componente Controlo das Aplicações será ativado na migração. Se não for configurado um agendamento para o componente nas definições do KSWS, o Controlo das Aplicações será desativado na migração. Não é possível configurar um agendamento separado para o componente. O componente está sempre ativado enquanto o Kaspersky Endpoint Security está operacional.

Instalar o KES em vez do KSWS

Pode instalar o Kaspersky Endpoint Security das seguintes formas:

- Instalar o KES após remover o KSWS (recomendado).
- Instalar o KES sobre o KSWS.

Remover o Kaspersky Security for Windows Server

Pode remover a aplicação remotamente ao usar a tarefa *Uninstall application remotely* ou localmente no servidor. Pode ser necessário reiniciar o servidor após remover o KSWS. Se deseja instalar o Kaspersky Endpoint Security sem reiniciar, certifique-se de que o Kaspersky Security for Windows Server foi completamente removido. Se a aplicação não for completamente removida, a instalação do Kaspersky Endpoint Security pode causar uma falha no funcionamento do servidor. Se tiver usado o utilitário kavremover, recomendamos que se certifique que a aplicação foi completamente removida. O utilitário kavremover não suporta a gestão do KSWS.

> Se a Proteção por password estiver ativada para restringir o acesso ao KSWS, introduza a password de desinstalação nas definições do pacote de instalação do KES.

Depois de remover o KSWS, instale o Kaspersky Endpoint Security for Windows através de qualquer método disponível.

A instalar o Kaspersky Endpoint Security

Quando instala o KES remotamente, os componentes que selecionou nas propriedades do pacote de instalação são instalados no servidor. Recomendamos a seleção de componentes padrão nas propriedades do pacote de instalação. Não é necessário reiniciar ao instalar o KES sobre o KSWS.

Antes da instalação local, o Kaspersky Endpoint Security verifica se existem outras aplicações da Kaspersky no computador. Se o Kaspersky Security for Windows Server estiver instalado no computador, o KES deteta o conjunto de componentes do KSWS que estão instalados e seleciona os mesmos componentes para instalação. Não é necessário reiniciar ao instalar o KES sobre o KSWS.

> Se a instalação do KES sobre o KSWS falhar, poderá reverter a instalação. Depois de reverter a instalação, é recomendável reiniciar o servidor e tentar novamente.

As definições e tarefas do KSWS não são migradas quando o Kaspersky Endpoint Security for Windows é instalado. Para migrar as definições e tarefas, execute o Assistente de conversão de políticas e tarefas em lote.

Pode verificar a lista de componentes instalados na secção **Segurança** da interface da aplicação, utilizando o comando `status` ou na consola do Kaspersky Security Center nas propriedades do computador. Pode alterar o conjunto de componentes após a instalação ao utilizar o *Alterar componentes da aplicação*.

Migrar a configuração [KSWS+KEA] para a configuração [KES+agente incorporado]

Para suportar a utilização do Kaspersky Endpoint Security for Windows como parte do EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA e MDR, foi adicionado um agente integrado à aplicação. Já não precisa de uma aplicação Kaspersky Endpoint Agent em separado para trabalhar com estas soluções.

Ao migrar do KSWS para o KES, as soluções EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMAe MDR continuam a funcionar 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 incorporado] envolve os passos seguintes:

1. **Migrar do KSWS para o KES**

   Migrar do KSWS para o KES envolve a instalação do Kaspersky Endpoint Security, em vez do Kaspersky Security for Windows Server.

   Os administradores geralmente ativam a proteção por password para restringir o acesso ao KSWS e ao KEA. A partir do Kaspersky Security Center Linux 15.1, pode inserir a password de desinstalação da aplicação nas definições da tarefa *Install application remotely*. A tarefa permite inserir apenas uma password de desinstalação. Ou seja, se for definida a mesma password para o KSWS e o KEA, as aplicações KSWS e KEA são removidas com êxito. Se as passwords forem diferentes, a remoção de uma das aplicações falha com um erro de acesso. Para concluir a migração, tem de desativar a Proteção por password para a aplicação cuja password não foi possível introduzir nas definições da tarefa *Install application remotely*.

   Para realizar a migração, tem de selecionar os componentes necessários para suportar as soluções Detection and Response como parte do Kaspersky Endpoint Security. Depois de instalar a aplicação, o Kaspersky Endpoint Security troca para a utilização do agente incorporado e remove o Kaspersky Endpoint Agent.

2. **Migração da política e das tarefas**

   A migração das políticas e tarefas [KSWS+KEA] para [KES+agente incorporado] envolve os passos seguintes:

   1. Migração de políticas e tarefas do KSWS para o KES usando o Assistente de conversão de políticas e tarefas em lote (disponível apenas na Consola de Administração (MMC)).

      Como resultado, é adicionado um perfil de política com o nome *UpgradedFromKSWS <Nome da política do Kaspersky Security for Windows Server>* à política KES. Também são criadas novas tarefas KES com os nomes *<Nome da tarefa KSWS> (convertido)*.

   2. Migração de políticas e tarefas de KEA para KES usando o assistente para migração do Kaspersky Endpoint Agent (disponível apenas na Consola Web e na Cloud Console).

      Como resultado, é criada uma nova política com o nome *<Nome da política do Kaspersky Endpoint Security> e <Nome da política do Kaspersky Endpoint Agent>*. Também são criadas novas tarefas e tarefas KES.

3. **Funcionalidade do licenciamento**

Se utilizar uma licença comum do Kaspersky Endpoint Detection and Response Optimum ou do Kaspersky Optimum Security para ativar o Kaspersky Endpoint Security for Windows e o Kaspersky Endpoint Agent, a funcionalidade EDR Optimum será ativada automaticamente após a atualização da aplicação para a versão 11.7.0. Não precisa de fazer mais nada.

Se utilizar uma licença autónoma do Suplemento do Kaspersky Endpoint Detection and Response Optimum para ativar a funcionalidade EDR Optimum, deve certificar-se de que a chave do Suplemento EDR Optimum é adicionada ao repositório do Kaspersky Security Center e de que a funcionalidade de distribuição automática da chave de licença está ativada. Depois de atualizar a aplicação para a versão 11.7.0, a funcionalidade EDR Optimum é ativada automaticamente.

Se utilizar 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, tem de substituir a chave do Kaspersky Endpoint Security for Windows pela chave comum do Kaspersky Endpoint Detection and Response Optimum ou do Kaspersky Optimum Security. Pode substituir a chave através da tarefa *Add key*.

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.

Apenas a licença da Kaspersky Anti Targeted Attack Platform pode ser usada para ativar o Kaspersky Endpoint Security como parte da solução da Kaspersky Anti Targeted Attack Platform. Depois de atualizar a aplicação para a versão 12.1, a funcionalidade EDR (KATA) é ativada automaticamente. Não precisa de fazer mais nada.

4. **Verificação do estado de funcionamento do Kaspersky Endpoint Detection and Response Optimum e do Kaspersky Sandbox**

   Se, após a atualização, o computador tiver o estado *Critical* na consola do Kaspersky Security Center:

   - Certifique-se de que o computador tem o Agente de Rede versão 13.2 ou superior instalado.
   - Verifique o estado de funcionamento do agente integrado ao consultar o *Report on status of application components*. Se um componente tiver o estado *Not installed*, instale o componente com a tarefa *Change application components*.
   - Certifique-se de que aceita a Declaração da Kaspersky Security Network na nova política do Kaspersky Endpoint Security for Windows.

   Certifique-se de que a funcionalidade EDR Optimum é ativada usando o *Report on status of application components*. Se um componente tiver o estado *Não abrangido pela licença*, certifique-se de que a funcionalidade de distribuição automática da chave de licença do EDR Optimum está ativada.

Certificar-se de que o Kaspersky Security for Windows Server foi removido com sucesso

Certifique-se de que o Kaspersky Security for Windows Server foi completamente removido:

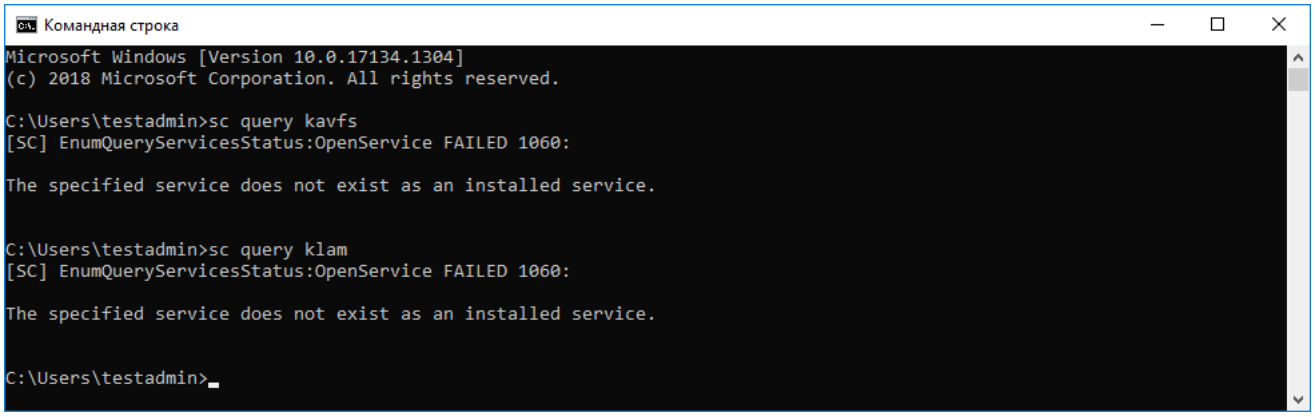
- A pasta `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` não existe.
- Os serviços seguintes não estão presentes:
  - Kaspersky Security Service (KAVFS)
  - Serviço do Kaspersky Security Management (KAVFSGT)

- Serviço do Kaspersky Security Exploit Prevention (KAVFSSLP)
- Serviço do Kaspersky Security Script Checker (KAVFSSCS)

Pode verificar os serviços em execução no Gestor de Tarefas ou ao emitir o comando `sc query` (veja a figura abaixo).

- Os controladores seguintes não estão presentes:
  - klam.sys
  - klflt.sys
  - klramdisk.sys
  - klelaml.sys
  - klfltdev.sys
  - klips.sys
  - klids.sys
  - klwtpee

  Pode verificar os controladores instalados na pasta `C:\Windows\System32\drivers` ou ao emitir o comando `sc query`. Se um serviço ou controlador estiver em falta, irá receber a seguinte resposta:



Certifique-se de que os serviços e controladores do Kaspersky Security for Windows Server foram removidos com sucesso

Se os ficheiros da aplicação ou do controlador permanecerem no servidor, elimine os ficheiros relevantes manualmente. Se os serviços do Kaspersky Security for Windows Server ainda estiverem em execução no servidor, pare (`sc stop`) e elimine (`sc delete`) os serviços manualmente. Para parar o controlador klam.sys, use o comando `fltmc unload klam`.

Ativar o KES com uma chave KSWS

Depois de instalar a aplicação, pode ativar o Kaspersky Endpoint Security for Windows (KES) usando uma chave da 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 suporta a *licença Kaspersky Security para armazenamento*. Para trabalhar com esta licença, tem de usar o Kaspersky Security for Windows Server.

Para ativar o KES com a chave KSWS, basta utilizar o código de ativação. Se estiver a utilizar um ficheiro-chave para ativar a aplicação, tem de contactar o Suporte Técnico para obter um ficheiro-chave do Kaspersky Endpoint Security.

Ativar o Kaspersky Endpoint Security for Windows com uma chave do Kaspersky Security for Windows Server

Método de ativação do Kaspersky Security for Windows Server	Migrar a chave para o Kaspersky Endpoint Security for Windows.
Distribuição automática da chave da licença do KSWS para computadores.	Se a distribuição automática de chaves estiver ativada nas propriedades da chave da licença do KSWS, o KES será automaticamente ativado com a chave do KSWS.
A chave do KSWS é adicionada por uma tarefa.	Se o seu KSWS for ativado usando a tarefa, a chave da licença do KSWS será eliminada durante a migração do KSWS. Deve ativar a aplicação novamente. Por exemplo, pode adicionar uma chave da licença ao pacote de instalação do Kaspersky Endpoint Security for Windows.
A chave do KSWS é adicionada localmente na interface da aplicação.	Se o seu KSWS for ativado localmente usando o Assistente de Ativação da Aplicação, a chave da licença do KSWS será eliminada durante a migração do KSWS. Deve ativar a aplicação novamente. Por exemplo, pode adicionar uma chave da licença ao pacote de instalação do Kaspersky Endpoint Security for Windows.
A chave do KSWS é adicionada ao pacote de instalação.	Se o seu KSWS for ativado usando a chave do pacote de instalação, a chave da licença do KSWS será eliminada durante a migração do KSWS. Deve ativar a aplicação novamente. Por exemplo, pode adicionar uma chave da licença ao pacote de instalação do Kaspersky Endpoint Security for Windows.
Imagem da máquina virtual paga (Amazon Machine Image – AMI) no Amazon Web Services (AWS).	Se comprou o Kaspersky Security Center como uma imagem da máquina virtual paga (Amazon Machine Image – AMI) no Amazon Web Services (AWS), não é necessário ativar o KES. Neste caso, o Kaspersky Security Center utiliza a subscrição da AWS que já está adicionada à aplicação.
Imagem gratuita pronta do Kaspersky Security Center com a sua própria licença (Traga a sua própria licença – modelo BYOL).	Se estiver a utilizar uma imagem gratuita pronta do Kaspersky Security Center com a sua própria licença num ambiente de nuvem (o modelo Traga a sua própria licença – BYOL), tem de ativar a aplicação utilizando qualquer método disponível. Irá precisar de uma licença do Kaspersky Hybrid Cloud Security.

Considerações especiais para migrar servidores de alta carga

Nos servidores de alta carga, é importante monitorizar o desempenho e evitar falhas. Após a migração para o Kaspersky Endpoint Security for Windows, recomendamos que desative temporariamente os componentes da aplicação que utilizam recursos substanciais do servidor em relação a outros componentes. Depois de verificar se o servidor está a funcionar normalmente, pode reativar os componentes da aplicação.

Recomendamos a migração de servidores de alta carga da seguinte forma:

1. Crie uma política do Kaspersky Endpoint Security com as definições predefinidas.

   As definições predefinidas são consideradas as ideais. Estas definições são recomendadas pelos peritos da Kaspersky. As definições predefinidas fornecem o nível de proteção recomendado e o uso ideal dos recursos.

2. Nas definições da política, desative os seguintes componentes: Proteção contra ameaças de rede, Deteção de comportamento, Prevenção de explorações, Motor de remediação, Controlo das Aplicações.

   Se a sua organização tiver a solução Kaspersky Managed Detection and Response (MDR) implementada, carregue o ficheiro 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.

   Se a sua organização tiver soluções Detection and Response implementadas, selecione os componentes relevantes nas propriedades do pacote de instalação.

5. Verifique as definições da aplicação:

   - A aplicação é ativada com a chave da licença do KSWS.
   - A nova política é aplicada. Os componentes selecionados anteriormente são desativados.

6. Certifique-se de que o servidor está a funcionar. Certifique-se de que o Kaspersky Endpoint Security for Windows não está a utilizar mais de 1% dos recursos do servidor.

7. Se necessário, crie exclusões de verificação, adicione aplicações fiáveis, crie uma lista de endereços da internet fiáveis.

8. Ative os componentes de Deteção de comportamento, Prevenção de explorações e Motor de remediação. Certifique-se de que o Kaspersky Endpoint Security for Windows não está a utilizar mais de 1% dos recursos do servidor.

9. Ative o componente Proteção contra ameaças de rede. Certifique-se de que o Kaspersky Endpoint Security for Windows não está a utilizar mais de 2% dos recursos do servidor.

10. Ative o componente Controlo das Aplicações no modo de teste de regras.

11. Certifique-se de que o Controlo das Aplicações está a funcionar. Se necessário, adicione novas regras de Controlo das Aplicações e desative o modo de teste de regras após confirmar que o Controlo das Aplicações está a funcionar.

Depois de migrar do KSWS para o KES, certifique-se de que a aplicação está a funcionar corretamente. Verifique o estado do servidor na consola (deve ser *OK*). Certifique-se de que não é relatado nenhum erro para a aplicação, verifique também a hora da última ligação com o Servidor de Administração, a hora da última atualização da base de dados e o estado da proteção do servidor.

Gerir a aplicação num servidor no modo Server Core

Um servidor no modo Server Core não possui um GUI. Portanto, apenas pode gerir a aplicação remotamente através da consola do Kaspersky Security Center ou localmente na linha de comandos.

Gerir a aplicação através da consola do Kaspersky Security Center

Instalar a aplicação através da consola do Kaspersky Security Center não é diferente de instalá-la da maneira normal. Quando criar um pacote de instalação, pode adicionar uma chave da licença para ativar a aplicação. Pode utilizar uma chave do Kaspersky Endpoint Security for Windows ou uma chave do Kaspersky Security for Windows Server.

Num servidor no modo Server Core, não estão disponíveis os seguintes componentes da aplicação: Proteção contra ameaças da web, Proteção contra ameaças de correio, Controle de Internet, Prevenção de ataques BadUSB, Encriptação ao nível dos ficheiros (FLE), Encriptação de disco Kaspersky (FDE).

Reinicio não é necessário ao instalar o Kaspersky Endpoint Security. O reinicio é necessário apenas se precisar de remover aplicações incompatíveis antes da instalação. Reinício pode também ser necessário ao atualizar a versão da aplicação. A aplicação não pode mostrar uma janela para solicitar ao utilizador que reinicie o servidor. Pode aprender sobre a necessidade de reiniciar o servidor a partir de relatórios na consola do Kaspersky Security Center.

Gerir a aplicação num servidor no modo Server Core não é diferente de gerir um computador. Pode utilizar políticas e tarefas para configurar a aplicação.

Gerir a aplicação num servidor no modo Server Core envolve as seguintes considerações especiais:

- O servidor no modo Server Core não possui um GUI, portanto, o Kaspersky Endpoint Security não mostra um aviso a informar o utilizador que a Desinfeção Avançada é necessária. Para desinfetar uma ameaça, tem de Ativar Tecnologia de Desinfeção Avançada nas definições da aplicação e ativar a desinfeção avançada imediata nas definições da *Verificação de software malicioso*. Depois, tem de iniciar uma tarefa *Verificação de software malicioso*.

- A Encriptação de Unidade BitLocker está disponível apenas com um Trusted Platform Module (TPM). Um PIN/password não pode ser utilizado para encriptação porque a aplicação não consegue apresentar a janela de pedido de password para autenticação de pré-arranque. Se o sistema operativo do computador tiver o modo de compatibilidade padrão do Tratamento de Informação Federal (FIPS) ativado, ligue uma unidade amovível para guardar a chave de encriptação antes de começar a encriptar a unidade.

Gerir a aplicação a partir da command line

Quando não puder usar um GUI, pode gerir o Kaspersky Endpoint Security a partir da linha de comandos.

Para instalar a aplicação num servidor no modo Server Core, execute o seguinte comando:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

Para ativar a aplicação, execute o seguinte comando:

```
avp.com license /add <activation code or key file>
```

Para verificar os estados do perfil da aplicação, execute o seguinte comando:

```
avp.com status
```

Para ver a lista de comandos de gestão da aplicação, execute o seguinte comando:

```
avp.com help
```

Migrar de [KSWS+KEA] para [KES+agente incorporado]

Ao migrar do Kaspersky Security for Windows Server (KSWS) para o Kaspersky Endpoint Security (KES), pode 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 gere as soluções da Kaspersky através da Consola de Administração (MMC). O Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) também é implementado

  São criado três grupos de administração no Kaspersky Security Center, que contêm 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 gerido pela sua própria política. As tarefas *Database Update* e *On-demand scan* são criadas para todos os servidores da organização.

  A chave de ativação do KSWS é adicionada ao Kaspersky Security Center. A distribuição automática de chaves é 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 gerido pelas 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 instalado.

  O KSWS é gerido pela política *Exchange_Policy*. As tarefas *Database Update*, *On-demand scan* também são criadas.

Planear a migração

A migração envolve os seguintes passos:

1. Migração de tarefas e políticas do KSWS que utilizam o Assistente de Conversão de Políticas e Tarefas em Lote.
2. Migração da política do Kaspersky Endpoint Agent que utiliza o Assistente de Conversão de Políticas e Tarefas em Lote.
3. Utilizar etiquetas para ativar perfis de política nas propriedades da nova política.
4. Instalar o KES sobre o KSWS.
5. A ativar o EDR Optimum.
6. A confirmar se o KES está a funcionar.

O cenário de migração é realizado inicialmente num dos clusters dos servidores SQL. Em seguida, o cenário de migração é realizado no outro cluster dos servidores SQL. Em seguida, o cenário de migração é realizado no Microsoft Exchange.

Migração de tarefas e políticas do KSWS que utilizam o Assistente de Conversão de Políticas e Tarefas em Lote

Para migrar tarefas do KSWS, pode usar o Assistente de Conversão de Políticas e Tarefas em Lote (o assistente de migração). Como resultado, em vez das políticas *SQL_Policy(1)*, *SQL_Policy(2)* e *Exchange_Policy*, irá obter uma única política com três perfis para os servidores SQL e Microsoft Exchange, respetivamente. O novo perfil de política com as definições do KSWS será nomeado *UpgradedFromKSWS <Nome da política do Kaspersky Security for Windows Server>*. Nas propriedades do perfil, o assistente de migração seleciona automaticamente a etiqueta do dispositivo `UpgradedFromKSWS` como critério de acionamento. Desta forma, as definições do perfil da política são aplicadas aos servidores automaticamente.

Migração da política do Kaspersky Endpoint Agent que utilizam o Assistente de Conversão de Políticas e Tarefas em Lote

Para migrar políticas do Kaspersky Endpoint Agent, pode usar o Assistente de Conversão de Políticas e Tarefas em Lote. O Assistente de Migração de Políticas e Tarefas do Kaspersky Endpoint Agent está disponível apenas na Consola Web.

Utilizar etiquetas para ativar perfis de política nas propriedades da nova política

Selecione a etiqueta do dispositivo que atribuiu anteriormente como a condição de ativação do perfil. Abra as propriedades da política e selecione *General rules for policy profile activation* como a condição de ativação do perfil.

Instalar o KES em vez do KSWS

Antes de instalar o KES, tem de desativar a Proteção por password nas propriedades da política do KSWS.

A instalação do KES envolve os seguintes passos:

1. Preparar o pacote de instalação. Nas propriedades do pacote de instalação, selecione o kit de distribuição do Kaspersky Endpoint Security for Windows 12.0 e selecione o conjunto de componentes padrão.
2. Crie uma tarefa *Install application remotely* para um dos grupos de administração do servidor SQL.
3. Nas propriedades da tarefa, selecione o pacote de instalação e o ficheiro da 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 etiqueta `UpgradedFromKSWS` aos nomes dos computadores na consola após a conclusão da instalação do KES.

Para verificar a instalação do KES, pode utilizar o *Report on protection deployment*. Também pode verificar o estado do dispositivo. Para confirmar a ativação da aplicação, pode utilizar o *Report on usage of license keys*.

Ativar o EDR Optimum

Pode ativar a funcionalidade EDR Optimum ao utilizar uma licença independente do Suplemento do Kaspersky Endpoint Detection and Response Optimum. Tem de confirmar se a chave EDR Optimum foi adicionada ao repositório do Kaspersky Security Center e se a funcionalidade de distribuição automática da chave de licença está ativada.

Para verificar a ativação do EDR Optimum, pode usar o *Report on status of application components*.

Confirmar se o KES está a funcionar

Para confirmar se o KES está a funcionar, pode verificar se não foi relatado nenhum erro. O estado do dispositivo tem de ser *OK*. Tarefas de atualização e verificação de software malicioso concluídas com êxito.

Modo Light Agent para proteger máquinas virtuais

A partir da versão 12.8, pode 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 esta solução, tem de instalar a aplicação no modo Light Agent.

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

Pode usar o Kaspersky Endpoint Security no modo Light Agent como parte do Kaspersky Security for Virtualization Light Agent a partir da versão 6.2.

Quando inicia o Light Agent, ele estabelece e mantém uma ligação à máquina virtual SVM (Secure Virtual Machine). Um servidor de proteção é implementado na SVM. O *Servidor de Proteção* é o componente da solução Kaspersky Security for Virtualization Light Agent que verifica ficheiros em busca de vírus e outros softwares maliciosos, atualiza bases de dados de antivírus e gere chaves de licença. O Light Agent envia ficheiros ou os seus fragmentos que precisam de ser verificados para a SVM. Os resultados da verificação estão disponíveis para todas as máquinas virtuais com o Light Agent instalado (a tecnologia SharedCache). A 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 muitas SVM. O Servidor de Integração faz a gestão da interação entre máquinas virtuais e SVM. O *Servidor de Integração* é um componente da solução Kaspersky Security for Virtualization Light Agent que gera uma lista de SVM disponíveis e transfere estes dados para os Light Agents, participa na deteção de SVM pelos Light Agents, protege a ligação entre os Light Agents e os SVM, e executa outras funções.

Considerações especiais para o modo Light Agent

Pode gerir o Kaspersky Endpoint Security no modo Padrão e no modo Light Agent Light Agent utilizando as políticas e tarefas do Kaspersky Endpoint Security. No modo Light Agent, alguns componentes e recursos da aplicação não estão disponíveis.

Atualização de bases de dados e módulos de software de aplicação

O Kaspersky Endpoint Security no modo Light Agent usa bases de dados de malware especiais que a aplicação precisa ao trabalhar como parte da solução Kaspersky Security for Virtualization Light Agent. O Kaspersky Endpoint Security obtém atualizações de bases de dados e módulos da aplicação do Servidor de Proteção.

As bases de dados e módulos nas máquinas virtuais protegidas são atualizados utilizando uma tarefa especial *Atualização das bases de dados e módulos da aplicação*, na qual uma pasta no SVM é especificada como a origem da atualização. O Light Agent executa a tarefa *Atualização das bases de dados e módulos da aplicação* automaticamente. Não pode selecionar uma origem da atualização diferente, configurar o agendamento de tarefas ou remover a tarefa.

Uma reversão da atualização mais recente da base de dados de software malicioso também é realizada no lado do Servidor de Proteção. Após uma reversão de uma atualização de bases de dados e módulos da aplicação no SVM, é iniciada uma tarefa local especial *Atualização das bases de dados e módulos da aplicação* na máquina virtual protegida. Esta tarefa faz com que o Light Agent volte a usar o conjunto anterior de bases de dados de software malicioso.

O Kaspersky Endpoint Security no modo Light Agent não suporta a tarefa *Reverter atualização*.

A ativar o Light Agent

Para ativar a aplicação, tem de adicionar uma chave de licença à SVM ao qual o Light Agent está ligado. Não precisa de ativar a aplicação em separado.

Outras considerações especiais para o modo Light Agent

- Ao criar uma política para a aplicação, recomendamos que selecione o modo Light Agent. Neste modo, o Novo assistente de políticas pede-lhe para configurar a ligação SVM. Estas definições são necessárias para que a aplicação funcione no modo Light Agent.
- Não é possível instalar componentes de Encriptação de dados e Controlo de Anomalias Adaptativo no modo Light Agent. O conjunto de componentes também depende do tipo de sistema operativo convidado: estação de trabalho ou servidor.
- O Light Agent não suporta a integração com as soluções Kaspersky Endpoint Detection and Response Expert e Kaspersky Endpoint Detection and Response Expert (cloud).
- Pode gerir o Light Agent na Consola de Administração (MMC) e na Consola Web do Kaspersky Security Center. Não é possível gerir o Light Agent na Consola de Nuvem do Kaspersky Security Center.
- Não é possível alterar o conjunto de componentes da aplicação em máquinas virtuais VDI.
- O Kaspersky Endpoint Security comunica com servidores KSN por meio de um servidor proxy KSN. A comunicação direta com o KSN não é suportada.
- O modo de nuvem do Kaspersky Security Network não é suportado.
- Não é possível utilizar o servidor proxy da aplicação ao ligar ao Servidor de Integração (VIIS), ao Servidor de Proteção (SVM) e aos servidores KSN.

Configuração preliminar da máquina virtual

Pode instalar o Kaspersky Endpoint Security numa máquina virtual que utilize a tecnologia de plataforma virtual. O Kaspersky Endpoint Security suporta as plataformas virtuais VMware, Microsoft Hyper-V, Citrix. Antes da instalação, tem de efetuar a configuração preliminar das máquinas virtuais.

Compatibilidade com a tecnologia Citrix App Layering

Se tenciona utilizar o Full User Layer para guardar o estado das máquinas virtuais temporárias, tem de fazer o seguinte antes de instalar no modelo da máquina virtual:

1. Crie o ficheiro C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt e adicione as seguintes exclusões ao mesmo:

   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`

2. No registo do sistema operativo, na chave HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr, crie um novo valor DWORD chamado MiniFilterBypass e defina-o como 1.

3. No registo do sistema operativo, na chave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd, crie um novo valor MULTI_SZ chamado ExcludeKey e defina-o como \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab.

4. Reinicie a máquina virtual.

Para a instalação em máquinas virtuais numa infraestrutura que usa o Citrix App Layering, tem de fazer o seguinte:

1. Instale o Kaspersky Security Center Administration Agent e o Kaspersky Endpoint Security for Windows no modelo da máquina virtual na Camada da Aplicação.

2. Crie uma imagem de máquina virtual composta por várias camadas.

3. Implemente a imagem criada em hipervisores que suportam a solução Citrix App Layering.

4. Configure a criação de máquinas virtuais temporárias a partir da imagem criada.

Para obter detalhes sobre a instalação de software antivírus juntamente com o Citrix App Layering, consulte a documentação do Citrix App Layering.

Compatibilidade com a tecnologia Citrix Provisioning (Citrix Provisioning Services)

Para garantir que a aplicação é compatível com a tecnologia Citrix Provisioning (Citrix Provisioning Services):

- Se o software Citrix Provisioning Target Device estiver instalado na máquina virtual, tem de o remover antes de instalar a aplicação Kaspersky Endpoint Security (para mais detalhes, visite o site de suporte técnico do Citrix). Depois de instalar a aplicação, tem de reinstalar o Citrix Provisioning Target Device. Também é necessário reinstalar o dispositivo de destino do Citrix Provisioning ao restaurar a aplicação, incluindo ao atualizar o sistema operativo.

A atualização do sistema operativo envolve os seguintes passos:

1. Elimine o dispositivo de destino do Citrix Provisioning.
2. Atualize o sistema operativo.
3. Depois de iniciar a máquina virtual, certifique-se de que a aplicação Kaspersky Endpoint Security está em execução e a funcionar corretamente.
4. Reinstale o dispositivo de destino do Citrix Provisioning.

- Ao instalar a aplicação através do Assistente de Configuração ou remotamente através do Kaspersky Security Center, tem de selecionar a caixa de verificação **Garanta a compatibilidade com Citrix PVS**.

Compatibilidade com a tecnologia Omnissa App Volumes

Antes de instalar no modelo da máquina virtual, tem de criar o ficheiro %SVAgent%\Config\Custom\snapvol.cfg e adicionar-lhe as seguintes exclusões:

- `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 do Omnissa.

A instalar o Light Agent

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

A instalação da aplicação no modo Light Agent é a mesma que no modo Padrão. Antes de instalar o Light Agent numa máquina virtual, tem de se certificar de que o Kaspersky Security Center Network Agent está instalado. O *Agente de Rede* facilita a interação entre o Servidor de Administração e uma máquina virtual.

O Light Agent pode ser instalado no computador de uma das seguintes formas:

- Remotamente, utilizando o Kaspersky Security Center.
- Localmente, utilizando o Assistente de Instalação.
- Localmente a partir da linha de comandos.

Para instalar o Light Agent, deve selecionar a configuração apropriada em definições do pacote de instalação ou no Assistente de Instalação.

Ao instalar o Light Agent num servidor, os componentes de proteção avançada (Deteção de comportamento, Prevenção de explorações, Motor de remediação) são excluídos da configuração padrão da aplicação. As predefinições da aplicação fornecem o nível de proteção recomendado e o uso ideal dos recursos do servidor. Ao instalar o Light Agent numa estação de trabalho, os componentes de proteção avançada são incluídos na configuração padrão da aplicação.

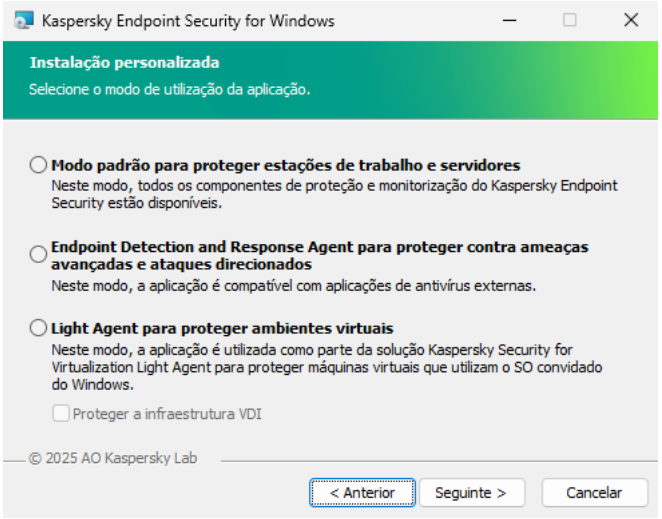
Ao instalar o Light Agent, recomendamos que selecione exclusões predefinidas e aplicações fiáveis para o ambiente virtual relevante. As exclusões de verificação predefinidas e as aplicações fiáveis ajudam-no a configurar rapidamente a aplicação e a evitar problemas de compatibilidade com o ambiente virtual. Também pode configurar exclusões de verificação predefinidas e aplicações fiáveis após a instalação, na política.

Como instalar o Light Agent utilizando o Assistente de Instalação

1. Copie a pasta do kit de distribuição para a máquina virtual.
2. Execute o ficheiro setup_kes.exe.

   O Assistente de configuração é iniciado.

Configuração do Kaspersky Endpoint Security



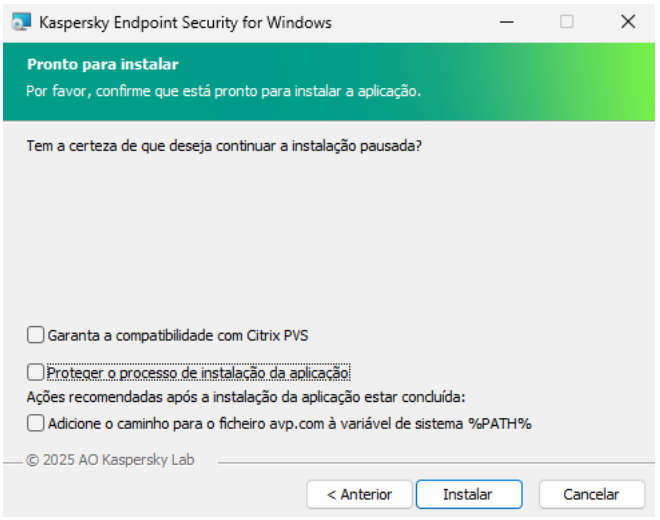
Escolher a configuração da aplicação

Selecione a configuração **Light Agent para proteger ambientes virtuais**. Esta configuração destina-se à aplicação que é usada como parte da solução Kaspersky Security for Virtualization Light Agent. O Light Agent tem de ser instalado em cada máquina virtual que precisa de ser protegida usando a solução. Nesta configuração, não pode utilizar componentes de Encriptação de Dados ou Controlo de Anomalias Adaptativo. Se estiver a instalar o Light Agent num modelo de máquina virtual que será usado para criar *máquinas virtuais não persistentes*, selecione a caixa de verificação **Proteger a 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. Neste modo, o Light Agent recusa atualizações de aplicações que exigem o reinício da máquina virtual. Ao receber atualizações de aplicações que exigem um reinício, o Light Agent gera um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas.

Componentes do Kaspersky Endpoint Security

Selecione os componentes que pretende instalar (veja a figura abaixo). Pode alterar os componentes da aplicação disponíveis após instalar a aplicação. Para o fazer, deve executar o Assistente de Instalação novamente e selecionar a alteração dos componentes disponíveis.

Definições avançadas



Definições avançadas de instalação da aplicação

Proteger o processo de instalação da aplicação. A proteção de instalação inclui a proteção contra a substituição do pacote de distribuição com aplicações maliciosas, bloqueando o acesso à pasta de instalação do Kaspersky Endpoint Security, e bloqueando o acesso à secção do registo do sistema contendo as chaves da aplicação. Contudo, se não for possível instalar a aplicação (por exemplo, ao executar uma instalação remota com a ajuda do Windows Remote Desktop), recomendamos que desative a proteção do processo de instalação.

Garanta a compatibilidade com Citrix PVS. Pode ativar o suporte dos Citrix Provisioning Services para instalar o Kaspersky Endpoint Security numa máquina virtual.

Adicione o caminho para o ficheiro avp.com à variável de sistema %PATH%. Pode adicionar o caminho de instalação à variável %PATH% para utilização conveniente da interface da linha de comando.

Como instalar o Light Agent utilizando a linha de comandos

1. Execute o interpretador de linha de comando (cmd.exe) como administrador.
2. Vá para 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. Neste modo, o Light Agent recusa atualizações de aplicações que exigem o reinício da máquina virtual. Ao receber atualizações de aplicações que exigem um reinício, o Light Agent gera um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas. Por predefinição, o modo de proteção VDI está ativado.

Como resultado, o Light Agent é instalado na máquina virtual com o conjunto padrão de componentes. Pode editar o conjunto de componentes e especificar definições avançadas com o ficheiro setup.ini. Também pode especificar as definições de instalação na linha de comandos.

Como instalar o Light Agent utilizando a Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione a pasta **Remote installation** → **Advanced** → **Installation packages**.

   Isto abre uma lista de pacotes de instalação que foram transferidos para o Kaspersky Security Center.
3. Abra as propriedades do pacote de instalação do Kaspersky Endpoint Security for Windows.

   Se necessário, crie um novo pacote de instalação.
4. Aceda à secção **Settings**.
5. Selecione a configuração **Light Agent para proteger ambientes virtuais**. Esta configuração destina-se à aplicação que é usada como parte da solução Kaspersky Security for Virtualization Light Agent. O Light Agent tem de ser instalado em cada máquina virtual que precisa de ser protegida usando a solução. Nesta configuração, não pode utilizar componentes de Encriptação de Dados ou Controlo de Anomalias Adaptativo. Se estiver a instalar o Light Agent num modelo de máquina virtual que será usado para criar *máquinas virtuais não persistentes*, selecione a caixa de verificação **Proteger a 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. Neste modo, o Light Agent recusa atualizações de aplicações que exigem o reinício da máquina virtual. Ao receber atualizações de aplicações que exigem um reinício, o Light Agent gera um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas.
6. Selecione os componentes que pretende instalar.

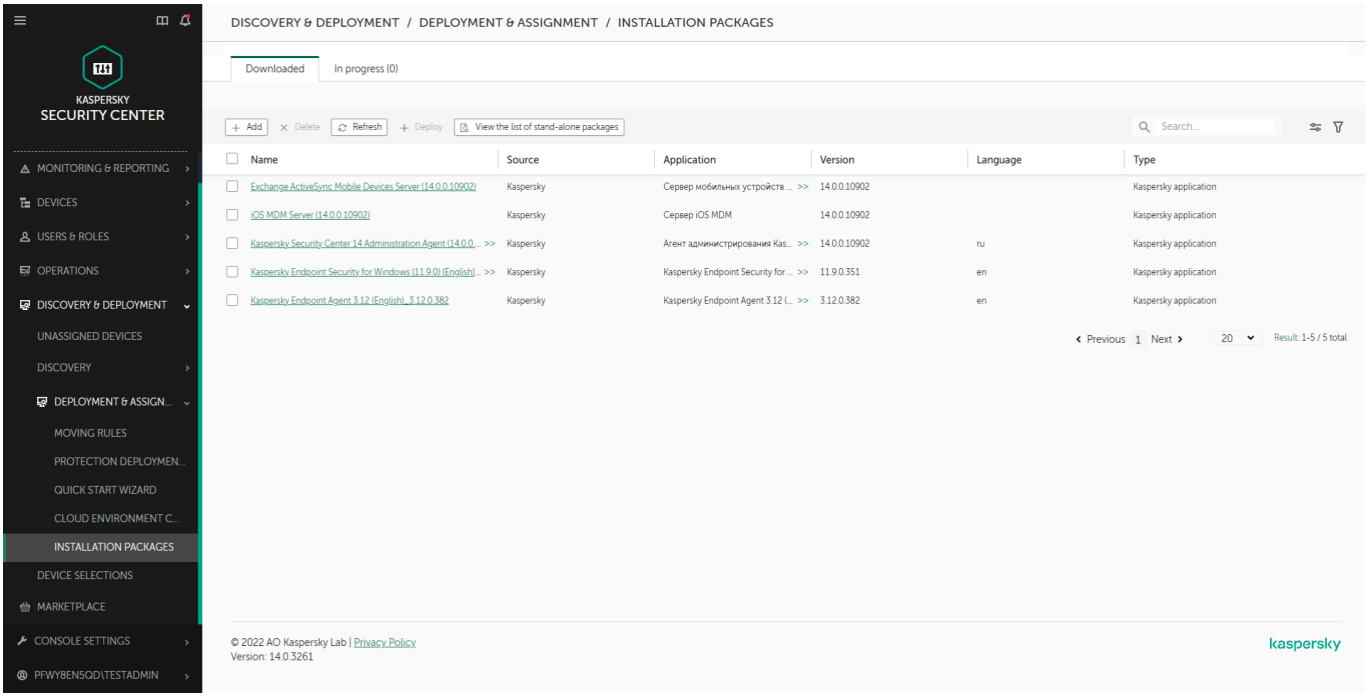
   Pode alterar os componentes da aplicação disponíveis após instalar a aplicação.
7. Configurar a zona fiável. Selecione exclusões de verificação predefinidas e aplicações fiáveis para o ambiente virtual no qual está a instalar a aplicação.

   As exclusões de verificação predefinidas e as aplicações fiáveis ajudam-no a configurar rapidamente a aplicação e a evitar problemas de compatibilidade com o ambiente virtual.
8. Guarde as suas alterações.
9. Criar uma tarefa de instalação remota. Nas propriedades da tarefa, selecione o pacote de instalação que criou.

Como instalar o Light Agent utilizando a Consola Web

1. Na janela principal da Consola Web, selecione **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.

Isto abre uma lista de pacotes de instalação que foram transferidos para o Kaspersky Security Center.



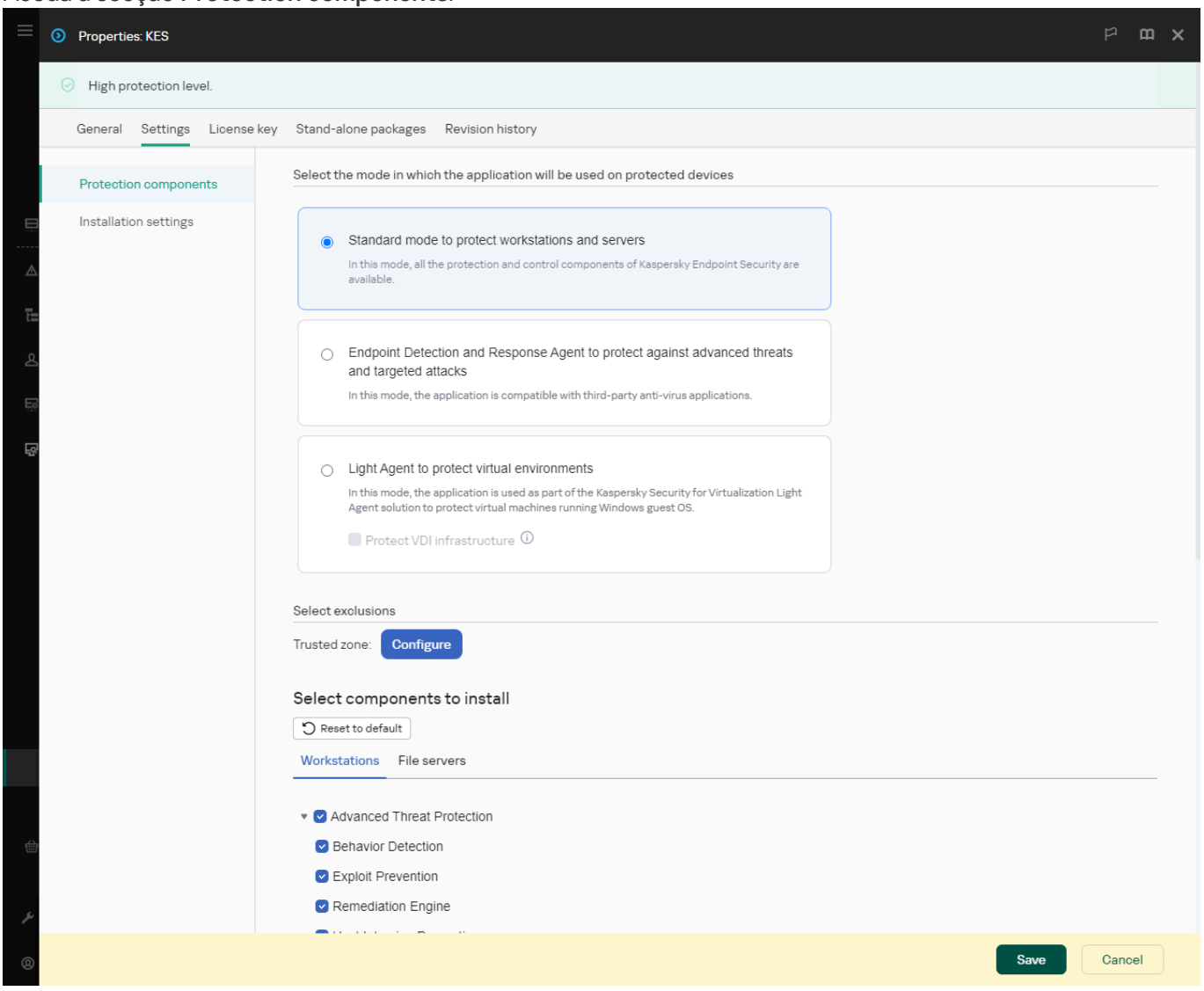
Lista de pacotes de instalação

2. Abra as propriedades do pacote de instalação do Kaspersky Endpoint Security for Windows.

   Se necessário, crie um novo pacote de instalação.

3. Selecione o separador **Settings**.

4. Aceda à secção **Protection components**.



Componentes incluídos no pacote de instalação

5. Selecione a configuração **Light Agent to protect virtual environments**. Esta configuração destina-se à aplicação que é usada como parte da solução Kaspersky Security for Virtualization Light Agent. O Light Agent tem de ser instalado em cada máquina virtual que precisa de ser protegida usando a solução. Nesta configuração, não pode utilizar componentes de Encriptação de Dados ou Controlo de Anomalias Adaptativo. Se estiver a instalar o Light Agent num modelo de máquina virtual que será usado para criar *máquinas virtuais não persistentes*, selecione a caixa de verificação **Protect VDI infrastructure** (VDI significa Virtual Desktop Infrastructure). O modo de proteção VDI ajuda a otimizar o desempenho do Kaspersky Endpoint Security em máquinas virtuais não persistentes. Neste modo, o Light Agent recusa atualizações de aplicações que exigem o reinício da máquina virtual. Ao receber atualizações de aplicações que exigem um reinício, o Light Agent gera um evento sobre a necessidade de atualizar o modelo das máquinas virtuais protegidas.

6. Selecione os componentes que pretende instalar.

   Pode alterar os componentes da aplicação disponíveis após instalar a aplicação.

7. Configurar a zona fiável. Selecione exclusões de verificação predefinidas e aplicações fiáveis para o ambiente virtual no qual está a instalar a aplicação.

   As exclusões de verificação predefinidas e as aplicações fiáveis ajudam-no a configurar rapidamente a aplicação e a evitar problemas de compatibilidade com o ambiente virtual.

8. Guarde as suas alterações.

9. Criar uma tarefa de instalação remota. Nas propriedades da tarefa, selecione o pacote de instalação que criou.

Como resultado, o Light Agent é instalado na máquina virtual. Pode usar a interface da aplicação e será apresentado um ícone da aplicação na área de notificação . Agora precisa de configurar a ligação do Light Agent à SVM.



Janela principal do Light Agent

A ligar o Light Agent à SVM

A solução Kaspersky Security for Virtualization Light Agent requer comunicação contínua do Light Agent e da SVM. Isto é necessário para verificar se contêm vírus e outros softwares maliciosos nos ficheiros enviados pelo Light Agent. Sem uma ligação SVM, o Light Agent não pode enviar ficheiros para verificação. Se a ligação não puder ser estabelecida por mais de cinco minutos, a verificação será concluída com um erro.

A ligação de um Light Agent a uma SVM envolve as seguintes etapas:

1. O Light Agent obtém a lista de SVM disponíveis.
2. O Light Agent determina um Servidor de Proteção (SVM) disponível que seja ideal para a ligação de acordo com o Algoritmo de seleção de SVM.
3. O Light Agent verifica as definições adicionais de ligação de SVM: as etiquetas, o estado de proteção de ligação, a funcionalidade da aplicação abrangida pela licença.
4. Ligar o Light Agent à SVM.

Pode obter informações sobre o estado da ligação do Light Agent à SVM no Kaspersky Endpoint Security ou através do comando da aplicação. A aplicação gera um evento sempre que a ligação da SVM do Light Agent é perdida ou estabelecida e envia estes eventos para o Kaspersky Security Center. Se estiver a utilizar um Servidor de Integração para a descoberta de SVM, poderá obter informações sobre o estado da SVM e o número de Light Agents ligados na Consola do Servidor de Integração. Para obter detalhes sobre a monitorização do estado da SVM, consulte a Ajuda do Kaspersky Security for Virtualization Light Agent.

Descoberta de SVM

Pode selecionar um dos métodos de descoberta de SVM para o Light Agent:

- Usar 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 das SVM disponíveis para ligação. O Light Agent estabelece uma ligação com o Servidor de Integração e obtém a lista de endereços SVM.

  O Servidor de Integração revela-se particularmente útil em grandes infraestruturas virtuais, uma vez que equilibra automaticamente a carga entre os SVM, obtém informações sobre os SVM disponíveis, analisa essas informações e fornece aos Light Agents uma lista dos Servidores de Proteção (SVM) mais adequados para a ligação.

  Para que o Light Agent consiga obter uma lista de SVM, apenas precisa de inserir o endereço do Servidor de Integração.

- Utilizar 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 assegura a proteção ininterrupta do ambiente virtual graças à comutação pós-falha das SVM e dos Light Agents para um Servidor de Integração de reserva sempre que o Servidor de Integração principal falha. Um componente especial do cluster, o *balanceador de carga*, é responsável pela comutação pós-falha 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 SVM, tem de introduzir o endereço do dispositivo no qual o balanceador de carga está instalado.

- Utilizar a lista de endereços SVM.

  Se precisar de especificar SVM individuais às quais deseja que o Light Agent se ligue, pode preparar uma lista manualmente.

  Precisa de listar endereços de SVM disponíveis aos quais o Light Agent se pode ligar.

Como configurar a descoberta de SVM pelo Light Agent na Consola de Administração (MMC)

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione **Policies**.
3. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
4. Na janela de política, selecione **Modo Light Agent** → **Definições de descoberta de SVM**.

5. Selecione um método de descoberta de SVM.

- **Usar servidor de integração**. Introduza as definições de ligação ao Servidor de Integração de acordo com a sua infraestrutura:
  - **Servidor de Integração único**. Introduza as definições de ligação ao Servidor de Integração: o endereço IPv4 ou o nome de domínio completamente qualificado (FQDN) do dispositivo.
  - **Cluster de alta disponibilidade de Servidores de Integração**. Introduza o endereço IP e a porta do balanceador de carga que faz parte do cluster.
- **Usar uma lista personalizada de endereços SVM**. Crie uma lista de SVM às quais o Light Agent se pode ligar. Especifique o endereço IP no formato IPv4 ou o nome de domínio totalmente qualificado (FQDN) da SVM. Cada item da lista deve ser inserido numa nova linha ou separado do item anterior por um ponto e vírgula (`;`).

  Na lista de endereços SVM, especifique apenas nomes de domínio completos (FQDN) que sejam correspondidos por um único endereço IP. Usar um nome de domínio totalmente qualificado que corresponde a vários endereços IP pode gerar erros na solução.

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

Como configurar a descoberta de SVM pelo Light Agent no Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Light Agent Mode** → **SVM discovery settings**.
5. Selecione um método de descoberta de SVM.

- **Use Integration Server**. Introduza as definições de ligação ao Servidor de Integração de acordo com a sua infraestrutura:
  - **Servidor de Integração único**. Introduza as definições de ligação ao Servidor de Integração: o endereço IPv4 ou o nome de domínio completamente qualificado (FQDN) do dispositivo.
  - **Cluster de alta disponibilidade de Servidores de Integração**. Introduza o endereço IP e a porta do balanceador de carga que faz parte do cluster.
- **Use a custom list of SVM addresses**. Crie uma lista de SVM às quais o Light Agent se pode ligar. Especifique o endereço IP no formato IPv4 ou o nome de domínio totalmente qualificado (FQDN) da SVM. Cada item da lista deve ser inserido numa nova linha ou separado do item anterior por um ponto e vírgula (`;`).

  Na lista de endereços SVM, especifique apenas nomes de domínio completos (FQDN) que sejam correspondidos por um único endereço IP. Usar um nome de domínio totalmente qualificado que corresponde a vários endereços IP pode gerar erros na solução.

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

Como configurar a descoberta de SVM pelo Light Agent na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela de definições da aplicação, em **Modo Light Agent** clique no mosaico **Definições da descoberta de SVM**.
3. Selecione um método de descoberta de SVM.
   - **Usar servidor de integração**. Introduza as definições de ligação ao Servidor de Integração de acordo com a sua infraestrutura:
     - **Servidor de Integração único**. Introduza as definições de ligação ao Servidor de Integração: o endereço IPv4 ou o nome de domínio completamente qualificado (FQDN) do dispositivo.
     - **Cluster de alta disponibilidade de Servidores de Integração**. Introduza o endereço IP e a porta do balanceador de carga que faz parte do cluster.
   - **Usar uma lista personalizada de endereços SVM**. Crie uma lista de SVM às quais o Light Agent se pode ligar. Especifique o endereço IP no formato IPv4 ou o nome de domínio totalmente qualificado (FQDN) da SVM. Cada item da lista deve ser inserido numa nova linha ou separado do item anterior por um ponto e vírgula (**;**).

     Na lista de endereços SVM, especifique apenas nomes de domínio completos (FQDN) que sejam correspondidos por um único endereço IP. Usar um nome de domínio totalmente qualificado que corresponde a vários endereços IP pode gerar erros na solução.
4. Guarde as suas alterações.

Configurar o algoritmo de seleção de SVM para Light Agent

A infraestrutura da organização pode ter várias SVM implementadas aos quais os Light Agents se podem ligar. Para equilibrar a carga na rede e os recursos da infraestrutura virtual, tem de distribuir os Light Agents entre as SVM.

Algoritmos de seleção de SVM

Os Light Agents podem utilizar os seguintes algoritmos de seleção de SVM para estabelecer ligação: algoritmo padrão (predefinido) e algoritmo alargado.

<table>
<tr><th>Algoritmo padrão</th><th>Algoritmo alargado</th></tr>
<tr><td>Se este algoritmo for utilizado, após a instalação e o arranque, o Light Agent na máquina virtual opta por se ligar a uma SVM que seja local em relação ao Light Agent.

Se não for encontrada nenhuma SVM local adequada para estabelecer ligação, o Light Agent seleciona a SVM à qual está ligado o menor número de Light Agents, independentemente da posição da SVM na infraestrutura virtual.

A aplicação não determina se a SVM é local em relação ao Light Agent, caso o modo de proteção de infraestrutura de grande escala esteja ativado para o Servidor de Proteção na SVM. Neste caso, recomenda-se utilizar o algoritmo de seleção da SVM alargado e selecionar o Servidor de Integração como método de deteção de SVM.

O facto de uma SVM ser considerada local em relação a um Light Agent depende do tipo de infraestrutura virtual.</td><td>Caso este algoritmo seja aplicado, poderá definir as seguintes opções de seleção de SVM:
• se deve ter em conta ou ignorar a localização da SVM na infraestrutura ao selecionar as SVM para ligação
• se tiver em conta a localização da SVM, o método para determinar a localização da SVM em relação ao Light Agent
Se os Light Agents ignorarem a localização das SVM na infraestrutura, poderão ligar-se a qualquer SVM disponível para ligação.

Caso os Light Agents tenham de ter em conta a localização das SVM na infraestrutura, deverá selecionar o tipo de caminho da SVM que será considerado na determinação da localização da SVM em relação ao Light Agent. O facto de uma SVM ser considerada local em relação ao Light Agent depende do tipo de infraestrutura virtual.

Se os Light Agents tiverem em conta a localização das SVM na infraestrutura ao escolherem a que SVM se devem ligar, só poderão ligar-se a SVM locais.

Por exemplo, se especificar um cluster de hipervisores como tipo de caminho da SVM, todas as SVM implementadas nesse cluster de hipervisores serão consideradas locais em relação ao Light Agent, e o Light Agent só poderá estabelecer ligação com uma dessas SVM. Se não existirem SVM disponíveis para ligação no mesmo cluster em que o Light Agent está a ser executado, o Light Agent não será ligado a uma SVM.

Ao selecionar as SVM, os Light Agents têm igualmente em conta o número de Light Agents ligados, a fim de garantir que estes se encontram distribuídos de forma equilibrada pelas SVM disponíveis para ligação.

Se o Light Agent utilizar o algoritmo de seleção de SVM alargado e o método de deteção de SVM estiver definido como Lista de endereços de SVM, e se o modo de proteção de infraestruturas de grande dimensão estiver ativado na SVM, então a ligação de um Light Agent a esta SVM só será possível se o caminho da SVM for ignorado.</td></tr>
<tr><td colspan="2">Basis Dynamix Enterprise</td></tr>
<tr><td>Numa infraestrutura virtual baseada no Basis Dynamix Enterprise, a SVM considerada local para um Light Agent é aquela que está implementada no mesmo nó que a máquina virtual onde o Light Agent está instalado.</td><td>Numa 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 é implementada no mesmo nó que a máquina virtual onde está instalado o Light Agent.
• Uma SVM é implementada na mesma zona que a máquina virtual na qual está instalado o Light Agent.
• Uma SVM é implementada no mesmo centro de dados que a máquina virtual na qual está instalado o Light Agent.</td></tr>
<tr><td colspan="2">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</td></tr>
</table>

Algoritmo padrão	Algoritmo alargado
Numa infraestrutura virtual baseada no 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 considerada local para um Light Agent é aquela que está implementada no mesmo hipervisor que a máquina virtual na qual o Light Agent está instalado.	Numa infraestrutura virtual baseada no 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, uma SVM pode ser considerada local em relação ao Light Agent em qualquer um dos seguintes casos: • Uma SVM é implementada no mesmo hipervisor que a máquina virtual na qual está instalado o Light Agent. • Uma SVM é implementada no mesmo cluster de hipervisores que a máquina virtual na qual está instalado o Light Agent. • Uma SVM é implementada no mesmo centro de dados que a máquina virtual na qual está instalado o Light Agent.
SVM do OpenStack e do VK Private Cloud	
Numa infraestrutura virtual executada na plataforma OpenStack ou VK Private Cloud, pode especificar como determinar a localização da SVM em relação ao Light Agent utilizando o parâmetro `StandardAlgorithmSvmLocality` na secção `HypervisorSpecificSettings:Openstack` do ficheiro de configuração do Servidor de Integração, appsettings.json. Dependendo da versão do Servidor de Integração, o ficheiro encontra-se num 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 este valor for selecionado, a SVM será considerada local para o Light Agent se estiver localizada no mesmo grupo de servidores que a máquina virtual com o Light Agent instalado. Este valor está ativado por predefinição. • `Project` – se este valor for selecionado, a SVM é considerada local em relação ao Light Agent, caso esteja implementada no mesmo projeto OpenStack que a máquina virtual na qual o Light Agent está instalado. • `AvailabilityZone` – se este valor for selecionado, a SVM será considerada local para o Light Agent se estiver localizada na mesma zona de disponibilidade que a máquina virtual com o Light Agent instalado.	Numa infraestrutura virtual executada na plataforma OpenStack ou 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 na qual o Light Agent está instalado. • Uma SVM é implementada no mesmo projeto OpenStack que a máquina virtual na qual está instalado o Light Agent. • Uma SVM está localizada na mesma zona de disponibilidade que a máquina virtual na qual o Light Agent está instalado.

Além dos algoritmos de ligação SVM, pode regular a ligação dos Light Agents a SVM utilizando etiquetas.

Configurar o algoritmo de seleção de SVM

Como configurar o algoritmo de seleção de SVM para Light Agent na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Modo Light Agent** → **Algoritmo de seleção de SVM**.
4. Selecione o algoritmo:
   - **Usar o algoritmo de seleção SVM padrão**. O Light Agent seleciona SVM, implementadas no mesmo hipervisor.
   - **Usar o algoritmo avançado de seleção SVM**. O Light Agent seleciona SVM implementadas no tipo de caminho da SVM selecionada (por defeito, **Hipervisor**).

5. Se necessário, selecione os caminhos da SVM para o algoritmo de seleção de SVM alargado:

- **Hipervisor**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

  - As SVM são implementadas no mesmo hipervisor que a máquina virtual com o Light Agent instalado (numa infraestrutura virtual no 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 (numa infraestrutura virtual em execução na plataforma OpenStack, na plataforma VK Private Cloud).

  - A SVM está localizada no mesmo nó que a máquina virtual com o Light Agent instalado (numa infraestrutura virtual Basis Dynamix Enterprise).

  Se não houver SVM disponíveis para ligação no mesmo hipervisor ou no mesmo grupo de servidores, onde a máquina virtual com o Light Agent está localizada, o Light Agent não será ligado à SVM.

- **Cluster**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

  - As SVM são implementadas no mesmo cluster de hipervisor que a máquina virtual com o Light Agent instalado (numa infraestrutura virtual no 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 SVM são implementadas no mesmo projeto OpenStack que a máquina virtual na qual está instalado o Light Agent (numa infraestrutura virtual executada na plataforma OpenStack ou VK Private Cloud).

  - A SVM está localizada na mesma zona que a máquina virtual na qual o Light Agent está instalado (numa infraestrutura virtual Basis Dynamix Enterprise).

  Se não houver SVM disponíveis para ligação no mesmo cluster de hipervisores ou no mesmo projeto OpenStack onde se encontra a máquina virtual com o Light Agent, o Light Agent não se liga à SVM.

- **Centro de dados**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

  - As SVM são implementadas no mesmo centro de dados que a máquina virtual com o Light Agent instalado (numa infraestrutura virtual baseada no 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 SVM estão localizadas na mesma Zona de Disponibilidade que a máquina virtual na qual está instalado o Light Agent (numa infraestrutura virtual executada na plataforma OpenStack ou VK Private Cloud).

  - A SVM está localizada no mesmo centro de dados que a máquina virtual na qual o Light Agent está instalado (numa infraestrutura virtual Basis Dynamix Enterprise).

Se não existirem SVM disponíveis para ligação no mesmo centro de dados ou na Zona de Disponibilidade onde a máquina virtual com o Light Agent está localizada, o Light Agent não será ligado à SVM.

- **Ignorar**. O Light Agent ignora a caminho da SVM para se ligar ao Servidor de Proteção. Os Light Agents têm em consideração outros critérios: etiquetas, o número de Light Agents ligados a uma SVM e assim por diante.

6. Guarde as suas alterações.

Como configurar o algoritmo de seleção SVM para Light Agent na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Light Agent Mode** → **SVM selection algorithm**.
5. Selecione o algoritmo:

   - **Use the standard SVM selection algorithm**. O Light Agent seleciona SVM, implementadas no mesmo hipervisor.
   - **Use the extended SVM selection algorithm**. O Light Agent seleciona SVM implementadas no tipo de caminho da SVM selecionada (por defeito, **Hypervisor**).
6. Se necessário, selecione os caminhos da SVM para o algoritmo de seleção de SVM alargado:

   - **Hypervisor**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

     - As SVM são implementadas no mesmo hipervisor que a máquina virtual com o Light Agent instalado (numa infraestrutura virtual no 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 (numa infraestrutura virtual em execução na plataforma OpenStack, na plataforma VK Private Cloud).
     - A SVM está localizada no mesmo nó que a máquina virtual com o Light Agent instalado (numa infraestrutura virtual Basis Dynamix Enterprise).

     Se não houver SVM disponíveis para ligação no mesmo hipervisor ou no mesmo grupo de servidores, onde a máquina virtual com o Light Agent está localizada, o Light Agent não será ligado à SVM.

- **Cluster**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

  - As SVM são implementadas no mesmo cluster de hipervisor que a máquina virtual com o Light Agent instalado (numa infraestrutura virtual no 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 SVM são implementadas no mesmo projeto OpenStack que a máquina virtual na qual está instalado o Light Agent (numa infraestrutura virtual executada na plataforma OpenStack ou VK Private Cloud).

  - A SVM está localizada na mesma zona que a máquina virtual na qual o Light Agent está instalado (numa infraestrutura virtual Basis Dynamix Enterprise).

  Se não houver SVM disponíveis para ligação no mesmo cluster de hipervisores ou no mesmo projeto OpenStack onde se encontra a máquina virtual com o Light Agent, o Light Agent não se liga à SVM.

- **Data center**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

  - As SVM são implementadas no mesmo centro de dados que a máquina virtual com o Light Agent instalado (numa infraestrutura virtual baseada no 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 SVM estão localizadas na mesma Zona de Disponibilidade que a máquina virtual na qual está instalado o Light Agent (numa infraestrutura virtual executada na plataforma OpenStack ou VK Private Cloud).

  - A SVM está localizada no mesmo centro de dados que a máquina virtual na qual o Light Agent está instalado (numa infraestrutura virtual Basis Dynamix Enterprise).

  Se não existirem SVM disponíveis para ligação no mesmo centro de dados ou na Zona de Disponibilidade onde a máquina virtual com o Light Agent está localizada, o Light Agent não será ligado à SVM.

- **Ignore**. O Light Agent ignora a caminho da SVM para se ligar ao Servidor de Proteção. Os Light Agents têm em consideração outros critérios: etiquetas, o número de Light Agents ligados a uma SVM e assim por diante.

7. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como configurar o algoritmo de seleção de SVM para Light Agent na interface da aplicação

1. Na janela principal da aplicação, clique no botão .

2. Na janela de definições da aplicação, em **Modo Light Agent** clique no mosaico **Definições da descoberta de SVM**.

3. Selecione o algoritmo:

   - **Usar o algoritmo de seleção SVM padrão**. O Light Agent seleciona SVM, implementadas no mesmo hipervisor.

   - **Usar o algoritmo avançado de seleção SVM**. O Light Agent seleciona SVM implementadas no tipo de caminho da SVM selecionada (por defeito, **Hipervisor**).

4. Se necessário, selecione os caminhos da SVM para o algoritmo de seleção de SVM alargado:

- **Hipervisor**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

  - As SVM são implementadas no mesmo hipervisor que a máquina virtual com o Light Agent instalado (numa infraestrutura virtual no 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 (numa infraestrutura virtual em execução na plataforma OpenStack, na plataforma VK Private Cloud).

  - A SVM está localizada no mesmo nó que a máquina virtual com o Light Agent instalado (numa infraestrutura virtual Basis Dynamix Enterprise).

  Se não houver SVM disponíveis para ligação no mesmo hipervisor ou no mesmo grupo de servidores, onde a máquina virtual com o Light Agent está localizada, o Light Agent não será ligado à SVM.

- **Cluster**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

  - As SVM são implementadas no mesmo cluster de hipervisor que a máquina virtual com o Light Agent instalado (numa infraestrutura virtual no 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 SVM são implementadas no mesmo projeto OpenStack que a máquina virtual na qual está instalado o Light Agent (numa infraestrutura virtual executada na plataforma OpenStack ou VK Private Cloud).

  - A SVM está localizada na mesma zona que a máquina virtual na qual o Light Agent está instalado (numa infraestrutura virtual Basis Dynamix Enterprise).

  Se não houver SVM disponíveis para ligação no mesmo cluster de hipervisores ou no mesmo projeto OpenStack onde se encontra a máquina virtual com o Light Agent, o Light Agent não se liga à SVM.

- **Centro de dados**. O Light Agent seleciona uma SVM para se conectar que atenda aos critérios (dependendo do tipo de infraestrutura virtual):

  - As SVM são implementadas no mesmo centro de dados que a máquina virtual com o Light Agent instalado (numa infraestrutura virtual baseada no 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 SVM estão localizadas na mesma Zona de Disponibilidade que a máquina virtual na qual está instalado o Light Agent (numa infraestrutura virtual executada na plataforma OpenStack ou VK Private Cloud).

  - A SVM está localizada no mesmo centro de dados que a máquina virtual na qual o Light Agent está instalado (numa infraestrutura virtual Basis Dynamix Enterprise).

Se não existirem SVM disponíveis para ligação no mesmo centro de dados ou na Zona de Disponibilidade onde a máquina virtual com o Light Agent está localizada, o Light Agent não será ligado à SVM.

- **Ignorar**. O Light Agent ignora a caminho da SVM para se ligar ao Servidor de Proteção. Os Light Agents têm em consideração outros critérios: etiquetas, o número de Light Agents ligados a uma SVM e assim por diante.

5. Guarde as suas alterações.

Distribuir as ligações de Light Agents para SVM (etiquetas)

Vários Light Agents podem ligar-se a uma SVM. Para equilibrar as ligações do Light Agent, pode especificar uma lista separada de SVM. Se estiver a usar um Servidor de Integração para descoberta de SVM, pode usar *etiquetas* para balancear as ligações do Light Agent com as SVM. Ou seja, para um Light Agent, pode atribuir uma lista de SVM para ligação com uma etiqueta. Para o fazer, tem de atribuir uma etiqueta ao Light Agent e especificar essa etiqueta nas definições da SVM. Para obter detalhes sobre como especificar etiquetas nas definições da SVM, consulte Ajuda do Kaspersky Security for Virtualization Light Agent.

Exemplo: a solução Kaspersky Endpoint Detection and Response Optimum é implementada na sua infraestrutura para anfitriões de máquinas virtuais designados. Neste caso, pode atribuir a etiqueta `[EDROptimum]` ao Light Agent para que ele se ligue às SVM que possuem a chave de licença EDR Optimum (Suplemento do EDR Optimum) adicionada. Como resultado, pode usar a funcionalidade EDR Optimum na máquina virtual com o Light Agent. Ao ligar o Light Agent a uma SVM sem uma chave de licença EDR Optimum, a funcionalidade Kaspersky Endpoint Detection and Response Optimum não fica disponível.

Como atribuir uma etiqueta de ligação SVM a um Light Agent na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Modo Light Agent** → **Etiqueta de ligação ao SVM**.
4. Selecione a caixa de verificação **Utilizar etiqueta de ligação** e insira uma etiqueta de ligação da SVM.

   Para uma etiqueta, pode inserir uma sequência de texto de até 255 caracteres. Pode usar qualquer carácter, exceto o carácter `;`.
5. Guarde as suas alterações.

Como atribuir uma etiqueta de ligação SVM a um Light Agent na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Light Agent Mode** → **SVM connection tag**.

5. Selecione a caixa de verificação **Use connection tag** e insira uma etiqueta de ligação da SVM.

   Para uma etiqueta, pode inserir uma sequência de texto de até 255 caracteres. Pode usar qualquer carácter, exceto o carácter `;`.

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

Como atribuir uma etiqueta de ligação SVM a um Light Agent na interface da aplicação

1. Na janela principal da aplicação, clique no botão .

2. Na janela de definições da aplicação, em **Modo Light Agent** clique no mosaico **Etiqueta de ligação ao SVM**.

3. Selecione a caixa de verificação **Utilizar etiqueta de ligação** e insira uma etiqueta de ligação da SVM.

   Para uma etiqueta, pode inserir uma sequência de texto de até 255 caracteres. Pode usar qualquer carácter, exceto o carácter `;`.

4. Guarde as suas alterações.

Proteger a ligação entre um Light Agent e a SVM

Pode configurar a encriptação de ligação entre os Light Agents e o Servidor de Proteção. Para o fazer, tem de ativar a encriptação do canal de dados entre o Light Agent e o Servidor de Proteção nas definições do Servidor de Proteção na SVM e nas definições do Light Agent.

Um Light Agent para o qual a proteção de ligação está ativada apenas se pode ligar a SVM para as quais a encriptação do canal de dados entre o Light Agent e o Servidor de Proteção está ativado. Um Light Agent para o qual a proteção de ligação está desativada apenas se pode ligar a SVM para as quais a encriptação de canal está desativada ou uma ligação insegura entre o Servidor de Proteção e o Light Agent é permitida.

Para obter detalhes sobre como configurar a proteção de ligação no Servidor de Proteção, consulte a Ajuda do Kaspersky Security for Virtualization Light Agent.

Proteger a ligação usando encriptação pode reduzir o desempenho do Kaspersky Security for Virtualization Light Agent.

Como configurar a proteção de ligação num Light Agent na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Modo Light Agent → Proteção de ligação**.

4. Selecione a caixa de verificação **Encriptar canal de dados entre o Light Agent e o Servidor de Proteção**.

5. Guarde as suas alterações.

Como configurar a proteção de ligação num Light Agent na Consola Web

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.
   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **Light Agent Mode** → **Connection protection**.
5. Selecione a caixa de verificação **Encrypt data channel between Light Agent and the Protection Server**.
6. Para aplicar a política aos computadores, feche os ícones de cadeado e guarde as suas alterações.

Como configurar a proteção de ligação num Light Agent na interface da aplicação

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, em **Modo Light Agent** clique no mosaico **Proteção de ligação**.
3. Selecione a caixa de verificação **Encriptar canal de dados entre o Light Agent e o Servidor de Proteção**.
4. Guarde as suas alterações.

A ativar o Light Agent

Se o Kaspersky Endpoint Security estiver a ser usado no modo Light Agent para proteger ambientes virtuais, não será necessário ativar a aplicação separadamente. Para ativar a aplicação, tem de adicionar uma chave da licença à SVM. Pode adicionar uma chave de licença a uma SVM usando a tarefa especial na consola do Kaspersky Security Center. Não pode gerir chaves de licença na interface do Light Agent, mas pode visualizar informações de licença (veja a figura abaixo). Também pode visualizar as informações de licenciamento do Light Agent na linha de comandos (veja as instruções abaixo). O Light Agent obtém estas informações da SVM. Para obter detalhes sobre como ativar a solução e gerir chaves de licença, consulte a Ajuda do Kaspersky Security for Virtualization Light Agent.

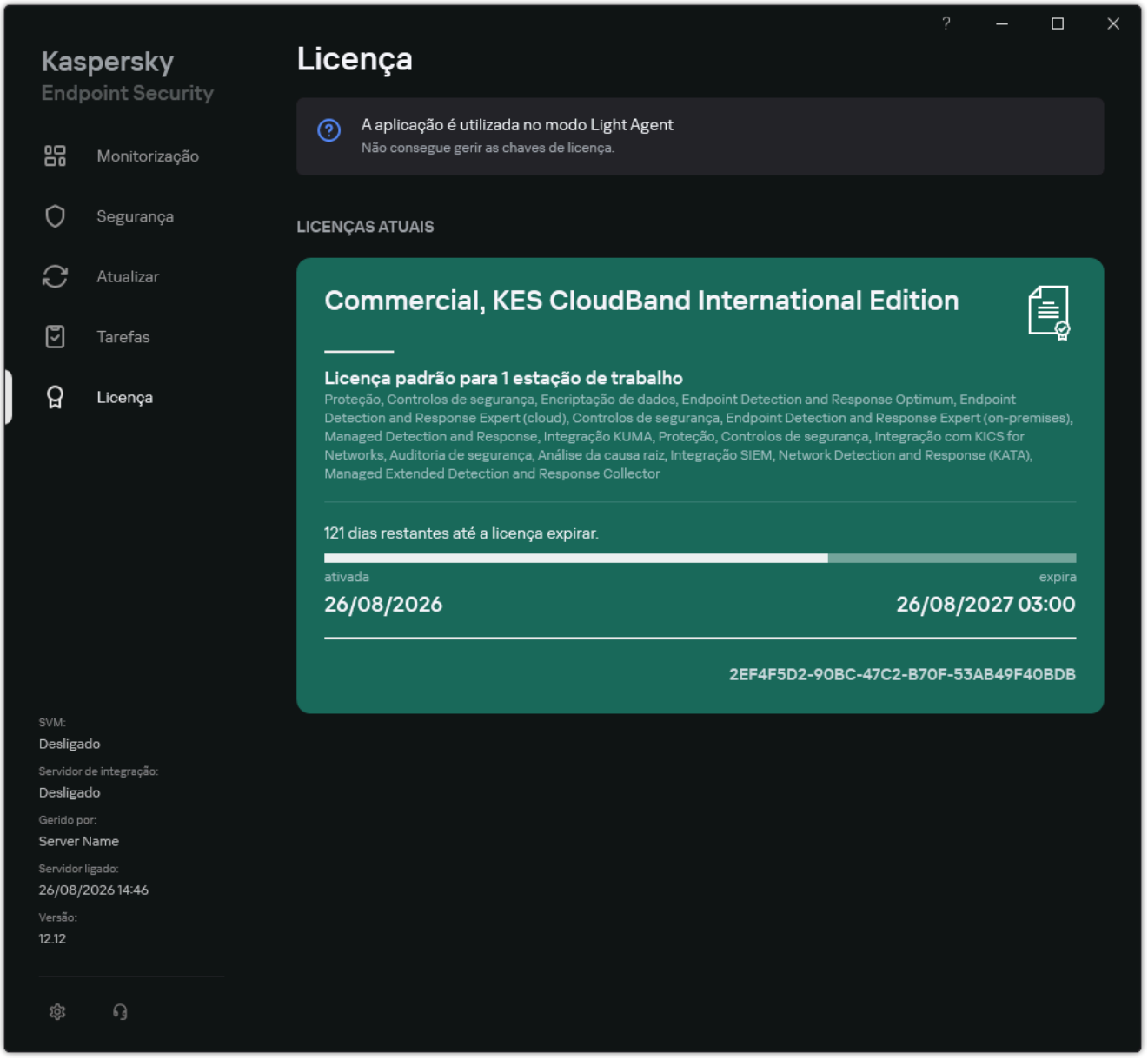
Para visualizar informações de licenciamento do Light Agent:

1. Execute o interpretador de linha de comandos (cmd) como administrador.
2. Vá para a pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.

3. Execute o seguinte comando:

```
avp.com LICENSE /CHECK
```

Como resultado, o Kaspersky Endpoint Security exibe informações sobre a licença: endereço da SVM ao qual o Light Agent está ligado, o número de dias até a licença expirar e outras informações. Se encontrar algum problema ao ativar o Light Agent, consulte a Base de conhecimento de Suporte Técnico.



Janela Licenciamento

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 para Windows 5.2 (doravante também denominado "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, tem de migrar do KSVLA Light Agent 5.2 para o Kaspersky Endpoint Security no modo Light Agent (doravante também chamado de "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 do software

Antes de iniciar a migração do KSVLA Light Agent para o KES Light Agent, certifique-se de que a sua máquina virtual cumpre os requisitos de hardware e software do Kaspersky Endpoint Security for Windows. As listas das versões do sistema operativo suportadas são diferentes para o KES e o KSWS. Por exemplo, o KES não suporta 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 for 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

  Se tiver uma versão anterior do Kaspersky Security Center instalada, atualize-a para a versão 14.2 ou uma mais recente. Nesta versão do Kaspersky Security Center, o Assistente de conversão de políticas e tarefas em lote permite migrar políticas para um perfil em vez de uma política. Nesta versão do Kaspersky Security Center, o Assistente de conversão de políticas e tarefas em lote também permite que migre uma gama mais ampla de definições de política.

Passos da migração

A migração do KSVLA Light Agent para o KES Light Agent é realizada de forma semiautomática. Isto é necessário devido às diferentes arquiteturas das aplicações.

Migre do KSVLA Light Agent para o KES Light Agent na seguinte ordem:

1. **Migrar tarefas e políticas do KSVLA Light Agent**

   Para migrar definições de política, tem de executar o Assistente de conversão de políticas e tarefas em lote (o assistente de migração). Depois de migrar as definições de política, tem de configurar manualmente as definições que o assistente de migração não pode migrar automaticamente (por exemplo, as definições de atualização da base de dados). Após a migração, também é recomendável verificar se o assistente de migração migrou corretamente todas as definições.

   > Se a Proteção por password estiver ativada para restringir o acesso ao KSVLA Light Agent, antes de instalar o KES Light Agent, tem de desativar a Proteção por password na política do KSVLA Light Agent. Não é possível inserir a password de desinstalação nas definições do pacote de instalação do KES Light Agent. Após concluir a instalação do KES Light Agent sobre o KSVLA Light Agent, tem de ativar a Proteção por password na política do KES.

2. **Instalar o Kaspersky Endpoint Security no modo Light Agent**

   Pode instalar o Kaspersky Endpoint Security das seguintes formas:

   - Instalar o KES Light Agent após remover o KSVLA Light Agent (recomendado)
   - Instalar o KES Light Agent sobre o KSVLA Light Agent

3. **Confirme se a aplicação está a funcionar corretamente após a migração**

   Depois de migrar do KSVLA Light Agent para o KES Light Agent, certifique-se de que a aplicação está a funcionar corretamente. Ative a política convertida. Verifique o estado da máquina virtual na consola do Kaspersky Security Center (deve ser *OK*). Certifique-se de que não são comunicados erros para a aplicação e verifique também a hora da última ligação à SVM e o estado de proteção da máquina virtual. Não precisa de ativar o Light Agent, porque a chave de licença é adicionada à SVM.

Instalar o KES Light Agent, em vez do KSVLA Light Agent

Pode instalar o KES Light Agent das seguintes formas:

- Instalar o KES Light Agent após remover o KSVLA Light Agent (recomendado)
- Instalar o KES Light Agent sobre o KSVLA Light Agent

Remover o KSVLA Light Agent

Pode remover a aplicação remotamente utilizando a tarefa *Install application remotely*, localmente na máquina virtual, ou no modelo da máquina virtual. Após remover o KSVLA Light Agent, talvez seja necessário reiniciar a máquina virtual.

Após remover o KSVLA Light Agent, instale o KES Light Agent utilizando um método adequado.

A instalar o Kaspersky Endpoint Security

Se a Proteção por password estiver ativada para restringir o acesso ao KSVLA Light Agent, antes de instalar o KES Light Agent, tem de desativar a Proteção por password na política do KSVLA Light Agent. Não é possível inserir a password de desinstalação nas definições do pacote de instalação do KES Light Agent. Após concluir a instalação do KES Light Agent sobre o KSVLA Light Agent, tem de ativar a Proteção por password na política do KES.

Ao instalar o Kaspersky Endpoint Security, tem de selecionar o modo **Light Agent para proteger ambientes virtuais**. Antes de instalar o KES Light Agent numa máquina virtual, o instalador deteta o KSVLA Light Agent como um software incompatível e remove-o. A migração da configuração do KSVLA Light Agent não é suportada. Ou seja, quando instala o KES Light Agent, o conjunto de componentes a ser instalado é determinado pela seleção feita nas propriedades do pacote de instalação ou no assistente de instalação. Após remover o KSVLA Light Agent, tem de reiniciar a máquina virtual.

As definições e tarefas do KSVLA Light Agent não são migradas ao instalar o KES Light Agent. Para migrar as definições e tarefas, execute o Assistente de conversão de políticas e tarefas em lote.

Pode verificar a lista de componentes instalados na secção **Segurança** da interface da aplicação, utilizando o comando `status` ou na consola do Kaspersky Security Center nas propriedades do computador. Pode alterar o conjunto de componentes após a instalação ao utilizar o *Alterar componentes da aplicação*.

Correspondência dos 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 definições do que o KSVLA Light Agent. Após a migração, as novas definições terão valores predefinidos.

Correspondência dos componentes do KSVLA Light Agent e do KES Light Agent

Light Agent 5.2	KES Light Agent
Scan kernel	Kernel do programa
File Anti-Virus	Proteção contra ameaças de ficheiros
Mail Anti-Virus	Proteção contra ameaças de correio
Web Anti-Virus	Proteção contra ameaças da web
Firewall	Firewall
Network Attack Blocker	Proteção contra ameaças de rede
Application Privilege Control	Prevenção contra invasões
Applications Launch Control	Controlo das Aplicações
Web Control	Controlo de Internet
Device Control	Controlo de Dispositivos
System Watcher	No Kaspersky Endpoint Security, este componente é dividido nos seguintes componentes: • Prevenção de explorações • Deteção de comportamento • Motor de remediação
System Integrity Monitoring	Monitorização da integridade do sistema

Light Agent 5.2	KES Light Agent
Integration with Kaspersky Endpoint Agent	*(não suportado)* A partir do Kaspersky Endpoint Security for Windows 11.9.0, o pacote de distribuição do Kaspersky Endpoint Agent já não faz parte do kit de distribuição.
AMSI Protection	Proteção AMSI

Migrar tarefas e políticas do KSVLA Light Agent

Pode migrar as definições das políticas e tarefas do KSVLA Light Agent através do Assistente de Conversão de Políticas e Tarefas em Lote (doravante também chamado de "Assistente de Migração").

O Assistente de Migração do KSVLA Light Agent está disponível apenas na Consola de Administração (MMC). As definições de políticas e tarefas não podem ser migradas na Consola Web e na Cloud Console.

As seguintes considerações especiais estão envolvidas na migração de políticas e tarefas:

- Uma nova política tem o nome *<Policy> (convertido)*.
- A nova política tem o estado *Inactive policy*.
- A proibição de modificar definições (o "cadeado") não é migrada. O Assistente de Migração define valores padrão.
- Os perfis de políticas não são migrados. Tem de adicionar manualmente os perfis de políticas.
- Gestão melhorada da zona fiável. No KSVLA Light Agent, pode adicionar exclusões predefinidas apenas ao criar uma política. Posteriormente, nas propriedades da política, pode configurar exclusões predefinidas adicionadas anteriormente ou adicionar exclusões manualmente. Não pode adicionar exclusões predefinidas nas propriedades da política. No KES Light Agent, as exclusões predefinidas estão disponíveis durante a criação da política e nas propriedades da política criada. Também pode selecionar exclusões predefinidas no pacote de instalação.
- A configuração do interface de utilizador da aplicação no Kaspersky Endpoint Security foi movida do instalador para a política. Se for necessário, por exemplo, ocultar a interface do utilizador da aplicação, faça a gestão das definições de políticas.
- Os conjuntos de funcionalidades para configurar o controlo de acesso baseado em direitos (RBAC) são diferentes no Kaspersky Endpoint Security e no KSVLA Light Agent. Tem de configurar os direitos de acesso dos utilizadores às áreas funcionais a partir do zero.

Como utilizar o Assistente de Conversão de Políticas e Tarefas em Lote para migrar as definições de políticas do KSVLA Light Agent

1. Na Consola de administração, selecione o Servidor de Administração e clique com o botão direito do rato para abrir o menu de contexto.
2. Selecione **All tasks** → **Policies and tasks batch conversion wizard**.

O Assistente de Conversão de Políticas e Tarefas em Lote vai iniciar. Siga as instruções do Assistente.

Passo 1. Selecionar a aplicação para o qual necessita de converter políticas e tarefas

Neste passo, tem de selecionar o Kaspersky Endpoint Security for Windows. Avance para o passo seguinte.

Passo 2. Conversão de políticas

Selecione a política do Kaspersky Security for Virtualization 5.2 Light Agent para Windows que deseja converter. Avance para o passo seguinte.

O Assistente de Migração irá começar a converter as políticas. Durante a conversão, o Assistente de Migração solicita que aceite as condições da Declaração da KSN. Uma nova política tem o nome *<Policy> (convertido)*.

Passo 3. 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 KSVLA Light Agent que pretende criar para o Kaspersky Endpoint Security. As novas tarefas serão nomeadas *<Nome da tarefa> (convertida)*. Avance para o passo seguinte.

Passo 4. Conclusão do assistente

Conclua o assistente.

Depois de migrar uma política, tem de abrir as propriedades da política, verificar as respetivas definições e guardar a política. Se estas etapas não forem concluídas, o KES Light Agent poderá ignorar a política convertida.

Preste atenção especial à migração de definições de ligação de SVM do Light Agent, listas de exclusão, aplicações fiáveis, endereços da Internet fiáveis, regras de Controlo das Aplicações.

Migrar a configuração [KSVLA Light Agent+KEA] para a configuração [KES Light Agent+agente incorporado]

Para suportar a utilização do Kaspersky Endpoint Security for Windows como parte do EDR (KATA), EDR Optimum, Kaspersky Sandbox foi adicionado um agente integrado à aplicação. Já não precisa de uma aplicação Kaspersky Endpoint Agent em separado para trabalhar com estas soluções.

Ao migrar do KSVLA Light Agent para o KES Light Agent, as soluções EDR (KATA), EDR Optimum, Kaspersky Sandbox continuam a funcionar com 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, tem de 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 [KESLight Agent+agente incorporado] envolve os passos seguintes:

1. **Migração da política e das tarefas**

   A migração das políticas e tarefas [KSVLA Light Agent+KEA] para [KES Light Agent+agente incorporado] envolve os passos seguintes:

   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 na Consola de Administração (MMC)).

      Como resultado, uma nova política é criada com o nome *<Política> (convertido)*. Também são criadas novas tarefas KES com os nomes *<Nome da tarefa> (convertido)*.

   2. Migração de políticas e tarefas de KEA para KES usando o assistente para migração do Kaspersky Endpoint Agent (disponível apenas na Consola Web e na Cloud Console).

      Como resultado, é criada uma nova política com o nome *<Nome da política do Kaspersky Endpoint Security> e <Nome da política do Kaspersky Endpoint Agent>*. Também são criadas novas tarefas e tarefas KES.

2. **Migrar 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.

   Os administradores geralmente ativam a proteção por password para restringir o acesso ao KSVLA Light Agent e ao KEA. Apenas pode introduzir a password de desinstalação do KEA nas propriedades da tarefa *Install application remotely*. Para a migração, tem de desativar a Proteção por password para o KSVLA Light Agent.

   Para realizar a migração, tem de selecionar os componentes necessários para suportar as soluções Detection and Response como parte do Kaspersky Endpoint Security. Depois de instalar a aplicação, o Kaspersky Endpoint Security troca para a utilização do agente incorporado e remove o Kaspersky Endpoint Agent.

3. **Funcionalidade do licenciamento**

   Se a aplicação estiver a ser usada no modo Light Agent, não será necessário ativar a aplicação. Para ativar a aplicação, tem de adicionar uma chave da licença à SVM. Também tem de adicionar a chave de licença para ativar a funcionalidade adicional (por exemplo, EDR Optimum) à SVM. Ou seja, como parte da migração, o licenciamento da funcionalidade acontece automaticamente.

4. **Verificação do estado de funcionamento do Kaspersky Endpoint Detection and Response Optimum e do Kaspersky Sandbox**

Se, após a atualização, o computador tiver o estado *Critical* na consola do Kaspersky Security Center:

- Certifique-se de que o computador tem o Agente de Rede versão 13.2 ou superior instalado.
- Verifique o estado de funcionamento do agente integrado ao consultar o *Report on status of application components*. Se um componente tiver o estado *Not installed*, instale o componente com a tarefa *Change application components*.
- Certifique-se de que aceita a Declaração da Kaspersky Security Network na nova política do Kaspersky Endpoint Security for Windows.
- Certifique-se de que a funcionalidade EDR Optimum é ativada usando o *Report on status of application components*. Se um componente tiver o estado *Não abrangido pela licença*, certifique-se de que a funcionalidade de distribuição automática da chave de licença do EDR Optimum está ativada.
- Verifique o estado da ligação da máquina virtual à SVM. Pode obter informações sobre o estado da ligação do Light Agent à SVM no Kaspersky Endpoint Security ou através do comando da aplicação.

Gerir a aplicação a partir da command line

Pode gerir o Kaspersky Endpoint Security através da command line. Pode ver a lista de comandos para gerir a aplicação, executando o comando `avp.com HELP`. Para ler sobre a sintaxe de um comando específico, digite `avp.com HELP <command>`.

Os carateres especiais no comando devem ser de escape. Para o escape dos caracteres `&`, `|`, `(`, `)`, `<`, `>`, `^`, utilize o caractere `^` (por exemplo, para utilizar o caractere `&`, introduza `^&`). Para usar o caráter `%`, introduza `%%`.

As alternativas ao valor `1` são os valores `yes`, `on`, `enable`, `enabled` e `true`. As alternativas ao valor `0` são os valores `no`, `off`, `disable`, `disabled` e `false`.

Setup. Instalar a aplicação

A instalação da aplicação a partir da linha de comandos envolve os seguintes passos:

1. **Escolher um pacote de distribuição**

   A Kaspersky fornece pacotes de distribuição para diferentes versões localizadas, compatíveis com diferentes arquiteturas de CPU e que incluem vários módulos de encriptação.

   O kit de distribuição inclui os seguintes pacotes de distribuição:

   - **AES256**

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

   - **AES56**

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

   - **Arm64**

     Este pacote de distribuição destina-se à instalação em computadores baseados em Arm. Este pacote de distribuição não se destina à instalação em servidores.

2. **Transferir o pacote de distribuição da aplicação para o armazenamento do computador**

   O pacote de distribuição é um arquivo auto-extraível em formato EXE. Para visualizar o conteúdo do pacote de distribuição, tem de extrair o arquivo para uma pasta separada. Para instalar a aplicação, necessita de todos os ficheiros do pacote de distribuição, incluindo o ficheiro bases.cab.

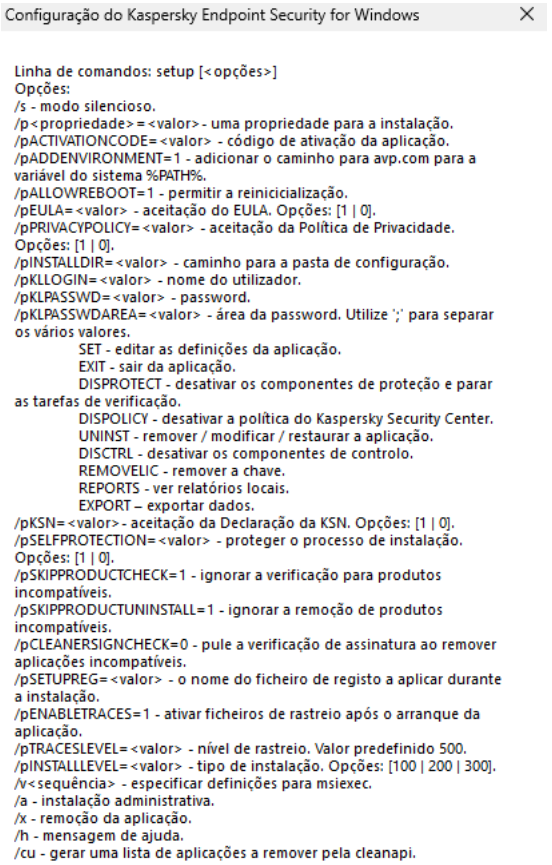
3. **Executar o comando de instalação**

O Kaspersky Endpoint Security pode ser instalado a partir da command line num dos seguintes modos:

- Em modo interativo, através da utilização do Assistente de Instalação da Aplicação.
- Em modo não assistido. Depois de a instalação ser iniciada no modo não assistido, o seu envolvimento no processo de instalação deixa de ser necessário (instalação silenciosa). Para instalar a aplicação no modo não assistido, use as teclas `/s` e `/qn`.

> Antes de instalar a aplicação no modo não assistido, abra e leia o Contrato de Licença do Utilizador Final e o texto da Política de Privacidade. O Contrato de Licença do Utilizador Final e o texto da Política de Privacidade estão incluídos no kit de distribuição do Kaspersky Endpoint Security. Pode instalar a aplicação apenas se tiver lido, compreendido e aceitado na totalidade as disposições e os termos do Contrato de Licença do Utilizador Final, se entender e concordar que os seus dados serão processados e transmitidos (inclusive para países terceiros) em conformidade com a Política de Privacidade e leu e entendeu na totalidade a Política de Privacidade. Não instale ou use o Kaspersky Endpoint Security se não aceitar as disposições e os termos do Contrato de Licença do Utilizador Final e da Política de Privacidade.

Pode ver a lista de comandos para instalar a aplicação, executando o comando `/h`. Para receber ajuda sobre a sintaxe de comando de instalação, escreva `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 a aplicação ou atualizar uma versão anterior da aplicação:

1. Execute o interpretador de linha de comando (cmd.exe) como administrador.
2. Vá para 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]
```

Como resultado, a aplicação será instalada no computador. Pode confirmar que a aplicação está instalada e verificar as definições da aplicação ao emitir o comando `status`.

Definições de instalação das aplicações

`EULA=1`	Aceitação dos termos do Contrato de Licença do Utilizador Final. O texto do Contrato de Licença está incluído no kit de distribuição do Kaspersky Endpoint Security. É necessário aceitar os termos do Contrato de Licença do Utilizador Final para instalar a aplicação ou para atualizar a versão da aplicação.
`PRIVACYPOLICY=1`	Aceitação da Política de Privacidade. O texto da Privacy Policy encontra-se incluído no kit de distribuição do Kaspersky Endpoint Security. Para instalar a aplicação ou atualizar a versão da aplicação, tem de aceitar a Privacy Policy.
`KSN`	Aceitar ou recusar participar na 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 na KSN, quando o Kaspersky Endpoint Security for iniciado pela primeira vez. Valores disponíveis: • `1` - acordo para participar na KSN. • `0` – recusar participar na KSN (valor predefinido). O pacote de distribuição do Kaspersky Endpoint Security está otimizado para utilização com a Kaspersky Security Network. Se optou por não participar na Kaspersky Security Network, deve atualizar o Kaspersky Endpoint Security imediatamente após concluir a instalação.
`CONFIGPATH=<path to the configuration file>`	Instalar a aplicação com configurações predefinidas. Para o fazer, tem de carregar um ficheiro que define as definições do Kaspersky Endpoint Security. Pode criar um ficheiro de configuração na interface local da aplicação.
`ALLOWREBOOT=1`	Reinício automático do computador, se necessário após a instalação ou atualização da aplicação. Se nenhum valor for definido para este parâmetro, a reinicialização automática do computador será bloqueada. Reinicio não é necessário ao instalar o Kaspersky Endpoint Security. O reinicio é necessário apenas se precisar de remover aplicações incompatíveis antes da instalação. Reinício pode também ser necessário ao atualizar a versão da aplicação.
`SKIPPRODUCTCHECK=1`	Desative a verificação de software instalado. A lista de softwares que podem causar problemas de compatibilidade está disponível no ficheiro incompatible.txt que está incluído no kit de distribuição. Se nenhum valor for definido para este parâmetro e for detetado software da lista, a instalação do Kaspersky Endpoint Security será cancelada.
`SKIPPRODUCTUNINSTALL=1`	Desative a remoção automática de software detetado 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 utilizando o instalador msiexec. Para remover automaticamente o software que pode causar problemas de compatibilidade, use o ficheiro setup_kes.exe.

`CLEANERSIGNCHECK=0|1`	Verificação das assinaturas digitais dos ficheiros de software detetados a partir da lista incompatible.txt. Para remover o software, o Kaspersky Endpoint Security executa o ficheiro do instalador do software. Se o ficheiro de instalação não tiver uma assinatura digital, o Kaspersky Endpoint Security considera o ficheiro não fiável e interrompe a remoção de software para evitar a execução de código potencialmente malicioso. Se a aplicação não puder verificar a assinatura digital do ficheiro de software detetado, a instalação do Kaspersky Endpoint Security é interrompida com um erro. O valor predefinido é diferente dependendo do método de instalação do software: • `0` significa que a verificação da assinatura digital está desativada (valor predefinido se for implementado através do Kaspersky Security Center). • `1` significa que a verificação de assinatura digital está ativada (valor predefinido se a aplicação estiver a ser instalada localmente).
`STANDALONEMODE=1`	Instalar a aplicação 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 se uma Plataforma do Endpoint Protection (EPP) de terceiros for implantada na sua organização em conjunto com a solução Kaspersky Endpoint Detection and Response. Isso torna o Kaspersky Endpoint Security na configuração do Endpoint Detection and Response Agent compatível com aplicações EPP de terceiros.
`KLLOGIN`	Defina o nome de utilizador para aceder aos recursos e configurações do Kaspersky Endpoint Security (o componente Proteção de password). O nome do utilizador é definido com as definições de `KLPASSWD` e `KLPASSWDAREA`. O nome de utilizador KLAdmin é usado por definição.
`KLPASSWD`	Especificar uma password para aceder às funcionalidades e definições do Kaspersky Endpoint Security (a password é especificada juntamente com os parâmetros `KLLOGIN` de sessão e `KLPASSWDAREA`). Se tiver especificado uma password mas não especificou um nome de utilizador com o parâmetro `KLLOGIN`, o nome de utilizador KLAdmin é utilizado por predefinição.
`KLPASSWDAREA`	Especificar o âmbito da password para aceder às funcionalidades e definições do Kaspersky Endpoint Security. Quando um utilizador tenta executar uma ação incluída neste âmbito, o Kaspersky Endpoint Security solicita as credenciais da conta do utilizador (parâmetros `KLLOGIN` e `KLPASSWD`). Utilize o caráter `;` para especificar vários valores. Valores disponíveis: • `SET` - modificar as configurações da aplicação. • `EXIT` - sair da aplicação. • `DISPROTECT` – desativar componentes de proteção e parar tarefas de verificação. • `DISPOLICY` — desativar a política do Kaspersky Security Center. • `UNINST` – remover a aplicação do computador. • `DISCTRL` - desativar os componentes de controlo. • `REMOVELIC` - remover a chave. • `REPORTS` - visualizar relatórios. • `EXPORT` – exportar definições da aplicação. Por exemplo, `KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT`. A conta KLAdmin tem o direito de executar qualquer ação protegida por password. Por conseguinte, é impossível configurar o âmbito da password para a conta KLAdmin. Se tentar configurar o âmbito da password para a conta KLAdmin, a aplicação proíbe as ações especificadas para o grupo “Todos”.
`PROTECTOSSERVICES`	Proteção da funcionalidade dos serviços do sistema operativo. A proteção dos serviços do sistema operativo impede que aplicações de terceiros interfiram com o funcionamento dos serviços do sistema operativo. Esses serviços incluem, por exemplo, o serviço de inicialização automática de aplicações. • `1` significa que a proteção dos serviços do sistema operativo está ativada (valor padrão). • `0` significa que a proteção dos serviços do sistema operativo está desativada.
`ENABLETRACES`	Ativar ou desativar os rastreios da aplicação. Depois de iniciado, o Kaspersky Endpoint Security guarda os ficheiros de rastreio na pasta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. Valores disponíveis: • `1` – os rastreios estão ativados. • `0` – os rastreios estão desativados (valor padrão).
`TRACESLEVEL`	Nível de detalhe do rastreio. 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 da aplicação no modo normal (predefinição). • `600` (baixo). Todas as mensagens.

ENABLEAZURESUPPORT	Ativar ou desativar o modo de compatibilidade do 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). Esta funcionalidade garante a exibição correta do estado da máquina virtual do Azure na consola da Kaspersky Anti Targeted Attack Platform. Para monitorizar o desempenho do computador, o Kaspersky Endpoint Security envia telemetria aos servidores KATA. A telemetria inclui um ID do computador (Sensor ID). O modo de compatibilidade do Azure WVD permite atribuir um Sensor ID único permanente a estas máquinas virtuais. Se o modo de compatibilidade estiver desativado, o Sensor ID poderá mudar depois de o computador ser reiniciado devido ao funcionamento das máquinas virtuais do Azure. Isto pode fazer com que os duplicados das máquinas virtuais apareçam na consola.
AMPPL	Ativa ou desativa a proteção do serviço Kaspersky Endpoint Security utilizando a tecnologia AM-PPL (Antimalware Protected Process Light). Para obter mais informações sobre a tecnologia AM-PPL, visite o website 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 – a proteção do serviço Kaspersky Endpoint Security com a tecnologia AM-PPL é ativada. • 0 – a proteção do serviço Kaspersky Endpoint Security utilizando a tecnologia AM-PPL é desativada.
UPGRADEMODE	Modo de atualização das aplicações: • Seamless significa atualizar a aplicação com um reinício do computador (valor padrão). • Force significa atualizar a aplicação sem um reinício. Pode atualizar a aplicação sem reiniciar a aplicação a partir da versão 11.10.0. Para atualizar uma versão anterior da aplicação, tem de reiniciar o computador. Também pode instalar correções sem reiniciar a aplicação a partir da versão 11.11.0. Reinicio não é necessário ao instalar o Kaspersky Endpoint Security. Assim, o modo de atualização da aplicação será especificado nas definições da aplicação. Pode alterar este parâmetro nas definições da aplicação ou na política. Ao atualizar a aplicação já instalada, a prioridade do parâmetro da linha de comandos é inferior à do parâmetro especificado nas definições da aplicação ou no ficheiro setup.ini. Por exemplo, se o modo Force atualização for especificado na linha de comandos e o modo Seamless for especificado nas definições da aplicação, a atualização será instalada com um reinício do computador Seamless).
RESTAPI	Gestão da aplicação com API REST. Para gerir a aplicação com API REST, deve especificar o nome do utilizador (parâmetro RESTAPI_User). Valores disponíveis: • 1 - a gestão com API REST é permitida. • 0 - a gestão com API REST é bloqueada (valor predefinido). Para gerir a aplicação com API REST, a gestão com sistemas administrativos deve ser permitida. Para tal, defina o parâmetro AdminKitConnector=1. Se gerir a aplicação com API REST, não é possível gerir a aplicação com os sistemas de administração da Kaspersky.
RESTAPI_User	Nome do utilizador da conta de domínio do Windows usada para gerir a aplicação com API REST. A gestão da aplicação com API REST está disponível apenas para este utilizador. Introduza o nome de utilizador no formato <DOMAIN>\<UserName> (por exemplo, RESTAPI_User=COMPANY\Administrator). Só pode selecionar um utilizador para trabalhar com API REST. Adicionar um nome de utilizador é um pré-requisito para gerir a aplicação com API REST.
RESTAPI_Port	Porta usada para gerir a aplicação com API REST. A porta 6782 é usada por defeito. 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 de solicitação. Para tal, deve instalar um certificado e, posteriormente, assinar o payload de cada solicitação.
ADMINKITCONNECTOR	Gestão de aplicações com sistemas de administração. Os sistemas de administração incluem, por exemplo, o Kaspersky Security Center. Para além dos sistemas de administração da Kaspersky, pode usar soluções de terceiros. O Kaspersky Endpoint Security fornece uma API para esta finalidade. Valores disponíveis: • 1 - a gestão de aplicações com sistemas de administração é permitida (valor predefinido). • 0 - a gestão de aplicações é permitida apenas com a interface local.

`EnableUniqueSensorID`	Criação de um identificador de computador exclusivo (Sensor ID) durante a instalação ou atualização da aplicação. O Sensor ID é usado na solução Kaspersky Anti Targeted Attack Platform para identificar computadores que enviam telemetria para o servidor. Ao criar o Sensor ID, a aplicação usa um algoritmo que tem em consideração a configuração do computador, como o número de série da placa-mãe. Em alguns casos, por exemplo, quando se utiliza a aplicação num 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 único, tem de definir o parâmetro `EnableUniqueSensorID=1`. Como resultado, a aplicação utilizará um algoritmo diferente para criar o Sensor ID, que tem em conta outros dados sobre o computador. Isto garante um Sensor ID exclusivo. Por defeito, o parâmetro não está definido. A aplicação herda o Sensor ID nos seguintes casos: • Atualizar a versão da aplicação; • migrar a configuração [KES+KEA] para a configuração [KES+agente incorporado]. Como parte da reparação da aplicação, o instalador tenta herdar o Sensor ID. Se o Sensor ID não puder ser restaurado, a aplicação cria um novo Sensor ID.
`SKIPKB5007186CHECK=1`	Desativar a verificação da atualização do sistema operativo instalada KB5007186. Antes de instalar a aplicação, o instalador verifica as atualizações do sistema operativo instalado. A atualização KB5007186 faz parte da lista de atualizações do sistema operativo que podem causar problemas à aplicação. Para obter informações detalhadas, consulte a Base de Conhecimento de Apoio Técnico da Kaspersky. Portanto, o instalador aborta a instalação se esta atualização for descoberta. Para avançar 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 a instalação do Kaspersky Endpoint Security, a licença de avaliação é ativada exceto se fornecer um código de ativação no ficheiro setup.ini. Uma licença de avaliação tem normalmente um período de validade curto. Quando a licença de avaliação expirar, todas as funcionalidades do Kaspersky Endpoint Security são desativadas. Para continuar a utilizar a aplicação, precisa de a ativar com uma licença comercial utilizando o Assistente para Ativação de Aplicações ou um comando especial.

Ao instalar a aplicação ou ao atualizar a versão da aplicação no modo não assistido, é suportada a utilização dos seguintes ficheiros:

- setup.ini - configurações gerais da instalação da aplicação.

  Para aplicar as configurações do ficheiro setup.ini, coloque esse ficheiro na pasta que contém o pacote de distribuição do Kaspersky Endpoint Security.

- install.cfg - definições da operação do Kaspersky Endpoint Security

  Para aplicar as definições do ficheiro de configuração install.cfg, tem de especificar o caminho para o ficheiro no comando de instalação da aplicação que se segue: `CONFIGPATH=<path to the configuration file>`.

- setup.reg – chaves de registo.

  As chaves de registo do ficheiro setup.reg são escritas no registo apenas se o valor de `setup.reg` for definido para o parâmetro `SetupReg` no ficheiro setup.ini. O ficheiro setup.reg é gerado pelos peritos da Kaspersky. Não recomendamos a modificação dos conteúdos deste ficheiro. Para aplicar as configurações do ficheiro setup.reg, coloque esse ficheiro na pasta que contém o pacote de distribuição do Kaspersky Endpoint Security. Também pode colocar o ficheiro setup.reg numa pasta diferente. Se o fizer, será necessário especificar o caminho para o ficheiro no comando de instalação da aplicação que se segue: `SETUPREG=<path to the setup.reg file>`.

Setup /x. Remover a aplicação

O Kaspersky Endpoint Security pode ser desinstalado a partir da command line num dos seguintes modos:

- Em modo interativo, através da utilização do Assistente de Instalação da Aplicação.
- Em modo não assistido. Depois de a desinstalação ser iniciada no modo silencioso, o seu envolvimento no processo de remoção deixa de ser necessário (desinstalação silenciosa). Para instalar a aplicação no não assistido, use as teclas `/s` e `/qn`.

Para desinstalar a aplicação no modo não assistido:

1. Execute o interpretador de linha de comando (cmd.exe) como administrador.
2. Vá para 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 password:

     ```
     setup_kes.exe /s /x
     ```

     ou

     ```
     msiexec.exe /x <GUID> /qn
     ```

     `<GUID>` é a ID única da aplicação. Pode consultar o GUID da aplicação na Base de conhecimento de Suporte Técnico ou utilizando o seguinte comando:

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

   - Se o processo de remoção estiver protegido por password:

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

     ou

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

   Também pode usar o parâmetro `SAVEQB` para guardar ficheiros digitalizados pela aplicação e colocados na Cópia de segurança. As cópias de segurança de ficheiros são armazenadas na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`. Por predefinição, a opção de guardar ficheiros na Cópia de Segurança está desativada (`SAVEQB=0`).

   Exemplo

   ```
   msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
   ```

msiexec /i. Recuperar a aplicação

Durante a recuperação, a aplicação verifica e restaura a integridade de todos os módulos danificados da aplicação e das chaves de registo do sistema criadas como parte do processo de instalação da aplicação.

O Kaspersky Endpoint Security pode ser recuperado a partir da linha de comandos num dos seguintes modos:

- Em modo interativo, através da utilização do Assistente de Instalação da Aplicação.
- Em modo não assistido. Depois de iniciar a recuperação no modo silencioso, o seu envolvimento no processo de recuperação deixa de ser necessário.

Se o instalador do Kaspersky Endpoint Security estiver em execução no modo de recuperação e a aplicação não precisar de recuperação, o instalador não fará alterações.

Se o instalador do Kaspersky Endpoint Security estiver em execução no modo de recuperação e a aplicação não estiver instalada, o instalador iniciará o processo de instalação.

Para recuperar a aplicação no modo silencioso:

1. Execute o interpretador de linha de comando (cmd.exe) como administrador.
2. Vá para a pasta onde o pacote de distribuição do Kaspersky Endpoint Security está localizado.
3. Execute o seguinte comando:
   - Se o processo de recuperação não estiver protegido por password:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     `<GUID>` é a ID única da aplicação. Pode consultar o GUID da aplicação na Base de conhecimento de Suporte Técnico ou utilizando o seguinte comando:

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

   - Se o processo de recuperação estiver protegido por password:

     ```
     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

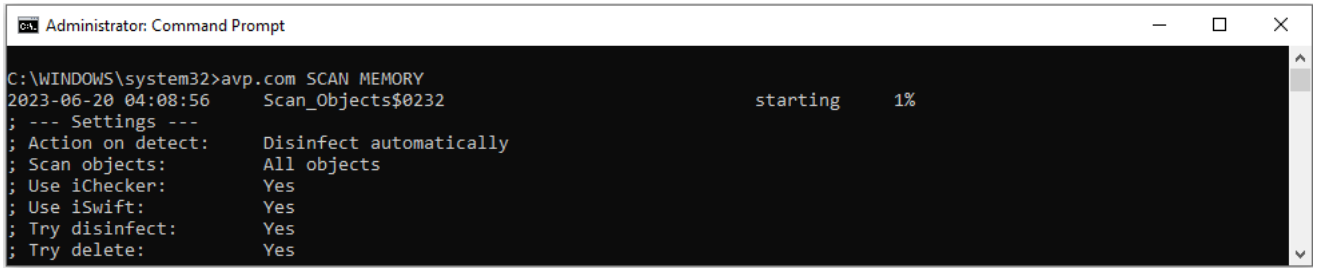
Para gerir o Kaspersky Endpoint Security a partir da command line:

1. Execute o interpretador de linha de comando (cmd.exe) como administrador.
2. Vá para a pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.

   Pode adicionar o caminho para o ficheiro executável à variável de sistema %PATH% durante a instalação da aplicação.
3. Utilize o seguinte modelo para executar o comando:

```
avp.com <command> [options]
```

Como resultado, o Kaspersky Endpoint Security executará o comando (ver figura abaixo).



Gerir a aplicação a partir da command line

SCAN. Verificação de software malicioso

Executar a tarefa *Verificação de software malicioso*.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

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>]
```

Âmbito de verificação	
`<files to scan>`	Uma lista separada por espaços de ficheiros e pastas. Caminhos longos devem ser colocados entre aspas. Caminhos curtos (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 software malicioso*. O Kaspersky Endpoint Security verifica os seguintes objetos: • Memória Kernel • Objetos carregados ao iniciar o sistema operativo • Setores de arranque • Cópia de segurança do sistema operativo • Todas as unidades de disco rígido e amovíveis No Kaspersky Endpoint Security for Windows 12.12, o e-mail está excluído do âmbito da verificação da aplicação. A verificação dos e-mails recebidos e enviados é realizada pelo componente Proteção contra ameaças de correio. Se estiver a utilizar uma versão anterior do plug-in de gestão, a aplicação exclui o e-mail do âmbito da verificação, mesmo que a política o inclua.
`/MEMORY`	Verifica a memória do Kernel
`/STARTUP`	Verifica os objetos que são carregados no arranque do sistema operativo
`/REMDRIVES`	Verifica as unidades amovíveis.
`/FIXDRIVES`	Verifica os discos rígidos.
`/NETDRIVES`	Verifica as unidades da rede.
`/QUARANTINE`	Verifica os ficheiros na Cópia de Segurança do Kaspersky Endpoint Security.
`/@:<file list.lst>`	Verifica os ficheiros e pastas de uma lista. Cada ficheiro na lista deve estar numa nova linha. Caminhos longos devem ser colocados entre aspas. Caminhos curtos (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 após deteção de ameaças	
`/i0`	**Informar**. Se esta opção for selecionada, o Kaspersky Endpoint Security adiciona a informação sobre ficheiros infetados à lista de ameaças ativas na deteção destes ficheiros.
`/i1`	**Desinfetar, informar se a desinfeção falhar**. Se esta opção estiver selecionada, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção falhar, o Kaspersky Endpoint Security adiciona a informação sobre os ficheiros infetados que são detetados à lista de ameaças ativas.
`/i2`	**Desinfetar, eliminar se a desinfeção falhar**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação elimina o ficheiro. Esta ação está selecionada por predefinição.
`/i3`	**Eliminar se a desinfeção falhar**. Elimine também ficheiros compostos (por exemplo, arquivos) se o ficheiro infetado não puder ser desinfetado ou eliminado.
`/i4`	**Eliminar**. Elimine também ficheiros compostos (por exemplo, arquivos) se o ficheiro infetado não puder ser eliminado.

Tipos de ficheiros	
`/fe`	**Ficheiros verificados por extensão**. Se esta configuração estiver ativada, a aplicação verifica apenas ficheiros infetáveis. O formato do ficheiro é então determinado com base na extensão do ficheiro.
`/fi`	**Ficheiros verificados por formato**. Se esta configuração estiver ativada, a aplicação verifica apenas ficheiros infetáveis. Antes de verificar um ficheiro para código malicioso, o cabeçalho interno do ficheiro é analisado para determinar o formato do ficheiro (por exemplo, .txt, .doc ou .exe). A verificação também procura ficheiros com extensões de ficheiro específicas.
`/fa`	**Todos os ficheiros**. Se esta definição estiver ativada, a aplicação verifica todos os ficheiros sem exceção (todos os formatos e extensões). Esta é a predefinição.

Exclusões de verificação	
`-e:a`	Os ficheiros RAR, ARJ, ZIP, CAB, LHA, JAR e ICE são excluídos do âmbito de verificação.
`-e:<file mask>`	Ficheiros que correspondem à máscara do ficheiro são excluídos do âmbito de verificação. Por exemplo: • A máscara `*.exe` inclui todos os caminhos para ficheiros com a extensão exe. • O `example*` de máscara incluirá todos os caminhos para ficheiros com o nome EXAMPLE.
`-e:<seconds>`	Os ficheiros que demoram mais a verificar do que o limite de tempo especificado (em segundos) são excluídos do âmbito de verificação.
`-es:<megabytes>`	Os ficheiros com um tamanho superior ao limite de tamanho especificado (em megabytes) são excluídos do âmbito de verificação.

Modo Guardar eventos num ficheiro de relatório (apenas para os perfis Scan, Updater e Rollback)	
`/R:<report file>`	Guarde apenas Critical events no ficheiro de relatório.
`/RA:<report file>`	Guarde todos os eventos num ficheiro de relatório.

Tecnologias de verificação	
`/iChecker=on|off`	Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. Existem limites para a tecnologia iChecker: não funciona com ficheiros grandes e aplica-se apenas a ficheiros com uma estrutura que o Kaspersky Internet Security reconheça (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).
`/iSwift=on|off`	Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. A tecnologia iSwift é um avanço da tecnologia iChecker para o sistema de ficheiros NTFS.

Definições avançadas	
`/C:<file with scan settings>`	Ficheiro com as definições da tarefa de *Verificação de software malicioso*. O ficheiro deve ser criado manualmente e guardado no formato TXT. O ficheiro 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. Atualização de bases de dados e módulos de software de aplicação

Executar a tarefa *Atualização das bases de dados e módulos da aplicação*.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Este comando não pode ser executado se a aplicação estiver instalada no Modo Light Agent.

Sintaxe de comando

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

Atualizar definições de tarefa	
`local`	Início da tarefa de *Atualização das bases de dados e módulos da aplicação* que foi criada automaticamente após a instalação da aplicação. Pode alterar as definições da tarefa de *Atualização das bases de dados e módulos da aplicação* na interface da aplicação local ou na consola do Kaspersky Security Center. Se esta definição não estiver configurada, o Kaspersky Endpoint Security iniciará a tarefa de *Atualização das bases de dados e módulos da aplicação* com as definições predefinidas ou com as definições especificadas no comando. Pode configurar as definições da tarefa de *Atualização das bases de dados e módulos da aplicação* do seguinte modo: • A opção `UPDATE` inicia a tarefa de *Atualização das bases de dados e módulos da aplicação* com as definições predefinidas: a origem da atualização são os servidores de atualização da Kaspersky, a conta é Sistema, e outras definições predefinidas. • A opção `UPDATE local` inicia a tarefa de *Atualização das bases de dados e módulos da aplicação* que foi criada automaticamente após a instalação (tarefa predefinida). • A opção `UPDATE <update settings>` inicia a tarefa de *Atualização das bases de dados e módulos da aplicação* com as definições definidas manualmente (ver abaixo).

Origem da atualização	
`"<update source>"`	Endereço de um servidor HTTP ou FTP ou de uma pasta partilhada com o pacote de atualização. Pode especificar apenas uma fonte de atualização. Se a origem da atualização não for especificada, o Kaspersky Endpoint Security utiliza a origem predefinida — os servidores de atualização da Kaspersky.

Modo Guardar eventos num ficheiro de relatório (apenas para os perfis Scan, Updater e Rollback)	
`/R:<report file>`	Guarde apenas Critical events no ficheiro de relatório.
`/RA:<report file>`	Guarde todos os eventos num ficheiro de relatório.

Definições avançadas	
`/C:<file with update settings>`	Ficheiro com as definições da tarefa de *Atualização das bases de dados e módulos da aplicação*. O ficheiro deve ser criado manualmente e guardado no formato TXT. O ficheiro 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. Reverter última atualização

Reverter a última atualização da base de dados de antivírus. Isto permite-lhe reverter as bases de dados e módulos da aplicação para a sua versão anterior quando necessário, por exemplo, quando a nova versão da base de dados contém uma assinatura inválida que faz com que o Kaspersky Endpoint Security bloqueie uma aplicação segura.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Este comando não pode ser executado se a aplicação estiver instalada no Modo Light Agent.

Sintaxe de comando

```
avp.com ROLLBACK [/R[A]:<report file>]
```

Modo Guardar eventos num ficheiro de relatório (apenas para os perfis Scan, Updater e Rollback)	
`/R:<report file>`	Guarde apenas Critical events no ficheiro de relatório.
`/RA:<report file>`	Guarde todos os eventos num ficheiro de relatório.

Exemplo

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Rastreio

Os ficheiros de rastreio são armazenados no computador desde que a aplicação esteja a ser utilizada, sendo permanentemente eliminados quando a aplicação é removida. Os ficheiros de rastreio, exceto os ficheiros de rastreio do Agente de Autenticação, são armazenados na pasta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. Por predefinição, o rastreio está desativado.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

Nível de rastreio	
`<tracing level>`	Nível de detalhe do rastreio. 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 da aplicação no modo normal (predefinição). • `600` (baixo). Todas as mensagens.

Definições avançadas	
`all`	Execute um comando com `file` e parâmetros `mem`.
`file`	Guarde um ficheiro de rastreio (sem limite de tamanho).
`rot`	Guarde os rastreios num número limitado de conjuntos de ficheiros de tamanho limitado e substitua os ficheiros mais antigos quando o tamanho máximo for alcançado.
`mem`	Guardar rastreios para descarregar ficheiros.

Exemplo

```
avp.com TRACES on 500
```

```
avp.com TRACES off
```

```
avp.com TRACES on 500 mem
```

```
avp.com TRACES off file
```

START. Iniciar um perfil

Iniciar um perfil (por exemplo, iniciar uma atualização da base de dados ou ativar um componente de proteção).

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com START <profile> [/R[A]:<report file>]
```

Perfil	
`<profile>`	Nome do perfil. Um *Perfil* é um componente, tarefa ou funcionalidade do Kaspersky Endpoint Security. Pode ver a lista de perfis disponíveis executando o comando `HELP START`.

Modo Guardar eventos num ficheiro de relatório (apenas para os perfis Scan, Updater e Rollback)	
`/R:<report file>`	Guarde apenas Critical events no ficheiro de relatório.
`/RA:<report file>`	Guarde todos os eventos num ficheiro de relatório.

Exemplo

```
avp.com START Scan_Objects
```

STOP. Interromper um perfil

Interromper a execução do perfil (por exemplo, interromper uma Verificação das unidades amovíveis ou desativar um componente de proteção).

Para executar este comando, a proteção por password deve estar ativada. O utilizador deve ter as permissões **Desativar componentes de proteção** e **Desativar componentes de controlo**.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

Perfil	
`<profile>`	Nome do perfil. Um *Perfil* é um componente, tarefa ou funcionalidade do Kaspersky Endpoint Security. Pode ver a lista de perfis disponíveis executando o comando `HELP STOP`.

Autenticação	
`/login=<user name> /password=<password>`	Credenciais da conta do utilizador com as permissões de Proteção por password necessárias.

STATUS. Estado do perfil

Apresentar informações do estado para perfis da aplicação (por exemplo, `running` ou `completed`). Pode ver a lista de perfis disponíveis executando o comando `HELP STATUS`.

O Kaspersky Endpoint Security apresenta também informações sobre o estado dos perfis de serviço. Podem ser necessárias informações sobre o estado dos perfis de serviço quando contactar o Suporte técnico da Kaspersky.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com STATUS [<profile>]
```

Se introduzir o comando sem um perfil, o Kaspersky Endpoint Security apresenta o estado para todos os perfis da aplicação.

STATISTICS. Estatísticas da operação do perfil

Apresentar estatísticas para um perfil da aplicação (por exemplo, duração da verificação ou o número de ameaças detetadas). Pode ver a lista de perfis disponíveis executando o comando `HELP STATISTICS`.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com STATISTICS <profile>
```

RESTORE. Restaurar ficheiros a partir da Cópia de segurança

Restaurar um ficheiro da cópia de segurança para a respetiva pasta original. Se já existir um ficheiro com o mesmo nome no caminho especificado, a aplicação irá solicitar a confirmação para substituir o ficheiro. O ficheiro que está a ser restaurado é copiado mantendo o seu nome original.

Para executar este comando, a proteção por password deve estar ativada. O utilizador deve ter a permissão para **Restaurar da cópia de segurança**.

A *cópia de segurança* armazena cópias de segurança de ficheiros que foram eliminados ou modificados durante a desinfeção. A *cópia de segurança* é a cópia de um ficheiro criada antes de o ficheiro ser desinfetado ou eliminado. As cópias de segurança dos ficheiros são armazenadas num formato especial e não constituem uma ameaça.

As cópias de segurança de ficheiros são armazenadas na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

Os utilizadores pertencentes aos grupos de administradores obtêm permissões completas de acesso a esta pasta. O utilizador cuja conta foi utilizada para instalar o Kaspersky Endpoint Security recebe direitos de acesso limitado para esta pasta.

O Kaspersky Endpoint Security não disponibiliza a capacidade de configurar as permissões de acesso do utilizador para a realização de cópias de segurança de ficheiros.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Definições avançadas	
`/REPLACE`	Substitui um ficheiro existente.
`<file name>`	O nome do ficheiro a restaurar.

Autenticação	
`/login=<user name> /password=<password>`	Credenciais da conta do utilizador com as permissões de Proteção por password necessárias.

Exemplo

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

EXPORT. Exportar definições da aplicação

A exportar as definições do Kaspersky Endpoint Security para um ficheiro. Se o comando tiver apenas o nome do ficheiro para o qual pretende exportar as definições, a aplicação coloca o ficheiro da seguinte forma:

- Se o caminho para avp.com for adicionado à variável do sistema %PATH%, a aplicação coloca o ficheiro na pasta `C:\Windows\SysWOW64`.
- Se executar o comando a partir da pasta de instalação da aplicação, a exportação irá falhar porque a auto-proteção da aplicação bloqueia a criação de um novo ficheiro na pasta da aplicação. Para exportar as definições da aplicação para um ficheiro, introduza o caminho do ficheiro.

Para executar este comando, a proteção por password deve estar ativada. O utilizador deve ter a permissão para **Exportar definições**.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

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 funcionalidade do Kaspersky Endpoint Security. Pode ver a lista de perfis disponíveis executando o comando `HELP EXPORT`.

Ficheiro para exportar	
`<file name>`	O nome do ficheiro para o qual as definições da aplicação serão exportadas. Também pode introduzir o caminho do ficheiro. Pode exportar as definições do Kaspersky Endpoint Security para um ficheiro de configuração DAT ou CFG, um ficheiro de texto TXT ou um documento XML.

Autenticação	
`/login=<user name> /password= <password>`	Credenciais da conta do utilizador com as permissões de Proteção por password necessárias.

Exemplo

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT. Importar definições da aplicação

Importar as definições do Kaspersky Endpoint Security a partir de um ficheiro que foi criado com o comando `EXPORT`.

Para executar este comando, a proteção por password deve estar ativada. O utilizador deve ter a permissão para **Configurar as definições da aplicação**.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

Ficheiro para importar	
`<file name>`	O nome do ficheiro do qual as definições da aplicação serão importadas. Pode importar as definições do Kaspersky Endpoint Security através de um ficheiro de configuração DAT ou CFG, um ficheiro de texto TXT ou um documento XML.

Autenticação	
`/login=<user name> /password= <password>`	Credenciais da conta do utilizador com as permissões de Proteção por password necessárias.

Exemplo

```
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword
```

ADDKEY. Aplicar um ficheiro de chave

Ativar o Kaspersky Endpoint Security utilizando um ficheiro de chave. Se a aplicação já estiver ativada, a chave será adicionada como chave de reserva.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Este comando não pode ser executado se a aplicação estiver instalada no Modo Light Agent.

Sintaxe de comando

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

Ficheiro-chave	
`<file name>`	Nome do key file.

Autenticação	
`/login=<user name> /password=<password>`	Credenciais da conta do utilizador. Estas credenciais só devem ser introduzidas se a Proteção por password estiver ativada.

Exemplo

```
avp.com ADDKEY file.key
```

LICENSE. Licenciamento

Gerir as chaves da licença do Kaspersky Endpoint Security, do EDR Optimum ou do EDR Expert (Suplemento do Kaspersky Endpoint Detection and Response).

Para executar este comando e remover uma chave de licença, a proteção por password deve estar ativada. O utilizador deve ter a permissão para **Remover chave**.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Este comando não pode ser executado se a aplicação estiver instalada no Modo Light Agent.

Sintaxe de comando

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

Operação	
`/ADD <file name>`	Ativar o Kaspersky Endpoint Security utilizando um ficheiro de chave. Se a aplicação já estiver ativada, a chave será adicionada como chave de reserva.
`/ADD <activation code>`	Ative o Kaspersky Endpoint Security utilizando um código de ativação. Se a aplicação já estiver ativada, a chave será adicionada como chave de reserva.
`/REFRESH`	Atualize o estado da licença do Kaspersky Endpoint Security. Como resultado, a aplicação recebe informação atualizada sobre o estado da licença dos servidores de ativação da Kaspersky.
`/REFRESH <license ID>`	Atualize o estado das licenças utilizando a ID da licença. Com este comando, pode atualizar o estado do Suplemento EDR, do Suplemento MDR, do Suplemento KUMA ou de outras licenças. Pode obter a ID da licença no certificado da licença. Como resultado, a aplicação recebe informação atualizada sobre o estado da licença dos servidores de ativação da Kaspersky.
`/CHECK`	Obtenha informação sobre a licença. O Kaspersky Endpoint Security exibe informações sobre todas as chaves de licença adicionadas, incluindo chaves de reserva, Suplemento EDR, Suplemento MDR, chaves de Suplemento KUMA e outras chaves. O Kaspersky Endpoint Security mostra a seguinte informação sobre a licença: • nome da licença; • identificador da licença; • endereço do Servidor de Proteção (SVM) ao qual a máquina virtual está ligada e no qual a aplicação está instalada no modo Light Agent; • tipo de licença: avaliação, comercial, beta, subscrição; • data e hora de ativação da aplicação; • data e hora de expiração da licença; • número de dias até à expiração da licença.
`/CHECK <license ID>`	Obtenha informação sobre a licença por ID. Pode usar este comando para obter informação sobre a licença. Pode obter a ID da licença no certificado da licença.
`/DEL /login=<user name> /password=<password>`	Remova a chave da licença da aplicação. A chave de reserva também será removida.
`/DEL <license ID> /login=<user name> /password=<password>`	Eliminar a chave utilizando a ID da licença. Com este comando, pode eliminar uma chave do Suplemento EDR, do Suplemento MDR, do Suplemento KUMA ou de outras licenças. Pode obter a ID da licença no certificado da licença.

Autenticação	
`/login=<user name> /password= <password>`	Credenciais da conta do utilizador com as permissões de Proteção por password 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

Abrir o website da Kaspersky para comprar ou renovar a sua licença.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Este comando não pode ser executado se a aplicação estiver instalada no Modo Light Agent.

PBATESTRESET. Repor os resultados da verificação do disco antes de encriptar o disco

Repor os resultados da verificação de compatibilidade para a Encriptação de disco completa (FDE), incluindo a tecnologia Encriptação de disco Kaspersky e a tecnologia Encriptação de Unidade BitLocker.

Antes de executar a Encriptação de disco completa, a aplicação executa várias verificações para verificar se o computador pode ser encriptado. Se o computador não suportar a Encriptação de disco completa, o Kaspersky Endpoint Security regista informações sobre a incompatibilidade. Quando voltar a tentar encriptar, a aplicação não executa esta verificação e irá apresentar um aviso de que não é possível realizar a encriptação. Se a configuração do hardware do computador tiver sido alterada, os resultados da verificação de compatibilidade registados anteriormente pela aplicação devem ser repostos para verificar novamente o disco rígido do sistema quanto à compatibilidade com as tecnologias de Encriptação de disco Kaspersky ou a Encriptação de Unidade BitLocker.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

EXIT. Sair da aplicação

Sair do Kaspersky Endpoint Security. A aplicação será descarregada da RAM do computador.

Para executar este comando, a proteção por password deve estar ativada. O utilizador deve ter a permissão para **Sair da aplicação**.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. Desativar política

Desativar uma política do Kaspersky Security Center no computador. Todas as definições do Kaspersky Endpoint Security estão disponíveis para configuração, incluindo definições que têm um cadeado fechado na política ( ).

Para executar este comando, a proteção por password deve estar ativada. O utilizador deve ter a permissão para **Desativar a política do Kaspersky Security Center**.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Ativar a política

Ativar uma política do Kaspersky Security Center no computador. As definições da aplicação serão configuradas de acordo com a política.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

DISABLE. Desativar a proteção

Desativar a Proteção contra ameaças a ficheiros num computador com uma licença expirada do Kaspersky Endpoint Security. Não é possível executar este comando num computador que tenha a aplicação que não está ativada, ou tenha uma licença válida.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

SPYWARE. Deteção de spyware

Gerir a deteção de spyware. Por predefinição, a deteção de spyware está ativada.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com SPYWARE on|off
```

KSN. Alternar entre KSN/KPSN

Selecionar uma solução do Kaspersky para determinar a reputação de ficheiros ou sites. O Kaspersky Endpoint Security suporta as seguintes soluções de infraestrutura para trabalhar com as bases de dados de reputação da Kaspersky:

- *Kaspersky Security Network (KSN)* é a solução usada pela maioria das aplicações da Kaspersky. Os participantes na KSN recebem informações da Kaspersky e enviam as informações à Kaspersky sobre os objetos detetados no computador do utilizador para fins de análise adicional pelos analistas da Kaspersky e inclusão nas bases de dados estatísticas e de reputação da Kaspersky Security Network.

- *Kaspersky Private Security Network (KPSN)* é uma solução que permite que utilizadores de computadores que alojam o Kaspersky Endpoint Security ou outras aplicações da Kaspersky tenham acesso às bases de dados de reputação do Kaspersky Security Network e a outros dados estatísticos sem enviar dados para o KSN a partir de seus próprios computadores. O KPSN foi criado para clientes empresariais que não podem participar na Kaspersky Security Network por qualquer um dos seguintes motivos:

  - As estações de trabalho locais não estão ligadas à Internet.

  - A transmissão de quaisquer dados para fora do país ou para fora da LAN empresarial é proibida por lei ou restringida por políticas de segurança empresariais.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Este comando não pode ser executado se a aplicação estiver instalada no Modo Light Agent.

Sintaxe de comando

```
avp.com KSN /global | /private <file name>
```

Ficheiro de configuração do Kaspersky Security Network	
`<file name>`	Nome do ficheiro de configuração que contém as definições do Kaspersky Private Security Network. Este ficheiro 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. Desativar a proteção da ligação do servidor

Executar a tarefa *Proteção da ligação do Servidor de Administração*, que remove a password de ligação do computador ao servidor de administração. Desta forma, a tarefa desativa a proteção da ligação do servidor de administração.

Para executar este comando, a proteção por password deve estar ativada.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

Password	
`/password=<password>`	A password da conta do utilizador KLAdmin ou a password da tarefa *Proteção da ligação do Servidor de Administração*. Se o parâmetro não for especificado, o Kaspersky Endpoint Security pede-lhe para introduzir uma password na linha seguinte.

Comandos KESCLI

Os comandos KESCLI permitem-lhe receber informações sobre o estado da proteção do computador com um componente OPSWAT e permitem-lhe realizar tarefas comuns, como as tarefas *Verificação de software malicioso* e *Atualização das bases de dados e módulos da aplicação*.

Pode ver a lista dos comandos KESCLI através do comando `kescli --help` ou do comando abreviado `kescli -h`.

Para gerir o Kaspersky Endpoint Security a partir da command line:

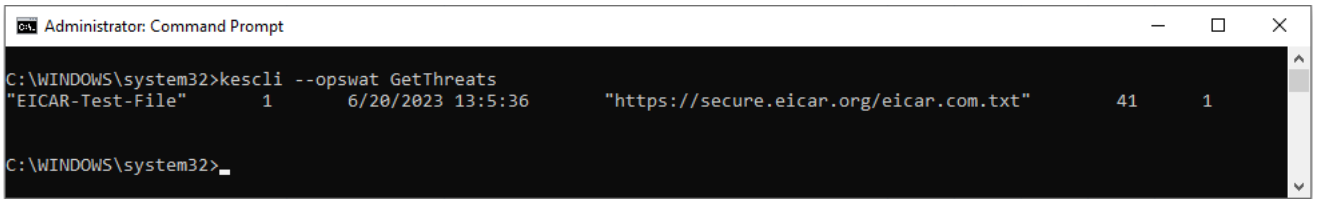
1. Execute o interpretador de linha de comando (cmd.exe) como administrador.
2. Vá para a pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.

   Pode adicionar o caminho para o ficheiro executável à variável de sistema %PATH% durante a instalação da aplicação.

3. Utilize o seguinte modelo para executar o comando:

```
kescli <comando> [opções]
```

Como resultado, o Kaspersky Endpoint Security executará o comando (ver figura abaixo).



Gerir a aplicação a partir da command line

Scan. Verificação de software malicioso

Executar a tarefa *Verificação de software malicioso* (Verificação completa).

Para executar a tarefa, o administrador tem de Permitir utilização de tarefas locais na política.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.

Sintaxe de comando

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

Pode verificar o estado da conclusão da tarefa de *Verificação de software malicioso* através do comando `GetScanState` e ver a data e hora quando a verificação foi concluída pela última vez através do comando `GetLastScanTime`.

Âmbito de verificação	
`<scan scope>`	`;`-lista separada por espaços de ficheiros e pastas. Por exemplo, `"C:\Program Files (x86)\Example Folder"`.

Ação após deteção de ameaças	
`0`	**Informar**. Se esta opção for selecionada, o Kaspersky Endpoint Security adiciona a informação sobre ficheiros infetados à lista de ameaças ativas na deteção destes ficheiros.
`1`	**Desinfetar, eliminar se a desinfeção falhar**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação elimina o ficheiro. Esta ação está selecionada por predefinição.

Exemplo

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

GetScanState. Estado de conclusão da verificação

Apresentação de informações sobre o estado da conclusão da tarefa *Verificação de software malicioso* (*Verificação completa*):

- `1` – a verificação está em curso.
- `0` – a verificação não está em execução.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.

Sintaxe de comando

```
kescli --opswat GetScanState
```

GetLastScanTime. Determinar a hora de conclusão da verificação

Apresentação de informações sobre a data e a hora da conclusão da última tarefa de *Verificação de software malicioso* (*Verificação completa*).

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.

Sintaxe de comando

```
kescli --opswat GetLastScanTime
```

GetThreats. Obter dados sobre ameaças detetadas

Apresentação de uma lista das ameaças detetadas (*Report on threats*). Este relatório contém informações sobre ameaças e atividades de vírus nos últimos 30 dias antes de criar o relatório.

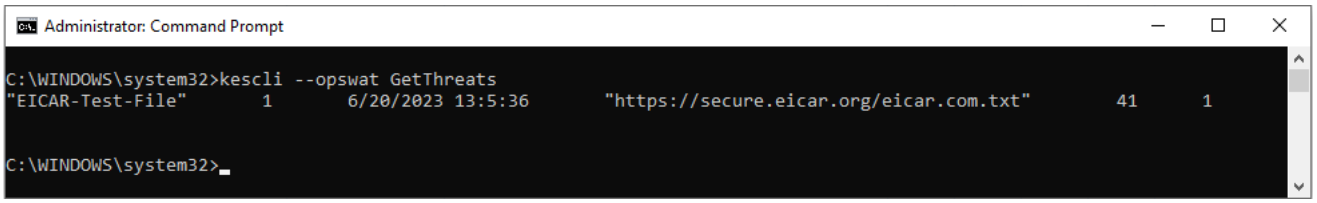
Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.

Sintaxe de comando

```
kescli --opswat GetThreats
```

Quando o comando for executado, o Kaspersky Endpoint Security irá enviar uma resposta no seguinte formato:

<name of detected object> <type of object> <detection date and time> <path to file> <action on threat detection> <threat danger level>



Gerir a aplicação a partir da command line

Tipo de objeto	
0	Não conhecido (Unknown).
1	Vírus (Virware).
2	Programas Trojan (Trojware).
3	Programas maliciosos (Malware).
4	Programas de propaganda (Adware).
5	Programas auto-dialer (Pornware).
6	Aplicações que podem ser utilizadas por um cibercriminoso para danificar o computador ou os dados do utilizador (Riskware).
7	Objetos comprimidos, cujo método de compactação pode ser utilizado para proteger um código malicioso (Packed).
20	Objetos desconhecidos (Xfiles).
21	Aplicações conhecidas (Software).
22	Ficheiros ocultos (Hidden).
23	Aplicações que necessitam de atenção (Pupware).
24	Comportamento anómalo (Anomaly).
30	Não determinado (Undetect).
40	Faixas de publicidade (Banner).
50	Ataque de rede (Attack).
51	Acesso ao registo (Registry).
52	Atividade suspeita (Suspicion).
60	Vulnerabilidades (Vulnerability).
70	Phishing (Phishing).
80	Anexos de mensagens de e-mail (Attachment).
90	Malware detetado pelo Kaspersky Security Network (Urgent).
100	Ligação desconhecida (Suspic URL).
110	Outro malware (Behavioral).

Ação após deteção de ameaças	
0	Não conhecido (unknown).
1	A ameaça foi remediada (ok).
2	O objeto estava infetado e não foi desinfetado (infected).
5	O objeto está num arquivo e não foi desinfetado (archive).
9	O objeto foi desinfetado (disinfected).
10	O objeto não foi desinfetado (not disinfected).

11	O objeto foi eliminado (`deleted`).
13	Foi criada uma cópia de segurança do objeto (`backupped`).
15	O objeto foi movido para a Cópia de segurança (`quarantined`).
23	O objeto foi eliminado ao reiniciar o computador (`delete on reboot`).
25	O objeto foi desinfetado ao reiniciar o computador (`disinfect on reboot`).
29	O objeto foi movido para a Cópia de segurança por um utilizador (`added by user`).
30	O objeto foi adicionado às exclusões (`added to exclude`).
31	O objeto foi movido para a Cópia de segurança ao reiniciar o computador (`quarantine on reboot`).
36	Falso positivo (`false alarm`).
38	O processo foi terminado (`terminated`).
40	O objeto não foi detetado (`not found`).
41	Não é possível resolver a ameaça (`untreatable`).
42	O objeto foi restaurado (`rolled back`).
43	O objeto foi criado como um resultado da atividade de ameaça (`produced by threat`).
44	O objeto foi restaurado ao reiniciar o computador (`roll back on reboot`).
0xffffffff	O objeto não foi processado (`discarded`).

Nível de perigo da ameaça	
0	Desconhecido
1	Alto
2	Nível médio
4	Baixo
8	Informações (inferior a *Baixo*)

UpdateDefinitions. Atualização de bases de dados e módulos de software de aplicação

Executar a tarefa *Atualização das bases de dados e módulos da aplicação*. O Kaspersky Endpoint Security utiliza a origem predefinida: Servidores de atualização da Kaspersky.

Para executar a tarefa, o administrador tem de Permitir utilização de tarefas locais na política.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.

Este comando não pode ser executado se a aplicação estiver instalada no Modo Light Agent.

Sintaxe de comando

```
kescli --opswat UpdateDefinitions
```

Pode ver a data e a hora de lançamento das bases de dados de antivírus atuais ao utilizar o comando `GetDefinitionsetState`.

GetDefinitionState. Determinação da última data e hora de atualização das bases de dados

Apresentação de informações sobre a última data e hora de lançamento das bases de dados antivírus que estão a ser utilizadas.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.

Sintaxe de comando

```
kescli --opswat GetDefinitionState
```

EnableRTP. Ativar proteção

A ativar os componentes de proteção Kaspersky Endpoint Security no computador: Proteção contra ameaças de ficheiros, Proteção contra ameaças da Web, Proteção contra ameaças de correio, Proteção contra Ameaças de Rede, Prevenção contra invasões.

> Para ativar os componentes de proteção, o administrador tem de certificar-se de que as definições da política relevantes podem ser modificadas ( os atributos estão abertos).

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.

Sintaxe de comando

```
kescli --opswat EnableRTP
```

Como resultado, os componentes de proteção são ativados mesmo que tenha proibido a modificação das definições da aplicação com Proteção por password.

Pode verificar o estado de funcionamento da Proteção contra ameaças de ficheiros através do comando `GetRealTimeProtectionState`.

GetRealTimeProtectionState. Estado da Proteção contra ameaças de ficheiros

Apresentação de informações sobre o estado do componente Proteção contra ameaças de ficheiros:

- `1` – o componente está ativado.
- `0` – o componente está desativado.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.

Sintaxe de comando

```
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. Estado da encriptação do disco

Apresentar informações sobre o estado da encriptação do disco:

- `1` significa que o disco está protegido pela tecnologia de encriptação de discos Kaspersky ou BitLocker.
- `0` significa que o disco não está encriptado.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.

Sintaxe de comando

```
kescli --opswat GetEncryptionState
```

Version. Identificar a versão da aplicação

Apresentar a versão do Kaspersky Endpoint Security for Windows.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.

Sintaxe de comando

```
kescli --Version
```

Também pode utilizar o comando abreviado `-v`.

Comandos Managed Detection and Response

Pode utilizar a command line para gerir a funcionalidade integrada das soluções de Detection and Response (por exemplo, Kaspersky Sandbox ou Kaspersky Endpoint Detection and Response Optimum). Pode gerir as soluções de Detection and Response se não for possível a gestão utilizando a Consola do Kaspersky Security Center. Pode ver a lista de comandos para gerir a aplicação, executando o comando `HELP`. Para ler sobre a sintaxe de um comando específico, digite `HELP <command>`.

Para gerir recursos integrados de soluções de Detection and Response usando a linha de comandos:

1. Execute o interpretador de linha de comando (cmd.exe) como administrador.
2. Vá para a pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.

3. Utilize o seguinte modelo para executar o comando:

```
avp.com <command> [options]
```

Como resultado, o Kaspersky Endpoint Security executará o comando.

SANDBOX. Gestão do Sandbox

Comandos para gerir 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:

  - Ligação do computador aos servidores do Sandbox.

    Os servidores utilizam imagens virtuais implementadas de sistemas operativos do Microsoft Windows para executar objetos que precisam de ser verificados. Pode inserir um endereço IP (IPv4 ou IPv6) ou um nome de domínio totalmente qualificado. Para obter mais informações sobre a implementação de imagens virtuais e a configuração de servidores Sandbox, consulte a Ajuda do Kaspersky Sandbox e a Ajuda da Kaspersky Anti Targeted Attack Platform.

  - Configuração do tempo limite de ligação para o servidor.

    Tempo limite de ligação para o servidor do Sandbox (para Kaspersky Sandbox) ou servidor do Nó Central (para KATA). Depois de decorrido o tempo limite definido, o Kaspersky Endpoint Security envia um pedido ao próximo servidor. Pode aumentar o tempo limite de ligação do servidor se a velocidade da sua ligação for baixa ou instável. O tempo limite recomendado do pedido é de 0.5 segundos ou menos.

  - Configuração de uma ligação fiável entre o computador e os servidores.

    Para configurar uma ligação fiável ao servidor do Sandbox (para o Kaspersky Sandbox) ou ao servidor do Nó Central (para KATA), tem de preparar um certificado TLS. De seguida, tem de adicionar o certificado ao computador utilizando uma política. Também tem de adicionar o certificado ao servidor do Sandbox (para Kaspersky Sandbox) ou ao servidor do Nó Central (para KATA).

  - Configurar o modo de integração.

    Tem de selecionar uma solução que inclua o Sandbox, ou seja, o Kaspersky Sandbox ou o KATA Sandbox. O *Kaspersky Sandbox* é uma solução Detection and Response autónoma da Kaspersky. O *KATA Sandbox* é um componente da solução Kaspersky Anti Targeted Attack Platform. Quando integrado com o KATA Sandbox, o componente pode funcionar nos seguintes modos:

    - **Manually**. O utilizador envia manualmente o ficheiro para verificação a partir do menu de contexto (**Enviar para Sandbox**).

    - **Automatically**. A aplicação deteta automaticamente os objetos e envia-os para o Sandbox para verificação.

    - **Combined**.

- Apresentação das definições atuais do componente.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

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. Pode configurar as seguintes definições:
	• Adicione servidores do Sandbox (`--servers`)
	• Adicione um certificado TLS (`--pinned-certificate`)
	• Adicione um cripto-contentor (`--client-certificate`).
	• Especifique uma password para o cripto-contentor (`--client-certificate-password`);
	• Definir o tempo limite de ligação ao servidor (`--timeout`)
	• Selecione 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`	Apresentar as definições atuais do componente. Obterá a seguinte resposta:
	`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 do utilizador com as permissões de Proteção por password 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. Gestão de prevenção de execução

Desativação do componente Prevenção da execução ou apresentação das definições atuais do componente, incluindo a lista de regras de prevenção da execução.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com prevention disable
```

```
avp.com prevention /show
```

Depois de executar o comando `prevention /show`, irá receber 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 suportado pela versão do Kaspersky Endpoint Agent instalada no computador.
- `0` significa que o comando foi executado com êxito.
- `1` significa que um argumento obrigatório não foi transmitido ao 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 este já está desativado).

ISOLATION. Gerir o isolamento da rede

Desativação do Isolamento da rede do computador ou apresentação das definições atuais do componente. As definições dos componentes também incluem uma lista de ligações de rede adicionadas às exclusões.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com isolation /OFF /login=<user name> /password=<password>
```

```
avp.com isolation /STAT
```

Como resultado da execução do comando `stat`, receberá a seguinte resposta: `Network isolation on|off`.

RESTORE. Restaurar ficheiros a partir da Quarentena

Restauro de um ficheiro da Quarentena para a respetiva pasta original. *Quarentena* é um armazenamento local especial no computador. O utilizador pode colocar em quarentena ficheiros que considere perigosos para o computador. Os ficheiros na quarentena são armazenados num estado encriptado e não põem em risco a segurança do dispositivo. O Kaspersky Endpoint Security utiliza a Quarentena apenas quando integrado com as soluções Kaspersky Detection and Response. Em todos os outros casos, o Kaspersky Endpoint Security coloca o ficheiro pertinentes na Cópia de Segurança. Para obter mais informações sobre a gestão da Quarentena como parte das soluções, consulte Ajuda do Kaspersky Sandbox, Ajuda do Kaspersky Endpoint Detection and Response Optimum e Ajuda do Kaspersky Endpoint Detection and Response Expert, Ajuda do Kaspersky Anti Targeted Attack Platform e Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises).

Para executar este comando, a proteção por password deve estar ativada. O utilizador deve ter a permissão para **Restaurar da cópia de segurança**.

O objeto é colocado em quarentena na conta do sistema (SYSTEM).

A restauração de ficheiros da Quarentena envolve as seguintes considerações especiais:

- Se a pasta de destino foi eliminada ou o utilizador não possui direitos de acesso a essa pasta, a aplicação coloca o ficheiro na pasta `%DataRoot%\QB\Restored`. Depois tem de mover manualmente o ficheiro para a pasta de destino.
- A aplicação diferencia as maiúsculas e minúsculas no nome do ficheiro que está a ser restaurado. Se não observar o caso ao inserir o nome do ficheiro, a aplicação não irá restaurar o ficheiro.
- Caso a pasta de destino já possua um ficheiro com o mesmo nome, a aplicação cancela a restauração do ficheiro.
- Se estiver a utilizar a solução KATA (EDR), a aplicação guardará uma cópia do ficheiro na Quarentena após restaurar o ficheiro. Pode esvaziar a Quarentena manualmente. Para soluções EDR Optimum e EDR Expert, a aplicação elimina o ficheiro após a restauração.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Definições avançadas	
`/REPLACE`	Substitui um ficheiro existente.
`<file name>`	O nome do ficheiro a restaurar.

Autenticação	
`/login=<user name> /password=<password>`	Credenciais da conta do utilizador com as permissões de Proteção por password necessárias.

Exemplo

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

Valores de retorno do comando:

- `-1` significa que o comando não suportado pela versão do Kaspersky Endpoint Agent instalada no computador.
- `0` significa que o comando foi executado com êxito.
- `1` significa que um argumento obrigatório não foi transmitido ao comando.
- `2` significa que ocorreu um erro geral.
- `4` significa que houve um erro de sintaxe.

IOCSCAN. Verificar indicadores de comprometimento (IOC)

Executar a tarefa *IOC Scan*. Um *Indicador de comprometimento (IOC)* é um conjunto de dados relativos a um objeto ou atividade que indica acesso não autorizado ao computador (comprometimento de dados). Por exemplo, muitas tentativas falhadas de iniciar sessão no sistema podem constituir um Indicador de Comprometimento. A tarefa *IOC Scan* permite localizar indicadores de comprometimento no computador e adotar medidas de resposta a ameaças.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Uma Verificação IOC é abortada após 128 correspondências com indicadores de compromisso descritos nos ficheiros IOC. Isto é necessário para limitar o número de entradas no relatório da tarefa de Verificação IOC, para ser mais fácil de analisar e impedir o relatório de ficar demasiado longo devido a indicadores de compromisso formulados de forma imprecisa que podem gerar uma série de 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>]
```

Ficheiros IOC	
`<full path to the IOC file>`	Caminho completo para o ficheiro IOC que deseja usar para a verificação. Pode especificar vários ficheiros IOC separados por espaços. O caminho completo para o ficheiro IOC deve ser introduzido 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 IOC files que deseja utilizar para a verificação. Os *IOC files* são ficheiros que contêm os conjuntos de indicadores que a aplicação tenta corresponder para contar uma deteção. Os IOC files 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`	Analise os dados do processo ao executar a verificação IOC (termo ProcessItem). Se o valor do argumento for `off` (não), o Kaspersky Endpoint Security não analisa os processos em execução no computador durante a verificação. Se o ficheiro IOC contiver termos IOC do documento ProcessItem IOC, estes serão ignorados (detetados como sem correspondência). Se o argumento não for especificado, o Kaspersky Endpoint Security só analisa os dados do processo se o documento ProcessItem IOC for descrito no ficheiro IOC fornecido para a verificação.
`/hint=<full path to the executable file of the process|full path to the file>`	Analise os dados do ficheiro ao executar a verificação IOC (termos ProcessItem e FileItem). Pode selecionar um ficheiro através de 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`	Analise os dados de registo do Windows ao executar uma verificação IOC (termo RegistryItem). Se o valor do argumento for `off` (não), o Kaspersky Endpoint Security não verifica o registo do Windows. Se o ficheiro IOC contiver termos do documento RegistryItem IOC, estes serão ignorados (detetados como sem correspondência). Se o argumento não for especificado, o Kaspersky Endpoint Security só analisa o registo do Windows se o documento RegistryItem IOC for descrito no ficheiro IOC fornecido para a verificação. Para o tipo de dados RegistryItem, o Kaspersky Endpoint Security verifica um conjunto de chaves de registo.
`/dnsentry=on|off`	Analise os dados sobre os registos na cache DNS local ao executar a verificação IOC (termo DnsEntryItem). Se o valor do argumento for `off` (não), o Kaspersky Endpoint Security não verifica a cache DNS local. Se o ficheiro IOC contiver termos do documento DnsEntryItem IOC, estes serão ignorados (detetados como sem correspondência). Se o argumento não for especificado, o Kaspersky Endpoint Security só analisa a cache DNS local se o documento DnsEntryItem IOC for descrito no ficheiro IOC fornecido para a verificação.
`/arpentry=on|off`	Analise os dados sobre os registos na tabela ARP ao realizar a verificação IOC (termo ArpEntryItem). Se o valor do argumento for `off` (não), o Kaspersky Endpoint Security não verifica a tabela ARP. Se o ficheiro IOC contiver termos do documento ArpEntryItem IOC, estes serão ignorados (detetados como sem correspondência). Se o argumento não for especificado, o Kaspersky Endpoint Security só analisa a tabela ARP se o documento ArpEntryItem IOC for descrito no ficheiro IOC fornecido para a verificação.
`/ports=on|off`	Analise os dados sobre as portas de escuta abertas ao executar a verificação IOC (termo PortItem). Se o valor do argumento for `off` (não), o Kaspersky Endpoint Security não verifica a tabela de ligações ativas no dispositivo. Se o ficheiro IOC contiver termos do documento PortItem IOC, estes serão ignorados (detetados como sem correspondência). Se o argumento não for especificado, o Kaspersky Endpoint Security só analisa a tabela de ligações ativas se o documento PortItem IOC for descrito no ficheiro IOC fornecido para a verificação.
`/services=on|off`	Analise os dados sobre os serviços instalados no dispositivo ao executar a verificação IOC (termo ServiceItem). Se o valor do argumento for `off` (não), o Kaspersky Endpoint Security não verifica os dados sobre os serviços instalados no dispositivo. Se o ficheiro IOC contiver termos do documento ServiceItem IOC, estes serão ignorados (detetados como sem correspondência). Se o argumento não for especificado, o Kaspersky Endpoint Security só analisa os dados sobre o serviço se o documento ServiceItem IOC for descrito no ficheiro IOC fornecido para a verificação.
`/system=on|off`	Analise os dados de ambiente ao executar a verificação IOC (termo SystemInfoItem). Se o valor do argumento for `off` (não), o Kaspersky Endpoint Security não analisa os dados de ambiente. Se o ficheiro IOC contiver termos do documento SystemInfoItem IOC, estes serão ignorados (detetados como sem correspondência). Se o argumento não for especificado, o Kaspersky Endpoint Security só analisa os dados de ambiente se o documento SystemInfoItem IOC for descrito no ficheiro IOC fornecido para a verificação.
`/users=on|off`	Analise os dados sobre os utilizadores ao executar a verificação IOC (termo UserItem). Se o valor do argumento for `off` (não), o Kaspersky Endpoint Security não analisa os dados sobre os utilizadores criados no sistema. Se o ficheiro IOC contiver termos do documento UserItem IOC, estes serão ignorados (detetados como sem correspondência). Se o argumento não for especificado, o Kaspersky Endpoint Security só analisa os dados sobre os utilizadores criados no sistema se o documento UserItem IOC for descrito no ficheiro IOC fornecido para a verificação.

`/volumes=on|off`	Analise os dados do volume ao executar a verificação IOC (termo VolumeItem). Se o valor do argumento for `off` (não), o Kaspersky Endpoint Security não verifica os dados do volume no dispositivo. Se o ficheiro IOC contiver termos do documento VolumeItem IOC, estes serão ignorados (detetados como sem correspondência). Se o argumento não for especificado, o Kaspersky Endpoint Security só analisa os dados do volume se o documento VolumeItem IOC for descrito no ficheiro IOC fornecido para a verificação.
`/eventlog=on|off`	Analise os dados sobre os registos no registo de eventos do Windows ao executar a verificação IOC (termo EventLogItem). Se o valor do argumento for `off` (não), o Kaspersky Endpoint Security não verifica os registos no registo de eventos do Windows. Se o ficheiro IOC contiver termos do documento EventLogItem IOC, estes serão ignorados (detetados como sem correspondência). Se o argumento não for especificado, o Kaspersky Endpoint Security só analisa o registo de eventos do Windows se o documento EventLogItem IOC for descrito no ficheiro IOC fornecido para a verificação. Para o termo IOC EventLogItem\source, utilize o valor **Nome do fornecedor** do esquema XML do evento.
`/datetime=<event publication date>`	Tenha em consideração a data em que o evento foi publicado no registo de eventos do Windows ao determinar o âmbito de verificação IOC para o documento IOC correspondente. Ao executar uma verificação IOC, o Kaspersky Endpoint Security verifica as entradas do registo de eventos do Windows publicadas durante desde o dia e hora especificados ao 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 só é executada para eventos publicados no registo de eventos do Windows após a data especificada e antes de a verificação ser executada. Se o argumento não for especificado, o Kaspersky Endpoint Security verifica os eventos independentemente da data de publicação. Não é possível editar a definição `TaskSettings::BaseSettings::EventLogItem::datetime`. A definição só é utilizada se o documento EventLogItem IOC for descrito no ficheiro IOC fornecido para a verificação.
`/channel=<list of channels>`	Lista de nomes de canais (registo) nos quais deseja executar uma verificação IOC. Se o argumento for especificado, o Kaspersky Endpoint Security verifica os registos publicados nos registos especificados. O documento IOC deve ter o termo EventLogItem descrito. O nome do registo é especificado como uma cadeia de acordo com o nome do registo (canal) especificado nas propriedades do registo (no parâmetro Full Name) ou nas propriedades do evento (no parâmetro `<Channel></Channel>`, no esquema XML do evento). Pode especificar vários canais separados por espaços. Se o argumento não for especificado, o Kaspersky Endpoint Security verifica os registos dos canais `Application`, `System`, `Security`.
`/files=on|off`	Analise os dados do ficheiro ao executar a verificação IOC (termo FileItem). Se o valor do argumento for `off` (não), o Kaspersky Endpoint Security não analisa os dados do ficheiro. Se o ficheiro IOC contiver termos do documento FileItem IOC, estes serão ignorados (detetados como sem correspondência). Se o argumento não for especificado, o Kaspersky Endpoint Security só analisa os dados do ficheiro se o documento FileItem IOC for descrito no ficheiro IOC fornecido para a verificação.
`/drives=<all|system|critical|custom>`	Defina o âmbito de verificação IOC ao analisar dados para o documento FileItem IOC. Pode definir os seguintes valores para o âmbito de verificação: • `<all>` para todos os âmbitos de ficheiro disponíveis. • `<system>` para ficheiros em pastas nas quais o sistema operativo está instalado. • `<critical>` para ficheiros temporários nas pastas do utilizador e do sistema. • `<custom>` para ficheiros em âmbitos definidos pelo utilizador (`/scope=<list of folders to scan>`). Se o argumento não for especificado, a verificação será executada em áreas críticas.
`/excludes=<list of exclusions>`	Defina o âmbito de exclusão ao analisar dados para o documento FileItem IOC. Pode especificar vários caminhos separados por espaços.
`/scope=<list of folders to scan>`	Âmbito de verificação IOC definido pelo utilizador ao analisar dados para o documento FileItem (`/drives=custom`). Pode especificar vários caminhos separados por espaços.

`/retro /<number of days>`	A *Verificação retrospetiva dos IOC* é um modo da tarefa *IOC Scan* na qual o Kaspersky Endpoint Security verifica indicadores de comprometimento usando dados de um determinado período de tempo. Este modo destina-se à pesquisa de indicadores de comprometimento através dos dados de telemetria do computador protegido, tais como atividade de rede, processos, ficheiros e outros dados de telemetria. Pode definir um período de tempo de 1 a 14 dias. Por padrão, a aplicação verifica indicadores de comprometimento durante um dia.
`/network=on|off`	Análise de dados de rede (o termo NetworkItem).
`/url=on|off`	Análise de dados em registos do navegador (o termo UrlHistoryItem). A Verificação retrospetiva dos IOC analisa os registos dos seguintes navegadores: Google Chrome, Mozilla Firefox, Microsoft Edge (versão 79 ou posterior).
`/email`	Análise de objetos de correio (o termo EmailItem).
`/route`	Análise das tabelas de encaminhamento e reencaminhamento (o termo RouteEntryItem).

Valores de retorno do comando:

- `-1` significa que o comando não suportado pela versão do Kaspersky Endpoint Agent instalada no computador.
- `0` significa que o comando foi executado com êxito.
- `1` significa que um argumento obrigatório não foi transmitido ao comando.
- `2` significa que ocorreu um erro geral.
- `4` significa que houve um erro de sintaxe.

Se o comando for executado com êxito (valor de retorno `0`) e tiverem sido detetados indicadores de comprometimento ao longo do caminho, o Kaspersky Endpoint Security envia as seguintes informações sobre os resultados da tarefa para a command line:

`Uuid`	ID do ficheiro IOC do cabeçalho da estrutura do ficheiro IOC (a etiqueta `<ioc id="">`)
`Name`	Descrição do ficheiro IOC do cabeçalho da estrutura do ficheiro IOC (a etiqueta `<description> </description>`)
`Matched Indicator Items`	Lista de ID de todos os indicadores correspondentes.
`Matched objects`	Dados de cada documento IOC para o qual houve uma correspondência.

MDRLICENSE. Ativação MDR

Adicionar o ficheiro de configuração BLOB para ativar o Managed Detection and Response. O ficheiro BLOB contém a ID do cliente e informações sobre a licença do Kaspersky Managed Detection and Response. O ficheiro BLOB está localizado dentro do arquivo ZIP do ficheiro de configuração do MDR. Pode obter o arquivo ZIP na Consola do Kaspersky Managed Detection and Response. Para obter mais informações sobre ficheiros BLOB, consulte a Ajuda do Kaspersky Managed Detection and Response.

Os privilégios de administrador são necessários para executar operações com um ficheiro BLOB. As definições do Managed Detection and Response na política também devem estar disponíveis para edição ( ).

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

Operação	
`/ADD <file name>`	Aplique o ficheiro de configuração BLOB para integração com o Kaspersky Managed Detection and Response (formato de ficheiro P7). Apenas pode aplicar um ficheiro BLOB. Se um ficheiro BLOB já tiver sido adicionado ao computador, o ficheiro será substituído.
`/DEL`	Elimine o ficheiro de configuração BLOB.

Autenticação	
`/login=<user name> /password=<password>`	Credenciais da conta do utilizador com as permissões de Proteção por password 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 gerir o componente Endpoint Detection and Response (KATA):

- Ativar ou desativar o componente EDR (KATA).

  O componente EDR (KATA) fornece interoperabilidade com a solução Kaspersky Anti Targeted Attack Platform.

- Configurar a ligação com os servidores da Kaspersky Anti Targeted Attack Platform.

- Apresentação das definições atuais do componente.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

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`	Desative o componente EDR (KATA).
`start`	Ative o componente EDR (KATA).
`set`	Configure o componente EDR (KATA). Pode configurar as seguintes definições: • Adicione servidores do Central Node (`servers=<server address>:<port>`) • Adicione um certificado TLS (`server-certificate=<path to the TLS certificate>`) • Defina o tempo limite de ligação ao servidor do Central Node (`/timeout=<Central Node server connection timeout (s)>`) • Defina o período de sincronização com o servidor do Central Node (`/sync-period=<Central Node server synchronization period (min)>`)
`show`	Apresentar as definições atuais do componente.

EDRExpertOnPrem. Integração com o EDR Expert (on-premises)

Comandos para gerir o agente incorporado para configurar a integração com o Kaspersky Endpoint Detection and Response Expert (on-premises):

- Ativação ou desativação do agente incorporado do EDR Expert (on-premises).
- Configuração das definições de ligação dos servidores do EDR Expert (on-premises).
- Apresentação das definições atuais do agente incorporado.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

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 incorporado do EDR Expert (on-premises).
`start`	Ative o agente incorporado do EDR Expert (on-premises).

`set`	Configure o agente incorporado do EDR Expert (on-premises).
	Pode configurar as seguintes definições de ligação 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 ligação fiável com o servidor. Pode 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>`. Utilize um contentor criptográfico para autenticação bidirecional. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada no formato PKCS#12. Para ativar este tipo de autenticação, tem de criar um cripto-contentor numa autoridade de certificação externa.
	• `timeout=<server connection timeout (s)>`. Tempo limite máximo de resposta do servidor. Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor diferente.
	• `sync-period=<server synchronization period (min)>`. Frequência de pedidos de sincronização enviados ao servidor. Durante a sincronização, o Kaspersky Endpoint Security recebe tarefas de resposta a ameaças e envia os resultados dessas tarefas.
	Pode configurar as seguintes definições de ligação para os *servidores de recolha de telemetria*:
	• `telemetry-servers=<server address:port>`. Endereço do servidor de recolha de telemetria (FQDN, IPv4, IPv6).
	• `telemetry-server-certificate=<path to the TLS certificat>`. Certificado TLS para estabelecer uma ligação fiável com o servidor. Pode 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>`. Utilize um contentor criptográfico para autenticação bidirecional. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada no formato PKCS#12. Para ativar este tipo de autenticação, tem de criar um cripto-contentor numa autoridade de certificação externa.
	• `telemetry-timeout=<server connection timeout (s)>`. Tempo limite máximo de resposta do servidor. Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor diferente.
	• `events-send-period=<seconds>`. Atraso máximo no envio de eventos. A aplicação sincroniza com o servidor para enviar eventos após o término do intervalo de sincronização. A predefinição é 30 segundos.
	• `events-limit=<0|1>`. Limite o número de pedidos. Esta ação ajuda a otimizar a carga no servidor. Se esta funcionalidade estiver ativada, a aplicação restringe a transmissão de eventos. Se o número de eventos exceder os limites configurados, o Kaspersky Endpoint Security irá interromper o envio de eventos.
	• `events-per-hour=<number of events>`. Número máximo de eventos por hora. A aplicação analisa o fluxo de dados de telemetria e restringe o envio de eventos se o fluxo de eventos exceder o limite de eventos por hora configurado. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. A predefinição é 3000 eventos por hora. Se a aplicação estiver instalada num servidor, o fluxo de dados de telemetria é mais elevado. Para os servidores, recomenda-se que o valor seja aumentado para 60.000 eventos por hora.
	• `max-packet-length=<number of packets>`. Comprimento máximo do pacote. A aplicação é sincronizada com o servidor quando a memória intermédia está cheia de eventos. A predefinição é 1024 eventos.
	• `telemetry-only-tagged-events=<0|1>`. Envio de telemetria apenas com IOA. *Indicador de Ataque (IOA)* é uma regra que contém uma descrição do comportamento suspeito no sistema que pode indicar um ataque direcionado. A aplicação compara o comportamento contínuo no sistema com essas regras e regista eventos que indicam um ataque direcionado. A aplicação utiliza a tecnologia de *análise em tempo real*, que permite o acompanhamento em tempo real desses eventos.
	Pode configurar as seguintes definições gerais:
	• `mode=EDRKATA | EDRExpertOnPrem`. Alternância entre soluções:
	  • `EDRKATA`. Endpoint Detection and Response Expert (version 7.1 or earlier).
	  • `EDRExpertOnPrem`. Endpoint Detection and Response Expert (version 8.0 or later). Valor predefinido.
	• `login=<user name> password=<password>`. Credenciais da conta do utilizador com as permissões de Proteção por password necessárias.

`show`	Apresentar as definições atuais do componente.

KUMA. Integração do KUMA

Comandos para gerir o agente KUMA integrado:

- Ativar ou desativar a integração com o KUMA.

  O agente KUMA integrado proporciona interoperabilidade com a solução Kaspersky Unified Monitoring and Analysis Platform.

- Configurar a ligação aos servidores da Kaspersky Unified Monitoring and Analysis Platform.
- Apresentação das definições atuais do componente.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

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`	Desative a integração com o KUMA.
`start`	Ative a integração com o KUMA.
`set`	Configure o agente KUMA integrado. Pode configurar as seguintes definições: • Adicione servidores KUMA (`/servers=<protocol>://<server address>:<port>`) A aplicação suporta os seguintes protocolos de ligação ao servidor: `tcp`, `udp`, `http`, `https`. • Adicione um certificado TLS (`/server-certificate=<path to the TLS certificate>`) • Definir o tempo limite de ligação ao servidor (`/timeout=<KUMA server connection timeout (s)>`) • Adicione um cripto-contentor (`/client-certificate=<path to the crypto-container> /client-certificate-password=<password>`). • Configure o atraso de transmissão do evento (`/maximum-data-transfer-time=<maximum events transmission delay (sec)`)
`show`	Apresentar as definições atuais do componente.

Autenticação	
`/login=<user name> /password=<password>`	Credenciais da conta do utilizador com as permissões de Proteção por password 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. Executar verificação YARA

A executar a tarefa *Executar verificação YARA*. A aplicação verifica ficheiros e objetos em busca de indicadores de ataques dirigidos à infraestrutura de TI corporativa utilizando bases de dados de regras YARA. *Regras YARA* são descrições de assinaturas de ataques direcionados e intrusões na infraestrutura de TI corporativa que o Kaspersky Endpoint Security usa para verificar objetos.

Para executar uma verificação YARA, tem de preparar ficheiros YARA que descrevam regras. Ao criar ficheiros YARA, considere os seguintes requisitos:

- O Kaspersky Endpoint Security suporta ficheiros YARA com as extensões .YARA e .YAR que seguem o padrão aberto YARA 4.2.3 para a descrição de indicadores de comprometimento.
- Apenas ficheiros com regras YARA podem ser especificados para a tarefa. A tarefa *Executar verificação YARA* não suporta outros tipos de regras.
- Se tiver adicionado ficheiros YARA que o Kaspersky Endpoint Security não suporta, ou se as regras tiverem erros de sintaxe, a tarefa é abortada com a mensagem de erro correspondente.
- Os identificadores de todos os ficheiros YARA utilizados numa única tarefa têm de ser únicos. Se existirem YARA files com o mesmo identificador, tal pode afetar os resultados da execução da tarefa.
- Uma verificação YARA é abortada após 128 correspondências com indicadores descritos nas regras YARA. Isto é necessário para limitar o número de entradas no relatório de verificação YARA, para ser mais fácil de analisar e impedir o relatório de ficar demasiado longo devido a regras YARA formuladas de forma imprecisa que podem gerar uma série de correspondências.

A Kaspersky recomenda criar uma regra por ficheiro YARA. Isto torna os resultados da verificação mais legíveis.

Uma verificação YARA pode levar um tempo considerável. Dependendo do tamanho da unidade, das definições da tarefa e do número de objetos no disco, uma verificação YARA pode durar de alguns minutos a várias horas. A aplicação não apresenta um indicador de progresso. Não é possível parar ou cancelar uma verificação YARA. É aconselhável esperar até que os resultados da 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>]
```

Ficheiros YARA	
`<full path to the YARA file>`	Caminho completo para o ficheiro YARA que deseja usar para a verificação. Pode especificar caminhos para vários ficheiros YARA separados por espaços. Argumento obrigatório se o valor `/path=<path to the folder with YARA files>` não foi 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 uma pasta com os ficheiros YARA que deseja utilizar para a verificação. Argumento obrigatório se o valor `<full path to the YARA file>` não foi especificado. Exemplo: `/path=C:\Users\Admin\Desktop\YARA`

Definições avançadas	
`/fastScan=<on|off>`	Verificação rápida YARA. Para cada objeto, a aplicação regista uma ocorrência do indicador detetado. A aplicação também oculta duplicados de indicadores detetados no registo. A Verificação rápida YARA permite verificar ficheiros grandes mais rapidamente. Se esta definição não for especificada, a aplicação efetua uma verificação YARA padrão. Neste modo, a aplicação regista os duplicados dos indicadores detetados.
`/maxRules=<maximum number of scan rules>`	Limite do número de regras únicas acionadas que faz com que a aplicação interrompa a verificação YARA quando atingida. Se o valor desta definição não for especificado ou se `0` for especificado, a aplicação efetua a verificação YARA sem limitações.
`/timeOut=<stop scan after the specified time in seconds>`	Quanto tempo uma verificação YARA pode demorar, em segundos. Quando este tempo acaba, a aplicação interrompe a verificação YARA. Se o valor desta definição não for especificado ou se `0` for especificado, a aplicação efetua a verificação YARA sem limitações.
`/recursive=<on|off>`	Este argumento inicia uma verificação recursiva de subpastas dentro da Verificação Personalizada `/scanFolders`.
`/scanFolders=<list of folders to be scanned>`	Este argumento inicia uma verificação YARA dos ficheiros na lista de pastas especificada. Pode especificar vários valores separados por espaços. O Kaspersky Endpoint Security suporta os caracteres `*` e `?` ao introduzir uma máscara de caminho da pasta. Se esta definição não for especificada, a aplicação executa uma verificação YARA de todos os discos locais, exceto partilhas de rede, unidades na nuvem e suportes amovíveis.
`/scanMemory=<on|off>`	Verificar a memória de todos os processos em execução.
`/scanProcess=<process name>`	Verificar a memória somente em busca de processos especificados. Especifique os caminhos completos, separados por espaços, para os ficheiros executáveis dos processos. Também pode usar os caracteres `*` e `?` para inserir uma máscara.
`/maxSize=<file size in bytes>`	Limite o tamanho do ficheiro para a verificação YARA. A aplicação ignora os ficheiros maiores.
`/includes=<list of objects to be scanned>>`	Editar o âmbito de verificação. Pode especificar vários valores separados por espaços. Estão disponíveis as seguintes valores: • Nome do ficheiro • Estensão do ficheiro O âmbito de verificação tem de ser especificado com o parâmetro `/scanFolders`. Exemplo: `/scanFolders C:\*.* /includes=*.exe *.dll` – a aplicação verifica todos os ficheiros com as extensões .EXE e .DLL no disco C.
`/excludes=<list of objects to be scanned>`	Excluir ficheiros da verificação do YARA. Pode especificar vários valores separados por espaços. Estão disponíveis as seguintes valores: • Caminho do ficheiro • Máscara do caminho do ficheiro As exclusões têm de ser especificadas com o parâmetro `/scanFolders`. Exemplo: `/scanFolders C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` – a aplicação ignora o ficheiro readme.txt, todos os ficheiros da pasta C:\trusted e todos os ficheiros com a extensão .XML na pasta raiz do disco C.
`/scanAutoruns=<on|off>`	Verificação YARA de objetos de ponto de execução automática.
`/excludeAutoruns=<list of autorun point areas to skip>`	Excluir os objetos de ponto de execução automática do âmbito da verificação. Especifique os caminhos completos, separados por espaços, para os ficheiros executáveis dos processos. Também pode usar os caracteres `*` e `?` para inserir uma máscara.
`/logFolder=<path to the folder for saving the scan results in a TXT file>`	Se indicar um caminho para uma pasta, a aplicação guarda os resultados da verificação nesse caminho, num ficheiro com o nome yara_<nome do computador>_<hora de conclusão da verificação>.txt. Se indicar o caminho para um ficheiro TXT específico, a aplicação guarda os resultados da verificação nesse ficheiro. Por exemplo, `/logFolder=C:\test` ou `/logFolder=C:\test\abc.txt`. Os resultados da verificação são exibidos na linha de comandos, independentemente de a opção `/logFolder` ter sido especificada.

Valores de retorno do comando:

- `-1` significa que o comando não suportado pela versão do Kaspersky Endpoint Agent instalada no computador.
- `0` significa que o comando foi executado com êxito.
- `1` significa que um argumento obrigatório não foi transmitido ao comando.
- `2` significa que ocorreu um erro geral.
- `4` significa que houve um erro de sintaxe.
- `5` significa que um ou mais ficheiros com regras YARA especificadas no parâmetro não foram encontrados.

Se o comando for executado com êxito (valor de retorno `0`) e tiverem sido detetados indicadores de comprometimento ao longo do caminho, o Kaspersky Endpoint Security envia as seguintes informações sobre os resultados da tarefa para a command line:

`Started at <time>` `Finished at <time>`	Hora de início e hora de término de uma verificação.
`Host name: <computer name>`	O nome do computador no qual o objeto foi detetado.
`Result: <error>`	Código de erro para o erro que ocorreu durante a execução da tarefa. Se não houver erros, a aplicação gera a seguinte saída: `0x00000000`.
`Comment: <comment text>`	Descrição do erro para o erro que ocorreu durante a execução da tarefa. Por exemplo, `Operation timeout`.
`Object Name:` ou `Process:` (ao verificar a memória do processo)	O nome do objeto ou processo que acionou a regra YARA.
`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>`
	Foram encontradas correspondências dentro do objeto que atendem às condições da regra YARA:
	• Deslocamento na memória do processo ou no ficheiro onde foi detetada uma correspondência (`Offset`).
	• O nome da cadeia correspondente na regra YARA (`String name`).
	• A cadeia correspondente na memória do processo ou no ficheiro (`String data`).

TELEMETRYFILTERS. Filtrar eventos a serem enviados para o KUMA

Por predefinição, o envio de eventos para o servidor KUMA está desativado. Para garantir que o KUMA funcione corretamente, tem de ativar o envio de dados de telemetria. Pode selecionar uma fonte do evento entre os registos padrão: *Application*, *Security* ou *System*. Para melhorar o desempenho e otimizar a transmissão de dados para o servidor KUMA, pode adicionar ou excluir manualmente eventos individuais da telemetria. Por exemplo, pode excluir eventos Sysmon.

Pode exportar a lista de exclusões para um ficheiro JSON a partir da linha de comandos.

Se o comando tiver apenas o nome do ficheiro para o qual pretende exportar as definições, a aplicação coloca o ficheiro da seguinte forma:

- Se o caminho para avp.com for adicionado à variável do sistema %PATH%, a aplicação coloca o ficheiro na pasta `C:\Windows\SysWOW64`.
- Se executar o comando a partir da pasta de instalação da aplicação, a exportação irá falhar porque a auto-proteção da aplicação bloqueia a criação de um novo ficheiro na pasta da aplicação. Para exportar as definições da aplicação para um ficheiro, introduza o caminho do ficheiro.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com TELEMETRYFILTERS /export <file name>
```

```
avp.com TELEMETRYFILTERS /import <file name>
```

Operação	
`export`	Exportar filtros de eventos para serem enviados ao KUMA.
`import`	Importar filtros de eventos para serem enviados ao KUMA. Se as regras de filtragem de eventos já existirem no computador, o Kaspersky Endpoint Security irá substitui-las durante a importação.

Ficheiro para exportar ou importar	
`<file name>`	Nome do ficheiro com filtros de eventos a ser enviado ao KUMA. Também pode introduzir o caminho do ficheiro. Pode exportar filtros para enviar ao KUMA para um ficheiro JSON.

Comandos de gestão do Light Agent

Pode gerir a aplicação no modo Light Agent para proteger ambientes virtuais na linha de comandos. Pode gerir a aplicação no modo Light Agent se não for possível a gestão utilizando a Consola do Kaspersky Security Center. Pode ver a lista de comandos para gerir a aplicação, executando o comando `HELP`. Para ler sobre a sintaxe de um comando específico, digite `HELP <command>`.

Para gerir a aplicação no modo Light Agent a partir da linha de comandos:

1. Execute o interpretador de linha de comando (cmd.exe) como administrador.
2. Vá para a pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.
3. Utilize o seguinte modelo para executar o comando:

   ```
   avp.com <command> [options]
   ```

   Como resultado, o Kaspersky Endpoint Security executará o comando.

A aplicação instalada no modo Light Agent suporta quase todos os Comandos AVP da aplicação instalada no modo Padrão. No modo Light Agent, as tarefas de atualização da base de dados antivírus e as tarefas de gestão de chaves de licença são limitadas.

KSVLAINFO. Determinar o modo Light Agent

A determinar o modo Light Agent.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com KSVLAINFO
```

O comando envia as seguintes informações para a consola:

- O modo Light Agent para proteger ambientes virtuais: ativado ou desativado.

  Se o modo Light Agent estiver ativado, a aplicação será usada como parte da solução 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 o reinício da máquina virtual protegida não serão instaladas em máquinas virtuais não persistentes. Ao receber atualizações que exigem um reinício, o Light Agent instalado numa máquina virtual não persistente envia uma mensagem ao Kaspersky Security Center informando que o modelo da máquina virtual protegida precisa de ser atualizado.

- Tipo de máquina virtual protegida: persistente ou não persistente.

- Função da máquina virtual protegida na infraestrutura virtual: servidor ou estação de trabalho.

- Identificador: UUID.

VIISINFO. Estado da ligação do Light Agent ao Servidor de Integração

A visualizar informações sobre a ligação do Light Agent ao Servidor de Integração.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com VIISINFO
```

O comando envia as seguintes informações para a consola:

- Endereço e porta do Servidor de Integração ao qual o Light Agent está ligado.
- Estado da ligação do Servidor de Integração.
- Data e hora da última ligação do Light Agent ao Servidor de Integração.

SVMINFO. Estado da ligação do Light Agent ao Servidor de Proteção

A visualizar informações sobre a ligação do Light Agent ao Servidor de Proteção.

Para executar o comando, aceda à pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado. Também pode adicionar o caminho do ficheiro executável à variável de sistema %PATH% e executar o comando sem navegar para a pasta da aplicação.

Sintaxe de comando

```
avp.com SVMINFO
```

O comando envia as seguintes informações para a consola:

- Endereço do SVM ao qual o Light Agent está ligado e a localização da SVM na infraestrutura virtual em relação ao Light Agent: local ou não local.
- Método de descoberta de SVM que o Light Agent usa: usando um Servidor de Integração ou uma lista personalizada de endereços SVM.
- Lista de endereços SVM se a lista de endereços SVM for selecionada como o método de descoberta de SVM.
- Etiqueta para ligar o Light Agent à SVM.
- Algoritmo de seleção de SVM: padrão ou alargado. Se o algoritmo de seleção de SVM alargado estiver a ser usado, o tipo de caminho da SVM na infraestrutura virtual também será exibido.
- Estado da proteção da ligação entre o Light Agent e o Servidor de Proteção.

Códigos de erro

Podem ocorrer erros ao trabalhar com a aplicação através da command line. Quando ocorrem erros, o Kaspersky Endpoint Security apresenta uma mensagem de erro, por exemplo, `Error: Cannot start task 'EntAppControl'`. O Kaspersky Endpoint Security também pode apresentar informações adicionais sob a forma de um código, por exemplo, `error=8947906D` (consulte a tabela abaixo).

Código de erro	Descrição
09479001	Esta chave já está a ser utilizada
0947901D	A licença expirou. Não é possível atualizar a base de dados
89479002	Chave não encontrada
89479003	A assinatura digital está em falta ou corrompida
89479004	Os dados estão corrompidos
89479005	O ficheiro-chave está corrompido
89479006	A licença expirou
89479007	O ficheiro-chave não foi especificado
89479008	Ficheiro-chave inválido
89479009	Não foi possível guardar os dados
8947900A	Não foi possível ler os dados
8947900B	Erro E/S
8947900C	Bases de dados não encontradas
8947900E	A biblioteca de licenciamento não está carregada
8947900F	Bases de dados corrompidas ou atualizadas manualmente
89479010	As bases de dados estão corrompidas
89479011	Não é possível utilizar um ficheiro-chave inválido para adicionar uma chave de reserva
89479012	Erro do sistema
89479013	Lista de bloqueio de chaves corrompida
89479014	A assinatura do ficheiro não corresponde à assinatura digital da Kaspersky
89479015	Não é possível utilizar uma chave para licença de avaliação como uma chave para licença comercial
89479016	A licença para testes beta é necessária para utilizar a versão beta da aplicação
89479017	O ficheiro-chave não é compatível com esta aplicação. Não é possível ativar o Kaspersky Endpoint Security for Windows com um ficheiro-chave de outra aplicação. Verifique a aplicação instalada
89479018	Chave da licença bloqueada pelo Kaspersky
89479019	A aplicação já foi utilizada com uma licença de avaliação. Não é possível adicionar uma chave de licença de avaliação novamente
8947901A	O ficheiro-chave está corrompido
8947901B	A assinatura digital está em falta, 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 de utilização do ficheiro-chave não é válida. Verifique a data do sistema
8947901F	Não é possível adicionar uma chave para a licença de avaliação: outra chave de licença de avaliação já está ativa
89479020	A lista de bloqueio de chaves está corrompida ou em falta
89479021	Descrição da atualização em falta ou corrompida
89479022	A chave não é adequada para esta aplicação
89479023	Não é possível utilizar um ficheiro-chave inválido para adicionar uma chave de reserva
89479025	Erro ao enviar o pedido de ativação ao servidor. Motivos possíveis: erro de ligação à Internet ou problemas temporários no servidor de ativação. Tente ativar a aplicação mais tarde (dentro de 1-2 horas) com o código de ativação. Se o erro persistir, contacte o seu fornecedor de Internet
89479026	O pedido contém código de ativação incorreto
89479027	Não é possível obter o estado da resposta

Código de erro	Descrição
89479028	Ocorreu um erro ao guardar o ficheiro temporário
89479029	Foi introduzido um código de ativação incorreto ou o computador tem definida uma data de sistema não válida. Verifique a data do sistema do computador
8947902A	A chave não é compatível com esta aplicação ou a licença expirou
8947902B	Falha ao receber o ficheiro-chave. Foi introduzido um código de ativação incorreto
8947902C	O servidor de ativação devolveu erro 400
8947902D	O servidor de ativação devolveu erro 401
8947902E	O servidor de ativação devolveu erro 403
8947902F	O recurso necessário não está disponível no servidor de ativação. O servidor de ativação devolveu o erro 404. Verifique as definições de ligação à Internet
89479030	O servidor de ativação devolveu erro 405
89479031	O servidor de ativação devolveu erro 406
89479032	Autenticação de proxy requerida. Verifique as definições de rede
89479033	O pedido excedeu o tempo limite
89479034	O servidor de ativação devolveu erro 409
89479035	O recurso necessário não está disponível no servidor de ativação. O servidor de ativação devolveu o erro 410. Verifique as definições de ligação à Internet
89479036	O servidor de ativação devolveu erro 411
89479037	O servidor de ativação devolveu erro 412
89479038	O servidor de ativação devolveu erro 413
89479039	O servidor de ativação devolveu erro 414
8947903A	O servidor de ativação devolveu erro 415
8947903C	Erro interno do servidor
8947903D	Funcionalidade não suportada
8947903E	Resposta de porta de ligação não válida. Verifique as definições de rede
8947903F	Recurso temporariamente indisponível
89479040	Excedido o tempo limite de resposta da porta de ligação. Verifique as definições de rede
89479041	O protocolo não é suportado pelo servidor
89479043	Erro de HTTP desconhecido
89479044	ID de recurso não válido
89479046	URL não válido
89479047	Pasta de destino inválida
89479048	Erro na distribuição da memória
89479049	Ocorreu um erro ao converter os parâmetros para a sequência ANSI (URL, pasta, agente)
8947904A	Ocorreu um erro ao criar uma linha de execução de trabalho
8947904B	A linha de execução de trabalho já está em execução
8947904C	A linha de execução de trabalho não está em execução
8947904D	Ficheiro-chave não encontrado no servidor de ativação
8947904E	A chave está bloqueada
8947904F	Erro interno no servidor de ativação
89479050	Não existem dados suficientes no pedido de ativação

Código de erro	Descrição
89479053	A licença que corresponde à chave adicionada já expirou
89479054	Data de sistema não válida no computador. Verifique o valor da data do sistema
89479055	A licença de avaliação expirou
89479056	O período de ativação da aplicação expirou
89479057	O limite de ativações da aplicação foi excedido para o código especificado
89479058	Processo de ativação concluído com erro do sistema
89479059	Não é possível utilizar uma chave para licença de avaliação como uma chave para licença comercial
8947905C	É necessário um código de ativação
89479062	Não é possível ligar ao servidor de ativação
89479064	O servidor de ativação não está disponível. Verifique as definições de ligação à Internet e tente ativar novamente
89479065	A licença expirou
89479066	Não é possível substituir a chave ativa por uma chave expirada
89479067	Não é possível adicionar uma chave de reserva se a licença correspondente expirar antes da licença atual
89479068	Chave de subscrição atualizada em falta
8947906A	Código de ativação inválido
8947906B	Chave já ativa
8947906C	Os tipos de licença que correspondem às chaves ativas e de reserva não correspondem
8947906D	Componente não suportado pela licença
8947906E	Não é possível adicionar a chave de subscrição como uma chave de reserva
89479213	Erro genérico de camada de transporte
89479214	Falhou a ligação ao servidor de ativação
89479215	Formato de endereço da Internet inválido
89479216	Falha ao converter o endereço de servidor de proxy
89479217	Falha ao converter o endereço de servidor Verifique as definições de ligação à Internet
89479218	Falha na tentativa de ligação ao servidor
89479219	Acesso recusado remotamente
8947921A	A operação excedeu o tempo limite
8947921B	Erro ao enviar pedido HTTP
8947921C	Erro de ligação SSL
8947921D	Operação interrompida por chamada de retorno
8947921E	Demasiados redirecionamentos
8947921F	Falha na verificação do destinatário
89479220	Resposta vazia do servidor
89479221	Erro ao enviar dados
89479222	Erro ao receber dados
89479223	Problema relacionado com o certificado SSL
89479224	Problema relacionado com a encriptação SSL
89479225	Problema relacionado com o centro de certificação SSL
89479226	Conteúdos do pacote de rede inválidos

Código de erro	Descrição
89479227	Acesso à conta recusado
89479228	Ficheiro de certificado SSL não válido
89479229	Não é possível terminar a ligação SSL
8947922A	Erro recorrente
8947922B	Ficheiro não válido com certificados revogados
8947922C	Erro de pedido de certificado SSL
89479401	Erro de servidor desconhecido
89479402	Erro interno do servidor
89479403	Não existe uma chave disponível para o código de ativação introduzido
89479404	Chave ativa bloqueada
89479405	Parâmetros requeridos do pedido de ativação em falta
89479406	Password ou número de cliente inválido
89479407	Código de ativação inválido
89479408	O código de ativação não é compatível com esta aplicação. Não é possível ativar o Kaspersky Endpoint Security for Windows com um código de ativação de outra aplicação. Verifique a aplicação instalada
89479409	É necessário um código de ativação
8947940B	O período de ativação expirou
8947940C	O número de ativações com este código foi excedido
8947940D	Formato inválido do ID de pedido
8947940E	O código de ativação já está a ser utilizado
8947940F	Falha ao renovar o código de ativação
89479410	O código de ativação é inválido para esta região
89479411	Este código de ativação não pode ser utilizado para esta localização da aplicação
89479412	O código de ativação destina-se à nova versão desta aplicação. Obtenha um código de ativação diferente para ativar a versão instalada da aplicação
89479413	O servidor de ativação devolveu o erro 643
89479414	O servidor de ativação devolveu o erro 644
89479415	O servidor de ativação devolveu o erro 645
89479416	O servidor de ativação devolveu o erro 646
89479417	É requerida a versão 1.0 do servidor de ativação
89479418	Formato incorreto do código de ativação
89479419	A hora do computador não está sincronizada com a hora do servidor de ativação
8947941A	Versão incorreta da aplicação
8947941B	A subscrição expirou
8947941C	Número de ativações excedido
8947941D	Assinatura de senha não válida
8947941E	São necessários dados adicionais
8947941F	Falha na verificação de dados
89479420	Subscrição inativa
89479421	Servidor de ativação em manutenção

Código de erro	Descrição
89479501	Erro inesperado
89479502	Transferido parâmetro não válido. Por exemplo, uma lista vazia de endereços de servidores de ativação
89479503	Código de ativação inválido (hash inválido)
89479504	ID de utilizador não válido
89479505	Password de utilizador não válida
89479506	Resposta não válida do servidor de ativação
89479507	O pedido de ativação foi interrompido
89479509	O servidor de ativação devolveu uma lista de reencaminhamento vazia

Anexo. Perfis da aplicação

Um *Perfil* é um componente, tarefa ou funcionalidade do Kaspersky Endpoint Security. Os perfis são usados para gerir a aplicação através da command line. Pode utilizar os perfis para executar os comandos `START`, `STOP`, `STATUS`, `STATISTICS` e `EXPORT`. Utilizando os perfis, pode configurar as definições da aplicação (por exemplo, `STOP DeviceControl`) ou executar tarefas (por exemplo, `START Scan_My_Computer`).

Estão disponíveis as seguintes perfis:

- `AdaptiveAnomaliesControl` – Controlo de Anomalias Adaptativo
- `AMSI` – Proteção AMSI.
- `AntiCryptor`
- `BehaviorDetection` – Deteção de comportamento.
- `DeviceControl` – Controlo de Dispositivos
- `EntAppControl` – Controlo das Aplicações
- `File_Monitoring` ou `FM` – Proteção contra ameaças de ficheiros
- `Firewall` ou `FW` – Firewall
- `HIPS` – Prevenção contra invasões.
- `IDS` – Proteção contra ameaças de Rede
- `IntegrityCheck` – Verificação de integridade
- `LogInspector` – Inspeção de Registo
- `Mail_Monitoring` ou `EM` – Proteção contra ameaças de correio
- `Rollback` – Reverter atualização (o perfil não pode ser aplicado se a aplicação estiver instalada no modo Light Agent)
- `Scan_ContextScan` – Verificar a partir do menu de contexto

- `Scan_IdleScan` – Verificação de fundo
- `Scan_Memory` – Verificação da memória do kernel
- `Scan_My_Computer` – Verificação Completa
- `Scan_Objects` – Verificação Personalizada
- `Scan_Qscan` - Verificar objetos carregados no arranque do sistema operativo
- `Scan_Removable_Drive` – Verificação das unidades amovíveis
- `Scan_Startup` ou `STARTUP` – Verificação de Áreas Críticas
- `Updater` – Atualização (o perfil não pode ser aplicado se a aplicação estiver instalada no modo Light Agent)
- `Web_Monitoring` ou `WM` – Proteção contra ameaças da Web
- `WebControl` – Controlo de Internet

O Kaspersky Endpoint Security suporta também perfis de serviço. Podem ser necessários perfis de serviço quando contactar o Suporte técnico da Kaspersky.

Gerir a aplicação com API REST

O Kaspersky Endpoint Security permite configurar as definições da aplicação, executar uma verificação, atualizar as bases de dados antivírus e executar outras tarefas com soluções de terceiros. O Kaspersky Endpoint Security fornece uma API para esta finalidade. A API REST do Kaspersky Endpoint Security opera sobre HTTP e consiste num conjunto de métodos de solicitação / resposta. Por outras palavras, pode gerir o Kaspersky Endpoint Security com uma solução de terceiros, e não com a interface da aplicação local ou a Consola de Administração do Kaspersky Security Center.

Para começar a utilizar a API REST, é necessário instalar o Kaspersky Endpoint Security com suporte para API REST. O cliente REST e o Kaspersky Endpoint Security devem estar instalados no mesmo computador.

Para garantir uma interação segura entre o Kaspersky Endpoint Security e o cliente REST:

- Configure a proteção de acessos não autorizados do cliente REST de acordo com as recomendações do programador para clientes REST. Configure a proteção de pastas do cliente REST contra gravação com a ajuda da lista de controlo de acesso discricionário — DACL.
- Para executar o cliente REST, utilize uma conta separada com direitos de administrador. Recuse o início de sessão interativo no sistema para esta conta.

A aplicação é gerida com API REST em http://127.0.0.1 ou http://localhost. Não é possível gerir remotamente o Kaspersky Endpoint Security com API REST.

ABRA A DOCUMENTAÇÃO DA API REST

Instalar a aplicação com API REST

Para gerir a aplicação com API REST, deve instalar o Kaspersky Endpoint Security com suporte para API REST. Se gerir o Kaspersky Endpoint Security com API REST, não poderá gerir a aplicação com o Kaspersky Security Center.

A preparar a instalação da aplicação com suporte para API REST

A interação segura do Kaspersky Endpoint Security com o cliente REST requer a configuração da identificação de solicitação. Para tal, deve instalar um certificado e, posteriormente, assinar o payload de cada solicitação.

Para criar um certificado, pode utilizar, por exemplo, OpenSSL.

Exemplo:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Utilize o algoritmo de encriptação RSA com um comprimento de chave de 2048 bits ou mais.

Deste modo, obterá um certificado `cert.pem` e uma chave privada `key.pem`.

Instalar a aplicação com suporte para API REST

Para instalar o Kaspersky Endpoint Security com suporte para API REST:

1. Execute o interpretador de linha de comando (cmd.exe) como 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 definições:

   - `RESTAPI=1`
   - `RESTAPI_User=<user name>`

     Nome de utilizador para gerir a aplicação com API REST. Introduza o nome de utilizador no formato `<DOMAIN>\<UserName>` (por exemplo, `RESTAPI_User=COMPANY\Administrator`). Só pode gerir a aplicação com API REST nesta conta. Só pode selecionar um utilizador para trabalhar com API REST.
   - `RESTAPI_Port=<port>`

     Porta usada para gerir a aplicação com API REST. A porta 6782 é usada por defeito. 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`)

     Pode instalar o certificado após instalar a aplicação ou atualizar o certificado após a expiração do certificado.

     Como instalar um certificado para identificação de solicitação API REST

     1. Desativar a Autodefesa do Kaspersky Endpoint Security

        O mecanismo de autodefesa impede a alteração ou a eliminação dos ficheiros de aplicações no disco rígido, dos processos na memória e de entradas no registo do sistema.
     2. Aceda à chave do registo que contém as definições da API REST:
        `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestAp`
     3. Introduza o caminho para o certificado, por exemplo, `Certificate = C:\Folder\cert.pem`.
     4. Ativar a Autodefesa do Kaspersky Endpoint Security
     5. Reinicie a aplicação.
   - `AdminKitConnector=1`

     Gestão de aplicações com sistemas de administração. A gestão é permitido por definição.

   Também pode usar o ficheiro setup.ini para configurar as definições para trabalhar com 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, poderá gerir a aplicação com API REST. Para verificar esta operação, abra a documentação da API REST com o pedido GET.

Exemplo:
```
GET http://localhost:6782/kes/v1/api-docs
```

Se tiver instalado a aplicação com suporte para API REST, o Kaspersky Endpoint Security cria automaticamente uma regra de permissão nas definições da Consola Web para o acesso aos recursos da Internet (*Regra de serviço para API REST*). Esta regra é necessária para permitir ao cliente REST acesso ao Kaspersky Endpoint Security em qualquer altura. Por exemplo, se tiver acesso do utilizador restrito a recursos da Internet, tal não irá afetar a gestão da aplicação através da API REST. É recomendado que não elimine a regra ou altere as definições da *Regra de serviço para API REST*. Se eliminar a regra, o Kaspersky Endpoint Security irá restaurá-la após reiniciar a aplicação.

Trabalhar com API

Não é possível restringir o acesso à aplicação com API REST usando a Proteção por password. Por exemplo, não é possível impedir que um utilizador desative a proteção com API REST. Pode configurar a Proteção por password com API REST e restringir o acesso dos utilizadores à aplicação através da interface local.

Para gerir a aplicação com API REST, é necessário executar o cliente REST na conta especificada quando instalar a aplicação com suporte de API REST. Só pode selecionar um utilizador para trabalhar com API REST.

ABRA A DOCUMENTAÇÃO DA API REST

A gestão da aplicação com API REST consiste nos seguintes passos:

1. Obtenha os valores atuais das definições da aplicação. Para tal, envie um pedido GET.

   Exemplo:
   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```

2. A aplicação enviará uma resposta com a estrutura e os valores das definições. O Kaspersky Endpoint Security suporta os formatos XML e JSON.

   Exemplo:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   "enabled": true
   }
   ```

3. Editar as definições da aplicação. Use a estrutura das definições recebidas em resposta ao pedido GET.

   Exemplo:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": false,
   "enabled": true
   }
   ```

4. Guarde as definições da aplicação (o payload) em 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
   ```

Deste modo, obtém um ficheiro assinado com o payload do pedido (`signed_payload.pem`).

6. Editar as definições da aplicação. Para tal, envie um pedido POST e anexe o ficheiro assinado com o payload do pedido (`signed_payload.pem`).

A aplicação aplica as novas configurações e envia uma resposta com os resultados da configuração da aplicação (a resposta pode estar vazia). Pode verificar se as configurações são atualizadas utilizando um pedido GET.

Fontes de informação sobre a aplicação

Esta secção descreve as fontes de informação sobre a aplicação.

Pode escolher a fonte de informação mais conveniente, dependendo da importância e da urgência do seu assunto.

Página do Kaspersky Endpoint Security no site da Kaspersky

Na página do Kaspersky Endpoint Security, pode ver informações gerais sobre a aplicação e as suas funções e características.

A página do Kaspersky Endpoint Security contém um link para a loja online. Na mesma, pode comprar ou renovar a aplicação.

Página do Kaspersky Endpoint Security na Base de Conhecimento

A Base de Conhecimento é uma secção do site de Suporte Técnico.

Na página do Kaspersky Endpoint Security na Base de Conhecimento, pode ler artigos que fornecem informações úteis, recomendações e respostas a perguntas frequentes sobre como comprar, instalar e utilizar a aplicação.

Os artigos da Base de Conhecimento podem responder a perguntas relacionadas não só com o Kaspersky Endpoint Security, mas também com outras aplicações da Kaspersky. Os artigos na Base de Conhecimento também podem conter notícias do Suporte Técnico.

Discussão das aplicações da Kaspersky no Fórum

Se a sua pergunta não requer uma resposta urgente, pode discuti-la com os especialistas Kaspersky e outros utilizadores no nosso Fórum.

No Fórum, pode ver os tópicos existentes, publicar os seus próprios comentários e criar novos tópicos de discussão.

Contactar o Suporte Técnico

Se não conseguir encontrar uma solução para o seu problema na documentação ou numa das fontes de informação sobre o Kaspersky Endpoint Security, recomendamos que contacte o Suporte Técnico. O Suporte Técnico irá responder às suas questões sobre a instalação e utilização do Kaspersky Endpoint Security.

A Kaspersky oferece suporte para o Kaspersky Endpoint Security durante o ciclo de vida da mesma (consulte a página relativa ao ciclo de vida da aplicação). Antes de contactar o Suporte Técnico, leia as regras relativas ao suporte técnico.

Pode contactar o Suporte Técnico através de uma das seguintes formas:

- Visitando o site de Suporte Técnico
- Enviando um pedido ao Suporte Técnico da Kaspersky através do portal Kaspersky CompanyAccount

Depois de informar o Suporte Técnico da Kaspersky sobre o seu problema, os técnicos poderão solicitar que crie um *ficheiro de rastreio*. O ficheiro de rastreio permite rastrear o processo de realizar comandos de aplicações passo a passo e determinar a etapa do funcionamento de uma aplicação na qual ocorre um erro.

Os especialistas do Suporte Técnico podem também solicitar informações adicionais sobre o sistema operativo, processos em execução no computador, relatórios detalhados sobre o funcionamento de componentes da aplicação.

Enquanto efetuam o diagnóstico, os especialistas do Suporte Técnico podem pedir-lhe para alterar definições da aplicação por:

- Ativar a funcionalidade que recebe informações de diagnóstico expandidas.
- Configurar componentes individuais da aplicação, alterando definições especiais que não estão acessíveis na interface de utilizador padrão.
- Alterar as definições para armazenamento das informações de diagnóstico.
- Configurar a interceção e registo de tráfego de rede.

Os especialistas de Suporte Técnico irão fornecer todas as informações necessárias para executar estes passos (descrevendo a sequência de passos, definições a alterar, ficheiros de configuração, scripts, funcionalidades de command line adicionais, módulos de depuração, utilitários específicos, etc.) e irão informá-lo sobre o âmbito dos dados utilizados para depuração. As informações de diagnóstico expandido são guardadas no computador do utilizador. Os dados não são transmitidos automaticamente para a Kaspersky.

As operações indicadas acima devem ser executadas apenas sob a supervisão dos especialistas de Suporte Técnico, seguindo as suas instruções. Alterar as definições da aplicação por iniciativa própria de formas diferentes das descritas na Ajuda online ou nas recomendações do Suporte Técnico pode tornar o sistema operativo mais lento ou causar falhas, reduzindo o nível de proteção do seu computador e afetando a disponibilidade e integridade das informações a serem processadas.

Conteúdos e armazenamento de ficheiros de rastreio

É pessoalmente responsável pela segurança dos dados armazenados no seu computador, especialmente por monitorizar e restringir o acesso aos dados até que sejam enviados para a Kaspersky.

Os ficheiros de rastreio são armazenados no computador desde que a aplicação esteja a ser utilizada, sendo permanentemente eliminados quando a aplicação é removida.

Os ficheiros de rastreio, exceto os ficheiros de rastreio do Agente de Autenticação, são armazenados na pasta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`.

Os ficheiros de rastreio são designados da seguinte maneira: `KES<14.2_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`.

Pode ver os dados guardados nos ficheiros de rastreio.

Todos os ficheiros de rastreio contêm os dados comuns seguintes:

- Hora do evento
- Número da linha de execução

  O ficheiro de rastreio do Agente de Autenticação não contém esta informação.

- O componente da aplicação que causou o evento
- O nível de gravidade do evento (evento informativo, de aviso, crítico, erro)
- Uma descrição do evento que envolve a execução do comando por um componente da aplicação e o resultado da execução deste comando.

Conteúdos dos ficheiros de rastreio SRV.log, GUI.log e ALL.log

Os ficheiros de rastreio `SRV.log`, `GUI.log` e `ALL.log` podem armazenar a informação seguinte além de dados gerais:

- Dados pessoais, incluindo o apelido, nome próprio e nome do meio, se tais dados estiverem incluídos no caminho para os ficheiros no computador local.
- Dados no hardware instalado no computador (como dados de firmware BIOS/UEFI). Estes dados são gravados em ficheiros de rastreio ao executar a Encriptação de disco Kaspersky.
- O nome de utilizador e a password se forem transmitidos abertamente. Estes dados podem ser gravados nos ficheiros de rastreio durante a verificação de tráfego da Internet.
- O nome de utilizador e a password se estiverem incluídos nos cabeçalhos HTTP.

- O nome da conta Microsoft Windows se o nome da conta estiver incluído num nome de ficheiro.
- O seu endereço de e-mail ou um endereço web com o nome da conta e password se estiverem incluídas no nome do objeto detetado.
- Sites que visita e os redirecionamentos desses sites. Estes dados são gravados em ficheiros de rastreio quando a aplicação verifica os sites.
- Endereço de servidor proxy, nome do computador, porta, endereço IP e nome de utilizador utilizado para iniciar sessão no servidor proxy. Estes dados são gravados em ficheiros de rastreio quando a aplicação utiliza um servidor proxy.
- Endereços IP remotos aos quais o computador estabelece ligações.
- Assunto da mensagem, ID, nome do remetente e endereço da página da Web do remetente da mensagem numa rede social. Estes dados são gravados em ficheiros de rastreio se o componente Controlo de Internet estiver ativado.
- Dados de tráfego de rede. Estes dados são gravados em ficheiros de rastreio se os componentes de monitorização de tráfego estiverem ativados (como o Controlo de Internet).
- Dados recebidos dos servidores Kaspersky (como a versão das bases de dados antivírus).
- Estado dos componentes do Kaspersky Endpoint Security e os seus dados operacionais.
- Dados sobre a atividade do utilizador na aplicação.
- Eventos do sistema operativo.

Conteúdos dos ficheiros de rastreio HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Além dos dados gerais, o ficheiro de rastreio `HST.log` contém informações sobre a execução de uma tarefa de atualização da base de dados e dos módulos da aplicação.

Além dos dados gerais, o ficheiro de rastreio `BL.log` contém informação sobre eventos que ocorrem durante o funcionamento da aplicação, bem como os dados necessários para solucionar os erros da aplicação. O ficheiro é criado se a aplicação for iniciada com o parâmetro avp.exe –bl.

Além dos dados gerais, o ficheiro de rastreio `Dumpwriter.log` contém informações do serviço necessárias para solucionar os erros que ocorrem quando o ficheiro dump da aplicação é gravado.

Além dos dados gerais, o ficheiro de rastreio `WD.log` contém informação sobre eventos que ocorrem durante o funcionamento do serviço avpsus, incluindo os eventos de atualização dos módulos da aplicação.

Além dos dados gerais, o ficheiro de rastreio `AVPCon.dll.log` contém informação sobre eventos que ocorrem durante o funcionamento do módulo de conectividade do Kaspersky Security Center.

Conteúdo dos ficheiros de rastreio do desempenho

Os ficheiros de rastreio do desempenho são designados da seguinte maneira: `KES<14.2_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl`.

Além dos dados gerais, os ficheiros de rastreio do desempenho contêm informações sobre a carga no processador, informações sobre o tempo de carga do sistema operativo e aplicações e informações sobre os processos em execução.

Conteúdo do ficheiro de rastreio do componente de Proteção AMSI

Além dos dados gerais, o ficheiro de rastreio do `AMSI.log` contém informação sobre os resultados da verificação executados um pedido de uma aplicação de terceiros.

Conteúdos de ficheiros de rastreio do componente de Proteção contra ameaças de correio

O ficheiro de rastreio `mcou.OUTLOOK.EXE.log` pode conter partes de mensagens de email, inclusive endereços de e-mail, além de dados gerais.

Conteúdos de ficheiros de rastreio do componente Verificar a partir do menu de contexto

O ficheiro de rastreio `shellex.dll.log` contém informações sobre a realização da tarefa de verificação e dados necessários para depurar a aplicação, além da informação geral.

Conteúdos dos ficheiros de rastreio do plug-in Web de aplicação

Os ficheiros de rastreio do plug-in Web da aplicação são armazenados no computador onde o Kaspersky Security Center Web Console é implementado, na pasta `Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs`.

Os ficheiros de rastreio do plug-in Web da aplicação têm os seguintes nomes: `logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log`. A Consola Web inicia os dados de gravação após a instalação e elimina os ficheiros de rastreio após a Consola Web ser removida.

Os ficheiros de rastreio dos plug-ins web da aplicação contêm as informações seguintes além dos dados gerais:

- Password do utilizador KLAdmin para desbloqueio da interface Kaspersky Endpoint Security (Proteção por password).
- Password temporária para desbloqueio da interface Kaspersky Endpoint Security (Proteção por password).

- Nome de utilizador e password para o servidor de e-mail SMTP.
- Nome de utilizador e password para o servidor proxy.
- Nome de utilizador e password para a tarefa *Alterar componentes da aplicação*.
- Credenciais de conta e caminhos especificados nas tarefas Kaspersky Endpoint Security e propriedades da política.

Conteúdos do ficheiro de rastreio do Agente de Autenticação

O ficheiro de rastreio do Agente de Autenticação é guardado na pasta System Volume Information e é designado da seguinte maneira: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Além dos dados gerais, o ficheiro de rastreio do Agente de Autenticação contém informação sobre o funcionamento do Agente de Autenticação e as ações executadas pelo utilizador com o Agente de Autenticação.

Rastreios da operação da aplicação

Os *rastreios da aplicação* são registos detalhados das ações executadas pela aplicação e das mensagens sobre eventos que ocorrem durante a operação da aplicação. Durante o processo de rastreio, a aplicação cria um conjunto de ficheiros com dados sobre o funcionamento de diferentes componentes da aplicação (por exemplo, SRV.log, WD.log e outros).

Os rastreios da aplicação devem ser realizados sob a supervisão do Suporte Técnico da Kaspersky.

Para criar um ficheiro de rastreio da aplicação:

1. Na janela principal da aplicação, clique no botão .
2. Na janela que abre, clique no botão **Ferramentas de suporte**.
3. Utilize o botão de alternar **Ativar rastreio das aplicações** para ativar ou desativar o rastreio de operação da aplicação.
4. Na lista pendente **Rastreio**, selecione um modo de rastreio de aplicação:
   - **Com limite de tamanho**. Guarde os rastreios num número limitado de conjuntos de ficheiros de tamanho limitado e substitua os ficheiros mais antigos quando o tamanho máximo for alcançado. Se este modo for selecionado, pode definir o número máximo de conjuntos de ficheiros para rotação e o tamanho máximo para cada conjunto de ficheiros.

     Por defeito, a aplicação guarda cinco conjuntos de ficheiros de rastreio. O tamanho de cada conjunto de ficheiros é de 3072 MB. Desta forma, são necessários 15 GB de espaço livre no disco para guardar os ficheiros de rastreio.
   - **Sem limites**. Guarde um ficheiro de rastreio (sem limite de tamanho).

5. Na lista pendente **Nível**, selecione o nível de rastreio:

   - **Normal** significa que o ficheiro de rastreio guarda mensagens sobre todos os erros e avisos, bem como informações sobre o funcionamento normal da aplicação (predefinição).
   - **Detalhado** significa que o ficheiro de rastreio guarda todas as informações sobre o funcionamento da aplicação.

   Estão disponíveis níveis de rastreio adicionais se gerir as definições de rastreio da aplicação na linha de comandos. Recomenda-se que clarifique qual o nível de rastreio necessário, junto de um especialista do Suporte Técnico. Se não tiver a orientação do Suporte Técnico, defina o nível de rastreio para **Normal**.

   Se o rastreio da aplicação tiver sido ativado na linha de comandos e tiver sido definido um nível de rastreio diferente de **Normal** ou **Detalhado**, a lista pendente **Nível** é definida para **Normal**.

6. Para interromper o processo de rastreio, regresse à janela **Ferramentas de suporte** e desative o rastreio.

Também pode criar ficheiros de rastreamento ao instalar a aplicação a partir da linha de comando, inclusivamente usando o ficheiro setup.ini.

Como resultado, são criados ficheiros de rastreio de funcionamento da aplicação na pasta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. Após a criação dos ficheiros de rastreio, envie os ficheiros para o Suporte Técnico da Kaspersky.

O Kaspersky Endpoint Security elimina automaticamente ficheiros de rastreio quando a aplicação é removida. Também pode eliminar os ficheiros manualmente. Para tal, deve desativar o rastreio e parar a aplicação.

Rastreios de desempenho da aplicação

O Kaspersky Endpoint Security permite-lhe receber informações sobre problemas operacionais do computador durante o uso da aplicação. Por exemplo, pode receber informações sobre atrasos na carga do sistema operativo após a instalação da aplicação. Para tal, o Kaspersky Endpoint Security cria ficheiros de rastreio de desempenho. *Os Rastreios de desempenho* referem-se ao registo das ações realizadas pela aplicação com o objetivo de diagnosticar problemas de desempenho do Kaspersky Endpoint Security. Para receber informações, o Kaspersky Endpoint Security utiliza o serviço ETW (Event Tracing for Windows). O Suporte Técnico da Kaspersky é responsável por diagnosticar problemas do Kaspersky Endpoint Security e estabelecer as razões desses problemas.

Os rastreios da aplicação devem ser realizados sob a supervisão do Suporte Técnico da Kaspersky.

Para criar um ficheiro de rastreio de desempenho:

1. Na janela principal da aplicação, clique no botão .
2. Na janela que abre, clique no botão **Ferramentas de suporte**.
3. Use o botão de alternar **Ativar rastreio de desempenho** para ativar ou desativar o rastreio do desempenho da aplicação.

4. Na lista pendente **Rastreio**, selecione um modo de rastreio de aplicação:

   - **Com limite de tamanho**. Guarde os rastreios num número limitado de ficheiros de tamanho limitado e substitua os ficheiros mais antigos quando o tamanho máximo for alcançado. Se este modo for selecionado, pode definir o tamanho máximo para cada ficheiro.

   - **Sem limites**. Guarde um ficheiro de rastreio (sem limite de tamanho).

5. Na lista pendente **Nível**, selecione o nível de rastreio:

   - **Superficial**. O Kaspersky Endpoint Security analisa os processos mais importantes do sistema operativo relacionados com o desempenho.

   - **Detalhado**. O Kaspersky Endpoint Security analisa todos os processos do sistema operativo relacionados com o desempenho.

6. Na lista pendente **Tipo de rastreio**, selecione o tipo de rastreio:

   - **Informação básica**. O Kaspersky Endpoint Security analisa processos enquanto o sistema operativo está em execução. Use este tipo de rastreio se um problema persistir após a carga do sistema operativo, como um problema em aceder à Internet no navegador.

   - **Ao reiniciar**. O Kaspersky Endpoint Security analisa processos apenas durante a carga do sistema operativo. O Kaspersky Endpoint Security interrompe o rastreio após a carga do sistema operativo. Use este tipo de rastreio se o problema estiver relacionado com a carga atrasada do sistema operativo.

7. Reinicie o computador e tente reproduzir o problema.

8. Para interromper o processo de rastreio, regresse à janela Ferramentas de suporte e desative o rastreio.

   Como resultado, é criado um ficheiro de rastreio de desempenho na pasta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. Após a criação do ficheiro de rastreio, envie o ficheiro para o Suporte Técnico da Kaspersky.

Gravação de descarga

Um ficheiro dump contém toda a informação sobre a memória funcional dos processos do Kaspersky Endpoint Security aquando da criação do ficheiro dump.

> Os ficheiros da descarga guardados podem conter dados confidenciais. Deve assegurar a segurança dos ficheiros da descarga para controlar o acesso aos dados.

Os ficheiros de descarga são armazenados no computador desde que a aplicação esteja a ser utilizada, sendo permanentemente eliminados quando a aplicação é removida. Os ficheiros de descarga são armazenados na pasta `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`.

Como ativar a gravação de descarga na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.

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

3. Na janela de política, selecione **Definições gerais** → **Definições da aplicação**.

4. No bloco **Informações de depuração**, clique no botão **Definições**.

5. Na janela que se abre, utilize a caixa de verificação **Ativar gravação de descarga** para ativar ou desativar a gravação de descarga da aplicação.

6. Guarde as suas alterações.

Como ativar a gravação de descarga na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management** → **Policies**.

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

   É apresentada a janela de propriedades da política.

3. Selecione o separador **Application settings**.

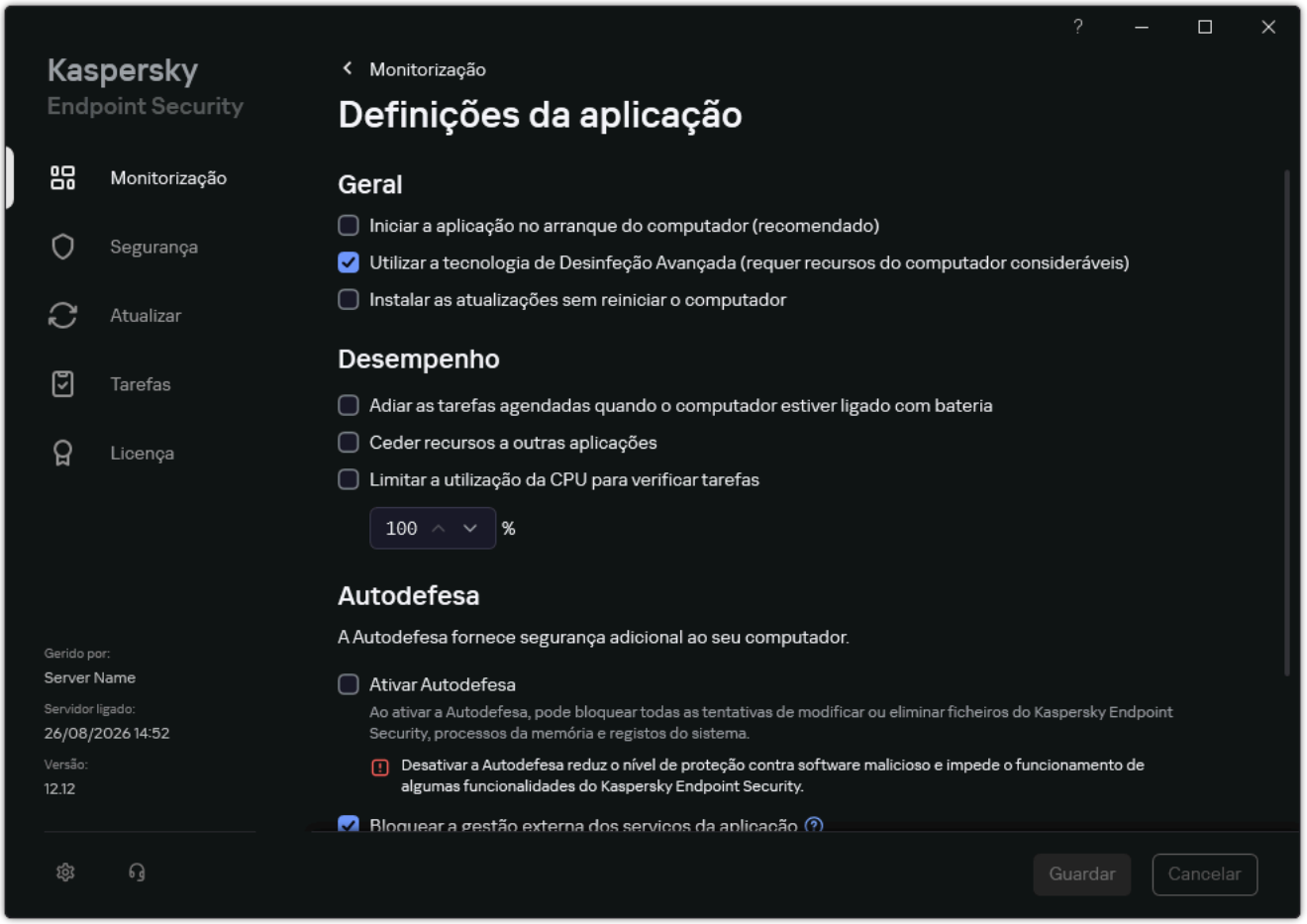
4. Aceda a **General Settings** → **Technical Support**.

5. No bloco **Debug information**, use a caixa de verificação **Dump writing ENABLED** para ativar ou desativar a gravação de descarga da aplicação.

6. Guarde as suas alterações.

Como ativar a gravação de descarga na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Definições da aplicação**.



Definições do Kaspersky Endpoint Security for Windows

3. No bloco **Informações de depuração**, use a caixa de verificação **Ativar gravação de descarga** para ativar ou desativar a gravação de descarga da aplicação.
4. Guarde as suas alterações.

Proteger ficheiros de descarga e ficheiros de rastreio

Os ficheiros de descarga e os ficheiros de rastreio contêm informações sobre o sistema operativo e também podem conter dados do utilizador. Para evitar o acesso não autorizado a estes dados, pode ativar a proteção de ficheiros de descarga e de rastreio.

Se a proteção de ficheiros de descarga e de rastreio estiver ativada, os ficheiros podem ser acedidos pelos seguintes utilizadores:

- Os ficheiros de rastreio podem ser acedidos pelo administrador do sistema e pelo administrador local, bem como pelo utilizador que ativou o registo de ficheiros de descarga e de rastreio.
- Os ficheiros de rastreio podem ser acedidos apenas pelo administrador do sistema e pelo administrador local.

Como ativar a proteção de ficheiros de descarga e de ficheiros de rastreio na Consola de Administração (MMC)

1. Na árvore da Consola de Administração do Kaspersky Security Center, selecione **Policies**.
2. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
3. Na janela de política, selecione **Definições gerais → Definições da aplicação**.
4. No bloco **Informações de depuração**, clique no botão **Definições**.
5. Na janela que se abre, clique no botão **Ativar proteção de ficheiros de descarga e de rastreio** para ativar ou desativar a proteção de ficheiros.
6. Guarde as suas alterações.

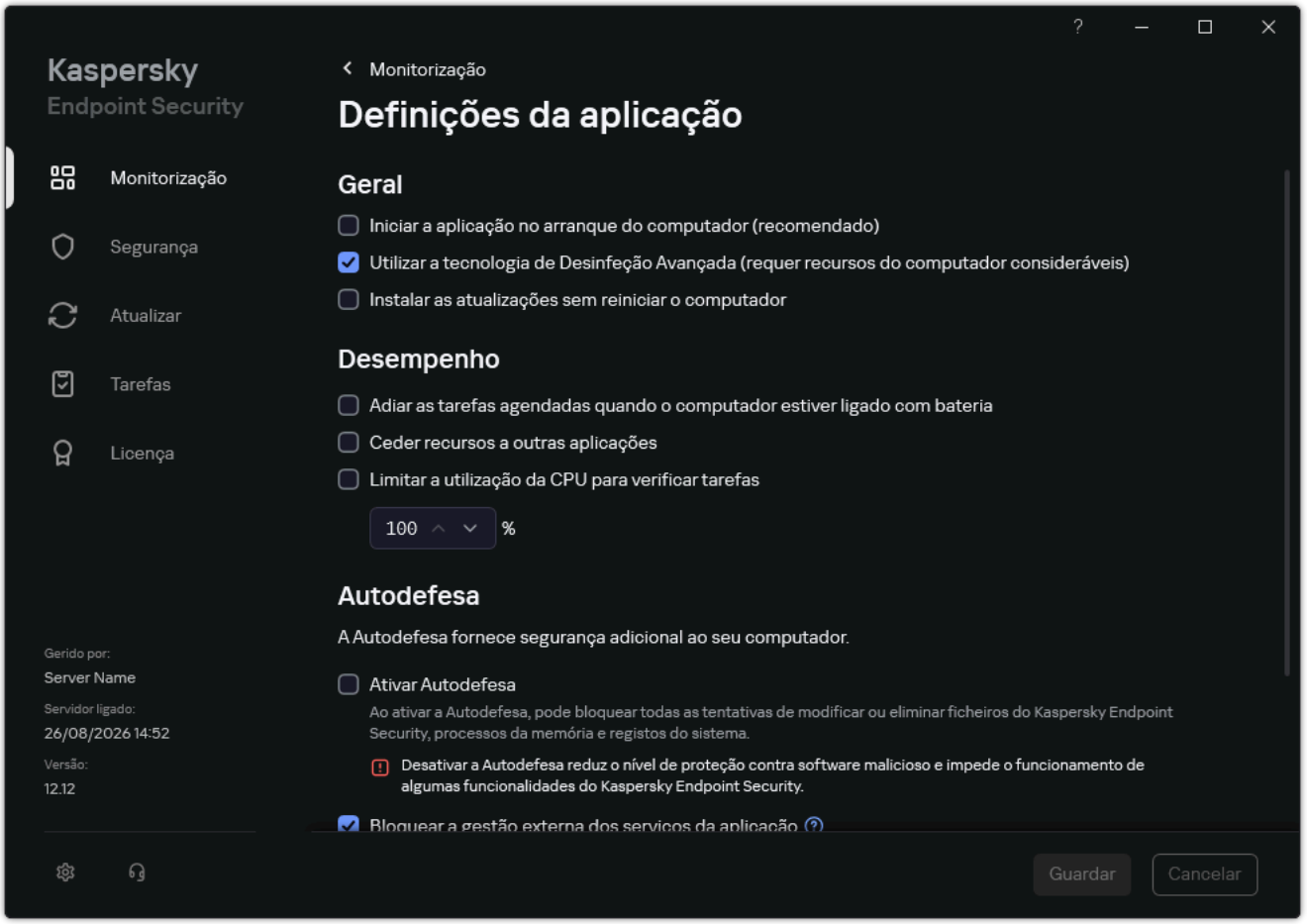
Como ativar a proteção de ficheiros de descarga e de ficheiros de rastreio na Web Console e na Cloud Console

1. Na janela principal da Consola Web, selecione **Asset management → Policies**.
2. Clique no nome da política do Kaspersky Endpoint Security.

   É apresentada a janela de propriedades da política.
3. Selecione o separador **Application settings**.
4. Aceda a **General Settings → Technical Support**.
5. No bloco **Debug information**, utilize a caixa de verificação **Dump and trace files protection ENABLED** para ativar ou desativar a proteção de ficheiros.
6. Guarde as suas alterações.

Como ativar a proteção dos ficheiros de descarga e dos ficheiros de rastreio na interface da aplicação

1. Na janela principal da aplicação, clique no botão ⚙.
2. Na janela Application settings, selecione **Definições gerais** → **Definições da aplicação**.



Definições do Kaspersky Endpoint Security for Windows

3. No bloco **Informações de depuração**, utilize a caixa de verificação **Ativar proteção de ficheiros de descarga e de rastreio** para ativar ou desativar a proteção de ficheiros.
4. Guarde as suas alterações.

Os ficheiros de descarga e de rastreio que foram editados enquanto a proteção estava ativa permanecem protegidos mesmo depois de esta ser desativada.

Obter dados do sistema operativo (Kaspersky Get System Info)

Após a instalação da aplicação Kaspersky Endpoint Security, o sistema operativo ou uma aplicação podem não funcionar corretamente. Existe um conflito entre a aplicação e o software ou os controladores dos componentes do computador.

Para identificar a causa do problema, o Suporte Técnico da Kaspersky requer um relatório do utilitário Kaspersky Get System Info (doravante referido como GSI). Para obter informações detalhadas sobre a utilização do utilitário, consulte a Base de Conhecimento da Kaspersky.

Limitações e avisos

O Kaspersky Endpoint Security tem várias limitações que não são críticas para o funcionamento da aplicação.

Instalar a aplicação

- Para obter detalhes sobre o suporte para os sistemas operativos Microsoft Windows 10, Microsoft Windows Server 2016 e Microsoft Windows Server 2019, consulte a Base de Conhecimento de Suporte Técnico.
- Para obter detalhes sobre o suporte para o sistema operativo Microsoft Windows 11 e o Microsoft Windows Server 2022, consulte a Base de conhecimento de Suporte Técnico.
- Depois de ser instalada num computador infetado, a aplicação não informa o utilizador sobre a necessidade de executar uma verificação do computador. Poderá ter problemas ao ativar a aplicação. Para resolver esses problemas, inicie uma Verificação de Áreas Críticas.
- Se forem utilizados caracteres não ASCII (por exemplo, letras russas) nos ficheiros setup.ini e setup.reg, é aconselhável editar o ficheiro utilizando o notepad.exe e guardar o ficheiro com a codificação UTF-16LE. Outras codificações não são suportadas.
- A aplicação não suporta o uso de caracteres não ASCII ao especificar o caminho de instalação da aplicação nas definições do pacote de instalação.
- Quando as definições da aplicação são importadas de um ficheiro CFG, o valor da definição que define a participação no Kaspersky Security Network não é aplicado. Depois de importar as definições, leia o texto da Declaração do Kaspersky Security Network e confirme o seu consentimento para participar no Kaspersky Security Network. Pode ler o texto da Declaração na interface da aplicação ou no ficheiro ksn_*.txt localizado na pasta que contém o kit de distribuição da aplicação.
- Se quiser remover e reinstalar a encriptação (FLE ou FDE) ou o componente de Controlo de Dispositivos, terá de reiniciar o sistema antes da reinstalação.
- Ao utilizar o sistema operativo Microsoft Windows 10, terá de reiniciar o sistema depois de remover o componente Encriptação ao Nível dos Ficheiros (File Level Encryption — FLE).
- Quando remover componentes de aplicações individuais (por exemplo, utilizando a tarefa *Alterar componentes da aplicação*), pode ser necessário reiniciar o computador.
- Nas propriedades da tarefa *Alterar componentes da aplicação*, ao mudar o modo de instalação (**Modo separado**/**Modo combinado**), a sincronização do conjunto de componentes entre modos não é suportada. A aplicação sincroniza o conjunto de componentes entre modos depois de reabrir as propriedades da tarefa.
- A instalação da aplicação pode terminar com um erro que informa que *O seu computador tem instalada uma aplicação cujo nome está em falta ou é ilegível*. Isso significa que aplicações incompatíveis ou fragmentos das mesmas permanecem no seu computador. Para remover artefactos de aplicações incompatíveis, envie um pedido com uma descrição detalhada da situação ao Suporte Técnico da Kaspersky através do Kaspersky CompanyAccount.
- Se tiver cancelado a remoção do Kaspersky Endpoint Security, inicie a recuperação da aplicação depois de reiniciar o computador.

- A aplicação requer o Microsoft .NET Framework 4.0 ou posterior. O Microsoft .NET Framework 4.6.1 tem vulnerabilidades. Se estiver a utilizar o Microsoft .NET Framework 4.6.1, deve instalar as atualizações de segurança. Para obter mais informações sobre as atualizações de segurança do Microsoft .NET Framework, consulte o site de suporte técnico da Microsoft.

- Se a instalação da aplicação não for bem-sucedida com o componente Kaspersky Endpoint Agent selecionado num sistema operativo de servidor e a janela *Erro do Coordenador do Windows Installer* aparecer, consulte as instruções no site de suporte da Microsoft.

- Se a aplicação tiver sido instalada localmente no modo não interativo, utilize o ficheiro setup.ini fornecido para substituir os componentes instalados.

- Depois de o Kaspersky Endpoint Security for Windows ser instalado em algumas configurações do Windows 7, o Windows Defender continua a funcionar. É aconselhável desativar manualmente o Windows Defender para evitar a degradação do desempenho do sistema.

- Ao instalar o Kaspersky Endpoint Security for Windows num servidor com o Kaspersky Security for Windows Server (KSWS) e aplicações do Windows Defender instaladas, tem de reiniciar o sistema. É necessário um reinício do sistema mesmo que tenha ativado a instalação da aplicação sem reiniciar o sistema. O Windows Defender for Windows Server está incluído na lista de software que é incompatível com o Kaspersky Endpoint Security for Windows. Antes de instalar a aplicação, o instalador remove o Windows Defender for Windows Server. A remoção de software incompatível torna necessário um reinício do sistema.

- Antes de instalar o Kaspersky Endpoint Security for Windows (KES) num servidor com o Kaspersky Security for Windows Server (KSWS) instalado, tem de desativar a Proteção por password do KSWS. Depois de migrar do KSWS para o KES, ative a Proteção por password nas definições da aplicação.

- Para instalar a aplicação em computadores que têm o Windows 7 ou o Windows Server 2008 R2 com o software Veeam Backup & Replication implementado, poderá ter de reiniciar o computador e executar novamente a instalação.

- A migração do Kaspersky Small Office Security (KSOS) para o Kaspersky Endpoint Security (KES) com a Proteção por password ativada está disponível a partir da versão 21.16 do KSOS.*.*. Para migrar versões anteriores do KSOS, tem de desativar a Proteção por password ou remover manualmente o KSOS. A migração do KSOS para o KES com a Proteção por password desativada é executada corretamente.

- Não é possível instalar o Kaspersky Endpoint Security numa unidade amovível de arranque. Durante a instalação, o Kaspersky Endpoint Security exibe uma mensagem de erro: *Selecionou uma pasta ou unidade não válida. A aplicação tem de ser instalada num disco rígido local*. Se conseguir instalar a aplicação numa unidade amovível utilizando ferramentas de terceiros, pode causar uma falha no sistema operativo (BSOD) durante o processo de arranque. Isto significa que o Kaspersky Endpoint Security não suporta o Windows To Go e soluções semelhantes. Para verificar um computador a partir de uma unidade amovível, pode utilizar a aplicação gratuita Kaspersky Rescue Disk.

- A instalação do Kaspersky Endpoint Security com componentes de rede num servidor terminal com sessões RDP com vários utilizadores envolve algumas considerações especiais. O sistema operativo força todas as sessões de utilizador a encerrarem após o encerramento da sessão do Administrador. Para se ligar ao servidor de terminais, tem de reiniciar o servidor ou iniciar sessão no sistema localmente. Este comportamento é ditado pelas peculiaridades do funcionamento do sistema operativo do Windows.

- Se os plug-ins da aplicação 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, a atualização do plug-in da aplicação 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: aceda à janela **Settings** → **Web plug-ins** e remova o plug-in da aplicação web do Kaspersky Endpoint Security for Windows, o plug-in da aplicação web do Kaspersky Endpoint Security for Linux e o Unified Protection and Management Plug-in da lista. Em seguida, instale primeiro o plug-in da aplicação web do Kaspersky Endpoint Security for Linux e, depois, o plug-in da aplicação web do Kaspersky Endpoint Security for Windows.

- Na Consola Web, a lista de componentes é apresentada incorretamente nas propriedades do pacote de instalação do Kaspersky Endpoint Security 12.11 for Windows. Um componente separado, o Anti-Cryptor, não está disponível nesta versão da aplicação. A proteção de pastas partilhadas contra funcionalidades de encriptação externas está incluída no componente Deteção de comportamento. No Kaspersky Endpoint Security 12.12 for Windows, esta funcionalidade é um componente separado. Ao mesmo tempo, na Consola de Administração (MMC), a lista de componentes é apresentada corretamente.

- Ao utilizar o plug-in da aplicação web, versão 7.0 ou posterior, a lista de componentes selecionados por predefinição para instalação é apresentada incorretamente nas propriedades do pacote de instalação do Kaspersky Endpoint Security 14.1 e versões anteriores. Se esta lista não for modificada durante a criação do pacote de instalação, a aplicação será instalada com o conjunto predefinido de componentes especificado para a versão correspondente da aplicação.

Atualizar a aplicação

- A partir da versão da aplicação 11.0.0, pode instalar o plug-in do Kaspersky Endpoint Security for Windows MMC sobre a versão anterior do plug-in. Para voltar a uma versão anterior do plug-in, elimine o plug-in atual e instale uma versão anterior do plug-in.

- Ao atualizar o Kaspersky Endpoint Security 11.0.0 ou 11.0.1 for Windows, as definições de agendamento de tarefas locais para as tarefas *Atualização das bases de dados e módulos da aplicação*, *Verificação de Áreas Críticas*, *Verificação Personalizada* e *Verificação de integridade da aplicação* não são guardadas.

- Em computadores com o Windows 10 versão 1903 e 1909, as 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 Encriptação ao Nível dos Ficheiros (FLE) instalado podem terminar com um erro. Isso ocorre porque a encriptação de ficheiros não é suportada para essas versões do Kaspersky Endpoint Security for Windows no Windows 10 versão 1903 e 1909. Antes de instalar esta atualização, é aconselhável remover o componente de encriptação de ficheiros.

- A aplicação requer o Microsoft .NET Framework 4.0 ou posterior. Microsoft NET Framework 4.6.1 tem vulnerabilidades. Se estiver a utilizar o Microsoft .NET Framework 4.6.1, deve instalar as atualizações de segurança. Para obter mais informações sobre as atualizações de segurança do Microsoft .NET Framework, consulte o site de suporte técnico da Microsoft.

- Ao atualizar o Kaspersky Endpoint Security, a aplicação desativa a utilização da KSN até a Declaração da Kaspersky Security Network ser aceite. Adicionalmente, o estado do computador pode ser alterado para *Critical* no Kaspersky Security Center; é recebido o evento *Os servidores da KSN não estão disponíveis*. Se utilizar o Kaspersky Managed Detection and Response, irá receber eventos sobre violações da operação da solução. É necessário utilizar a KSN para a operação do Kaspersky Managed Detection and Response. O Kaspersky Endpoint Security ativa a utilização da KSN após aplicar a política na qual o administrador aceita os termos de utilização da KSN. Quando a Declaração da Kaspersky Security Network é aceite, o Kaspersky Endpoint Security retoma a operação.

- Depois de atualizar o Kaspersky Endpoint Security para a versão 11.10.0 ou posterior sem reiniciar, o computador terá duas aplicações do Kaspersky Endpoint Security instaladas. Não remova manualmente a versão anterior da aplicação. A versão anterior será removida automaticamente quando o computador for reiniciado.

- Depois de atualizar o Kaspersky Endpoint Security num computador com Microsoft Windows 11, o menu de contexto dos ficheiros pode apresentar itens para a versão anterior e atual da aplicação. Reinicie o seu computador duas vezes para garantir o correto funcionamento do menu de contexto dos ficheiros.

- Se a Autodefesa da aplicação estiver desativada e todos os adaptadores de rede parados, os componentes de rede da aplicação não funcionarão entre o final da atualização da aplicação e o reinício do computador. Os componentes de rede da aplicação incluem Proteção contra ameaças da Web, Proteção contra ameaças de correio, Proteção contra ameaças de rede, Firewall, Prevenção contra invasões e Controlo de Internet. Reinicie o computador para que a aplicação funcione corretamente.

- O componente Prevenção de ataques BadUSB não funciona entre o final da atualização da aplicação e o reinício do computador. Reinicie o computador para que a aplicação funcione corretamente.

- A aplicação não pode ser atualizada se o processo de atualização anterior não tiver sido concluído. Reinicie o computador para que a aplicação funcione corretamente.

- Depois de a aplicação ser atualizada de versões anteriores ao Kaspersky Endpoint Security 11 for Windows, o computador tem de ser reiniciado.

- Se gerir o Kaspersky Endpoint Security através da Consola Cloud do Kaspersky Security Center, não é permitido atualizar a aplicação localmente. Ao atualizar a aplicação localmente, não é possível aceitar o Contrato de Tratamento de Dados da Consola Cloud do Kaspersky Security Center.

Suporte para arquitetura Arm

- A instalação do Kaspersky Endpoint Security no modo Light Agent em máquinas virtuais baseadas em Arm não é suportada.

- O Encriptação de disco Kaspersky não é compatível com computadores baseados em Arm.

- A encriptação de ficheiros não é suportada em computadores baseados em Arm.

- A encriptação de unidades removíveis não é suportada em computadores baseados em Arm.

- Em computadores com Windows 11 para Arm64, o Agente EDR não é compatível com Bitdefender Endpoint Security Tools.

- A funcionalidade de proteção do sinal de áudio e a funcionalidade de proteção do acesso à câmara Web não são suportadas em computadores baseados em Arm.

- Em computadores baseados em Arm, a extensão Proteção contra ameaças de correio suporta as versões de 32 bits 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 controlo de impressão não é suportado em computadores baseados em Arm.

- Em computadores baseados em Arm, a tarefa *IOC Scan* suporta ficheiros de e-mail apenas dos seguintes clientes de e-mail: versões de 32 e 64 bits do Outlook 2016 e Outlook 2021, 2024 e 365 para Arm64.

- Em computadores com o Windows 11 para Arm64, a autenticação baseada em token poderá não estar disponível porque o sistema operativo não consegue detetar um certificado válido no token. Este comportamento deve-se à forma como o sistema operativo interage com o software do token. Por exemplo, o sistema operativo poderá não ter os controladores necessários para o funcionamento do token. Neste caso, o Kaspersky Endpoint Security também não suporta a autenticação baseada em token (Proteção por password). Pode utilizar outros métodos de autenticação, como as credenciais do utilizador.

Suporte para plataformas de servidor

- Nos servidores com a *deduplicação de dados* ativada, tem de adicionar o ficheiro fsdmhost.exe à lista de aplicações fiáveis. Isto ajuda a otimizar o desempenho da aplicação e a evitar uma carga excessiva na CPU.

- O sistema de ficheiros ReFS é suportado com limitações:

  - O Kaspersky Endpoint Security pode processar eventos de desinfeção de ameaças incorretamente. Por exemplo, se a aplicação tiver eliminado um ficheiro malicioso, o relatório pode ter uma entrada "objeto não processado". Simultaneamente, o Kaspersky Endpoint Security desinfeta as ameaças de acordo com as definições da aplicação. O Kaspersky Endpoint Security pode também criar um duplicado do evento *O objeto será desinfetado ao reiniciar* para o mesmo objeto.

  - O componente Proteção contra ameaças de ficheiros pode ignorar algumas ameaças. Simultaneamente, a Verificação de software malicioso funciona corretamente.

  - Depois de a tarefa *Verificação de software malicioso* ser iniciada, as exclusões adicionadas com o iChecker são repostas quando o servidor é reiniciado.

  - A tecnologia iSwift não é suportada. O Kaspersky Endpoint Security não considera exclusões de verificação adicionadas com a tecnologia iSwift.

  - O Kaspersky Endpoint Security não deteta os ficheiros eicar.com e susp-eicar.com, se o ficheiro meicar.exe estava no computador antes da instalação do Kaspersky Endpoint Security.

  - O Kaspersky Endpoint Security pode apresentar incorretamente notificações de desinfeção de ameaças. Por exemplo, a aplicação pode apresentar uma notificação de ameaça referente a uma ameaça previamente desinfetada.

- As tecnologias de encriptação ao nível dos ficheiros (FLE) e de encriptação de disco Kaspersky (FDE) não são suportadas nas plataformas de servidor. Simultaneamente, o Kaspersky Endpoint Security pode processar incorretamente eventos de encriptação de dados.

- Em sistemas operativos de servidor, não é apresentado nenhum aviso sobre a necessidade de desinfeção avançada.

- O Microsoft Windows Server 2008 foi excluído do suporte. A instalação da aplicação num computador com o sistema operativo Microsoft Windows Server 2008 não é suportada.

- O Kaspersky Endpoint Security instalado num servidor com o Microsoft Data Protection Manager (DPM) implementado pode causar o mau funcionamento do DPM. Está relacionado com limitações no funcionamento do DPM. Para eliminar o mau funcionamento, deve adicionar unidades de servidor locais a exclusões para o componente Proteção contra ameaças de ficheiros e tarefas de *Verificação de software malicioso*.

- O modo Server Core é suportado com limitações:
  - A interface gráfica do utilizador local não está disponível, incluindo notificações, notificações pop-up e outros controlos da interface. A aplicação não consegue apresentar janelas de pedido, incluindo as seguintes janelas:
    - Versão da aplicação e pedido de confirmação de atualização do módulo;
    - Pedido de reinício do computador;
    - Pedido de credenciais de autenticação do servidor de proxy;
    - Pedido para obter acesso a um dispositivo (Controlo de Dispositivos).
  - Os seguintes componentes não estão disponíveis: Proteção contra ameaças da web, Proteção contra ameaças de correio, Controlo de Internet, Prevenção de ataques BadUSB.
  - O Anti-Bridging não está disponível.
  - Só pode aceitar a Declaração da Kaspersky Security Network na política da aplicação na consola do Kaspersky Security Center.
  - A Encriptação de Unidade BitLocker está disponível apenas com um Trusted Platform Module (TPM). Um PIN/password não pode ser utilizado para encriptação porque a aplicação não consegue apresentar a janela de pedido de password para autenticação de pré-arranque. Se o sistema operativo do computador tiver o modo de compatibilidade padrão do Tratamento de Informação Federal (FIPS) ativado, ligue uma unidade amovível para guardar a chave de encriptação antes de começar a encriptar a unidade.

Suporte para plataformas virtuais

- A encriptação de disco completa (FDE) nas máquinas virtuais Hyper-V não é suportada.
- A encriptação de disco completa (FDE) nas plataformas virtuais Citrix não é suportada.
- Os sistemas operativos Windows 10 Enterprise multissessão e Windows 11 Enterprise multissessão são suportados com limitações:
  - O Kaspersky Endpoint Security desinfeta as ameaças ativas sem notificar o utilizador, tal como quando desinfeta ameaças ativas nos servidores. Uma vez que o sistema operativo continua a funcionar em modo multi-sessão, outros utilizadores ativos podem perder os seus dados se a ameaça não for resolvida de imediato.
  - A Encriptação de disco completa (FDE) não é suportada.
  - A gestã do BitLocker não é suportada.
  - Usar o Kaspersky Endpoint Security com unidades removíveis não é suportado. A infraestrutura do Microsoft Azure define as unidades removíveis como unidades de rede.
- A instalação e utilização de encriptação ao nível dos ficheiros (FLE) em plataformas virtuais Citrix não é suportada.

- Para oferecer suporte à compatibilidade do Kaspersky Endpoint Security for Windows com Citrix PVS, realize a instalação com a opção **Garanta a compatibilidade com Citrix PVS** ativada. Esta opção pode ser ativada no Assistente de Configuração ou utilizando o parâmetro de linha de comando `/pCITRIXCOMPATIBILITY=1`. No caso da instalação remota, o ficheiro KUD tem de ser editado adicionando-se-lhe o seguinte parâmetro: `/pCITRIXCOMPATIBILITY=1`.

- Citrix XenDesktop. Antes de iniciar a clonagem, deve desativar a Autodefesa para clonar máquinas virtuais que usam o vDisk.

- Ao preparar um modelo de máquina para a imagem principal do 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 ficheiro 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 Citrix Support.

- Em alguns casos, uma tentativa para desligar com segurança uma unidade amovível pode ser malsucedida numa máquina virtual implementada num hipervisor VMware ESXi. Tente novamente desligar o dispositivo em segurança.

- O Kaspersky Endpoint Security é compatível com o hipervisor VMware ESXi com as seguintes limitações:

  - O Kaspersky Endpoint Security pode ser incompatível com controladores de Introspeção de Convidado (vnetWFP.sys, vnetFLT.sys e outros). Para resolver a incompatibilidade, atualize os controladores para a versão mais recente ou desinstale os controladores.

  - Em alguns casos, uma tentativa de remover com segurança um disco amovível numa máquina virtual pode não ter sucesso. Tente novamente desligar o dispositivo em segurança.

- A instalação do Kaspersky Endpoint Security em máquinas virtuais com o agente Citrix VDA pode resultar num erro de compatibilidade. Isto acontece porque o Citrix Provisioning Services tem compatibilidade limitada com soluções antivírus. Para obter as melhores práticas de utilização de soluções antivírus com o Citrix Provisioning Services, consulte o website de suporte da Citrix.

- O Kaspersky Endpoint Security ignora a verificação de uma unidade amovível se a unidade estiver ligada a uma máquina virtual no hipervisor Citrix (a tarefa *Verificação das unidades amovíveis*). Nesses dispositivos, o sistema operativo reconhece a unidade removível ligada como uma unidade de rede. Nesses casos, pode utilizar a tarefa *Verificação Personalizada*. O comportamento da aplicação no modo padrão e no modo Light Agent é o mesmo.

- Se o Kaspersky Endpoint Security estiver instalado numa máquina virtual numa infraestrutura que utiliza a tecnologia Citrix App Layering, os ficheiros detetados pela aplicação como infetados com o estado *O objeto será eliminado ao reiniciar* não serão removidos automaticamente quando a máquina virtual for reiniciada.

  Para eliminar estes ficheiros, deve montar o ficheiro VHDX que contém a User Layer no computador do administrador do Citrix App Layering e executar uma verificação de malware no disco montado.

- Antes de criar um snapshot da Golden Image de uma máquina virtual com o Kaspersky Endpoint Security instalado, recomenda-se que encerre a máquina virtual e crie um snapshot "a frio". Se criar um snapshot enquanto a máquina virtual estiver em execução (um snapshot "a quente"), não é garantido o funcionamento correto da aplicação.

Compatibilidade com o Kaspersky Security Center

- Na versão 14.1 e anterior da Consola Web do Kaspersky Security Center, os nomes das áreas funcionais para os componentes da Inspeção de Registo e Monitor de integridade do ficheiro não são apresentados corretamente na secção de definições de permissões de acesso do utilizador das propriedades do Servidor de Administração.

- Depois de reparar a aplicação, a proteção da ligação do computador ao Servidor de Administração é desativada. Depois de reparar a aplicação, execute a tarefa *Proteção da ligação do Servidor de Administração* novamente.

- Na Consola de Administração do Kaspersky Security Center, a janela **Selecionar um utilizador ou grupo de utilizadores** exibe apenas os primeiros 50 000 utilizadores da lista de utilizadores do Kaspersky Security Center. Consulte a Ajuda do Kaspersky Security Center para obter mais detalhes.

- Ao pesquisar dispositivos geridos na Consola de Administração do Kaspersky Security Center, o separador **Application components** pode apresentar simultaneamente várias variantes do nome do mesmo componente da aplicação, incluindo nomes correspondentes a versões mais antigas do Kaspersky Endpoint Security. Os nomes de alguns componentes também podem estar duplicados.

  Para pesquisar por componente, basta selecionar uma das variantes exibidas. Para obter mais informações sobre a deteção de dispositivos, consulte a Ajuda do Kaspersky Security Center.

- No Kaspersky Security Center Web Console 15.1 Update 2, com o plug-in Web do Kaspersky Endpoint Security for Windows versão 12.11 ou posterior e o Unified Protection and Management Plug-in instalados, as condições de ativação de perfil da política não funcionam. O Kaspersky Security Center não adiciona à consola novos dispositivos que cumpram as condições de ativação de perfil.

Licenciamento

- Se a mensagem do sistema *Erro ao receber dados* aparecer, verifique se o computador no qual está a realizar a ativação tem acesso à rede ou configure as definições de ativação através do Proxy de Ativação do Kaspersky Security Center.

- Na interface da aplicação, a data de validade da licença é apresentada na hora local do computador.

- A instalação da aplicação com um ficheiro de chave integrado num computador com acesso instável à Internet pode resultar na apresentação temporária de eventos que indicam que a aplicação não está ativada ou que a licença não permite o funcionamento do componente. Isto deve-se ao facto de, durante o processo de instalação, a aplicação ativar primeiro a licença de avaliação incorporada. Requer acesso à Internet.

- Durante o período de avaliação, a instalação de qualquer atualização ou patch de aplicação num computador com acesso instável à Internet pode resultar na apresentação temporária de eventos que informam que a aplicação não está ativada. Isto deve-se ao facto de, durante o processo de instalação da atualização, a aplicação ativar primeiro a licença de avaliação incorporada. Requer acesso à Internet.

- Se a licença de avaliação tiver sido ativada automaticamente durante a instalação da aplicação e, em seguida, a aplicação tiver sido removida sem guardar as informações da licença, a aplicação não será ativada automaticamente com a licença de avaliação quando reinstalada. Nesse caso, ative manualmente a aplicação.

- Se estiver a utilizar o Kaspersky Security Center versão 11 e o Kaspersky Endpoint Security versão 14.2, os relatórios de desempenho dos componentes poderão funcionar incorretamente. Se tiver instalado componentes do Kaspersky Endpoint Security que não estejam incluídos na sua licença, o Agente de Rede poderá enviar erros do estado do componente para o Registo de Eventos do Windows. Para evitar erros, remova os componentes que não estiverem incluídos na licença.

Proteção contra ameaças de correio

- Ao verificar e-mails com a extensão Proteção contra ameaças de correio para Microsoft Outlook, recomendamos que utilize o Modo Exchange em Cache (Use Cached Exchange Mode).
- O Kaspersky Endpoint Security não oferece suporte à versão de 64 bits do cliente de e-email Microsoft Outlook. Isto significa que o Kaspersky Endpoint Security não verifica ficheiros do Microsoft Outlook (ficheiros PST e OST), se uma versão de 64 bits do Microsoft Outlook estiver instalada no computador, mesmo se o correio estiver incluído no âmbito de verificação.
- O Kaspersky Endpoint Security não é compatível com o novo cliente de e-mail do Microsoft Outlook.
- Se tiver desativado a desinfeção de ameaças detetadas pela Proteção contra ameaças de correio e tiver recebido um e-mail infetado na sua caixa de correio do Outlook, a Proteção contra ameaças da Web poderá bloquear a comunicação com o servidor Exchange através de MAPI. Em seguida, a Proteção contra ameaças da Web gera um evento de deteção de ameaças e envia-o para o Kaspersky Security Center. Para restaurar a ligação entre o computador e o servidor Exchange, tem de eliminar manualmente o e-mail infetado da caixa de correio do Outlook.

  Ao atualizar a versão da aplicação sem reiniciar o computador, o nível da Proteção contra ameaças de correio é temporariamente reduzido (durante um período máximo de um minuto). Se receber um e-mail infetado na caixa de correio do Outlook durante a atualização da aplicação, a Proteção contra ameaças da Web também bloqueará a ligação ao servidor Exchange através de MAPI. Para restaurar a ligação, elimine o e-mail infetado da caixa de correio do Outlook.

Motor de remediação

- A aplicação restaura ficheiros apenas em dispositivos que têm o sistema de ficheiros NTFS ou FAT32.
- A aplicação restaura ficheiros de até 100 MB.
- A aplicação pode restaurar ficheiros 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 ficheiros guardados em unidades de rede ou em discos CD/DVD regraváveis.
- Não é possível restaurar ficheiros que foram encriptados com o Sistema de encriptação de ficheiros (EFS). Para obter mais informações sobre a operação EFS, visite Microsoft website.
- A aplicação não monitoriza modificações para ficheiros realizados por processos ao nível do kernel do sistema operativo.

Firewall

- Se uma regra de pacote de rede ou uma regra de rede de aplicação especificar nomes DNS, o Kaspersky Endpoint Security pode enviar pedidos ao servidor DNS para determinar os endereços IP destes recursos. A Firewall utiliza endereços IP para monitorizar a atividade da rede. Por conseguinte, a aplicação resolve nomes DNS para endereços IP. Recomenda-se a utilização de nomes DNS nas regras apenas para computadores 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. A firewall não suporta a máscara ::/0.

- A filtragem de pacotes ou ligações por endereço local, interface física e tempo de vida do pacote (TTL) é suportada nos seguintes casos:
  - Por endereço local para pacotes de saída ou ligações em regras de aplicações para TCP e UDP e regras de pacotes.
  - Por endereço local para pacotes de entrada ou ligações (exceto UDP) em regras de bloqueio de aplicações e regras de pacotes.
  - Por tempo de vida do pacote (TTL) nas regras de pacotes de bloqueio para pacotes de entrada ou saída.
  - Por interface de rede para pacotes de entrada e saída ou ligações em regras de pacotes.
- Se configurou um adaptador de rede ou o tempo de vida do pacote (TTL) de uma regra de permissão de pacotes, a prioridade desta regra é mais baixa do que uma regra de bloqueio de aplicação. Por outras palavras, se a atividade de rede for bloqueada por uma aplicação (por exemplo, a aplicação faz parte do grupo fiável de *Restrições altas*), não poderá permitir que a aplicação tenha atividade de rede utilizando regras de pacote com estas definições. Em todos os outros casos, a prioridade de uma regra de pacote é mais elevada do que uma regra de rede de aplicação.
- Ao importar regras de pacotes da Firewall, o Kaspersky Endpoint Security pode alterar os nomes das regras. A aplicação determina regras que têm o mesmo conjunto de parâmetros gerais: protocolo, direção, portas remotas e locais e tempo de vida do pacote (TTL). Se este conjunto de parâmetros gerais for idêntico para várias regras, a aplicação atribui o mesmo nome a estas regras ou acrescenta uma etiqueta de parâmetro ao nome. Deste modo, o Kaspersky Endpoint Security importa todas as regras de pacotes, mas o nome das regras que têm parâmetros gerais idênticos pode ser alterado.
- Se tiver ativado os relatórios de eventos da aplicação numa regra de rede, ao mover a aplicação para um grupo fiável diferente, as restrições deste grupo fiável não serão aplicadas. Portanto, se a aplicação estiver no grupo fiável, não terá quaisquer restrições de rede. Depois ative os relatórios de eventos para esta aplicação e mova-a para o grupo *Não fiáveis*. A Firewall não irá aplicar restrições de rede para tal aplicação. É recomendado que mova primeiro a aplicação para o grupo fiável adequado e depois ative os relatórios de eventos. Se este método não for adequado, pode configurar manualmente restrições para a aplicação nas definições da regra de rede. A restrição só é aplicável à interface local da aplicação. Mover a aplicação entre grupos fiáveis na política funciona corretamente.
- Os componentes Firewall e Prevenção contra invasões têm definições comuns: direitos de aplicações e recursos protegidos. Se alterar estas definições da Firewall, o Kaspersky Endpoint Security aplica automaticamente as novas definições à Prevenção contra invasões. Se, por exemplo, tiver permitido alterações às definições gerais da política da Firewall (o cadeado estiver aberto), as definições da Prevenção contra invasões serão igualmente editáveis.
- Quando uma regra de pacotes de rede é acionada no Kaspersky Endpoint Security 11.6.0 ou anterior, a coluna **Nome da aplicação** no relatório da Firewall irá apresentar sempre o valor *Kaspersky Endpoint Security*. Além disso, a Firewall irá bloquear a ligação ao nível do pacote para todas as aplicações. Este comportamento foi modificado para o Kaspersky Endpoint Security 11.7.0 ou posterior. A coluna **Tipo de regra** foi adicionada ao relatório da Firewall. Quando uma regra de pacote de rede é acionada, o valor da coluna **Nome da aplicação** permanece vazio.
- Se proibiu toda a atividade de rede utilizando a Firewall, o componente Proteção contra ameaças de rede pode detetar um ataque do tipo Mapeamento de portas. Isto pode acontecer porque a aplicação inicia a Proteção contra ameaças de rede antes da Firewall para detetar atividade suspeita na rede.

Prevenção de ataques BadUSB

- O Kaspersky Endpoint Security repõe o tempo limite do bloqueio do dispositivo USB quando o computador é bloqueado (por exemplo, decorrido o tempo limite do bloqueio de ecrã). Ou seja, se introduzir várias vezes o código de autorização do dispositivo USB incorretamente e a aplicação bloquear o dispositivo USB, o Kaspersky Endpoint Security permite-lhe repetir a tentativa de autorização depois de desbloquear o computador. Neste caso, o Kaspersky Endpoint Security não bloqueia o dispositivo USB por um tempo específico nas definições do componente de Prevenção de ataques BadUSB.

- O Kaspersky Endpoint Security repõe o tempo limite do bloqueio do dispositivo USB quando a proteção do computador está em pausa. Ou seja, se introduzir várias vezes o código de autorização do dispositivo USB incorretamente e a aplicação bloquear o dispositivo USB, o Kaspersky Endpoint Security permite-lhe repetir a tentativa de autorização depois de retomar a proteção do computador. Neste caso, o Kaspersky Endpoint Security não bloqueia o dispositivo USB por um tempo específico nas definições do componente de Prevenção de ataques BadUSB.

Kaspersky Security Network

- O Kaspersky Endpoint Security não suporta HTTPS quando se liga ao KSN Proxy (caixa de verificação **Use HTTPS** selecionada nas definições de ligação do KSN Proxy) se o endereço do servidor incluir letras não latinas (símbolos não ASCII).

- No Kaspersky Security Center, ao passar da Kaspersky Security Network global para uma Kaspersky Security Network privada (KPSN), ou vice-versa, a opção de participar da Kaspersky Security Network é desativada na política do produto específico. Após a mudança, leia atentamente o texto da Declaração da Kaspersky Security Network e confirme o seu consentimento para participar na KSN. Pode ler o texto da Declaração na interface da aplicação 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, tem de voltar a confirmar que concorda com a Declaração da Kaspersky Security Network. Para tal, tem de ativar a utilização do Kaspersky Security Network nas propriedades da política ou na interface da aplicação e confirmar que concorda com a Declaração da Kaspersky Security Network. Se já utilizou a KSN global, desative primeiro a Utilização da KSN, depois reative-a e confirme que concorde com a Declaração da Kaspersky Security Network. Se não concordar com a Declaração da Kaspersky Security Network, a aplicação não poderá aceder aos dados da Kaspersky Security Network.

- O Kaspersky Endpoint Security não envia ficheiros de texto (como ficheiros TXT, CSV, LOG e DOCX sem macros) para a Kaspersky Security Network para verificação. A aplicação envia ficheiros que podem representar uma ameaça para a KSN para serem verificados. Estes ficheiros incluem ficheiros executáveis ou ficheiros que podem conter código executável (como macros em ficheiros DOCX). Outros componentes da aplicação são responsáveis pela leitura de ficheiros de texto. Também pode verificar manualmente a reputação de um ficheiro de texto a partir do menu de contexto do ficheiro. Se um ficheiro de texto tiver uma reputação *Não fiável (Kaspersky Security Network)*, a aplicação ignora a ação definida para as ameaças detetadas.

Controlo das Aplicações

- Ao trabalhar com as regras de Controlo das Aplicações, não é recomendável adicionar mais de 100 000 condições totais de inclusão e eliminação para aplicações em diferentes categorias, desde que o Kaspersky Endpoint Security esteja a ser executado num computador que cumpra os requisitos mínimos de hardware e opere no Microsoft Windows 10.

- Sapenas são suportados ficheiros no formato ZIP são suportados ao trabalhar com regras de controlo das aplicações no Kaspersky Security Center Web Console. Não são suportados ficheiros noutros formatos, como RAR ou 7z. Esta restrição não existe se trabalhar com regras de controlo das aplicações na Administration Console (MMC).

- Ao trabalhar com as regras de Controlo das Aplicações na Consola Web do Kaspersky Security Center, o tamanho máximo suportado de um ficheiro carregado é de 104 MB. Esta restrição não existe se trabalhar com regras de controlo das aplicações na Administration Console (MMC).

- Ao trabalhar no Microsoft Windows 10 no modo de lista de bloqueio de aplicações, as regras de bloqueio poderão ser aplicadas incorretamente, o que pode causar o bloqueio de aplicações não especificadas nas regras.

- Se adicionou novas *regras predefinidas de Controlo das aplicações* ao atualizar o Kaspersky Endpoint Security, não é possível aplicar estas regras a versões anteriores da aplicação.

- Quando as aplicações da Web progressivas (PWA) são bloqueadas pelo componente Controlo das Aplicações, appManifest.xml é indicado como a aplicação bloqueada no relatório.

- Ao adiconar a aplicação padrão Notepad a uma Regra de Controlo das Aplicações para Windows 11, não é recomendado especificar o caminho para a aplicação. Nos computadores com Windows 11, o sistema operativo utiliza o Metro Notepad localizado na pasta `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe`. Nas versões anteriores do sistema operativo, o Notepad está localizado nas seguintes pastas:

  - `C:\Windows\notepad.exe`
  - `C:\Windows\System32\notepad.exe`
  - `C:\Windows\SysWOW64\notepad.exe`

  Ao adiconar o Notepad a uma Regra de Controlo das Aplicações, é possível especificar o nome da aplicação e o hash do ficheiro das propriedades da aplicação em execução, por exemplo.

- Ao migrar a política KSWS para o perfil de política do KES, o Assistente de conversão de políticas e tarefas em lote (Assistente de Migração) renomeia as categorias de aplicações se os nomes das categorias tiverem caracteres proibidos: `'` `*` `<` `>` `?` `\` `:` `|`. O Assistente de Migração substitui estes caracteres por caracteres `_`. Por exemplo, a categoria da aplicação `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` é renomeada para `KSWS_Everyone_[C61F-3B7C-4D89-96A1]`.

Controlo de Dispositivos

- O Kaspersky Endpoint Security pode registar eventos de ligação e desativação de dispositivos externos. Os serviços do Windows utilizam a conta de utilizador do sistema para ligar ou desligar dispositivos. Isto torna impossível saber que utilizador está a ligar ou a desligar o dispositivo. O Kaspersky Endpoint Security especifica a conta de utilizador do SISTEMA no evento.

- O acesso aos dispositivos de impressora adicionados à lista fiável é bloqueado pelas regras de bloqueio de dispositivo e barramento.

- Para dispositivos MTP, o controlo das operações de leitura, gravação e ligação é suportado se estiver a utilizar os controladores integrados da Microsoft do sistema operativo. Se um utilizador instalar um controlador personalizado para trabalhar com um dispositivo (por exemplo, como parte do iTunes ou Android Debug Bridge), o controlo das operações de leitura e gravação pode não funcionar.

- Ao trabalhar com dispositivos MTP, as regras de acesso são alteradas depois de voltar a ligar o dispositivo.

- O componente Controlo de Dispositivos regista eventos relacionados com os dispositivos monitorizados, como a ligação e o desligamento de um dispositivo, leitura de um ficheiro a partir de um dispositivo, gravação de um ficheiro num dispositivo e outros eventos. O Kaspersky Endpoint Security regista eventos de desativação apenas para os seguintes tipos de dispositivos: Dispositivos portáteis (MTP), Unidades amovíveis, Disquetes, Unidades de CD/DVD. Para outros tipos de dispositivos, a aplicação não regista eventos de desativação. A aplicação regista a operação de ligação de um dispositivo a um computador para todos os tipos de dispositivos.

- Se estiver a adicionar um dispositivo à lista fiável com base numa máscara de modelo e utilizar caracteres incluídos na ID, mas não no nome do modelo, esses dispositivos não serão adicionados. Numa estação de trabalho, esses dispositivos serão adicionados à lista fiável com base numa máscara de ID.

- Quando a aplicação é atualizada sem reiniciar o computador, o Controlo de Dispositivos não aplica as regras de acesso aos dispositivos que se ligam novamente. No entanto, se o dispositivo estiver ligado antes da atualização, o Controlo de Dispositivos aplica as regras corretamente. Reinicie o computador para que a aplicação funcione corretamente com os dispositivos que se ligaram novamente.

- Em computadores com a versão 12.0 do Kaspersky Endpoint Security instalada, o modo de acesso à impressora **Permitir e não registar** para o tipo de dispositivo **Impressoras de rede** é chamado **Depende do barramento de ligação**, se a política do Kaspersky Endpoint Security versão 12.1 for aplicada ao computador. Nestes modos, a aplicação executa as mesmas ações. No Kaspersky Endpoint Security, versão 12.1, o modo de acesso para impressoras de rede é nomeado corretamente **Permitir e não registar**.

- A partir da versão 12.0 do Kaspersky Endpoint Security for Windows, a aplicação permite definir regras de impressão para impressoras (controlo de impressão). Após instalar a aplicação com controlo de impressão ou atualizar a aplicação para uma versão com controlo de impressão, reinicie o computador. Até que o computador seja reiniciado, o Kaspersky Endpoint Security não aplica regras de impressão e só pode controlar o acesso às impressoras. Se reiniciar o computador afetar negativamente os fluxos de trabalho na sua organização, poderá reiniciar apenas o serviço spoolsv (spooler de impressão). O controlo de impressão não é suportado em computadores baseados em Arm.

- A partir do Kaspersky Endpoint Security 12.0 for Windows, o protocolo WPA3 é suportado pela aplicação para dispositivos do tipo **Wi-Fi**. Se uma política do Kaspersky Endpoint Security versão 12.2 for aplicada a um computador, o protocolo WPA2 será selecionado nos computadores com o Kaspersky Endpoint Security versão 11.11.0 e anterior; WPA2/WPA3 é selecionado para as versões 12.0 a 12.1; WPA3 é selecionado para versões 12.2 e posteriores.

- Os dispositivos Apple são classificados como dispositivos portáteis (MTP) e dispositivos iTunes. O sistema operativo pode identificar incorretamente a ligação do dispositivo Apple e não determinar o dispositivo Apple como um dispositivo portátil (MTP). Por este motivo, o dispositivo Apple não estará disponível no gestor de ficheiros, mas estará acessível na aplicação iTunes. Como resultado, o Kaspersky Endpoint Security irá controlar o acesso ao dispositivo Apple apenas na aplicação iTunes. Para aceder ao seu dispositivo Apple como dispositivo portátil (MTP), precisa de aceder ao Gestor de Dispositivos e remover o Controlador USB do Dispositivo Móvel Apple da lista de Controladores USB. Após reiniciar o computador, o sistema operativo irá identificar o dispositivo Apple como um dispositivo portátil (MTP) e dispositivo iTunes. O Kaspersky Endpoint Security irá controlar o acesso ao dispositivo na aplicação iTunes e no gestor de ficheiros.

- No Kaspersky Endpoint Security 12.3 for Windows, as definições de acesso são diferentes para o tipo de dispositivo **Bluetooth**. Se especificou o valor de **Depende do barramento de ligação** na versão anterior da aplicação, depois de atualizar a aplicação para a versão 12.3, o valor configurado muda para **Permitir e não registar**. Esta opção não altera o comportamento do dispositivo.

- O Controlo de Dispositivos oferece suporte a dispositivos Bluetooth apenas por meio da pilha Bluetooth do Microsoft Windows. O Controlo de Dispositivos pode funcionar incorretamente com pilhas Bluetooth de terceiros.

- Se o dispositivo Bluetooth ocultar ou falsificar a Classe de Dispositivo (COD), o Controlo de Dispositivos poderá funcionar incorretamente.

- Em computadores Windows 7 ou Windows 8 com determinados controladores dongle Realtek Bluetooth, pode não ser possível permitir apenas a ligação de dispositivos Bluetooth como dispositivos de entrada (classe HID). Ou seja, se proibir o acesso a dispositivos Bluetooth nas definições da aplicação e adicionar dispositivos de entrada às exclusões, o Controlo de Dispositivos poderá em vez disso impedir o acesso a todos os dispositivos Bluetooth.

Controlo de Internet

- Os formatos OGV e WEBM não são suportados.

- O protocolo RTMP não é suportado.

- O Controlo de Internet suporta apenas WSL1. A aplicação não controla o tráfego WSL2.

Controlo de Anomalias Adaptativo

- Recomenda-se a criação de exclusões automaticamente com base no evento. Ao adicionar manualmente uma exclusão, adicione o carácter `*` ao início do caminho quando especificar o objeto de destino.

- Não é possível gerar o **Reportar as regras acionadas do Controlo de Anomalias Adaptativo** se a amostra incluir sequer um evento cujo nome contenha mais de 260 caracteres.

- Adicionar exclusões do repositório do Acionamento de Regras do Controlo de Anomalias Adaptativo não é suportado se as propriedades de um objeto ou de um processo possuírem um valor superior a 256 caracteres (por exemplo, o caminho para o objeto de destino). Pode adicionar uma exclusão manualmente nas definições da Política. Também pode adicionar uma exclusão no Relatório de regras do Controlo de Anomalias Adaptativo acionadas.

- O Kaspersky Security Center 15.1 não pode gerar um relatório detalhado **Reportar o estado das regras do Controlo de Anomalias Adaptativo** para uma regra específica.

- As regras de Controlo Adaptativo de Anomalias estão disponíveis apenas no idioma correspondente ao idioma de instalação do plug-in da aplicação web. Se alterar o idioma da interface, a Web Console apresenta uma lista de regras vazia. Para aceder às regras, volte a alterar o idioma da interface para o idioma de instalação do plug-in da aplicação web.

Encriptação de Unidades (FDE)

- O Encriptação de disco Kaspersky não é compatível com computadores baseados em Arm.

- A Encriptação de Unidade BitLocker não é compatível com computadores com o Windows Home.

- Com a Encriptação BitLocker de Unidade, o utilizador pode alterar manualmente a palavra-passe de autenticação através da API do Windows. Nesses casos, o BitLocker ignora os requisitos de palavra-passe definidos na política do Kaspersky Endpoint Security. Por outras palavras, o utilizador pode definir qualquer palavra-passe.

- Depois de instalar a aplicação, deve reiniciar o sistema operativo para que a encriptação do disco rígido funcione corretamente.

- O Agente de Autenticação não suporta hieróglifos ou os caracteres especiais `|` e `\`.

- Para obter um desempenho ideal do computador após a encriptação, é necessário que o processador suporte o conjunto de instruções AES-NI (Intel Advanced Encryption Standard New Instructions). Se o processador não suportar as AES-NI, o desempenho do computador pode diminuir.

- Quando há processos que tentam aceder a dispositivos encriptados antes de a aplicação ter concedido acesso a esses dispositivos, a aplicação mostra um aviso informando de que tais processos devem ser parados. Se os processos não puderem ser parados, volte a ligar os dispositivos encriptados.

- As ID exclusivas dos discos rígidos são apresentadas nas estatísticas de encriptação do dispositivo em formato invertido.

- Não é recomendado formatar dispositivos enquanto estão a ser encriptados.

- Quando existem várias unidades amovíveis ligadas simultaneamente a um computador, a política de encriptação só pode ser aplicada a uma unidade amovível. Quando os dispositivos amovíveis voltam a ser ligados, a política de encriptação é aplicada corretamente.

- A encriptação pode não conseguir iniciar num disco rígido extremamente fragmentado. Desfragmente o disco rígido.

- Quando os discos rígidos são encriptados, a hibernação é bloqueada desde o momento em que a tarefa de encriptação é iniciada até à primeira reinicialização de um computador com o Microsoft Windows 7/8/8.1/10 e, após a instalação da encriptação do disco rígido, até à primeira reinicialização dos sistema operativos Microsoft Windows 8/8.1/10. Quando os discos rígidos são desencriptados, a hibernação é bloqueada desde o momento em que a unidade de inicialização é totalmente desencriptada até à primeira reinicialização do sistema operativo. Quando a opção Início rápido está ativada no Microsoft Windows 8/8.1/10, o bloqueio da hibernação impede que desligue o sistema operativo.

- Os computadores com Windows 7 não permitem alterar a password durante a recuperação quando o disco está encriptado com a tecnologia BitLocker. Depois de a chave de recuperação ser introduzida e o sistema operativo carregado, o Kaspersky Endpoint Security não irá solicitar ao utilizador que altere a password ou o código PIN. Como tal, é impossível definir uma nova password ou código PIN. Este problema resulta das peculiaridades do sistema operativo. Para continuar, é necessário voltar a encriptar o disco rígido.

- Não recomendamos a utilização da ferramenta xbootmgr.exe com fornecedores adicionais ativados. Por exemplo, Dispatcher, Rede ou Controladores.

- A formatação de uma unidade amovível encriptada não é suportada num computador com o Kaspersky Endpoint Security for Windows instalado.

- A formatação de uma unidade amovível encriptada com o sistema de ficheiros FAT32 não é suportada (a unidade é apresentada como encriptada). Para formatar uma unidade, reformate-a para o sistema de ficheiros NTFS.

- Não é possível a coexistência de vários agentes de transferência num computador encriptado.

- Uma tentativa de restaurar uma imagem de um disco GPT de arranque num estado não encriptado, o sistema operativo pode tornar o sistema operativo inoperacional. Para o evitar, siga estas recomendações:

    - Desencripte totalmente o disco antes de restaurar a imagem a partir da cópia de segurança.

    - Utilize a cópia setor a setor ao criar a imagem.

    - Elimine os dados dos primeiros setores do disco encriptado antes de restaurar a imagem e reinicializar o disco.

- É impossível aceder uma unidade amovível que tenha sido anteriormente encriptada num computador diferente quando todas as condições que se seguem são cumpridas em simultâneo:

  - Não há ligação ao servidor do Kaspersky Security Center.

  - O utilizador está a tentar a autorização com um novo token ou uma nova password.

  Se ocorrer uma situação semelhante, reinicie o computador. Depois de o computador ter sido reiniciado, o acesso à unidade amovível encriptada será concedido.

- A descoberta de dispositivos USB pelo Agente de Autenticação pode não ser suportada quando o modo xHCI para USB está ativado nas definições do BIOS.

- A Encriptação de Disco Kaspersky (FDE) para a parte SSD de um dispositivo utilizado para armazenar na cache os dados usados com mais frequência não é suportado para dispositivos SSHD.

- A encriptação de discos rígidos em sistemas operacionais Microsoft Windows 8/8.1/10 de 32 bits executados no modo UEFI não é suportada.

- Reinicie o computador antes de encriptar um disco rígido desencriptado novamente.

- A encriptação do disco rígido não é compatível com o Kaspersky Anti-Virus for UEFI. Não recomendamos a utilização da encriptação do disco rígido em computadores com o Kaspersky Anti-Virus for UEFI instalado.

- A criação de contas do Agente de Autenticação com base em contas da Microsoft é suportada com as seguintes limitações:

  - A tecnologia Single Sign-On não é suportada.

  - A criação automática de contas do Agente de Autenticação não é suportada se a opção de criar contas para utilizadores que iniciaram sessão 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, também será necessário alterar os nomes das contas que foram criadas para os utilizadores locais deste computador. Por exemplo, imagine que existe um utilizador local `Ivanov` no computador `Ivanov` e que foi criada uma conta do Agente de Autenticação com o nome `Ivanov/Ivanov` para este utilizador. Se o nome do computador `Ivanov` tiver sido alterado para `Ivanov-PC`, precisará de alterar o nome da conta do Agente de Autenticação para o utilizador `Ivanov` de `Ivanov/Ivanov` para `Ivanov-PC/Ivanov`. Pode alterar o nome da conta utilizando a tarefa de gestão de contas do Agente de Autenticação local. Antes de o nome da conta ter sido alterado, a autenticação no ambiente de pré-inicialização é possível utilizando o nome antigo (por exemplo, `Ivanov/Ivanov`).

- Se um utilizador tiver permissão para aceder a um computador que foi encriptado utilizando a tecnologia de Encriptação de Disco Kaspersky apenas usando um token e este utilizador precisar de concluir o procedimento de recuperação de acesso, certifique-se de que o mesmo tem acesso com base em password a este computador depois de o acesso ao computador encriptado ser restaurado. A password definida pelo utilizador ao restaurar o acesso pode não ter sido guardada. Nesse caso, o utilizador terá de concluir novamente o procedimento para restaurar o acesso ao computador encriptado na próxima vez que o computador for reiniciado.

- Ao desencriptar uma unidade de disco rígido utilizando a Ferramenta de Recuperação FDE, o processo de desencriptação pode terminar com um erro se os dados no dispositivo de origem forem substituídos pelos dados desencriptados. Parte dos dados do disco rígido permanecerá encriptada. Recomenda-se escolher a opção de guardar os dados desencriptados num ficheiro nas definições de desencriptação do dispositivo ao usar a Ferramenta de Recuperação FDE.

- Se a password do Agente de Autenticação tiver sido alterada, aparece uma mensagem contendo o texto *A sua password foi alterada com sucesso.Clique em OK* e o utilizador reinicia o computador, a nova password não é guardada. A password antiga tem de ser utilizada para autenticação subsequente no ambiente de pré-inicialização.

- A encriptação do disco é incompatível com a tecnologia Intel Rapid Start.

- A encriptação do disco é incompatível com a tecnologia ExpressCache.

- Em alguns casos, ao tentar desencriptar uma unidade encriptada utilizando a Ferramenta de Recuperação FDE, a ferramenta deteta erradamente o estado do dispositivo como «não encriptado» após a conclusão do procedimento de «Pedido-Resposta». O registo da ferramenta mostra um evento que informa de que o dispositivo foi desencriptado com êxito. Nesse caso, deve reiniciar o procedimento de recuperação de dados para desencriptar o dispositivo.

- Depois de o plug-in do Kaspersky Endpoint Security for Windows ter sido atualizado na Consola da Web, as propriedades do computador cliente não mostram a chave de recuperação do BitLocker enquanto o serviço da Consola da Web não for reiniciado.

- Para ver as outras limitações do suporte de encriptação de disco total e uma lista de dispositivos para os quais a encriptação de discos rígidos é suportada com restrições, consulte a Base de Conhecimento de Suporte Técnico.

Encriptação ao nível dos ficheiros (FLE)

- A encriptação de ficheiros não é suportada em computadores baseados em Arm.

- A encriptação de ficheiros e pastas não é compatível com os sistemas operativos Microsoft Windows Embedded.

- Depois de instalar a aplicação, é necessário reiniciar o sistema operativo para que a encriptação de ficheiros e pastas funcione devidamente.

- A aplicação suporta a encriptação de ficheiros apenas em dispositivos com sistemas de ficheiros NTFS e FAT32. Se um ficheiro encriptado for transferido para um dispositivo com um sistema de ficheiros não suportado (por exemplo, exFAT), o ficheiro nesse dispositivo não será encriptado e estará disponível para modificação.

- Se um ficheiro encriptado for armazenado num computador que tenha a funcionalidade de encriptação disponível e aceder ao ficheiro a partir de um computador onde a encriptação não está disponível, será disponibilizado o acesso direto a este ficheiro. Um ficheiro encriptado armazenado numa pasta de rede num computador com a funcionalidade de encriptação disponível é copiado de forma desencriptada para um computador que não possui a funcionalidade de encriptação disponível.

- Recomendamos que desencripte os ficheiros que foram encriptados com o Encrypting File System antes de encriptar ficheiros com o Kaspersky Endpoint Security for Windows.

- Depois de um ficheiro ser encriptado, o seu tamanho aumenta em 4 KB.

- Depois de um ficheiro ser encriptado, o atributo *Archive* é definido nas propriedades do ficheiro.

- Ao copiar o ficheiro desencriptado, por exemplo, para um suporte amovível, o ficheiro pode permanecer encriptado. Isto pode acontecer porque quando o gestor de ficheiros (por exemplo, explorer.exe) tenta obter acesso ao ficheiro encriptado, guarda o hash do ficheiro numa lista especial do processo. Depois de desencriptar o ficheiro, quando o gestor de ficheiros tenta obter acesso ao ficheiro, o processo procura o hash do ficheiro na lista. Se o hash for encontrado, o Kaspersky Endpoint Security deixa o ficheiro encriptado. Para o evitar, tem de limpar a lista do processo. O sistema operativo limpa automaticamente a lista do processo à medida que esta se vai enchendo. Também pode limpar a lista manualmente. Para o fazer, pode reiniciar o computador, reiniciar o processo que está a utilizar para obter acesso ao ficheiro (por exemplo, explorer.exe), ou pode utilizar um gestor de ficheiros diferente que não tenha utilizado para aceder ao ficheiro encriptado.

- Se um ficheiro não extraído de um arquivo encriptado tiver o mesmo nome de um ficheiro existente no seu computador, este último será substituído pelo novo ficheiro que é extraído do arquivo encriptado. O utilizador não é notificado sobre a operação de substituição.

- Antes de descompactar um arquivo encriptado, certifique-se de que tem espaço livre no disco suficiente para acomodar os ficheiros descompactados. Se não tiver espaço no disco suficiente, a descompactação do arquivo pode ser concluída, mas os ficheiros podem estar corrompidos. Neste caso, é possível que o Kaspersky Endpoint Security não exiba uma mensagem de erro.

- A interface do Gestor de ficheiros portátil não apresenta mensagens sobre erros que ocorrem durante a sua operação.

- O Kaspersky Endpoint Security for Windows não inicia o Gestor de Ficheiros Portátil num computador com o componente de Encriptação ao Nível dos Ficheiros instalado.

- Não é possível utilizar o Gestor de Ficheiros Portátil para aceder a uma unidade amovível se as seguintes condições forem verdadeiras em simultâneo:

  - Não há ligação ao Kaspersky Security Center;

  - O Kaspersky Endpoint Security for Windows está instalado no computador;

  - A encriptação de dados (FDE ou FLE) não foi realizada no computador.

  O acesso é impossível mesmo se souber a palavra-chave do Gestor de Ficheiros Portátil.

- Quando se utiliza a encriptação de ficheiros, a aplicação é incompatível com o cliente de correio Sylpheed.

- O Kaspersky Endpoint Security for Windows não suporta as regras de restrição do acesso a ficheiro encriptados para algumas aplicações. Isto deve-se ao facto de algumas operações de ficheiro serem realizadas por uma aplicação de terceiros. Por exemplo, a cópia de ficheiros é executada pelo gestor de ficheiros, e não pela aplicação. Desta forma, se o acesso a ficheiros encriptados for negado ao cliente de correio eletrónico do Outlook, o Kaspersky Endpoint Security permitirá que o cliente de correio eletrónico aceda ao ficheiro encriptado, se o utilizador copiou ficheiros para a mensagem de correio eletrónico através da área de transferência ou utilizando a função de arrastar e soltar. A operação de cópia foi realizada por um gestor de ficheiros, para o qual as regras de restrição de acesso a ficheiros encriptados não estão especificadas, ou seja, o acesso é permitido.

- Quando as unidades amovíveis são encriptadas com suporte no modo portátil, o controlo de antiguidade da password não pode ser desativado.

- A alteração das definições do ficheiro da página não é suportada. O sistema operativo usa os valores predefinidos em vez dos valores de parâmetro especificados.

- Utilize a remoção segura ao trabalhar com unidades amovíveis encriptadas. Não podemos garantir a integridade dos dados se a unidade amovível não for removida em segurança.

- Depois de os ficheiros serem encriptados, os seus originais não encriptados são eliminados com segurança.
- A sincronização de ficheiros offline utilizando o Client-Side Caching (CSC) não é suportada. A encriptação de ficheiros offline ou a tecnologia Branch Caching sobre SMB para servidores também não são suportadas. Recomenda-se proibir o gestão offline de recursos partilhados ao nível da política de grupo. Os ficheiros que estão no modo offline podem ser editados. Após a sincronização, as alterações feitas a um ficheiro offline podem ser perdidas.
- A criação de um arquivo encriptado na raiz do disco rígido do sistema não é suportada.
- Pode ter problemas ao aceder a ficheiros encriptados pela rede. É aconselhável mover os ficheiros para uma origem diferente ou certificar-se de que o computador que está a ser utilizado como servidor de ficheiros é gerido pelo mesmo Servidor de Administração do Kaspersky Security Center.
- Alterar o esquema do teclado pode fazer com que a janela de entrada da password para um arquivo encriptado de autoextração fique suspensa. Para resolver este problema, feche a janela de entrada da password, mude para o esquema de teclado no seu sistema operativo e volte a introduzir a password para o arquivo encriptado.
- Quando a encriptação de ficheiros é utilizada em sistemas com várias partições num disco, é aconselhável utilizar a opção que determina automaticamente o tamanho do ficheiro pagefile.sys. Depois de o computador ser reiniciado, o ficheiro pagefile.sys pode mover-se entre as partições do disco.
- Depois de aplicar as regras de encriptação de ficheiros, incluindo ficheiros na pasta *Os Meus Documentos*, certifique-se de que os utilizadores para os quais a encriptação foi aplicada podem aceder corretamente aos ficheiros encriptados. Para tal, cada utilizador deve iniciar sessão no sistema quando uma ligação ao Kaspersky Security Center estiver disponível. Se um utilizador tentar aceder a ficheiros encriptados sem uma ligação ao Kaspersky Security Center, o sistema pode ficar suspenso.
- Se os ficheiros do sistema forem de alguma forma incluídos no âmbito da encriptação ao nível dos ficheiros, poderão aparecer nos relatórios eventos relacionados com erros ao encriptar esses ficheiros. Os ficheiros especificados nesses eventos não são realmente encriptados.
- Os processos do Pico não são suportados.
- Os caminhos com distinção entre maiúsculas e minúsculas não são suportados. Quando se aplicam regras de encriptação ou regras de desencriptação, os caminhos nos eventos do produto são apresentados em letras minúsculas.
- Não é recomendado encriptar ficheiros utilizados pelo sistema na inicialização. Se esses ficheiros estiverem encriptados, uma tentativa para aceder a ficheiros encriptados sem uma ligação ao Kaspersky Security Center pode fazer com que o sistema fique suspenso ou resultar em pedidos de acesso a ficheiros não encriptados.
- Se os utilizadores trabalharem em conjunto com um ficheiro na rede ao abrigo das regras FLE através de aplicações que utilizam o método de mapeamento de ficheiro para memória (como o WordPad ou FAR) e aplicações concebidas para trabalhar com ficheiros grandes (como o Notepad ++), o ficheiro na forma não encriptada pode ser bloqueado indefinidamente sem a capacidade de ser acedido a partir do computador no qual reside.
- O Kaspersky Endpoint Security não encripta ficheiros localizados no armazenamento na nuvem do OneDrive ou noutras pastas que tenham OneDrive como nome. O Kaspersky Endpoint Security também bloqueia a cópia de ficheiros encriptados para as pastas do OneDrive se esses ficheiros não forem adicionados à regra de desencriptação.
- Quando o componente de encriptação ao nível dos ficheiros é instalado, a gestão de utilizadores e grupos não funciona no modo WSL (Windows Subsystem for Linux).

- Quando o componente de encriptação ao nível dos ficheiros é instalado, a POSIX (Portable Operating System Interface — Interface do Sistema Operativo Portátil) para renomear e eliminar ficheiros não é suportada.

- Não é recomendado encriptar ficheiros temporários, uma vez que pode causar a perda de dados. Por exemplo, o Microsoft Word cria ficheiros temporários ao processar um documento. Se os ficheiros temporários forem encriptados, mas o ficheiro original não for, o utilizador poderá receber o erro *Acesso negado* ao tentar guardar o documento. Além disso, o Microsoft Word pode guardar o ficheiro, mas não será possível abrir o documento na próxima vez, ou seja, os dados serão perdidos. Para evitar a perda de dados, precisa de excluir a pasta de ficheiros temporários das regras de encriptação.

Detection and Response (EDR, NDR, MDR, XDR, Sandbox)

- Não pode verificar um objeto colocado em quarentena como resultado da tarefa *Move file to Quarantine*.

- Não é possível colocar em quarentena um Alternate Data Stream (ADS) maior do que 4 MB. O Kaspersky Endpoint Security ignora qualquer ADS deste tamanho sem notificar o utilizador.

- O Kaspersky Endpoint Security não executa as tarefas *IOC Scan* em unidades de rede se o caminho da pasta nas propriedades da tarefa começar pela letra da unidade. O Kaspersky Endpoint Security apenas suporta o formato de caminho UNC para tarefas *IOC Scan* em unidades de rede. Por exemplo, `\\server\shared_folder`.

- Para garantir que a tarefa *IOC Scan* que utiliza os termos EmailItem funciona corretamente, o plug-in do Kaspersky Endpoint Security para a Web tem de ser atualizado para a versão mais recente.

- Em computadores baseados em Arm, a tarefa *IOC Scan* suporta ficheiros de e-mail apenas dos seguintes clientes de e-mail: versões de 32 e 64 bits do Outlook 2016 e Outlook 2021, 2024 e 365 para Arm64.

- A importação de um ficheiro de configuração de aplicação termina com um erro se a definição integração com o Kaspersky Sandbox estiver ativada no ficheiro de configuração. Antes de exportar definições da aplicação, desative o Kaspersky Sandbox. De seguida, execute o procedimento de exportação/importação. Após importar o ficheiro de connfiguração, ative o Kaspersky Sandbox.

- Ao importar uma política a partir de um ficheiro 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, depois de a política ser importada, o Kaspersky Endpoint Security não executa as funções do Agente EDR. Para que o Agente EDR funcione, abra a política, altere qualquer parâmetro e guarde as definições da política.

- Quando for detetado um indicador de comprometimento ao executar uma tarefa *IOC Scan*, a aplicação coloca um ficheiro em quarentena apenas para o termo FileItem. A colocação de um ficheiro em quarentena para outros termos não é suportada.

- O plug-in Web do Kaspersky Endpoint Security for Windows 11.7.0 ou posterior é necessário para gerir os detalhes de alerta. Os detalhes do alerta são necessários ao trabalhar com as soluções Endpoint Detection and Response (EDR Optimum e EDR Expert). Os detalhes do Detection estão disponíveis apenas na Consola Web do Kaspersky Security Center e na Cloud Console do Kaspersky Security Center.

- Migrar a configuração [KES+KEA] para a configuração [KES+agente incorporado] pode ser completada com um erro de remoção da aplicação Kaspersky Endpoint Agent. O erro de remoção da aplicação é corrigido na versão mais recente do Kaspersky Endpoint Agent. Para remover o Kaspersky Endpoint Agent, reinicie o computador e crie uma tarefa de remoção da aplicação.

- A configuração [agente integrado KES KEA] não é suportada. Esta configuração interfere com a interação entre as aplicações e a solução de Detection and Response que está implementada na sua organização. Além disso, a utilização do Kaspersky Endpoint Agent e do agente integrado no mesmo computador pode levar à duplicação da telemetria e ao aumento da carga no computador e na rede. Após migrar para a configuração [KES + agente incorporado], certifique-se de que o Kaspersky Endpoint Agent foi removido do computador. Se o Kaspersky Endpoint Agent continuar a funcionar após a migração, desinstale a aplicação manualmente (por exemplo, com a tarefa *Uninstall application remotely*).

  O instalador permite-lhe implementar o Kaspersky Endpoint Agent num computador com o Kaspersky Endpoint Security e o agente integrado instalados. O Kaspersky Endpoint Agent e o agente integrado também podem ser instalados num computador como resultado da tarefa *Alterar componentes da aplicação*. O comportamento depende das versões do Kaspersky Endpoint Security e do Kaspersky Endpoint Agent.

- Ao gerar detalhes de alerta, a aplicação fornece informações sobre a ameaça detetada, incluindo hashes de ficheiros modificados. O Kaspersky Endpoint Security calcula o hash do ficheiro enquanto gera detalhes de alerta. Considere que o hash original do ficheiro quando o evento de modificação do ficheiro foi gerado pode não ser o mesmo que o hash calculado quando os detalhes do alerta foram gerados.

- O agente integrado, EDR (KATA), retoma o isolamento de rede de um computador após o reinício do computador, mesmo que o período de isolamento tenha expirado. Para evitar o isolamento repetido do computador, precisa de desativar o isolamento de rede na consola da Kaspersky Anti Targeted Attack Platform.

- Recomendamos que atualize a aplicação após a conclusão do Isolamento da rede. Depois de atualizar o Kaspersky Endpoint Security, o Isolamento da rede pode ser parado.

- Os agentes integrados para o EDR (KATA), o EDR Optimum e o EDR Expert não são compatíveis entre si. Portanto, a ativação do agente integrado EDR com uma licença do Suplemento do Kaspersky Endpoint Detection and Response autónoma pode ser ignorada se tiver ativado o Kaspersky Endpoint Security com uma funcionalidade EDR diferente. Por exemplo, a ativação do agente integrado EDR (KATA) com uma licença autónoma é ignorada se tiver ativado o Kaspersky Endpoint Security com a licença [KES+EDR Optimum].

- No Kaspersky Endpoint Security, versão 12.1, o EDR (KATA) Agent integrado não oferece suporte aos seguintes metaficheiros para a tarefa *Obter metaficheiros 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. Suporte para estes metaficheiros foi adicionado ao Kaspersky Endpoint Security versão 12.2.

- Ao migrar do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security para a solução do Kaspersky Anti Targeted Attack Platform (EDR), pode encontrar erros ao ligar o computador aos servidores do Central Node. O motivo é que o assistente de migração na Consola Web salta as seguintes definições de política e não as migra:

  - Proibição de modificação de definições **Connection settings** ("cadeado").

    Por defeito, as definições podem ser modificadas (o "cadeado" está aberto). Por conseguinte, as definições não são aplicadas no computador. Tem de proibir a modificação das definições e fechar o "cadeado".

  - Cripto-contentor.

    Se estiver a utilizar autenticação bidirecional para ligar aos servidores do Central Node, tem de voltar a adicionar o cripto-contentor. O assistente de migração migra corretamente o certificado TLS do servidor.

  O Assistente de Política e Migração de Tarefas na Consola de Administração (MMC) migra todas as definições para a solução do Kaspersky Anti Targeted Attack Platform (EDR).

- O estado de ativação da aplicação é apresentado incorretamente quando a aplicação é instalada no modo Endpoint Detection and Response Agent para suportar a solução Kaspersky Managed Detection and Response sem ligação ao Kaspersky Security Center. Após a transferência do ficheiro BLOB, a área de notificação da barra de tarefas do Windows apresenta um estado incorreto: *A aplicação não está ativada*. No entanto, a interface de aplicação apresenta o estado de ativação corretamente. Reinicie o computador para que a aplicação funcione corretamente.

- O Kaspersky Endpoint Security permite a integração com a solução Kaspersky Anti Targeted Attack Platform usando o componente EDR (KATA) ou o Endpoint Sensor (não suportado). Note que só pode usar um dos componentes para interagir com a Kaspersky Anti Targeted Attack Platform. Para ver o estado do componente, abra as propriedades do computador na Consola de Administração (MMC), na secção **Applications**, abra as propriedades do Kaspersky Endpoint Security for Windows e aceda à secção **Components**. As seguintes considerações especiais aplicam-se à exibição do estado do componente para a interação com a Kaspersky Anti Targeted Attack Platform:

  - Para o plug-in de gestão 12.0 e versões anteriores, a aplicação apresenta o estado atual do **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 gestão 12.1 e versões posteriores, a aplicação exibe o estado geral do **Endpoint Detection and Response (KATA)**, que pode significar o estado do Endpoint Sensor ou o estado do componente EDR (KATA). Isto depende da versão da aplicação instalada no computador do utilizador e dos componentes disponíveis que pode utilizar para interagir com a Kaspersky Anti Targeted Attack Platform.

- A partir do Kaspersky Endpoint Security versão 12.6 e versões superiores, o Kaspersky Security Center Web Console versão 14.2 e versões inferiores não exibe corretamente o nome do componente **Endpoint Detection and Response (KATA)** nas propriedades do computador. Em vez do componente **Endpoint Detection and Response (KATA)**, a aplicação exibe o nome do componente **Endpoint Detection and Response Expert (KATA EDR)**. Para ver a lista de componentes, abra as propriedades do computador na Consola Web, na secção **Applications**, abra as propriedades do Kaspersky Endpoint Security for Windows e aceda à secção **Components**. A partir do Kaspersky Security Center Web Console versão 15.1 e versões superiores, a aplicação exibe corretamente o nome do componente.

- Ao atualizar o plug-in de gestão do Kaspersky Endpoint Detection and Response para a versão 15.3 instalada nas versões 14.0-14.2 da Consola Web, os detalhes do alerta são apresentados incorretamente. Para que os detalhes do alerta funcionem corretamente, reinicie o Servidor de Administração do Kaspersky Security Center.

- O plug-in de gestão do Kaspersky Endpoint Detection and Response versão 15.4 e posteriores não suporta o Kaspersky Security Center versão 14.0. Após a atualização do plug-in de gestão, os detalhes do alerta são apresentados incorretamente.

- As soluções do Kaspersky Extended Detection and Response (XDR) versão 1.4 não suportam o plug-in da Web do Kaspersky Endpoint Security for Windows versão 12.12 ou posterior. Pode manter a versão atual do plug-in da Web ou atualizar a solução XDR para a versão 2.0 ou posterior.

- O Kaspersky Endpoint Security não envia objetos destinados à arquitetura Arm para o Kaspersky Sandbox.

- O Kaspersky Endpoint Security suporta, no total, até 10 000 regras de filtragem de eventos de inclusão e exclusão do EDR Expert (on-premises).

- As regras de filtragem de eventos do EDR Expert (on-premises) não serão transferidas da política para os dispositivos geridos que executam o Kaspersky Endpoint Security versão 14.0 ou anterior, caso seja excedido o limite permitido para regras de filtragem armazenadas. A aplicação irá apresentar um aviso a esse respeito.

- As versões 12.11–14.1 do Kaspersky Endpoint Security for Windows não suportam os seguintes eventos de telemetria do EDR Expert (on-premises):
  - 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 suporta todos estes eventos de telemetria do EDR Expert (on-premises), exceto LDAP Attribute Change.

Outras limitações

- Os sistemas operativos Windows, a partir da versão 11 24H2, suportam a tecnologia UDP Receive Segment Coalescing Offload (URO). A tecnologia é ativada por predefinição se estiver instalada no computador uma placa de rede e controladores compatíveis. A desativação da URO no computador de um utilizador pode reduzir significativamente o desempenho da aplicação.
- O Kaspersky Endpoint Security suporta o subsistema WSL (Windows Subsystem for Linux) com restrições:
  - WSL 1. A aplicação monitoriza o tráfego de rede e deteta ameaças através de HTTP/HTTPS. Devido ao facto de o Kaspersky Endpoint Security usar o seu próprio certificado para verificar ligações HTTPS seguras, o funcionamento de algumas aplicações de terceiros pode ser interrompido.
  - WSL 2. A aplicação não suporta WSL 2.
- Se a aplicação devolve com erros ou suspende o funcionamento, poderá reiniciar automaticamente. Se a aplicação detetar erros recorrentes que causam o seu encerramento, a aplicação executa as operações seguintes:
  1. Desativa as funções de proteção e controlo (a funcionalidade de encriptação permanece ativada).
  2. Notifica o utilizador que as funções foram desativadas.
  3. Tenta restaurar a aplicação para um estado funcional após atualizar as bases de dados de antivírus ou aplicar as atualizações de módulo da aplicação.
- Os endereços Web adicionados à lista fiável poderão ser processados incorretamente.
- Na consola do Kaspersky Security Center, não pode guardar um ficheiro no disco a partir da pasta **Advanced** → **Repositories** → **Active threats**. Para guardar o ficheiro, tem de desinfetar o ficheiro infetado. Ao desinfetar, a aplicação guarda uma cópia do ficheiro na Cópia de segurança. Agora pode guardar o ficheiro no disco a partir da pasta **Advanced** → **Repositories** → **Backup**.

- A herança das definições de transferência de dados para o Servidor de Administração (**Definições gerais → Relatórios e armazenamento → Transferência de dados para o Servidor de administração**) difere da herança de outras definições. Se tiver permitido a alteração das definições de transmissão de dados na política (o "cadeado" está aberto), estas definições serão repostas para os valores predefinidos nas propriedades do computador local na consola, se não tiverem sido previamente definidas. Se estas definições tiverem sido definidas anteriormente, os seus valores serão restaurados. Ao eliminar uma política, as definições são herdadas da mesma forma. Nestes casos, são herdadas outras definições nas propriedades do computador local da política.

- O Kaspersky Endpoint Security monitoriza o tráfego HTTP que está em conformidade com os padrões RFC 2616, RFC 7540, RFC 7541, RFC 7301. Se o Kaspersky Endpoint Security detetar um outro formato de troca de dados no tráfego HTTP, a aplicação bloqueia esta ligação para impedir que sejam descarregados ficheiros maliciosos da Internet.

- O Kaspersky Endpoint Security impede a comunicação através do protocolo QUIC. Os navegadores utilizam o protocolo de transporte padrão (TLS ou SSL), independentemente de o suporte QUIC estar ou não ativado no navegador.

- Erros de ligação TLS podem ocorrer quando o software de terceiros funciona com a biblioteca Libcurl. Tal pode estar relacionado com o certificado Kaspersky que o Kaspersky Endpoint Security usa para verificar ligações encriptadas. Para continuar a trabalhar, pode desativar a validação de certificado para software de terceiros (não recomendado) ou adicionar um certificado 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, é possível que uma aplicação assinada digitalmente seja temporariamente colocada no grupo errado. A aplicação assinada digitalmente será posteriormente colocada no grupo correto.

- Durante uma nova verificação de um objeto malicioso que foi bloqueado por um software de terceiros, o utilizador não é notificado quando a ameaça é detetada novamente. O evento de nova deteção de ameaça é apresentado no relatório da aplicação e no relatório do Kaspersky Security Center.

- O relatório do Kaspersky Security Center sobre encriptação de dispositivos não incluirá informações sobre dispositivos que foram encriptados utilizando o Microsoft BitLocker em plataformas de servidor ou em estações de trabalho nas quais o componente Controlo de Dispositivos não está instalado.

- Não é possível ativar a apresentação de todas as entradas do relatório na Consola Web do Kaspersky Security Center. Na Consola Web, apenas pode alterar o número de entradas apresentadas nos relatórios. Por predefinição, a Consola Web do Kaspersky Security Center apresenta 1000 entradas do relatório. Pode ativar a apresentação de todas as entradas do relatório na Consola de Administração (MMC).

- Não é possível definir a apresentação de mais de 1000 entradas do relatório na Consola do Kaspersky Security Center. Se definir um valor superior a 1000, a Consola do Kaspersky Security Center irá apenas apresentar 1000 entradas do relatório.

- Ao utilizar uma hierarquia de políticas, as definições da secção Encriptação de Unidades Amovíveis numa política subordinada estão acessíveis para edição se a política principal proibir a modificação dessas definições.

- Deve ativar a opção Auditar Início de Sessão nas definições do sistema operativo para garantir o funcionamento adequado das exclusões para a proteção de pastas partilhadas contra encriptação externa.

- Se a proteção de pastas partilhadas estiver ativada, o Kaspersky Endpoint Security for Windows monitoriza as tentativas de encriptação de pastas partilhadas para cada sessão de acesso remoto que tenha sido iniciada antes do arranque do Kaspersky Endpoint Security for Windows, inclusive se o computador a partir do qual a sessão de acesso remoto foi iniciada tiver sido adicionado às exclusões. Se não quiser que o Kaspersky Endpoint Security for Windows monitorize as tentativas de encriptação de pastas partilhadas nas sessões de acesso remoto que foram iniciadas a partir de um computador adicionado às exclusões e que foram iniciadas antes do arranque do Kaspersky Endpoint Security for Windows, termine e restabeleça a sessão de acesso remoto ou reinicie o computador no qual o Kaspersky Endpoint Security for Windows se encontra instalado.

- Se a tarefa de atualização for executada com as permissões de uma conta de utilizador específica, os patches do produto não serão transferidos durante a atualização a partir de uma origem que requeira autorização.

- A aplicação poderá não se conseguir iniciar devido ao desempenho insuficiente do sistema. Para resolver este problema, utilize a opção Ready Boot ou aumente o tempo limite do sistema operativo para iniciar os serviços.

- A aplicação não pode funcionar no Safe Mode do Windows.

- Não podemos garantir que o Controlo de Áudio funcionará até depois da primeira reinicialização, após a instalação da aplicação.

- Na Consola de Administração (MMC), nas definições da Prevenção contra invasões na janela de configuração de permissões da aplicação, o botão **Remover** está indisponível. Pode remover uma aplicação de um grupo fiável através do menu de contexto da aplicação.

- Na interface local da aplicação, nas definições da Prevenção contra invasões, as permissões da aplicação e os recursos protegidos não estão disponíveis para visualização se o computador for gerido por uma política. As opções deslocar, pesquisar, filtros e outros controlos da janela estão indisponíveis. Pode ver as permissões da aplicação nas propriedades da políticas na Consola do Kaspersky Security Center.

- Quando os ficheiros de rastreio rodados estão ativados, não é criado nenhum rastreio para o componente AMSI e para o plug-in do Outlook.

- Os rastreios de desempenho não podem ser recolhidos manualmente no Windows Server 2008.

- Os rastreios de desempenho para o tipo de rastreio «Reiniciar» não são suportados.

- O registo de informação não é suportado em processos do Pico.

- Desativar a opção **Desativar a gestão externa dos serviços do sistema** não permitirá a interrupção do serviço da aplicação que foi instalada com o parâmetro `AMPPL=1` (por predefinição, o valor do parâmetro é definido como `1` a partir da versão do sistema operativo do Windows 10RS2). O parâmetro `AMPPL` com o valor `1` permite a utilização da tecnologia de Processos de Proteção para o serviço do produto.

- Para executar a verificação personalizada de uma pasta, o utilizador que inicia a verificação personalizada tem de ter as permissões para ler os atributos desta pasta. Caso contrário, a verificação personalizada da pasta será impossível e terminará com um erro.

- Quando uma regra de verificação definida numa política inclui um caminho sem o carácter `\` no final, por exemplo, `C:\folder1\folder2`, a verificação será executada para o caminho `C:\folder1\`.

- Se estiver a utilizar (Software Restriction Policies, SRP), o computador pode não conseguir carregar (ecrã preto). Para evitar o funcionamento incorreto, é necessário permitir a utilização de bibliotecas da aplicação nas propriedades do SRP. Nas propriedades do SRP, adicione a regra com nível de segurança **Sem restrições** ao ficheiro khkum.dll (item do menu **Nova Regra de Hash**). O ficheiro encontra-se na pasta `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.2\klhk\klhk_x64\`. Se selecionou este método, é necessário limpar adicionalmente a caixa de verificação **Transferir atualizações dos módulos da aplicação** nas definições de tarefas *Atualizar* para o Kaspersky Endpoint Security. Para obter mais informações sobre a utilização das SRP, consulte a documentação da Microsoft.

  Também pode desativar o SRP e utilizar o componente Controlo das Aplicações do Kaspersky Endpoint Security para controlar a utilização da aplicação.

- Se o computador pertencer a um domínio sob o Objeto da Política de Grupo do Windows (Group Policy Object, GPO) com o parâmetro DriverLoadPolicy definido para 8 (Good only), reiniciar o computador com o Kaspersky Endpoint Security instalado causa um BSOD. Para evitar uma falha, o parâmetro Early Launch Antimalware (ELAM) na Política de Grupo deve ser definido como 1 (Good and unknown). As definições do ELAM estão localizadas na política em: **Computer Configuration** → **Administrative Templates** → **System** → **Early Launch Antimalware**.

- A gestão das definições do plug-in do Outlook através da API Rest não é suportada.

- As definições de execução de tarefas para um utilizador específico não podem ser transferidas entre dispositivos através de um ficheiro de configuração. Depois de as definições serem aplicadas a partir de um ficheiro de configuração, especifique manualmente o nome de utilizador e a password.

- Depois de instalar uma atualização, a tarefa de verificação de integridade não funciona enquanto o sistema não for reiniciado para aplicar a atualização.

- Quando o nível de rastreio rodado é alterado através do utilitário de diagnóstico remoto, o Kaspersky Endpoint Security for Windows apresenta incorretamente um valor em branco para o nível de rastreio. No entanto, os ficheiros de rastreio são gravados de acordo com o nível de rastreio correto. Quando o nível de rastreio rodado é alterado através da interface local da aplicação, o nível de rastreio é modificado corretamente, mas o utilitário de diagnóstico remoto apresenta incorretamente o nível de rastreio que foi definido pela última vez pelo utilitário. Isso pode fazer com que o administrador não tenha informações atualizadas sobre o nível de rastreio atual e, se um utilizador alterar manualmente o nível de rastreio na interface local da aplicação, poderão faltar informações relevantes nos rastreios.

- Na interface local, as definições de proteção da password não permitem a alteração do nome da conta do administrador (por predefinição, KLAdmin). Para alterar o nome da conta do administrador, tem de desativar a proteção por password, depois ativá-la e especificar o novo nome da conta do administrador.

- A aplicação Kaspersky Endpoint Security, quando instalada num servidor do Windows Server 2019, não é compatível com o Docker. A implementação de contentores do Docker num computador com o Kaspersky Endpoint Security provoca uma falha (BSOD).

- Se o Kaspersky Endpoint Security estiver instalado num servidor do DBMS SQL Server, a aplicação envia pedidos à instância do servidor. Isto é necessário para analisar os trabalhos do Agente SQL Server e impedir a execução de trabalhos maliciosos. O Kaspersky Endpoint Security usa a conta de utilizador do SQL Server para verificar trabalhos. A aplicação envia pedidos ao servidor quando analisa a memória do sistema e depois de atualizar as bases de dados antivírus.

- A compatibilidade do Kaspersky Endpoint Security e do software Secret Net Studio é limitada:

  - A aplicação Kaspersky Endpoint Security não é compatível com o componente Antivírus do software Secret Net Studio.

    A aplicação não pode ser instalada num computador onde o Secret Net Studio é implementado com o componente Antivírus. Para possibilitar a interoperabilidade, tem de remover o componente Antivírus do Secret Net Studio.

  - A aplicação Kaspersky Endpoint Security não é compatível com o componente Proteção de disco e encriptação de dados do software Secret Net Studio.

    A aplicação não pode ser instalada num computador onde o Secret Net Studio é implementado com o componente Proteção de disco e encriptação de dados. Para possibilitar a interoperabilidade, tem de remover o componente Proteção de disco e encriptação de dados do Secret Net Studio.

  - O Secret Net Studio não é compatível com o componente Encriptação ao nível dos ficheiros (FLE) do Kaspersky Endpoint Security.

    Ao instalar o Kaspersky Endpoint Security com o componente Encriptação ao nível dos ficheiros (FLE), o Secret Net Studio pode funcionar com erros. Para garantir a interoperabilidade, tem de remover o componente Encriptação ao nível dos ficheiros (FLE) do Kaspersky Endpoint Security.

- Ao importar as regras de Monitorização da integridade do sistema, a aplicação verifica o ID e o nome da regra. Se os ID das regras forem os mesmos, o Kaspersky Endpoint Security substitui as regras existentes pela nova regra. Ao exportar as regras, a aplicação atribui automaticamente ID. Podem existir regras com ID idênticos, por exemplo, se tiver editado manualmente ficheiros XML de regras exportados. Se os ID das regras forem únicos, mas os nomes das regras forem os mesmos, o Kaspersky Endpoint Security adiciona `(1)` e assim por diante ao nome da regra.

- A partir da versão 12.11 do Kaspersky Endpoint Security for Windows, não é possível ver as definições de uma política principal que esteja aberta num grupo secundário na Consola Web. A Consola Web também exibe um aviso: *This policy is inherited. You can edit the policy settings only in the administration group in which it was created*.

- Notificações pop-up com mais de 256 caracteres não são exibidas na Consola de Administração (MMC).

- Os nomes dos componentes na política e no pacote de instalação podem ser diferentes. Por exemplo, o Endpoint Detection and Response Expert (on-premises) pode ser denominado 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 variar dependendo da versão da aplicação.

Glossário

Agente de Autenticação

Interface que lhe permite realizar o processo de autenticação de modo a aceder a unidades de disco rígido encriptadas e carregar o sistema operativo após a encriptação da unidade de disco rígido de arranque.

Agente de Rede

Um componente do Kaspersky Security Center que permite a interação entre o Servidor de Administração e as aplicações da Kaspersky instaladas num nó da rede específico (estação de trabalho ou servidor). Este componente é comum a todas as aplicações da Kaspersky executadas com o Windows. As versões dedicadas do Agente de Rede são destinadas a aplicações executadas com outros sistemas operativos.

Âmbito de Proteção

Objetos que estão a ser constantemente verificados pelo componente Proteção essencial contra ameaças quando está em execução. Os âmbitos de proteção de componentes diferentes têm propriedades diferentes.

Âmbito de verificação

Objetos que o Kaspersky Endpoint Security verifica durante a execução de uma tarefa de verificação.

Arquivo

Um ou vários ficheiros compactados num único ficheiro comprimido. Uma aplicação especializada, denominada arquivador, é necessária para compactar e descompactar dados.

Autenticação Kerberos

Mecanismo de autenticação mútua entre o cliente e o servidor antes do estabelecimento de uma ligação, o que permite a comunicação em redes inseguras. O mecanismo baseia-se num pedido, que o utilizador obtém de um centro de autenticação fiável.

Base de dados de endereços de phishing

Uma lista de endereços da Internet que os especialistas da Kaspersky determinaram estarem relacionados com phishing. A base de dados é atualizada regularmente e pertence ao kit de distribuição da aplicação da Kaspersky.

Base de dados de endereços web maliciosos

A lista de endereços web cujo conteúdo pode ser considerado perigoso. A lista é criada pelos especialistas da Kaspersky. É regularmente atualizada e está incluída no kit de distribuição da aplicação da Kaspersky.

Bases de dados de antivírus

As bases de dados que contêm informação sobre as ameaças à segurança do computador conhecidas da Kaspersky, até à data de lançamento da base de dados de antivírus. As assinaturas das bases de dados de antivírus ajudam a detetar código malicioso nos objetos verificados. As bases de dados de antivírus são criadas pelos especialistas da Kaspersky e são atualizadas de hora a hora.

Certificado de licença

Um documento que a Kaspersky transfere para o utilizador em conjunto com o ficheiro-chave ou o código de ativação. Contém informações sobre a licença concedida ao utilizador.

Chave ativa

Uma chave atualmente utilizada pela aplicação.

Cloud Discovery

O Cloud Discovery gere o acesso dos utilizadores 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, *Partilha de ficheiros*, *Mensagens*, *E-mail*.

Desinfeção

Um método de processamento de objetos infetados que resulta numa recuperação total ou parcial dos dados. Nem todos os objetos infetados podem ser desinfetados.

Emissor do certificado

O centro de certificação que emitiu o certificado.

Falso alarme

Ocorre um falso alarme quando a aplicação da Kaspersky reporta como infetado um ficheiro que não está infetado, porque a assinatura do ficheiro é semelhante à assinatura do vírus.

Ficheiro infetado

Um ficheiro que contém código malicioso (código de software malicioso conhecido detetado ao verificar o ficheiro). A Kaspersky não recomenda a utilização destes ficheiros, uma vez que podem infetar o computador.

Ficheiro infetável

Um ficheiro que, devido à sua estrutura ou formato, pode ser utilizado por intrusos como "recipiente" para armazenar e difundir código malicioso. Estes são, normalmente, ficheiros executáveis, como extensões como .com, .exe e .dll. Existe um risco razoavelmente elevado de intrusão de código malicioso nestes ficheiros.

Ficheiro IOC

Um ficheiro que contém um conjunto de indicadores de comprometimento (IOC) que a aplicação tenta corresponder para contar uma deteção. A probabilidade de deteção pode ser maior se forem encontradas correspondências exatas com vários IOC files para o objeto como resultado da verificação.

Forma normalizada do endereço de um recurso da Internet

O formato normalizado do endereço de um recurso da Internet consiste numa representação textual de um endereço de recurso da Internet obtido através de normalização. A *normalização* é um processo através do qual a representação textual de um endereço de recurso da Internet é alterado de acordo com regras específicas (por exemplo, exclusão do início de sessão do utilizador, password e porta de ligação da representação de texto do endereço de recurso da Internet; além disso, o endereço do recurso da Internet é alterado de caracteres maiúsculos para minúsculos).

No que diz respeito ao funcionamento dos componentes de proteção, a finalidade da normalização de endereços de recursos da Internet é evitar a verificação de endereços de Internet, que podem apresentar uma sintaxe diferente, sendo, no entanto, fisicamente equivalentes, mais do que uma vez. No contexto da proteção antivírus, a finalidade da normalização de endereços de recursos da Internet é evitar a verificação de endereços de Internet, que podem apresentar uma sintaxe diferente, sendo, no entanto, fisicamente equivalentes, mais do que uma vez.

Exemplo:

Formato não normalizado de um endereço: www.Example.com\.

Formato normalizado de um endereço: www.example.com.

Gestor de ficheiros portátil

Esta é uma aplicação que fornece uma interface para trabalhar com ficheiros encriptados em unidades amovíveis quando a funcionalidade de encriptação não está disponível no computador.

Grupo de administração

Um conjunto de dispositivos que partilham funções comuns e um conjunto de aplicações da Kaspersky instaladas nos mesmos. Os dispositivos estão agrupados para que possam ser geridos como uma única unidade. Um grupo pode incluir outros grupos. É possível criar políticas de grupos e tarefas de grupos para cada aplicação instalada 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 de ser protegida.

Máscara

Representação do nome e extensão de um ficheiro, utilizando meta caracteres.

As máscaras de ficheiro podem conter quaisquer caracteres permitidos em nomes de ficheiros, incluindo meta caracteres:

- O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.

- Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. 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 criar exclusões de verificação.

- O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.

Objeto OLE

Um ficheiro anexado ou um ficheiro incorporado noutro ficheiro. As aplicações da Kaspersky permitem a verificação da existência de vírus em objetos OLE. Por exemplo, se inserir uma tabela do Microsoft Office Excel® num documento do Microsoft Office Word, a tabela é verificada como um objeto OLE.

OpenIOC

Um padrão aberto de descrições de Indicador de Comprometimento (IOC) com base em XML, que inclui mais de 500 diferentes Indicadores de Comprometimento.

Servidor de Integração

Componente do Kaspersky Endpoint Security for Virtualization Light Agent. Interage entre os componentes do Kaspersky Endpoint Security e a infraestrutura virtual.

SVM

Máquina virtual segura – uma máquina virtual especial na qual o serviço scanserver (Protection Server, um componente do Kaspersky Endpoint Security for Virtualization Light Agent) está instalado.

Tarefa

Funções executadas pela aplicação da Kaspersky como tarefas, por exemplo: Proteção de ficheiros em tempo real, Verificação completa do dispositivo, Atualização da Base de Dados.

Trusted Platform Module

Um microchip desenvolvido para fornecer funções básicas relacionadas com segurança (por exemplo, para armazenar chaves de encriptação). Um Trusted Platform Module está normalmente instalado na placa principal (motherboard) e interage com todos os outros componentes de sistema através do hardware de barramento.

Apêndices

Esta secção contém informações que complementam o corpo do documento.

Anexo 1. Definições da aplicação

Pode usar uma política, tarefas ou a interface da aplicação para configurar o Kaspersky Endpoint Security. É fornecida informação detalhada sobre os componentes da aplicação nas secções correspondentes.

Proteção contra ameaças de ficheiros

O componente Proteção contra ameaças de ficheiros permite-lhe impedir a infeção do sistema de ficheiros de um computador. Por predefinição, o componente de Proteção contra ameaças de ficheiros reside permanentemente na RAM do computador e verifica todos os ficheiros abertos, guardados ou executados em tempo real. Este componente verifica ficheiros em todas as unidades do computador, incluindo unidades conectadas. O componente fornece proteção ao computador com a ajuda das bases de dados antivírus, o serviço de nuvem da Kaspersky Security Network e análise heurística.

O componente verifica os ficheiros acedidos por um utilizador ou aplicação. Se for detetado um ficheiro malicioso, o Kaspersky Endpoint Security bloqueará a operação do ficheiro. A aplicação desinfeta ou elimina o ficheiro malicioso, dependendo das definições do componente Proteção contra ameaças de ficheiros.

Quando tenta aceder a um ficheiro cujos conteúdos são guardados no armazenamento da nuvem do OneDrive, o Kaspersky Endpoint Security transfere e verifica os conteúdos do ficheiro.

Definições do componente Proteção contra ameaças de ficheiros

Parâmetro	Descrição
Nível de segurança *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	Para a Proteção contra ameaças de ficheiros, o Kaspersky Endpoint Security pode aplicar diferentes grupos de definições. Estes grupos de definições armazenados na aplicação chamam-se *níveis de segurança*. • **Alto**. Quando este nível de segurança de ficheiros está selecionado, o componente Proteção contra ameaças de ficheiros assume o controlo mais rigoroso de todos os ficheiros abertos, guardados e iniciados. O componente Proteção contra ameaças de ficheiros verifica todos os tipos de ficheiro em todos os discos rígidos, unidades amovíveis e unidades de rede do computador. Também verifica arquivos, pacotes de instalação e objetos OLE incorporados. • **Recomendado**. Esse nível de segurança de ficheiro é recomendado pelos especialistas da Kaspersky Lab. O componente Proteção contra ameaças de ficheiros apenas verifica os formatos de ficheiro especificados em todos os discos rígidos, unidades amovíveis, unidades de rede do computador e objetos de OLE incorporados. O componente Proteção contra ameaças de ficheiros não verifica arquivos ou pacotes de instalação. • **Baixo**. As definições deste nível de segurança do ficheiro garantem a velocidade máxima da verificação. O componente Proteção contra ameaças de ficheiros verifica apenas ficheiros com as extensões especificadas em todos os discos rígidos, unidades amovíveis e unidades de rede do computador. O componente Proteção contra ameaças de ficheiros não verifica ficheiros compostos.
Tipos de ficheiros *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	**Todos os ficheiros**. Se esta definição estiver ativada, o Kaspersky Endpoint Security verifica todos os ficheiros sem exceção (todos os formatos e extensões). **Ficheiros verificados por formato**. Se esta configuração estiver ativada, a aplicação verifica apenas ficheiros infetáveis. Antes de verificar um ficheiro para código malicioso, o cabeçalho interno do ficheiro é analisado para determinar o formato do ficheiro (por exemplo, .txt, .doc ou .exe). A verificação também procura ficheiros com extensões de ficheiro específicas. **Ficheiros verificados por extensão**. Se esta configuração estiver ativada, a aplicação verifica apenas ficheiros infetáveis. O formato do ficheiro é então determinado com base na extensão do ficheiro.

Parâmetro	Descrição
Âmbito de verificação	Contém objetos que são verificados pelo componente Proteção contra ameaças de ficheiros. Um objeto de verificação pode ser um disco rígido, uma unidade amovível, uma unidade de rede, pasta, ficheiro ou vários ficheiros definidos por uma máscara. Por predefinição, o componente Proteção contra ameaças de ficheiros verifica os ficheiros iniciados em quaisquer discos rígidos, unidades de rede ou unidades amovíveis. O âmbito de proteção para estes objetos não pode ser alterado nem eliminado. Só é possível excluir apenas um objeto (como unidades amovíveis) das verificações.
Aprendizagem automática e análise de assinaturas *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	O método de análise de assinaturas e aprendizagem automática utiliza a base de dados do Kaspersky Endpoint Security que contém descrições de ameaças conhecidas e formas de as neutralizar. A proteção que utiliza este método fornece o nível de segurança mínimo aceitável. Com base nas recomendações dos especialistas da Kaspersky, a aprendizagem automática e a análise de assinaturas estão sempre ativadas.
Análise heurística *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	A tecnologia foi desenvolvida para detetar ameaças que não é possível detetar utilizando a versão atual das bases de dados da aplicação da Kaspersky. Permite detetar ficheiros que podem estar infetados com um vírus desconhecido ou com uma variante de um vírus conhecido. Ao verificar ficheiros de códigos maliciosos, o analisador heurístico executa instruções nos ficheiros executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível da análise heurística garante um equilíbrio entre o detalhe das procuras de novas ameaças, a carga nos recursos do sistema operativo e a duração da análise heurística.
Ação após deteção de ameaças	**Desinfetar, eliminar se a desinfeção falhar**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação elimina o ficheiro. **Desinfetar, bloquear se a desinfeção falhar**. Se esta opção estiver selecionada, a aplicação tenta automaticamente desinfetar o ficheiro infetado que foi detetado. Se a desinfeção falhar, a aplicação bloqueia este ficheiro. **Bloquear**. Se esta opção for selecionada, a aplicação bloqueia automaticamente o ficheiro infetado sem tentar desinfetá-lo ou eliminá-lo. Antes de tentar desinfetar ou eliminar um ficheiro infetado, a aplicação cria uma cópia de segurança do ficheiro para o caso de vir a precisar de o restaurar ou de o mesmo poder ser desinfetado no futuro.
Verificar apenas os ficheiros novos e modificados	Verifica apenas os ficheiros novos e os que foram modificados desde a última vez em que foram verificados. Isto ajuda a reduzir a duração de uma verificação. Este modo aplica-se a ficheiros simples e compostos.
Verificar arquivos	A verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros arquivos. A aplicação verifica arquivos não só pela extensão, mas também pelo formato. Ao verificar os arquivos, a aplicação efetua uma descompactação recursiva. Isto permite a deteção de ameaças dentro de arquivos multinível (um arquivo dentro de um arquivo).
Verificar pacotes de distribuição	Verificar pacotes de distribuição de aplicações de terceiros.
Verificar ficheiros em formatos do Microsoft Office	Verifica ficheiros do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Ficheiros de formato do Office incluem objetos OLE também. A aplicação verifica ficheiros em formato de escritório menores que 1 MB, independentemente de a caixa de seleção estar marcada ou não.
Verificar ficheiros de formatos de e-mail	Verifica ficheiros em formato de e-mail. A aplicação verifica ficheiros MSG e EML. Ficheiros em formato de e-mail incluem objetos OLE e ficheiros MHT também. O Kaspersky Endpoint Security verifica ficheiros de e-mail com menos de 1 MB, independentemente de a caixa de seleção estar marcada ou não.
Não descompactar ficheiros compostos extensos	Se esta caixa de verificação estiver selecionada, a aplicação não verifica ficheiros compostos se o tamanho destes exceder o valor especificado. Se esta caixa de verificação for desmarcada, a aplicação verifica ficheiros compostos de todos os tamanhos. A aplicação verifica ficheiros grandes extraídos de arquivos, independentemente de a caixa de seleção estar selecionada ou não.

Parâmetro	Descrição
Descompactar ficheiros compostos em 2.º plano	Se a caixa de seleção estiver assinalada, a aplicação fornece acesso a ficheiros compostos que são maiores do que o valor especificado antes da verificação desses ficheiros. Neste caso, o Kaspersky Endpoint Security descompacta e verifica os ficheiros compostos em segundo plano. A aplicação fornece acesso a ficheiros compostos mais pequenos que esse valor somente após descompactar e verificar esses ficheiros. Se a caixa de seleção não estiver assinalada, a aplicação apenas fornece acesso a ficheiros compostos após descompactar e verificar os ficheiros de qualquer tamanho.
Modo de verificação *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	O Kaspersky Endpoint Security verifica os ficheiros acedidos pelo utilizador, o sistema operativo ou uma aplicação em execução na conta do utilizador. **Modo inteligente**. Neste modo, a Proteção contra ameaças de ficheiros verifica um objeto com base numa análise das ações tomadas relativamente ao objeto. Por exemplo, ao trabalhar com um documento do Microsoft Office, o Kaspersky Endpoint Security verifica o ficheiro quando é aberto pela primeira vez e fechado pela última vez. As operações intermédias gravadas no ficheiro não fazem com que o mesmo seja verificado. **Ao aceder e modificar**. Neste modo, a Proteção contra ameaças de ficheiros verifica os objetos sem que há uma tentativa para os abrir ou modificar. **Ao aceder**. Neste modo, a Proteção contra ameaças de ficheiros verifica os objetos apenas aquando de uma tentativa para os abrir. **Ao executar**. Neste modo, a Proteção contra ameaças de ficheiros verifica os objetos aquando de uma tentativa para os executar.
Utilizar tecnologia iSwift *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. A tecnologia iSwift é um avanço da tecnologia iChecker para o sistema de ficheiros NTFS.
Utilizar tecnologia iChecker *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	Esta tecnologia permite aumentar a velocidade da verificação ao excluir determinados ficheiros da verificação. Os ficheiros são excluídos da verificação utilizando um algoritmo especial que tem em conta a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições de verificação. Existem limites para a tecnologia iChecker: não funciona com ficheiros grandes e aplica-se apenas a ficheiros com uma estrutura que o Kaspersky Internet Security reconheça (por exemplo, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).
Pausar a proteção contra ameaças de ficheiros *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	Isto interrompe temporariamente e automaticamente a operação da Proteção Contra Ameaças de Ficheiros no horário especificado ou ao trabalhar com as aplicações especificadas.
Verificação das operações de ficheiros executadas em contentores do Windows	Se uma ameaça for detetada dentro de um contentor, a aplicação aplica a ação selecionada para o componente Proteção contra ameaças de ficheiros. **Parar o contentor se a desinfeção falhar**. A aplicação pode não ter direitos de leitura e gravação suficientes para o objeto detetado. Nesse caso, não é possível desinfetar ou eliminar o objeto detetado. Se esta caixa de verificação estiver selecionada, a aplicação bloqueia o objeto detetado e para o contentor. Se esta caixa de verificação estiver desmarcada, a aplicação apenas bloqueia o objeto detetado. **Não verificar operações de ficheiros executadas em contentores do Windows**. Se a caixa de verificação estiver selecionada, a aplicação verifica o contentor apenas no arranque do contentor. Se a caixa de verificação estiver desmarcada, a aplicação analisa o contentor continuamente em tempo real.

Proteção contra ameaças da Web

O componente Proteção contra ameaças da Web impede a transferência de ficheiros maliciosos da Internet e também bloqueia a ligação a sites maliciosos e de phishing. O componente fornece proteção ao computador com a ajuda das bases de dados antivírus, o serviço de nuvem da Kaspersky Security Network e análise heurística.

O Kaspersky Endpoint Security monitoriza os tráfegos HTTP, HTTPS e FTP. O Kaspersky Endpoint Security monitoriza URL e endereços IP.

Para utilizar a Proteção contra ameaças da Web, tem de concluir a configuração inicial da aplicação:

- Para monitorização do tráfego HTTPS, ative a verificação de ligações encriptadas (ativado por padrão).
- Selecione as portas que o Kaspersky Endpoint Security deve monitorizar (por defeito, a aplicação monitoriza todas as portas).
- Selecione as aplicações cujo tráfego pretende que o Kaspersky Endpoint Security monitorize. A maioria dos navegadores já está presente na lista de aplicações recomendadas pela Kaspersky. Se o seu navegador não estiver na lista, adicione-o manualmente.
- Recomendamos que injete um script de interação de página de Internet no tráfego de Internet (por padrão, a injeção de script está desativada). Este script permite o registo de eventos de Proteção contra ameaças da Web para o registo de eventos da aplicação, registo de eventos do SO e relatórios.

Quando um utilizador tenta abrir um website de phishing ou malicioso, o Kaspersky Endpoint Security bloqueia o acesso e apresenta um aviso.

Definições do componente Proteção contra ameaças da Web

Parâmetro	Descrição
Nível de segurança *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	Para Proteção contra ameaças da Web, a aplicação pode aplicar diferentes grupos de definições. Estes grupos de definições armazenados na aplicação chamam-se *níveis de segurança*: • **Alto**. O nível de segurança utilizado pelo componente Proteção contra ameaças da Web para efetuar a verificação máxima do tráfego de Internet que um computador recebe via HTTP e FTP. A Proteção contra ameaças da Web verifica detalhadamente todos os objetos de tráfego de Internet, recorrendo à utilização do conjunto completo de bases de dados da aplicação, e executa a análise heurística mais aprofundada possível. • **Recomendado**. O nível de segurança que fornece o equilíbrio ideal entre o desempenho da aplicação e a segurança do tráfego de Internet. O componente Proteção contra ameaças da Web executa a análise heurística com o Nível médio de verificação. Este nível de segurança de tráfego de Internet é recomendado pelos especialistas da Kaspersky. • **Baixo**. As definições deste nível de segurança de tráfego de Internet asseguram a verificação mais rápida de tráfego de Internet. O componente Proteção contra ameaças da Web executa a análise heurística com o Nível superficial de verificação.
Ação após deteção de ameaças	**Bloquear**. Se esta opção estiver selecionada e um objeto for detetado do tráfego de Internet, o componente Proteção contra ameaças da Web bloqueia o acesso ao objeto e apresenta uma mensagem no navegador. **Informar**. Se essa opção for selecionada e um objeto infetado for detetado no tráfego de Internet, o Kaspersky Endpoint Security permitirá que esse objeto seja descarregado para o computador, mas adiciona informações sobre o objeto infetado à lista de ameaças ativas.
Verificar o endereço da Internet contra a base de dados de endereços da internet maliciosos *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	A verificação das ligações para determinar se estão incluídas na base de dados de endereços Web maliciosos permite localizar sites que foram adicionados à lista de bloqueio. A base de dados de endereços da Web maliciosos é mantida pela Kaspersky, incluída no pacote de instalação da aplicação e atualizada durante as atualizações da base de dados do Kaspersky Endpoint Security.
Usar análise heurística *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	A tecnologia foi desenvolvida para detetar ameaças que não é possível detetar utilizando a versão atual das bases de dados da aplicação da Kaspersky. Permite detetar ficheiros que podem estar infetados com um vírus desconhecido ou com uma variante de um vírus conhecido. Quando o tráfego da Internet é verificado quanto a vírus e outras aplicações que apresentam uma ameaça, o analisador heurístico executa instruções nos ficheiros executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível da análise heurística garante um equilíbrio entre o detalhe das procuras de novas ameaças, a carga nos recursos do sistema operativo e a duração da análise heurística.

Parâmetro	Descrição
Verificar o endereço da Internet contra a base de dados de endereços da Internet de phishing *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	A base de dados de endereços da Web de phishing inclui os endereços da Web de sites atualmente conhecidos, que são utilizados para iniciar ataques de phishing. A Kaspersky complementa esta base de dados de ligações de phishing com endereços obtidos da organização internacional Anti-Phishing Working Group. A base de dados de endereços de phishing está incluída no pacote de instalação da aplicação e é complementada com atualizações da base de dados do Kaspersky Endpoint Security.
Não verificar tráfego de Internet de URL fiáveis	Se esta opção estiver selecionada, o componente Proteção contra ameaças da Web não verifica o conteúdo de páginas de Internet ou websites cujos endereços estejam incluídos na lista de URL fiáveis. Pode adicionar o endereço específico e a máscara de endereço de uma página de Internet/site à lista de URL fiáveis. Também pode criar uma lista de exclusões gerais para ligações encriptadas. Neste caso, o Kaspersky Endpoint Security não verifica o tráfego HTTPS de endereços da Internet fiáveis quando os componentes Proteção contra ameaças da web, Proteção contra ameaças de correio e Controlo de Internet estão a fazer o seu trabalho.

Proteção contra ameaças de correio

O componente Proteção contra ameaças de correio verifica a existência de vírus e outras ameaças nos anexos das mensagens de e-mail recebidas e enviadas. O componente fornece proteção ao computador com a ajuda das bases de dados antivírus, o serviço de nuvem da Kaspersky Security Network e análise heurística.

A proteção contra ameaças ao correio verifica as mensagens recebidas e enviadas. A aplicação suporta POP3, SMTP, IMAP e NNTP nos seguintes clientes de e-mail:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Para verificar o tráfego nos clientes de e-mail Mozilla Thunderbird, MyOffice Mail e R7-Office Organizer, tem de adicionar um certificado Kaspersky ao armazenamento de certificados e selecionar o próprio armazenamento de certificados.

A Proteção contra ameaças de correio não oferece suporte a outros protocolos e clientes de e-mail.

A Proteção contra ameaças de correio pode nem sempre ser capaz de obter acesso de *nível de protocolo* a mensagens (por exemplo, ao usar a solução Microsoft Exchange). Por este motivo, a Proteção contra ameaças de correio inclui uma extensão para Microsoft Office Outlook. A extensão permite verificar mensagens ao *nível do cliente de e-mail*. A extensão Proteção contra ameaças de correio suporta as versões de 32 bits e 64 bits do Outlook 2010, 2013, 2016, 2019, 2021, 2024 e 365. Em computadores baseados em Arm, a extensão Proteção contra ameaças de correio suporta as versões de 32 bits e 64 bits do Outlook 2016, Outlook 2021, Outlook 2024 e Outlook 365 para Arm64.

O componente Proteção contra ameaças de correio não verifica as mensagens se o cliente de correio estiver aberto num navegador.

Quando se deteta um ficheiro malicioso num anexo, o Kaspersky Endpoint Security adiciona as informações sobre a ação executada ao assunto da mensagem, por exemplo, *[A mensagem foi processada] <assunto da mensagem>*.

Definições do componente Proteção contra ameaças de correio

Parâmetro	Descrição
Nível de segurança *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	Para Proteção contra ameaças de correio, a aplicação pode aplicar diferentes grupos de definições. Estes grupos de definições armazenados na aplicação chamam-se *níveis de segurança*: • **Alto**. Quando este nível de segurança de e-mail é selecionado, o componente Proteção contra ameaças de correio verifica mensagens de e-mail o mais completamente. O componente Proteção contra ameaças de correio verifica mensagens de e-mail de entrada e de saída, e executa a análise heurística profunda. O nível de segurança de correio Elevado é recomendado para ambientes de alto risco. Um exemplo de um ambiente deste tipo é a ligação a um serviço de e-mail gratuito, a partir de uma rede doméstica que não está protegida por uma proteção de e-mail centralizada. • **Recomendado**. O nível de segurança do e-mail que fornece o equilíbrio ideal entre o desempenho da aplicação e a segurança do e-mail. O componente Proteção contra ameaças de correio verifica mensagens de e-mail de entrada e de saída e executa a análise heurística de nível médio. Este nível de segurança de tráfego de e-mail é recomendado pelos especialistas da Kaspersky. • **Baixo**. Quando este nível de segurança de e-mail está selecionado, o componente Proteção contra ameaças de correio verifica apenas mensagens de e-mail de entrada, executa uma análise heurística superficial e não verifica arquivos anexados a mensagens de e-mail. Com este nível de segurança de e-mail, o componente Proteção contra ameaças de correio verifica mensagens de e-mail à velocidade máxima, com uma utilização mínima dos recursos do sistema operativo. O nível Baixo de segurança de e-mail é recomendado para utilização num ambiente bem protegido. Um exemplo de um ambiente deste tipo pode ser a rede local (LAN) de uma empresa com segurança de e-mail centralizada.
Ação após deteção de ameaças	**Desinfetar, eliminar se a desinfeção falhar**. Quando um objeto infetado é detetado numa mensagem de entrada ou saída, a aplicação tenta desinfetar o objeto detetado. O utilizador poderá aceder à mensagem com um anexo seguro. Se não for possível desinfetar o objeto, a aplicação elimina o objeto infetado. A aplicação adiciona as informações sobre a ação executada ao assunto da mensagem, por exemplo, *[A mensagem foi processada] <assunto da mensagem>*. **Desinfetar, bloquear se a desinfeção falhar**. Quando um objeto infetado é detetado numa mensagem de entrada, a aplicação tenta desinfetar o objeto detetado. O utilizador poderá aceder à mensagem com um anexo seguro. Se não for possível desinfetar o objeto, a aplicação adiciona um aviso ao assunto da mensagem. O utilizador poderá aceder à mensagem com o anexo original. Quando um objeto infetado é detetado numa mensagem de saída, a aplicação tenta desinfetar o objeto detetado. Se não for possível desinfetar o objeto, a aplicação bloqueia a transmissão da mensagem e o cliente de e-mail apresenta um erro. **Bloquear**. Se for detetado um objeto infetado numa mensagem de entrada, a aplicação adiciona um aviso ao assunto da mensagem. O utilizador poderá aceder à mensagem com o anexo original. Se for detetado um objeto infetado numa mensagem de saída, a aplicação bloqueia a transmissão da mensagem e o cliente de e-mail apresenta um erro.
Âmbito de proteção *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	O *Âmbito de proteção* inclui objetos que o componente verifica quando está em execução: Mensagens de entrada e de saída ou Apenas mensagens de entrada. Para proteger os seus computadores, precisa apenas de verificar as mensagens de entrada. Pode ativar a verificação de mensagens de saída para impedir que ficheiros infetados sejam enviados nos arquivos. Também pode ativar a verificação de mensagens de saída se quiser impedir que ficheiros em formatos específicos sejam enviados, como ficheiros de áudio e vídeo, por exemplo.
Verificar tráfego POP3, SMTP, NNTP e IMAP	A verificação pelo componente Proteção contra ameaças de correio do tráfego transferido através dos protocolos POP3, SMTP, NNTP e IMAP.
Ligar a extensão do Microsoft Outlook	Se esta caixa de verificação estiver selecionada, a verificação de mensagens de e-mail transmitidas através dos protocolos POP3, SMTP, NNTP, IMAP é ativada na extensão integrada no Microsoft Outlook. Se o correio for verificado utilizando a extensão do Microsoft Outlook, recomenda-se a utilização do Cached Exchange Mode. Para obter informações mais detalhadas sobre o Modo Exchange em Cache e recomendações sobre a sua utilização, consulte a Base de Conhecimentos da Microsoft.
Análise heurística *(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)*	A tecnologia foi desenvolvida para detetar ameaças que não é possível detetar utilizando a versão atual das bases de dados da aplicação da Kaspersky. Permite detetar ficheiros que podem estar infetados com um vírus desconhecido ou com uma variante de um vírus conhecido. Ao verificar ficheiros de códigos maliciosos, o analisador heurístico executa instruções nos ficheiros executáveis. O número de instruções executadas pelo analisador heurístico depende do nível especificado para o analisador heurístico. O nível da análise heurística garante um equilíbrio entre o detalhe das procuras de novas ameaças, a carga nos recursos do sistema operativo e a duração da análise heurística.

Parâmetro	Descrição
Verificar arquivos anexados	A verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros arquivos. A aplicação verifica arquivos não só pela extensão, mas também pelo formato. Ao verificar os arquivos, a aplicação efetua uma descompactação recursiva. Isto permite a deteção de ameaças dentro de arquivos multinível (um arquivo dentro de um arquivo). Se, durante a verificação, a aplicação detetar uma password para um arquivo no texto da mensagem, esta password será utilizada para verificar o conteúdo do arquivo em busca de aplicações maliciosas. Neste caso, a password não é guardada. Um arquivo é descompactado durante a verificação. Se ocorrer um erro de aplicação durante o processo de descompactação, poderá eliminar manualmente os ficheiros descompactados que são guardados no caminho seguinte: %systemroot%\temp. Os ficheiros têm o prefixo PR.
Analisar ficheiros anexados com formatos do Microsoft Office	Verifica ficheiros do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Ficheiros de formato do Office incluem objetos OLE também. A aplicação verifica ficheiros em formato de escritório menores que 1 MB, independentemente de a caixa de seleção estar marcada ou não.
Não verificar arquivos com tamanho superior a N MB	Se esta caixa de verificação estiver selecionada, o componente Proteção contra ameaças de correio exclui os arquivos anexados a mensagens de e-mail da verificação se o seu tamanho exceder o valor especificado. Se a caixa de verificação estiver desmarcada, o componente Proteção contra ameaças de correio verifica arquivos de qualquer tamanho anexados a mensagens de e-mail.
Limite o tempo de verificação de arquivos a N seg	Se a caixa de verificação estiver selecionada, o tempo reservado para a verificação de arquivos anexados a mensagens de e-mail está limitado ao período especificado.
Filtro de anexo	A filtragem de anexos não é aplicada às mensagens de e-mail enviadas. **Desativar filtragem**. Se esta opção estiver selecionada, o componente Proteção contra ameaças de correio não filtra ficheiros anexados a mensagens de e-mail. **Mudar o nome dos anexos dos tipos selecionados**. Se esta opção for selecionada, o componente de Proteção contra ameaças de correio substituirá o último carácter de extensão encontrado nos ficheiros anexados dos tipos especificados pelo carácter de sublinhado (por exemplo, anexo.doc_). Portanto, para abrir o ficheiro, o utilizador deve renomear o ficheiro. **Eliminar anexos dos tipos selecionados**. Se esta opção estiver selecionada, o componente Proteção contra ameaças de correio elimina ficheiros anexados dos tipos especificados das mensagens de e-mail. Na lista de máscaras de ficheiros, pode especificar os tipos de ficheiros anexados para mudar o nome ou eliminar mensagens de e-mail.

Proteção contra ameaças de Rede

O componente *Proteção contra ameaças de Rede* (também chamado de Intrusion Detection System, IDS) monitoriza o tráfego de entrada da rede quanto à existência de atividade característica de ataques à rede. Quando a aplicação deteta uma tentativa de ataque à rede no computador do utilizador, bloqueia a ligação da rede a o computador atacante. As bases de dados da aplicação fornecem descrições dos tipos de ataques de rede conhecidos e das formas utilizadas para os combater. A lista de ataques à rede que o componente Proteção contra ameaças de Rede deteta é atualizada durante as atualizações da base de dados e do módulo da aplicação.

Parâmetro	Descrição
Tratar a análise de portas e o congestionamento de rede como ataques	A *saturação de redes* é um ataque aos recursos da rede de uma organização (como os servidores de Internet). Este ataque consiste no envio de um grande número de solicitações, de modo a sobrecarregar a largura de banda dos recursos da rede. Quando tal acontece, os utilizadores não conseguem aceder aos recursos da rede da organização. Um ataque de *mapeamento de portas* consiste no mapeamento de portas UDP, portas TCP e serviços de rede no computador. Este ataque permite que o cibercriminoso identifique o grau de vulnerabilidade do computador antes de efetuar tipos mais perigosos de ataques à rede. O mapeamento de portas também permite que o cibercriminoso identifique o sistema operativo no computador e selecione os ataques de rede apropriados para tal sistema. Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security monitoriza o tráfego de rede para detetar estes ataques. Se um ataque for detetado, a aplicação notifica o utilizador e envia o evento correspondente ao Kaspersky Security Center. A aplicação fornece informações sobre o computador atacante, que são necessárias para tomar as ações oportunas de resposta à ameaça. Pode desativar a detecção destes tipos de ataques no caso de algumas das suas aplicações permitidas executarem operações que são típicas para estes tipos de ataques. Esta ação ajudará a evitar falsos diagnósticos positivos.
Bloquear dispositivos de ataque durante N min	Se esta opção estiver ativada, o componente Proteção contra ameaças de Rede adiciona o computador de ataque à lista de bloqueios. Isto significa que o componente Proteção contra ameaças de Rede bloqueia a ligação de rede do computador atacante após a primeira tentativa de ataque de rede durante o período de tempo especificado. Este bloqueio protege automaticamente o computador do utilizador de possíveis ataques de rede no futuro, com origem no mesmo endereço. O tempo mínimo que um computador atacante deve passar na lista do bloco é de um minuto. O tempo máximo é de 999 minutos. Pode ver a lista do bloco na janela da ferramenta Monitor de Rede. O Kaspersky Endpoint Security limpa a lista do bloco quando a aplicação é reiniciada e quando as definições da Proteção contra ameaças de Rede são alteradas.
Exclusões	Esta lista contém os endereços IP a partir dos quais a Proteção contra ameaças de Rede não bloqueia ataques de rede. Pode adicionar um endereço IP com porta e protocolo específicos. A aplicação não regista informação sobre os ataques de rede dos endereços IP que estejam na lista de exclusões.
Proteção contra ataques de MAC Spoofing	Um *ataque de simulação MAC* consiste em mudar o endereço MAC de um dispositivo de rede (placa de rede). Como resultado, um criminoso pode redirecionar os dados enviados para um dispositivo para outro dispositivo e obter acesso a estes dados. O Kaspersky Endpoint Security permite bloquear ataques de simulação MAC e receber notificações sobre os ataques.

Firewall

O componente da Firewall bloqueia ligações não autorizadas a um computador enquanto trabalha na Internet ou numa rede local. A Firewall controla também a atividade de rede das aplicações no computador. Isto permite-lhe proteger a sua LAN empresarial contra roubo de identidade e outros ataques. O componente fornece proteção ao computador com a ajuda das bases de dados antivírus, o serviço de nuvem da Kaspersky Security Network e *regras de rede* predefinidas.

O Agente de Rede é utilizado para interação com o Kaspersky Security Center. A Firewall cria automaticamente regras de rede necessárias para o funcionamento da aplicação e do Agente de Rede. Por conseguinte, a Firewall abre várias portas no computador. A função do computador determina as portas que são abertas (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

Pode configurar as regras da rede aos seguintes níveis:

- *Regras de pacotes de rede*. As regras de pacotes de rede impõem restrições aos pacotes de rede, independentemente da aplicação. Estas regras restringem o tráfego de entrada e de saída de rede, 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 aplicações*. As regras de rede de aplicações impões restrições à atividade de rede de uma aplicação especificada. Estas influenciam não só as características do pacote de rede, mas também a aplicação específica à qual este pacote de rede se destina ou que emitiu este pacote de rede.

O acesso controlado de aplicações aos recursos, processos e dados pessoais do sistema operativo é fornecido pelo componente Prevenção contra invasões utilizando *direitos da aplicação*.

Durante a primeira inicialização da aplicação, a Firewall executa as seguintes ações:

1. Verifica a segurança da aplicação ao usar bases de dados antivírus transferidas.

2. Verifica a segurança da aplicação na Kaspersky Security Network.

   Recomenda-se a participação na Kaspersky Security Network para ajudar a Firewall a funcionar de forma mais eficiente.

3. Coloca a aplicação num dos grupos de confiança: *Fiáveis*, *Restrições baixas*, *Restrições altas*, *Não fiáveis*.

   Um grupo fiável define os direitos em que o Kaspersky Endpoint Security se baseia para controlar a atividade da aplicação. O Kaspersky Endpoint Security coloca uma aplicação num grupo fiável, dependendo do nível de perigo que essa aplicação pode representar para o computador.

   O Kaspersky Endpoint Security coloca uma aplicação num grupo fiável para os componentes Firewall e Prevenção de Intrusão do Host. Não pode alterar o grupo fiável apenas para a Firewall ou Prevenção contra invasões.

   Caso se tenha recusado participar na KSN ou não haja rede, o Kaspersky Endpoint Security coloca a aplicação num grupo fiável, dependendo das definições do componente Prevenção de Intrusão do Host. Após receber a reputação da aplicação da KSN, o grupo fiável pode ser alterado automaticamente.

4. Bloqueia a atividade de rede da aplicação, dependendo do grupo fiável. Por exemplo, as aplicações no grupo fiável de *Restrições altas* não têm permissão para utilizar nenhuma das ligações de rede.

Na próxima vez que a aplicação for iniciada, o Kaspersky Endpoint Security verifica a integridade da aplicação. Se a aplicação não tiver sido modificada, o componente utiliza as atuais regras da rede da aplicação. Se a aplicação tiver sido modificada, a Kaspersky Endpoint Security analisa a aplicação como se estivesse a ser iniciada pela primeira vez.

Prioridades de regra de rede

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

As regras de pacotes de rede têm uma prioridade mais elevada do que as regras de rede para aplicações. Se estiverem especificadas regras de pacotes de rede e regras de rede para aplicações para o mesmo tipo de atividade de rede, a atividade de rede é processada de acordo com as regras de pacotes de rede.

As regras de rede para aplicações funcionam de uma forma específica. Uma regra de rede para aplicações inclui regras de acesso com base no estado da rede: *Rede pública*, *Rede local* ou *Rede fiável*. Por exemplo, por predefinição, não é permitida nenhuma atividade de rede das aplicações no grupo fiável *Restrições altas* em redes de todos os estados. Se for especificada uma regra de rede para uma aplicação individual (aplicação principal), os processos secundários de outras aplicações serão executados de acordo com a regra de rede da aplicação principal. Se não houver uma regra de rede para a aplicação, os processos subordinados serão executados de acordo com a regra de acesso à rede do grupo fiável da aplicação.

Por exemplo, proibiu toda a atividade de rede nas redes de todos os estados para todas as aplicações, salvo para o navegador X. Se iniciar a instalação do navegador Y (processo subordinado) a partir do navegador X (aplicação principal), o instalador do navegador Y acederá à rede e transferirá os ficheiros necessários. Após a instalação, não será permitida ao navegador Y nenhuma ligação de rede de acordo com as definições da Firewall. Para proibir a atividade de rede do instalador do navegador Y como um processo secundário, deve adicionar uma regra de rede para o instalador do navegador Y.

Tipos da ligação de rede

A Firewall permite controlar a atividade da rede, dependendo do tipo da ligação de rede. O Kaspersky Endpoint Security recebe o tipo da ligação de rede a partir do sistema operativo do computador. O tipo da ligação de rede no sistema operacional é definido pelo utilizador ao configurar a ligação. Pode alterar o tipo da ligação de rede nas definições do Kaspersky Endpoint Security. A Firewall monitoriza a atividade da rede, dependendo do tipo de rede, especificado nas definições do Kaspersky Endpoint Security, e não do sistema operativo.

Estão disponíveis os seguintes tipos de ligação de rede:

- **Rede pública**. A rede não está protegida por aplicações antivírus, firewalls ou filtros (como Wi-Fi num café). Quando um utilizador utiliza um computador ligado a uma destas redes, a Firewall bloqueia o acesso aos ficheiros e às impressoras deste computador. Os utilizadores externos também não conseguem aceder aos dados através de pastas partilhadas e acesso remoto ao ambiente de trabalho deste computador. A Firewall filtra a atividade de rede de cada aplicação, de acordo com as regras de rede definidas para a mesma.

  Por predefinição, a Firewall atribui o tipo *Rede pública* à Internet. Não é possível alterar o tipo da Internet.

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

- **Rede fiável**. Uma rede segura na qual um computador não está exposto a ataques ou a tentativas não autorizadas de acesso aos dados. A Firewall permite qualquer atividade da rede nas redes que tenham este estado.

Definições do componente Firewall

Parâmetro	Descrição
Regras de pacotes	Tabela com uma lista das regras de pacotes de rede. As regras de pacotes de rede servem para impor restrições aos pacotes de rede, independentemente da aplicação. Estas regras restringem o tráfego de entrada e de saída de rede, através de portas específicas do protocolo de dados selecionado. A tabela lista as regras de pacotes de rede pré-configuradas, recomendadas pela Kaspersky para uma proteção otimizada do tráfego de rede dos computadores que utilizam os sistemas operativos Microsoft Windows. A Firewall define a prioridade de execução de cada regra de pacotes de rede. A Firewall processa as regras de pacotes de rede pela ordem na qual são apresentadas na lista de regras de pacotes de rede, de forma descendente. A Firewall localiza a primeira regra de pacotes de rede adequada à ligação de rede e aplica-a, permitindo ou bloqueando a atividade da rede. A Firewall ignora depois todas as regras de pacotes de rede subsequentes para a ligação de rede específica. As regras de pacotes de rede têm uma prioridade mais elevada do que as regras de rede para aplicações.
Redes disponíveis	Esta tabela contém informações sobre as ligações de rede que a Firewall deteta no computador. Por predefinição, é atribuído o estado *Rede pública* à Internet. Não é possível alterar o estado da internet.
Regras de aplicações	**Aplicação**. Tabela de aplicações que são controladas pelo componente Firewall. As aplicações são atribuídas a grupos fiáveis. Um grupo fiável define os direitos utilizados pelo Kaspersky Endpoint Security ao controlar a atividade de rede das aplicações. Pode selecionar uma aplicação de uma única lista de todas as aplicações instaladas nos computadores sob a influência de uma política e adicionar a aplicação a um grupo fiável. **Regras de rede**. Tabela de regras de rede para aplicações que fazem parte de um grupo fiável. Em conformidade com estas regras, a Firewall regula a atividade da rede das aplicações. A tabela apresenta as regras de rede predefinidas recomendadas pelos especialistas da Kaspersky. Estas regras de rede foram adicionadas para proteger de maneira ideal o tráfego de rede dos computadores que executam sistemas operativos Windows. Não é possível eliminar as regras de rede predefinidas.

Prevenção de ataques BadUSB

Alguns vírus modificam o firmware de dispositivos USB para enganar o sistema operativo e fazer com que ele detete o dispositivo USB como teclado. Como resultado, o vírus pode executar comandos na sua conta de utilizador para transferir malware, por exemplo.

O componente "Prevenção de ataques BadUSB" bloqueia a ligação de dispositivos USB infetados que emulam um teclado ao computador.

Quando um dispositivo USB é ligado a um computador e identificado pelo sistema operativo como um teclado, a aplicação solicita ao utilizador que introduza um código numérico gerado pela aplicação a partir deste teclado ou utilizando um Teclado no Ecrã, se estiver disponível (consulte a figura abaixo). Este procedimento é conhecido como autorização de teclado.

Se o código tiver sido introduzido corretamente, a aplicação guarda os parâmetros de identificação – VID/PID do teclado e o número da porta à qual foi ligado – na lista de teclados autorizados. A autorização de teclado não precisa de ser repetida quando o teclado voltar a ser ligado ou depois de o sistema operativo ser reiniciado.

Quando o teclado autorizado é ligado ao computador numa porta USB diferente, a aplicação mostra uma solicitação para uma nova autorização deste teclado.

Se o código numérico tiver sido introduzido incorretamente, a aplicação gera um novo código. Pode configurar o número de tentativas de introdução do código numérico. Se o código numérico for introduzido incorretamente várias vezes ou a janela de autorização de teclado estiver fechada (ver figura abaixo), a aplicação bloqueia a ativação deste teclado. Após decorrido o tempo de bloqueio de dispositivo USB ou o sistema operativo ser reiniciado, a aplicação solicita ao utilizador que execute novamente a autorização do teclado.

A aplicação permite a utilização de um teclado autorizado e bloqueia um teclado que não foi autorizado.



Autorização de teclado

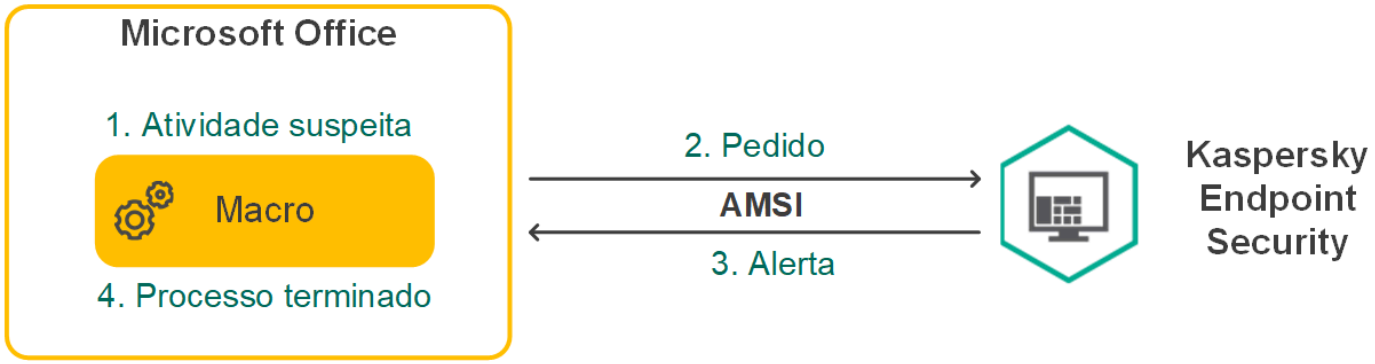
Definições do componente de Prevenção de ataques BadUSB

Parâmetro	Descrição
Proibir a utilização do teclado no ecrã para autorização de dispositivos USB	Se o botão estiver ativado, a aplicação bloqueia a utilização do Teclado no Ecrã para autorização de um dispositivo USB a partir do qual não pode ser introduzido um código de autorização.
Proibir a utilização de um código de barras para autorização de dispositivos USB	Se este botão estiver ativado, a aplicação não apresenta o código de barras na notificação de autenticação da verificação de código de barras.
Número máximo de tentativas de autorização do dispositivo USB	Bloquear automaticamente o dispositivo USB se o código de autorização for introduzido incorretamente o número especificado de vezes. Os valores válidos são de 1 a 10. Por exemplo, se permitir cinco tentativas de introdução do código de autorização, a aplicação bloqueia o dispositivo USB após a quinta tentativa sem sucesso. O Kaspersky Endpoint Security apresenta a duração do bloqueio do dispositivo USB. Após decorrido este tempo, tem novamente cinco tentativas para introduzir 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 sem sucesso de inserir o código de autorização. Os valores válidos são de 1 a 180 (minutos).

Proteção AMSI

O componente de Proteção AMSI destina-se a fins de suporte da Antimalware Scan Interface da Microsoft. A *Antimalware Scan Interface (AMSI)* permite às aplicações de terceiros com suporte AMSI enviar objetos (por exemplo, scripts PowerShell) ao Kaspersky Endpoint Security para uma verificação adicional e receber depois os resultados de verificação destes objetos. As aplicações de terceiros podem incluir, por exemplo, aplicações do Microsoft Office (ver a figura abaixo). Consulte a documentação da Microsoft, para obter informações mais detalhadas sobre AMSI.

A Proteção AMSI só pode detetar uma ameaça e notificar uma aplicação de terceiros sobre a ameaça detetada. Uma aplicação de terceiros depois de receber uma notificação de uma ameaça não permite as ações maliciosas (por exemplo, termina a ação).



Exemplo de operação AMSI

O componente de Proteção AMSI pode recusar um pedido de uma aplicação de terceiros, por exemplo, se esta aplicação exceder o número máximo de pedidos dentro de um intervalo especificado. O Kaspersky Endpoint Security envia informações sobre um pedido rejeitado de uma aplicação de terceiros para o servidor de administração. O componente Proteção AMSI não nega pedidos de aplicações de terceiros para os quais a integração contínua com o componente Proteção AMSI está ativado.

A Proteção AMSI está disponível para os seguintes sistemas operativos para estações de trabalho e servidores:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-sessão
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-sessão
- 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

Definições de Proteção AMSI

Parâmetro	Descrição
Verificar arquivos	A verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros arquivos. A aplicação verifica arquivos não só pela extensão, mas também pelo formato. Ao verificar os arquivos, a aplicação efetua uma descompactação recursiva. Isto permite a deteção de ameaças dentro de arquivos multinível (um arquivo dentro de um arquivo).
Verificar pacotes de distribuição	Verificar pacotes de distribuição de aplicações de terceiros.
Verificar ficheiros em formatos do Microsoft Office	Verifica ficheiros do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Ficheiros de formato do Office incluem objetos OLE também. A aplicação verifica ficheiros em formato de escritório menores que 1 MB, independentemente de a caixa de seleção estar marcada ou não.
Não descompactar ficheiros compostos extensos	Se esta caixa de verificação estiver selecionada, a aplicação não verifica ficheiros compostos se o tamanho destes exceder o valor especificado. Se esta caixa de verificação for desmarcada, a aplicação verifica ficheiros compostos de todos os tamanhos. A aplicação verifica ficheiros grandes extraídos de arquivos, independentemente de a caixa de seleção estar selecionada ou não.

Prevenção de explorações

O componente Prevenção de explorações deteta o código de programa que aproveita vulnerabilidades no computador para explorar privilégios de administrador ou realizar atividades maliciosas. Por exemplo, as explorações podem utilizar um ataque de capacidade da memória intermédia excedida. Para tal, a exploração envia uma grande quantidade de dados para uma aplicação vulnerável. Ao processar estes dados, a aplicação vulnerável executa código malicioso. Como resultado deste ataque, a exploração pode iniciar uma instalação não autorizada de software malicioso. Ao detetar que uma tentativa para executar um ficheiro executável a partir de uma aplicação vulnerável não foi executada pelo utilizador, o Kaspersky Endpoint Security bloqueia a execução desse ficheiro ou notifica o utilizador.

O componente Prevenção de explorações também monitoriza portas de rede em busca de processos de aplicações que podem ameaçar a segurança do computador. A aplicação obtém informações sobre tais processos com bases de dados de antivírus.

Definições do componente Prevenção de explorações

Parâmetro	Descrição
Ao detetar exploração	**Bloquear**. Se este item for selecionado, ao detetar uma exploração, o Kaspersky Endpoint Security bloqueia as operações desta exploração e cria uma entrada no registo com informação sobre a exploração. **Informar**. Se este item for selecionado, o Kaspersky Endpoint Security, ao detetar uma exploração, cria uma entrada no registo com informação sobre a exploração e adiciona informação sobre esta à lista de ameaças ativas.
Ativar proteção da memória de processos do sistema	Se este botão estiver ativado, o Kaspersky Endpoint Security bloqueia processos externos que tentam aceder à memória do processo de sistema.

Deteção de comportamento

O componente Deteção de comportamento recebe dados sobre as ações das aplicações no computador e transmite essas informações para outros componentes de proteção, de modo a melhorar o respetivo desempenho. O componente Deteção de comportamento utiliza Assinaturas de Fluxos de Comportamento (BSS) para aplicações. Se a atividade das aplicações corresponder uma assinatura de fluxo de comportamento, o Kaspersky Endpoint Security irá executar a ação de resposta selecionada. A funcionalidade do Kaspersky Endpoint Security é baseado em assinaturas de fluxos de comportamento e proporciona defesa proativa ao computador.

O componente Deteção de comportamento também monitoriza portas de rede em busca de processos de aplicações que podem ameaçar a segurança do computador. A aplicação obtém informações sobre tais processos com bases de dados de antivírus.

Definições do componente Deteção de comportamento

Parâmetro	Descrição
Ação ao detetar atividade de malware	**Eliminar**. Se esta opção estiver selecionada, ao detetar atividade maliciosa, o Kaspersky Endpoint Security elimina o ficheiro executável da aplicação maliciosa e cria uma cópia de segurança do ficheiro na Cópia de segurança. **Bloquear**. Se esta opção estiver selecionada, ao detetar atividade maliciosa, o Kaspersky Endpoint Security encerra a aplicação em questão. **Informar**. Se esta opção estiver selecionada e se for detetada atividade maliciosa de uma aplicação, o Kaspersky Endpoint Security não fecha a aplicação mas adiciona a informação sobre a atividade maliciosa da mesma à lista de ameaças ativas.

Prevenção contra invasões

O componente Prevenção contra invasões impede as aplicações de executarem ações que possam ser perigosas para o sistema operativo e garante o controlo do acesso aos recursos do sistema operativo e a dados pessoais. O componente fornece proteção ao computador com a ajuda das bases de dados antivírus e o serviço de nuvem da Kaspersky Security Network.

O componente controla a operação de aplicações utilizando *direitos da aplicação*. Os direitos da aplicação incluem os seguintes parâmetros de acesso:

- Acesso aos recursos do sistema operativo (por exemplo, opções de inicialização automática, chaves de registo)
- Acesso a dados pessoais (por exemplo, ficheiros e aplicações)

A atividade de rede das aplicações é controlada pelo componente da Firewall usando *regras de rede*.

Durante a primeira inicialização da aplicação, o componente Prevenção de Intrusão do Host executa as seguintes ações:

1. Verifica a segurança da aplicação ao usar bases de dados antivírus transferidas.
2. Verifica a segurança da aplicação na Kaspersky Security Network.

   Recomenda-se que participe na Kaspersky Security Network para ajudar o componente Prevenção contra invasões a funcionar de forma mais eficiente.

3. Coloca a aplicação num dos grupos de confiança: *Fiáveis*, *Restrições baixas*, *Restrições altas*, *Não fiáveis*.

   Um grupo fiável define os direitos em que o Kaspersky Endpoint Security se baseia para controlar a atividade da aplicação. O Kaspersky Endpoint Security coloca uma aplicação num grupo fiável, dependendo do nível de perigo que essa aplicação pode representar para o computador.

   O Kaspersky Endpoint Security coloca uma aplicação num grupo fiável para os componentes Firewall e Prevenção de Intrusão do Host. Não pode alterar o grupo fiável apenas para a Firewall ou Prevenção contra invasões.

   Caso se tenha recusado participar na KSN ou não haja rede, o Kaspersky Endpoint Security coloca a aplicação num grupo fiável, dependendo das definições do componente Prevenção de Intrusão do Host. Após receber a reputação da aplicação da KSN, o grupo fiável pode ser alterado automaticamente.

4. Bloqueia as ações da aplicação, dependendo do grupo fiável. Por exemplo, aplicações do grupo fiável *Restrições altas* têm acesso negado aos módulos do sistema operativo.

Na próxima vez que a aplicação for iniciada, o Kaspersky Endpoint Security verifica a integridade da aplicação. Se a aplicação não tiver sido modificada, o componente utiliza os direitos atuais da aplicação. Se a aplicação tiver sido modificada, a Kaspersky Endpoint Security analisa a aplicação como se estivesse a ser iniciada pela primeira vez.

Parâmetro	Descrição
Direitos de aplicações	Tabela de aplicações que são monitorizadas pelo componente Prevenção de Intrusão do Host. As aplicações são atribuídas a grupos fiáveis. Um grupo fiável define os direitos em que o Kaspersky Endpoint Security se baseia para controlar a atividade da aplicação. Pode selecionar uma aplicação de uma única lista de todas as aplicações instaladas nos computadores sob a influência de uma política e adicionar a aplicação a um grupo fiável. Os direitos de acesso à aplicação são apresentados nas seguintes tabelas: • **Ficheiros e registo do sistema**. Tabela de direitos de acesso a recursos do sistema operativo e dados pessoais para aplicações pertencentes ao grupo fiável. • **Direitos**. Tabela de direitos de acesso para processos e recursos do sistema operativo para aplicações pertencentes ao grupo fiável. • **Regras de rede**. Tabela de regras de rede para aplicações que fazem parte de um grupo fiável. Em conformidade com estas regras, a Firewall regula a atividade da rede das aplicações. A tabela apresenta as regras de rede predefinidas recomendadas pelos especialistas da Kaspersky. Estas regras de rede foram adicionadas para proteger de maneira ideal o tráfego de rede dos computadores que executam sistemas operativos Windows. Não é possível eliminar as regras de rede predefinidas.
Recursos protegidos	A tabela contém recursos do computador categorizados. O componente Prevenção contra invasões monitoriza as tentativas de outras aplicações de aceder aos recursos na tabela. Um recurso pode ser uma categoria de registo, ficheiro ou pasta, ou chave de registo.
Grupo fiável para aplicações iniciadas antes de o Kaspersky Endpoint Security	Um grupo fiável no qual o Kaspersky Endpoint Security colocará aplicações iniciadas antes do Kaspersky Endpoint Security.
Atualizar regras para aplicações anteriormente desconhecidas do KSN	Se a caixa de verificação estiver selecionada, o componente Prevenção contra invasões atualiza os direitos das aplicações anteriormente desconhecidas utilizando a base de dados do Kaspersky Security Network.
Confiar nas aplicações assinadas digitalmente	Se esta caixa de verificação estiver selecionada, o componente Prevenção contra invasões adiciona as aplicações com a assinatura digital de fornecedores fiáveis ao grupo *Fiáveis*. *Fornecedores fiáveis* são os fornecedores de software considerados fiáveis pela Kaspersky. Pode também adicionar manualmente um certificado de fornecedor ao arquivo de certificado fiável. Se esta caixa de verificação estiver desmarcada, o componente Prevenção contra invasões não considera tais aplicações como fiáveis e utiliza outros parâmetros para determinar o respetivo grupo fiável.
Eliminar regras para as aplicações que não são iniciadas há mais de N dias (de 1 a 90)	Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security eliminará automaticamente as informações sobre a aplicação (grupo fiável e direitos de acesso) se forem cumpridas as seguintes condições: • Se colocar manualmente uma aplicação num grupo fiável ou configurar os seus direitos de acesso. • A aplicação não for iniciada dentro do período de tempo definido. Se o grupo fiável e os direitos de uma aplicação forem determinados automaticamente, o Kaspersky Endpoint Security elimina as informações sobre essa aplicação após 30 dias. Não é possível alterar o período de armazenamento para obter informações sobre a aplicação ou desativar a eliminação automática. Na próxima vez que iniciar essa aplicação, o Kaspersky Endpoint Security analisa a aplicação como se fosse iniciada pela primeira vez.
Grupo fiável para aplicações não incluídas noutros grupos	Os itens nesta lista pendente determinam a que grupo fiável o Kaspersky Endpoint Security atribuirá uma aplicação desconhecida. Pode selecionar um dos itens seguintes: • **Restrições baixas**. • **Restrições altas**. • **Não fiáveis**.

Motor de remediação

O componente Motor de remediação permite que o Kaspersky Endpoint Security reverta ações que foram executadas por software malicioso no sistema operativo.

Ao reverter a atividade de software malicioso no sistema operativo, o Kaspersky Endpoint Security controla os seguintes tipos de atividade de software malicioso:

- **Atividade de ficheiros**

  O Kaspersky Endpoint Security executar as seguintes ações:

  - Elimina ficheiros executáveis que foram criados pelo malware (em toda a multimédia exceto unidades de rede).
  - Elimina ficheiros executáveis que foram criados por programas que foram infiltrados por software malicioso.
  - Restaura ficheiros que foram modificados ou eliminados por malware.

  A funcionalidade de recuperação de ficheiros possui um certo número de limitações.

- **Atividade de registo**

  O Kaspersky Endpoint Security executar as seguintes ações:

  - Elimina chaves de registo que foram criadas por malware.
  - Não restaura chaves de registo que foram modificadas ou eliminadas por malware.

- **Atividade de sistema**

  O Kaspersky Endpoint Security executar as seguintes ações:

  - Termina processos que foram iniciados por malware.
  - Termina processos nos quais tenha penetrado uma aplicação maliciosa.
  - Não retoma processos que tenham sido interrompidos por malware.

- **Atividade de rede**

  O Kaspersky Endpoint Security executar as seguintes ações:

  - Bloqueia a atividade da rede de malware.
  - Bloqueia a atividade da rede de processos que foram infiltrados por malware.

A reversão das ações do software malicioso pode ser iniciada pelo componente Proteção contra ameaças de ficheiros ou Deteção de comportamentos, ou durante uma verificação de software malicioso.

A reversão das operações de software malicioso afeta um conjunto de dados estritamente definido. A reversão não tem efeitos adversos no sistema operativo nem na integridade dos dados do seu computador.

Kaspersky Security Network



Para proteger o seu computador de forma mais eficaz, o Kaspersky Endpoint Security utiliza dados recebidos de utilizadores em todo o mundo. A Kaspersky Security Network foi concebida 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 na nuvem que fornece o acesso à Base de Conhecimento online da Kaspersky, que contém informações sobre a reputação de ficheiros, recursos da Internet e software. A utilização de dados da Kaspersky Security Network permite uma resposta mais rápida do Kaspersky Endpoint Security a novas ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos diagnósticos positivos. Se participar na Kaspersky Security Network, os serviços da KSN irão fornecer ao Kaspersky Endpoint Security informações sobre a reputação dos endereços Web verificados, bem como informações sobre a categoria e a reputação dos ficheiros verificados. Para obter mais informações sobre como configurar o acesso ao KSN, consulte a Ajuda do Kaspersky Security Center.

A utilização da Kaspersky Security Network é voluntária. A aplicação solicita que utilize a KSN durante a configuração inicial da aplicação. Os utilizadores podem começar ou interromper a participação na KSN em qualquer momento.

Para obter informações mais detalhadas sobre a informação estatística da Kaspersky gerada durante a participação na KSN e sobre o armazenamento e a destruição de tal, consulte a Declaração de Recolha de Dados da KSN e o site da Kaspersky. O ficheiro ksn_<ID do idioma>.txt com o texto da Declaração de Recolha de Dados da KSN está incluído no kit de distribuição da aplicação.

A infraestrutura das bases de dados de reputação da Kaspersky

O Kaspersky Endpoint Security suporta as seguintes soluções de infraestrutura para trabalhar com as bases de dados de reputação da Kaspersky:

- *Kaspersky Security Network (KSN)* é a solução usada pela maioria das aplicações da Kaspersky. Os participantes na KSN recebem informações da Kaspersky e enviam as informações à Kaspersky sobre os objetos detetados no computador do utilizador para fins de análise adicional pelos analistas da Kaspersky e inclusão nas bases de dados estatísticas e de reputação da Kaspersky Security Network.

- *Kaspersky Private Security Network (KPSN)* é uma solução que permite que utilizadores de computadores que alojam o Kaspersky Endpoint Security ou outras aplicações da Kaspersky tenham acesso às bases de dados de reputação do Kaspersky Security Network e a outros dados estatísticos sem enviar dados para o KSN a partir de seus próprios computadores. O KPSN foi criado para clientes empresariais que não podem participar na Kaspersky Security Network por qualquer um dos seguintes motivos:

  - As estações de trabalho locais não estão ligadas à Internet.

A transmissão de quaisquer dados para fora do país ou para fora da LAN empresarial é proibida por lei ou restringida por políticas de segurança empresariais.

Parâmetro	Descrição
Ativar o modo KSN alargado	*O modo KSN avançado* é um modo no qual o Kaspersky Endpoint Security envia dados adicionais à Kaspersky. O Kaspersky Endpoint Security usa a KSN para detetar ameaças, independentemente da posição do botão.
Ativar o modo de nuvem	*O Modo de nuvem* refere-se ao modo operacional da aplicação no qual o Kaspersky Endpoint Security utiliza uma versão simplificada das bases de dados antivírus. A Kaspersky Security Network suporta a operação da aplicação quando estão a ser usadas bases de dados antivírus simplificadas. A versão simplificada das bases de dados antivírus permite-lhe utilizar cerca de metade da RAM do computador que de outra forma seria utilizada com as bases de dados habituais. Se não participar na Kaspersky Security Network ou se o Modo de nuvem estiver desativado, o Kaspersky Endpoint Security transfere a versão completa das bases de dados antivírus dos servidores da Kaspersky. Se o botão estiver ativado, o Kaspersky Endpoint Security utiliza a versão simplificada das bases de dados de antivírus, o que reduz a carga nos recursos do sistema operativo. O Kaspersky Endpoint Security transfere a versão simplificada das bases de dados de antivírus durante a próxima atualização, após a caixa de verificação ser selecionada. Se o botão estiver desativado, o Kaspersky Endpoint Security utiliza a versão completa das bases de dados de antivírus. O Kaspersky Endpoint Security transfere a versão completa das bases de dados de antivírus durante a próxima atualização, após a caixa de verificação ser desmarcada.
Estado do computador quando os servidores da KSN não estão disponíveis *(disponível apenas na Consola do Kaspersky Security Center)*	Os itens nesta lista pendente determinam o estado de um computador no Kaspersky Security Center quando os servidores da KSN estão indisponíveis.
Usar um Servidor de administração como um servidor proxy KSN *(disponível apenas na Consola do Kaspersky Security Center)*	Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security utiliza o serviço de proxy da KSN. Pode configurar as definições do serviço de proxy da KSN nas propriedades do Servidor de administração.
Usar os servidores do Kaspersky Security Network se o servidor KSN proxy estiver indisponível *(disponível apenas na Consola do Kaspersky Security Center)*	Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security utiliza os servidores da KSN quando o serviço KSN Proxy estiver indisponível. Os servidores da KSN podem estar localizados quer na Kaspersky quer em terceiros (quando a Kaspersky Private Security Network é utilizada).

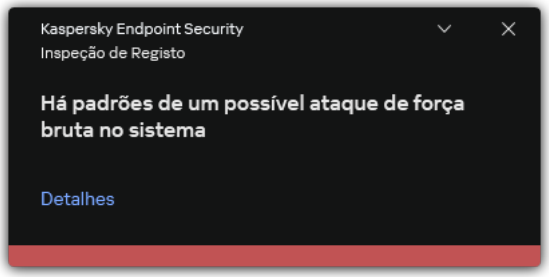
Inspeção do Registo

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para servidores. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para estações de trabalho.

A Inspeção de Registo monitoriza a integridade do ambiente protegido com base na análise do registo de eventos do Windows. Quando a aplicação deteta sinais de comportamento atípico no sistema, ela informa o administrador, visto que este comportamento pode indicar uma tentativa de ciberataque.

O Kaspersky Endpoint Security analisa os registos de eventos do Windows e deteta violações de acordo com as regras. O componente inclui regras predefinidas. As regras predefinidas são alimentadas por análise heurística. Também pode adicionar as suas próprias regras (regras personalizadas). Quando uma regra é acionada, a aplicação cria um evento com o estado *Critical* (veja a figura abaixo).

Se quiser utilizar a Inspeção de Registo, certifique-se de que as definições de segurança da política de auditoria estão configuradas e que o sistema está a registar os eventos relevantes (para obter detalhes, consulte o site de suporte técnico da Microsoft.).



Notificação da Inspeção de Registo

Definições da Inspeção de Registo

Parâmetro	Descrição
Regras predefinidas	Lista de regras da Inspeção de Registo. As regras predefinidas incluem modelos de atividade anormal no computador protegido. Atividade anormal pode significar uma tentativa de ataque.
Regras personalizadas	Lista de regras da Inspeção de Registo adicionadas pelo utilizador. Pode definir os seus próprios critérios de acionamento da regra da Inspeção de Registo. Para o fazer, tem de inserir um ID do evento e selecionar uma fonte do evento. Pode selecionar uma fonte do evento entre os registos padrão: *Application*, *Security* ou *System*. Também pode especificar o registo de uma aplicação de terceiros.

Anti-Cryptor

O componente Anti-Cryptor analisa a atividade em pastas partilhadas. Se esta atividade corresponder a uma assinatura de fluxo de comportamento que seja comum para encriptação externa, o Kaspersky Endpoint Security executa a ação selecionada.

O Kaspersky Endpoint Security apenas impede a encriptação externa dos ficheiros localizados em suportes que têm o sistema de ficheiros NTFS e não são encriptados pelo sistema EFS.

Parâmetro	Descrição
Exclusões por nome ou endereço IP	**Exclusões por nome ou endereço IP**. A lista de computadores a partir dos quais as tentativas de encriptar pastas partilhadas não serão monitorizadas. Para aplicar a lista de exclusões de computadores da proteção de pastas partilhadas contra encriptação externa, deve ativar a tarefa Auditar início de sessão na política de auditoria de segurança do Windows. Por predefinição, a tarefa Auditar início de sessão está desativada. Para obter mais informações detalhadas sobre uma política de auditoria de segurança do Windows, visite o site da Microsoft. **Exclusões por máscara**. Exclusões do âmbito de proteção. A exclusão de uma pasta de um âmbito de proteção pode reduzir a quantidade de falsos positivos se a sua organização utilizar encriptação de dados ao trocar ficheiros utilizando pastas partilhadas. Por exemplo, a Deteção de comportamento pode levantar falsos positivos quando o utilizador trabalha com ficheiros com a extensão ENC numa pasta partilhada. Essa atividade corresponde a um padrão de comportamento típico da encriptação externa. Se tiver ficheiros encriptados numa pasta partilhada para proteger dados, adicione essa pasta às exclusões. Usar máscaras: • O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas. • Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida. • O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.
Ação após deteção de ameaças	• **Informar**. Se esta opção for selecionada, ao detetar uma tentativa de modificar ficheiros em pastas partilhadas, o Kaspersky Endpoint Security adiciona informações sobre esta tentativa à lista de ameaças ativas, adiciona uma entrada a relatórios de interface de aplicação local e envia informações sobre a atividade maliciosa detetada ao Kaspersky Security Center. • **Bloquear ligação durante (min) N min**. Se esta opção for selecionada, quando o Kaspersky Endpoint Security detetar uma tentativa de modificar ficheiros em pastas partilhadas, ele irá bloquear o acesso à modificação do ficheiro para a sessão que iniciou a atividade maliciosa e irá criar cópias de segurança dos ficheiros modificados. Se o componente Motor de remediação for ativado e a opção **Bloquear ligação durante (min) N minutos** for selecionada, os ficheiros modificados são restaurados de cópias de segurança.
Âmbito de proteção	O *âmbito de proteção* é uma lista de caminhos para pastas partilhadas nas quais o Kaspersky Endpoint Security monitoriza a atividade de ficheiros. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara. Por padrão, a aplicação identifica automaticamente pastas partilhadas e monitoriza a atividade de ficheiros em todas as pastas.

Controlo de Internet

O Controlo de Internet gere o acesso do utilizador aos recursos da Web. Isto ajuda a reduzir o tráfego e o uso inadequado do tempo de trabalho. Quando um utilizador tenta abrir um website restrito pelo Controlo de Internet, o Kaspersky Endpoint Security bloqueia o acesso ou apresenta um aviso (consulte a figura abaixo).

Para utilizar o Controlo de Internet, tem de concluir a configuração inicial da aplicação:

- Para monitorização do tráfego HTTPS, ative a verificação de ligações encriptadas (ativado por padrão).
- Selecione as portas que o Kaspersky Endpoint Security deve monitorizar (por defeito, a aplicação monitoriza todas as portas).

- Selecione as aplicações cujo tráfego pretende que o Kaspersky Endpoint Security monitorize. A maioria dos navegadores já está presente na lista de aplicações recomendadas pela Kaspersky. Se o seu navegador não estiver na lista, adicione-o manualmente.

- Recomendamos que injete um script de interação de página de Internet no tráfego de Internet (por padrão, a injeção de script está desativada). Este script permite o registo de eventos do Controlo de Internet para o registo de eventos da aplicação, registo de eventos do SO e relatórios.

Métodos de gestão do acesso a sites

O Controlo de Internet permite-lhe configurar o acesso a sites usando os seguintes métodos:

- **Categoria do site**. Os sites são categorizados de acordo com o serviço de nuvem do Kaspersky Security Network, a análise heurística e a base de dados de sites conhecidos (incluídos nas bases de dados da aplicação). Por exemplo, pode restringir o acesso do utilizador à categoria *Redes sociais* ou a outras categorias.

- **Tipo de dados**. Pode restringir o acesso do utilizador aos dados num site e ocultar imagens, por exemplo. O Kaspersky Endpoint Security determina o tipo de dados com base no formato do ficheiro e não com base na sua extensão.

  O Kaspersky Endpoint Security não verifica ficheiros dentro de arquivos. Por exemplo, se os ficheiros de imagem forem colocados num arquivo, o Kaspersky Endpoint Security identifica o tipo de dados *Arquivos* e não *Gráficos*.

- **Endereço individual**. Pode introduzir um endereço da Web ou usar máscaras.

Pode usar simultaneamente vários métodos para regular o acesso a sites. Por exemplo, pode restringir o acesso ao tipo de dados *Ficheiros de aplicações de escritório* apenas para a categoria do site *E-mail baseado na Web*.

Regras de acesso a sites

O Controlo de Internet regula o acesso do utilizador a sites através das *regras de acesso*. Pode configurar as seguintes definições avançadas para uma regra de acesso ao site:

- Utilizadores aos quais a regra se aplica.

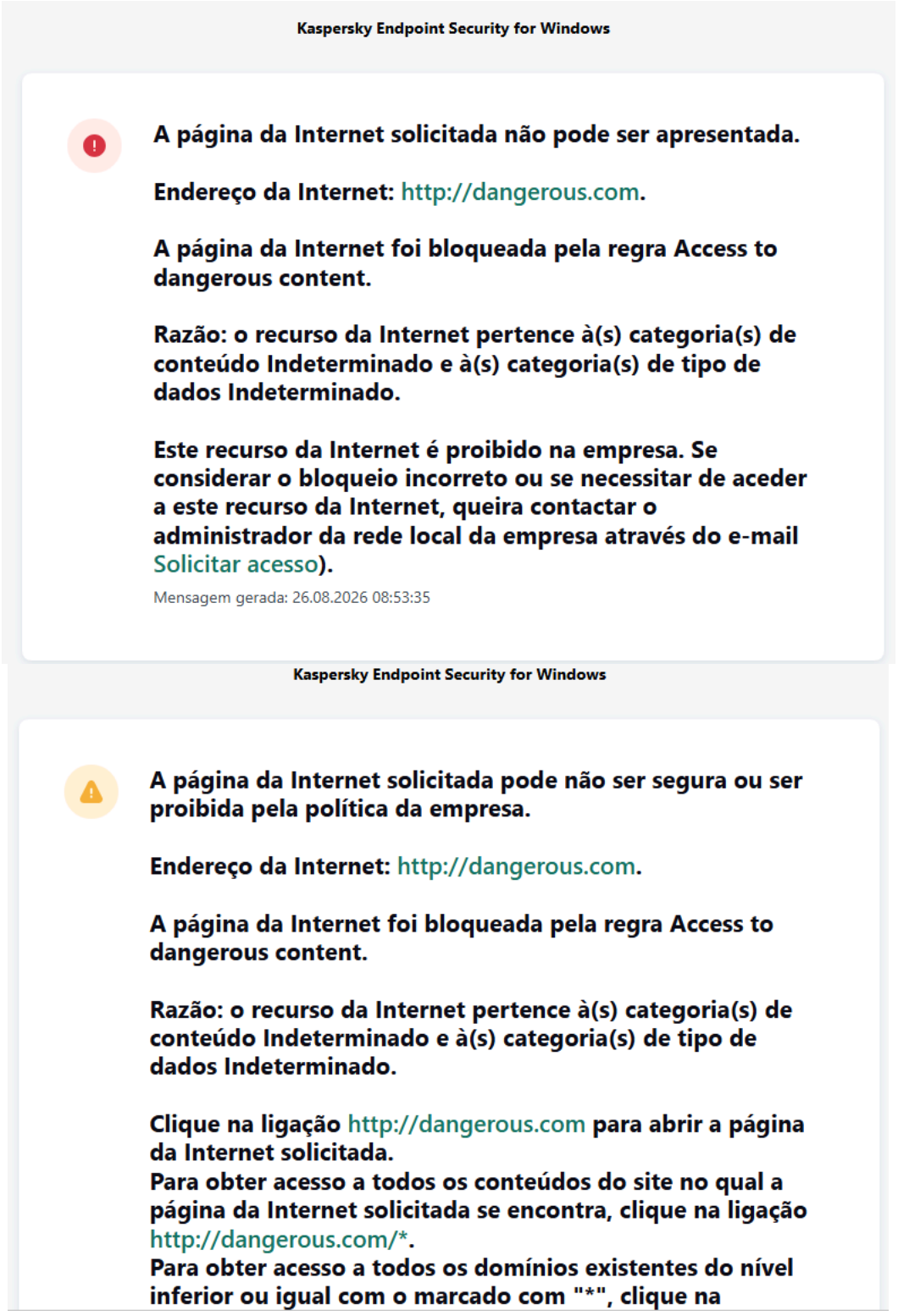
  Por exemplo, pode restringir o acesso à Internet através de um navegador para todos os utilizadores da empresa, exceto o departamento de TI.

- Agendamento de regras.

  Por exemplo, pode restringir o acesso à Internet através de um navegador apenas durante o horário de expediente.

Prioridades das regras de acesso

Cada regra tem uma prioridade. Quanto mais alta for a posição de uma regra na lista, mais alta será a sua prioridade. Se um site for adicionado a várias regras, o Controlo de Internet regula o acesso ao site com base na regra com a prioridade mais alta. Por exemplo, o Kaspersky Endpoint Security pode identificar um portal empresarial como uma rede social. Para restringir o acesso a redes sociais e fornecer acesso ao portal da Web empresarial, crie duas regras: uma regra de bloqueio para a categoria de site *Redes sociais* e uma regra de permissão para o portal da Web empresarial. A regra de acesso para o portal da Web empresarial deve ter uma prioridade mais alta que a regra de acesso para redes sociais.



Mensagens do Controlo de Internet

Parâmetro	Descrição
Regras de acesso a recursos web	Lista contendo as regras de acesso a recursos da Web. Cada regra tem uma prioridade. Quanto mais alta for a posição de uma regra na lista, mais alta será a sua prioridade. Se um site for adicionado a várias regras, o Controlo de Internet regula o acesso ao site com base na regra com a prioridade mais alta.
Regra predefinida	A *Regra predefinida* é uma regra para aceder a recursos da Web que não são cobertos por nenhuma outra regra. Estão disponíveis as seguintes opções: • **Permitir tudo, exceto a lista de regras**, também conhecido como modo de lista de bloqueio para sites proibidos. • **Recusar tudo, exceto a lista de regras**, também conhecido como modo de lista de permissão para sites permitidos.
Termine as sessões do navegador do utilizador ativas depois de a regra ser aplicada	Se a caixa de verificação estiver selecionada, o Controlo de Internet termina a ligação aos recursos da Web bloqueados imediatamente após a aplicação da política. O navegador para imediatamente de transferir dados da página Web. Quando atualiza a página Web ou acede a outra página proibida, a aplicação apresenta um aviso. O Controlo de Internet permite desconectar imediatamente recursos da Web apenas em navegadores. Para outras aplicações, o Controlo de Internet restringe apenas novas ligações. Se a caixa de verificação estiver desmarcada, o Controlo de Internet restringe apenas as novas ligações a recursos da Web proibidos. O Controlo de Internet não encerra ligações ativas.
Modelos	**Aviso**. O campo de entrada é constituído por um modelo da mensagem apresentada quando é acionada uma regra de aviso de tentativas de acesso a um recurso da Internet indesejado. **Mensagem sobre o bloqueio**. O campo de registo contém o modelo da mensagem que é apresentada caso seja acionada uma regra que bloqueie o acesso a um recurso da Internet. **Mensagem para o administrador**. Modelo da mensagem a enviar ao administrador da rede local, caso o utilizador considere que o bloqueio foi um erro. Depois de o utilizador solicitar acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio do acesso à página da Web para o administrador**. A descrição do evento contém uma mensagem para o administrador com variáveis substituídas. Pode visualizar estes eventos na consola do Kaspersky Security Center utilizando a seleção de eventos predefinida **User requests**. Se a sua organização não tiver o Kaspersky Security Center implementado ou não houver uma ligação ao Servidor de Administração, a aplicação irá enviar uma mensagem ao administrador para o endereço de e-mail especificado. São fornecidas variáveis especiais para gerir os modelos da mensagem (por exemplo, `%USER_NAME%`). As variáveis permitem que um único modelo de mensagem seja usado para diferentes computadores.
Registar a abertura de páginas permitidas	O Kaspersky Endpoint Security regista dados de visitas a todos os sites, incluindo sites permitidos. O Kaspersky Endpoint Security envia eventos para o Kaspersky Security Center, para o registo local do Kaspersky Endpoint Security e o registo de eventos do Windows. Para monitorizar a atividade da Internet do utilizador, precisa de configurar as definições para guardar eventos. Navegadores que suportam a função de monitorização: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. A monitorização da atividade do utilizador não funciona noutros navegadores. Monitorizar a atividade da Internet do utilizador pode exigir mais recursos do computador ao desencriptar o tráfego HTTPS.

Controlo de Dispositivos

O Controlo de Dispositivos gere o acesso de utilizador a dispositivos que são instalados no ou ligados ao computador (por exemplo, discos rígidos, câmaras ou módulos Wi-Fi). Tal permite proteger o computador da infeção quando os dispositivos são ligados, e impede a perda ou fuga de dados.

Se o Controlo de Dispositivos estiver ativado, a aplicação transmitirá informações sobre os dispositivos ligados ao Kaspersky Security Center. Pode ver a lista de dispositivos ligados no Kaspersky Security Center na pasta **Advanced → Repositories → Hardware**.

Níveis de acesso ao dispositivo

O Controlo de Dispositivos controla o acesso aos seguintes níveis:

- **Tipo de dispositivo**. Por exemplo, impressoras, unidades amovíveis e unidades de CD/DVD.

  Pode configurar o acesso ao dispositivo do seguinte modo:

  - Permitir – .
  - Bloquear – .
  - Por regras (apenas impressoras e dispositivos portáteis) – .
  - Depende do barramento de ligação (exceto Wi-Fi) – .
  - Bloquear com exceções (apenas Wi-Fi) - .

- **Barramento de ligação**. Um *barramento de ligação* é uma interface utilizada para ligar dispositivos ao computador (por exemplo, USB ou FireWire). Se o modo **Depende do barramento de ligação** for selecionado para o tipo de dispositivo, a aplicação permite ou nega o acesso ao dispositivo, dependendo da interface de ligação (por exemplo, USB).

  Pode configurar o acesso ao dispositivo do seguinte modo:

  - Permitir – .
  - Bloquear – .

- **Dispositivos fiáveis**. *Dispositivos fiáveis* são dispositivos aos quais os utilizadores especificados nas definições de dispositivo fiável têm acesso total, em qualquer altura.

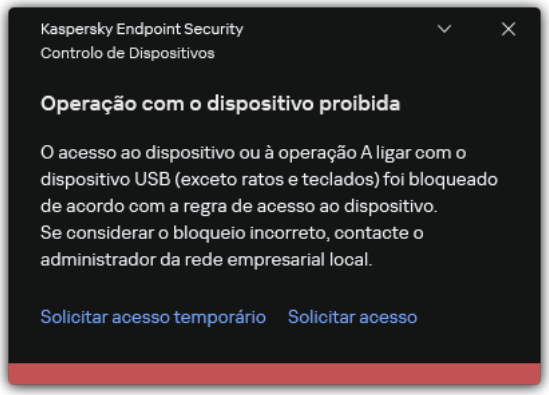
  Pode adicionar dispositivos fiáveis com base nos seguintes dados:

  - **Dispositivos por ID**. Cada dispositivo possui um identificador exclusivo (Hardware ID ou HWID). Pode ver a ID nas propriedades de dispositivo utilizando ferramentas do sistema operativo. Exemplo de um ID do dispositivo: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Se desejar adicionar vários dispositivos específicos, é conveniente adicionar dispositivos por ID.
  - **Dispositivos por modelo**. Cada dispositivo possui um Vendor ID (VID) e um Product ID (PID). Pode examinar os IDs nas propriedades do dispositivo utilizando ferramentas do sistema operativo. Modelo para inserir o VID e o PID: `VID_1234&PID_5678`. Se usar dispositivos de um determinado modelo na sua organização, é conveniente adicionar dispositivos por modelo. Deste modo, pode adicionar todos os dispositivos deste modelo.
  - **Dispositivos por máscara de ID**. Se estiver a utilizar vários dispositivos com IDs semelhantes, pode utilizar máscaras para adicionar dispositivos à lista fiável. O caráter `*` substitui qualquer conjunto de carateres. O Kaspersky Endpoint Security não suporta o caráter `?` ao introduzir uma máscara. Por exemplo, `WDC_C*`.
  - **Dispositivos por máscara de modelo**. Se estiver a utilizar vários dispositivos com VIDs ou PIDs semelhantes (por exemplo, dispositivos do mesmo fabricante), pode utilizar máscaras para adicionar dispositivos à lista fiável. O caráter `*` substitui qualquer conjunto de carateres. O Kaspersky Endpoint Security não suporta o caráter `?` ao introduzir uma máscara. Por exemplo, `VID_05AC&PID_*`.

O Controlo de Dispositivos regula o acesso do utilizador a dispositivos através de *regras de acesso*. O Controlo de Dispositivos também o permite guardar eventos de ligação/desconexão de dispositivo. Para guardar eventos, tem de configurar o registo de eventos numa política.

Se o acesso a um dispositivo depender do barramento de ligação (o estado), o Kaspersky Endpoint Security não guarda eventos de ativação/desativação de dispositivos. Para ativar o Kaspersky Endpoint Security para guardar eventos de ativação/desativação de dispositivos, permita o acesso ao tipo correspondente de dispositivo (o estado) ou adicione o dispositivo à lista fiável.

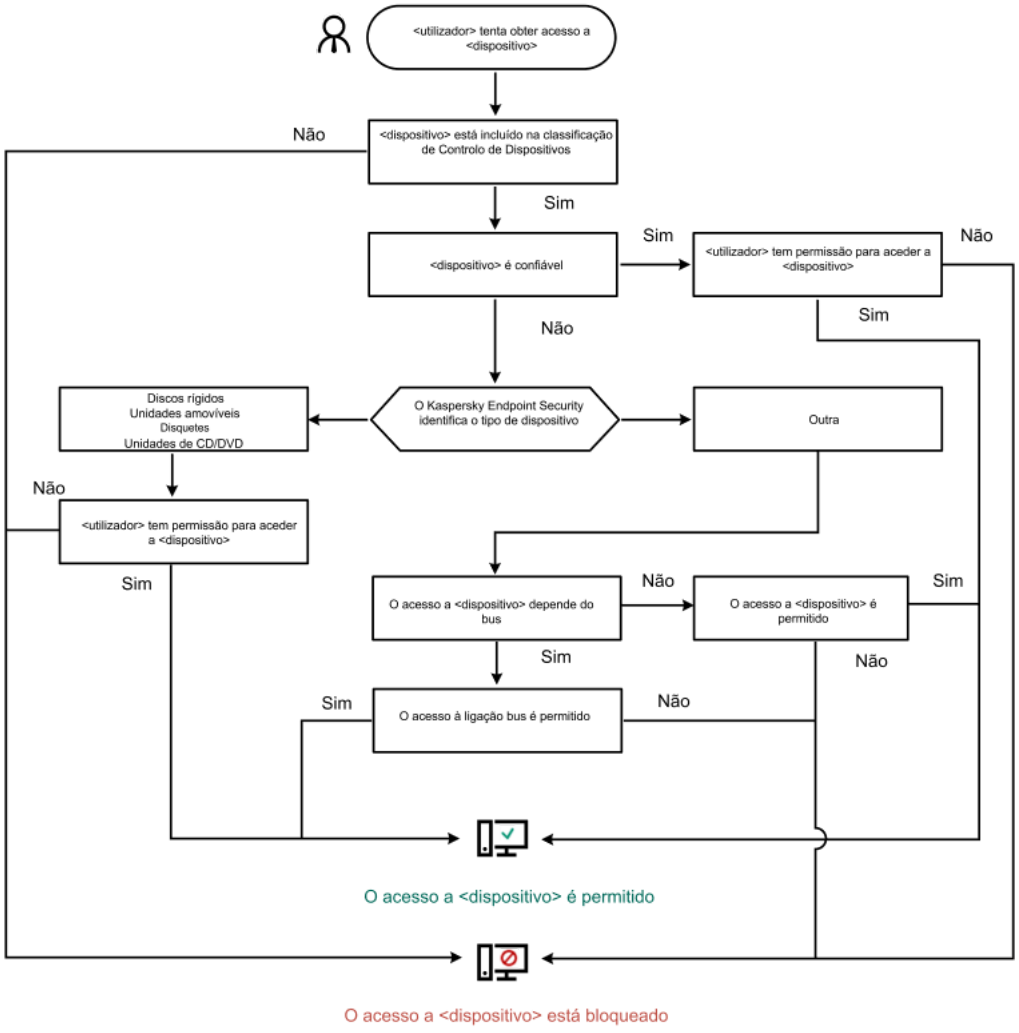
Quando um dispositivo que está bloqueado pelo Controlo de Dispositivos é ligado ao computador, o Kaspersky Endpoint Security bloqueará o acesso e apresentará uma notificação (ver a figura abaixo).



Notificação de Controlo de Dispositivos

Algoritmo operacional do Controlo de Dispositivos

O Kaspersky Endpoint Security toma uma decisão sobre se é permitido o acesso a um dispositivo depois do utilizador ligar o mesmo ao computador (ver figura abaixo).



Algoritmo operacional do Controlo de Dispositivos

Se um dispositivo estiver ligado e o acesso for permitido, pode editar a regra de acesso e bloquear o acesso. Neste caso, na próxima vez que alguém tentar aceder ao dispositivo (tal como para visualizar a árvore de pastas ou executar operações de leitura ou escrita), o Kaspersky Endpoint Security bloqueia o acesso. Um dispositivo sem sistema de ficheiros apenas é bloqueado na próxima vez que o dispositivo for ligado.

Se um utilizador do computador com Kaspersky Endpoint Security instalado tiver de solicitar acesso a um dispositivo que o utilizador acredite ter sido bloqueado por engano, envie ao utilizador as instruções de pedido de acesso.

Parâmetro	Descrição
Permitir pedidos de acesso temporário *(disponível apenas na Consola do Kaspersky Security Center)*	Se a caixa de verificação estiver selecionada, o botão **Solicitar acesso** está disponível na interface local do Kaspersky Endpoint Security. Com este botão, o utilizador pode solicitar o acesso temporário a um dispositivo bloqueado.
Dispositivos e redes Wi-Fi	Esta tabela inclui todos os tipos de dispositivos possíveis, de acordo com a classificação do componente Controlo de Dispositivos, incluindo os respetivos estados de acesso.
Barramentos de ligação	Uma lista de todos os barramentos de ligação disponíveis, de acordo com a classificação do componente Controlo de Dispositivos, incluindo os respetivos estados de acesso. O Kaspersky Endpoint Security permite ou nega o acesso aos dispositivos, dependendo do tipo de barramento de ligação, se o modo **Depende do barramento de ligação** estiver selecionado.
Dispositivos fiáveis	Lista de dispositivos fiáveis e utilizadores com acesso a estes dispositivos.
Unir valores ao herdar *(disponível apenas na Consola do Kaspersky Security Center)*	Esta opção une a lista de dispositivos fiáveis nas políticas principal e subordinadas do Kaspersky Security Center. Para unir listas, a política subordinada tem de ser configurada para herdar as definições da política principal do Kaspersky Security Center. Se a caixa de verificação estiver selecionada, os itens da lista da política principal do Kaspersky Security Center serão apresentados nas políticas subordinadas. Deste modo, pode por exemplo, criar uma lista consolidada de dispositivos fiáveis em toda a organização. Os itens de lista herdados numa política subordinada não podem ser eliminados nem editados. Os itens na lista de dispositivos fiáveis que são unidos durante a herança só podem ser eliminados e editados na política principal. Pode adicionar, editar ou eliminar itens de listas nas políticas de nível mais baixo. Se os itens nas listas das políticas subordinada e principal corresponderem, esses itens serão apresentados como o mesmo item da política principal. Se a caixa de verificação não estiver selecionada, os itens das listas não serão unidos ao herdar as definições das políticas do Kaspersky Security Center. Esta funcionalidade também permite unir listas em perfis de políticas. Para unir listas, no perfil de maior prioridade, ative a herança das definições de um perfil com menos prioridade. Para obter mais informações sobre as prioridades do perfil da política, consulte a Ajuda do Kaspersky Security Center.
Anti-Bridging	O Anti-Bridging inibe a criação de pontes de rede ao impedir o estabelecimento simultâneo de várias ligações de rede a um computador. Isto permite-lhe proteger uma rede empresarial contra ataques através de redes não protegidas e não autorizadas. O Anti-Bridging bloqueia o estabelecimento de múltiplas ligações de acordo com as prioridades dos dispositivos. Quanto mais alta for a posição de um dispositivo na lista, mais alta será a sua prioridade. Se uma ligação ativa e uma nova ligação forem do mesmo tipo (por exemplo, Wi-Fi), o Kaspersky Endpoint Security bloqueia a ligação ativa e permite o estabelecimento da nova ligação. Se uma ligação ativa e uma nova ligação forem de tipos diferentes (por exemplo, um adaptador de rede e Wi-Fi), o Kaspersky Endpoint Security bloqueia a ligação com a prioridade mais baixa e permite a ligação com a prioridade mais alta. O Anti-Bridging suporta a operação com os seguintes tipos de dispositivos: adaptador de rede, Wi-Fi e modem.
Modelos de mensagem	**Mensagem sobre o bloqueio**. Modelo da mensagem que surge quando um utilizador tenta aceder a um dispositivo bloqueado. Esta mensagem surge também quando um utilizador tenta executar uma operação no conteúdo do dispositivo que foi bloqueado para este utilizador. **Mensagem para o administrador**. Um modelo da mensagem que é enviada para o administrador da rede local quando o utilizador considera que o acesso ao dispositivo foi bloqueado por erro ou que uma operação com conteúdo do dispositivo foi proibida por erro. Depois de o utilizador solicitar acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio do acesso ao dispositivo para o administrador**. A descrição do evento contém uma mensagem para o administrador com variáveis substituídas. Pode visualizar estes eventos na consola do Kaspersky Security Center utilizando a seleção de eventos predefinida **User requests**. Se a sua organização não tiver o Kaspersky Security Center implementado ou não houver uma ligação ao Servidor de Administração, a aplicação irá enviar uma mensagem ao administrador para o endereço de e-mail especificado.

Controlo das Aplicações

O Controlo das Aplicações gere a inicialização de aplicações nos computadores dos utilizadores. Isso permite-lhe implementar uma política de segurança empresarial ao usar aplicações. O Controlo das Aplicações reduz também o risco de infeção do computador, restringindo o acesso às aplicações.

A configuração do Controlo das Aplicações consiste nas seguintes etapas:

1. Criar categorias de aplicações.

   O administrador cria categorias de aplicações que o administrador deseja gerir. As categorias de aplicações destinam-se a todos os computadores da rede empresarial, independentemente dos grupos de administração. Para criar uma categoria, pode utilizar os seguintes critérios: categoria KL (por exemplo, *Navegadores*), hash do ficheiro, fornecedor da aplicação e outros critérios.

2. Criar Regras de Controlo das Aplicações.

   O administrador cria regras do Controlo das aplicações na política para o grupo de administração. A regra inclui as categorias de aplicações e o estado de inicialização das aplicações destas categorias: bloqueados ou permitidos. O administrador pode criar muitas regras. Uma aplicação pode corresponder aos critérios de várias regras. A prioridade de uma regra de bloqueio é superior à prioridade de uma regra de permissão. O Kaspersky Endpoint Security verifica se uma aplicação corresponde a uma regra sempre que é iniciado. O Kaspersky Endpoint Security compara sequencialmente a aplicação com todas as regras do Controlo de aplicações.

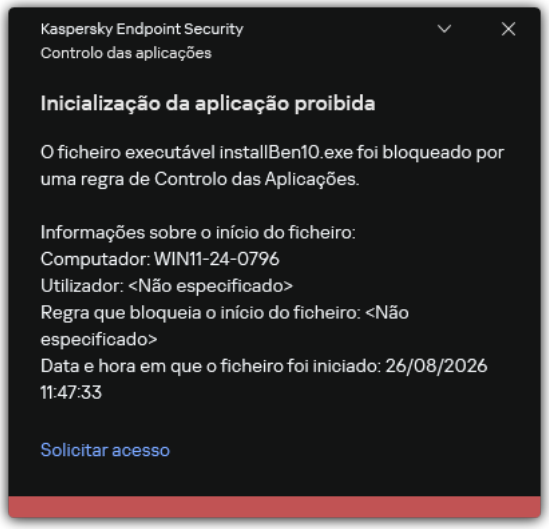
3. Selecionar o modo de Controlo das Aplicações.

   O administrador escolhe o modo para trabalhar com aplicações que não estão incluídas em nenhuma das regras (lista de bloqueio e lista de permissão de aplicações).

Quando um utilizador tenta iniciar uma aplicação proibida, o Kaspersky Endpoint Security impede o início da aplicação e exibe uma notificação (ver a figura abaixo).

Um *modo de teste* é fornecido para verificar a configuração do Controlo das Aplicações. Neste modo, o Kaspersky Endpoint Security faz o seguinte:

- Permite a inicialização de aplicações, incluindo as proibidas.
- Mostra uma notificação sobre a inicialização de uma aplicação proibida e adiciona informações ao relatório no computador do utilizador.
- Envia dados sobre a inicialização de aplicações proibidas ao Kaspersky Security Center.



Notificação do Controlo das Aplicações

Modos de funcionamento do Controlo das Aplicações

O componente Controlo das Aplicações funciona em dois modos:

- **Lista de bloqueio**. Neste modo, o Controlo das Aplicações permite que todos os utilizadores iniciem todas as aplicações, exceto as aplicações proibidas nas regras do Controlo das Aplicações.

  Este modo do Controlo das Aplicações está ativado, por predefinição.

- **Lista de permissão**. Neste modo, o Controlo das Aplicações bloqueia o início de todas as aplicações por parte de todos os utilizadores, exceto as aplicações permitidas e não proibidas nas regras do Controlo das Aplicações.

  Se as regras de permissão do Controlo das Aplicações estiverem configuradas na íntegra, o componente bloqueia o arranque de todas as novas aplicações que não tenham sido verificadas pelo administrador da rede local e permite o funcionamento do sistema operativo e das aplicações fiáveis das quais os utilizadores dependem para realizarem as suas tarefas.

  Pode ler as recomendações sobre a configuração das Regras de Controlo das Aplicações no modo de lista de permissão.

O Controlo das Aplicações pode ser configurado para funcionar nestes modos com a interface local do Kaspersky Endpoint Security e utilizando o Kaspersky Security Center.

Contudo, o Kaspersky Security Center fornece ferramentas que não estão disponíveis na interface local do Kaspersky Endpoint Security, como por exemplo, as ferramentas necessárias para as tarefas seguintes:

- Criar categorias de aplicações.

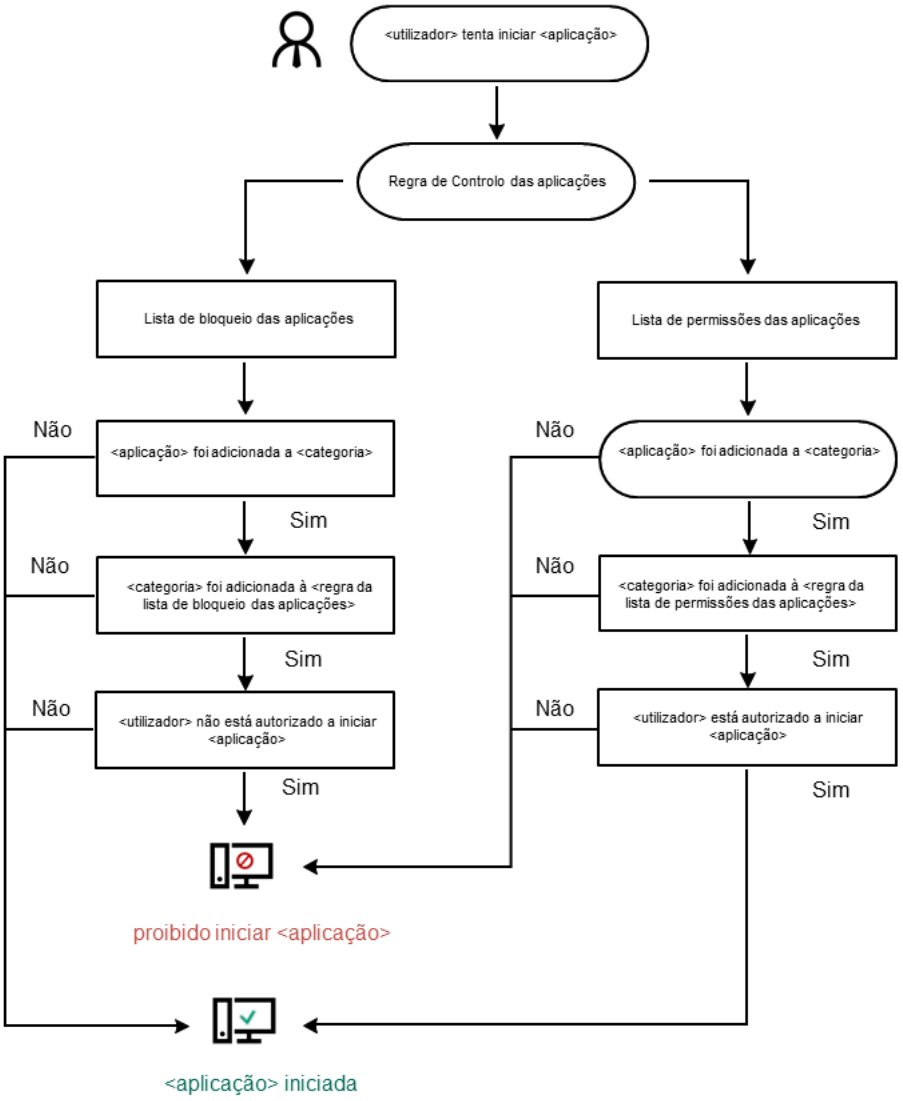
  As Regras de Controlo das aplicações criadas na Consola de Administração do Kaspersky Security Center baseiam-se nas suas categorias de aplicações personalizadas e não nas condições de inclusão ou de exclusão, como na interface local do Kaspersky Endpoint Security.

- Recolher informações sobre as aplicações instaladas nos computadores da rede local empresarial.

Por este motivo, recomenda-se a utilização do Kaspersky Security Center para configurar o funcionamento do componente Controlo das Aplicações.

Algoritmo operacional do Controlo das Aplicações

O Kaspersky Endpoint Security usa um algoritmo para tomar uma decisão sobre o início de uma aplicação (ver a figura abaixo).



Algoritmo operacional do Controlo das Aplicações

Parâmetro	Descrição
Ação no arranque das aplicações bloqueadas por regras	**Aplicar regras**. O Kaspersky Endpoint Security gere o arranque das aplicações de acordo com o modo selecionado. **Testar regras**. O Kaspersky Endpoint Security permite o arranque da aplicação que está bloqueada no modo atual de Controlo das Aplicações, mas regista informação relativamente ao seu arranque no relatório.
Modo de controlo do arranque da aplicação	Pode selecionar um das itens opções: • **Lista de bloqueio**. Se esta opção estiver selecionada, o Controlo das Aplicações permite que todos os utilizadores iniciem qualquer tipo de aplicação, exceto nos casos em que as aplicações satisfazem as condições das regras de bloqueio do Controlo das Aplicações. • **Lista de permissão**. Se esta opção estiver selecionada, o Controlo das Aplicações bloqueia todos os utilizadores de iniciarem qualquer tipo de aplicação, exceto nos casos em que satisfazem as condições das regras de permissão do Controlo das Aplicações. Quando o modo **Lista de permissão** está selecionado, são automaticamente criadas duas regras de Controlo das Aplicações: • **Golden Image**. • **Atualizadores fiáveis**. Não pode editar as definições nem eliminar as regras automaticamente criadas. Pode ativar ou desativar estas regras.
Monitorizar o carregamento de módulos DLL	Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security controla o carregamento dos módulos DLL quando os utilizadores tentam iniciar as aplicações. A informação sobre o módulo DLL e a aplicação que carregou este módulo DLL está registada no relatório. Ao ativar o controlo sobre o carregamento dos módulos DLL e controladores, certifique-se de que uma das regras seguintes está ativada nas definições de Controlo das Aplicações: a regra predefinida **Golden Image** ou outra regra que contenha a categoria KL **Golden Image\Certificados confiáveis**", e certifique-se de que os módulos DLL e os controladores fiáveis são carregados antes de iniciar o Kaspersky Endpoint Security. Permitir o controlo do carregamento de módulos DLL e controladores quando a regra **Golden Image** está desativada pode provocar instabilidade no sistema operativo. O Kaspersky Endpoint Security só monitoriza os módulos DLL e os controladores carregados desde a seleção da caixa de verificação. Depois de selecionar a caixa de verificação, é aconselhável reiniciar o computador para garantir que a aplicação monitoriza todos os módulos DLL e controladores, incluindo os carregados antes de o Kaspersky Endpoint Security iniciar.
Utilizar verificação estrita da assinatura digital	Pode selecionar um certificado como condição de ativação para uma regra de Controlo das Aplicações. Se esta caixa de verificação estiver selecionada, o Kaspersky Endpoint Security aplica regras a aplicações assinadas com certificados apenas do arquivo de certificados do sistema fiável. As aplicações assinadas com esse certificado também são consideradas fiáveis pelos componentes de proteção, por exemplo, a tarefa *Verificação de software malicioso*. No entanto, se especificar um certificado de um armazenamento diferente numa regra de Controlo das Aplicações, o Kaspersky Endpoint Security não aplica essa regra. Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security aplica regras a aplicações assinadas por um certificado do Arquivo de Certificados de Raiz Fiável do Windows. Estas aplicações não fazem parte da zona fiável. Os componentes de proteção monitorizam a atividade dessas aplicações.
Modelos de mensagens sobre bloqueio de aplicações	**Mensagem sobre o bloqueio**. Modelo da mensagem que é apresentada quando é acionada uma regra de Controlo das Aplicações que bloqueia o início de uma aplicação. **Mensagem para o administrador**. Modelo da mensagem que um utilizador pode enviar ao administrador da LAN empresarial se o utilizador acreditar que uma aplicação foi bloqueada por engano. Depois de o utilizador solicitar acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio da inicialização da aplicação para o administrador**. A descrição do evento contém uma mensagem para o administrador com variáveis substituídas. Pode visualizar estes eventos na consola do Kaspersky Security Center utilizando a seleção de eventos predefinida **User requests**. Se a sua organização não tiver o Kaspersky Security Center implementado ou não houver uma ligação ao Servidor de Administração, a aplicação irá enviar uma mensagem ao administrador para o endereço de e-mail especificado.

Controlo de Anomalias Adaptativo

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para estações de trabalho. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para servidores.

O componente Controlo de Anomalias Adaptativo monitoriza e bloqueia ações que não são típicas dos computadores na rede de uma empresa. O Controlo de Anomalias Adaptativo usa um conjunto de regras para rastrear comportamento invulgar (por exemplo, a regra *Início da Microsoft PowerShell da aplicação de ambiente de trabalho*). As regras são criadas pelos especialistas da Kaspersky com base em cenários típicos de atividade maliciosa. Pode configurar o modo como o Controlo de Anomalias Adaptativo manuseia cada regra e, por exemplo, permitir a execução de scripts do PowerShell que automatizam determinadas tarefas do fluxo de trabalho. O Kaspersky Endpoint Security atualiza o conjunto de regras a par das bases de dados da aplicação. As atualizações dos conjuntos de regras devem ser confirmadas manualmente.

Definições do Controlo de Anomalias Adaptativo

A configuração do Controlo de Anomalias Adaptativo consiste nas seguintes etapas:

1. Formação do Controlo de Anomalias Adaptativo.

   Depois de ativar o Controlo de Anomalias Adaptativo, as suas regras funcionam no *modo de formação*. Durante a formação, o Controlo de Anomalias Adaptativo monitoriza o acionamento de regras e envia os eventos de acionamento para o Kaspersky Security Center. Cada regra tem sua própria duração do modo de formação. A duração do modo de formação é estabelecida por peritos da Kaspersky. Normalmente, o modo de formação fica ativo durante duas semanas.

   Se uma regra não for acionada de todo durante a formação, o Controlo de Anomalias Adaptativo irá considerar as ações associadas a esta regra como não típicas. O Kaspersky Endpoint Security irá bloquear todas as ações associadas a essa regra.

   Se uma regra for acionada durante a formação, o Kaspersky Endpoint Security regista os eventos no relatório de acionamento da regra e no repositório **Rule triggers in Smart Training state**.

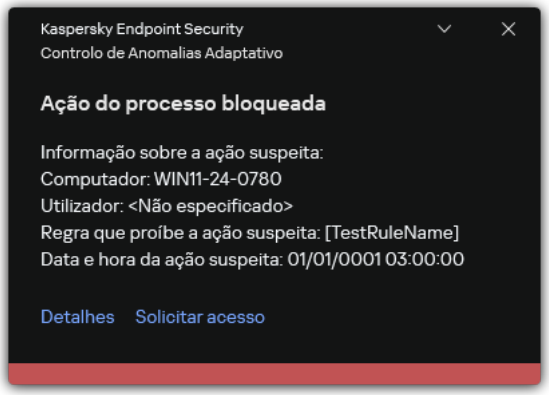
2. A analisar o relatório de acionamento de regras.

   O administrador analisa o relatório de acionamento de regras ou o conteúdo do repositório do **Rule triggers in Smart Training state**. O administrador pode então selecionar o comportamento do Controlo de Anomalias Adaptativo quando a regra é acionada: bloquear ou permitir. O administrador pode também continuar a monitorizar o funcionamento da regra e prolongar a duração do modo de formação. Se o administrador não realizar nenhuma ação, a aplicação continuará também a funcionar no modo de formação. O prazo do modo de formação é reiniciado.

O Controlo de Anomalias Adaptativo é configurado em tempo real através dos seguintes canais:

- O Controlo de Anomalias Adaptativo começa automaticamente a bloquear as ações associadas às regras que nunca foram acionadas no modo de formação.
- O Kaspersky Endpoint Security adiciona novas regras ou remove as obsoletas.
- O administrador configura a operação do Controlo de Anomalias Adaptativo depois de rever o relatório do acionamento de regras e o conteúdo do repositório de **Rule triggers in Smart Training state**. Recomendamos que verifique o relatório sobre o acionamento das regras e os conteúdos do armazenamento **Rule triggers in Smart Training state**.

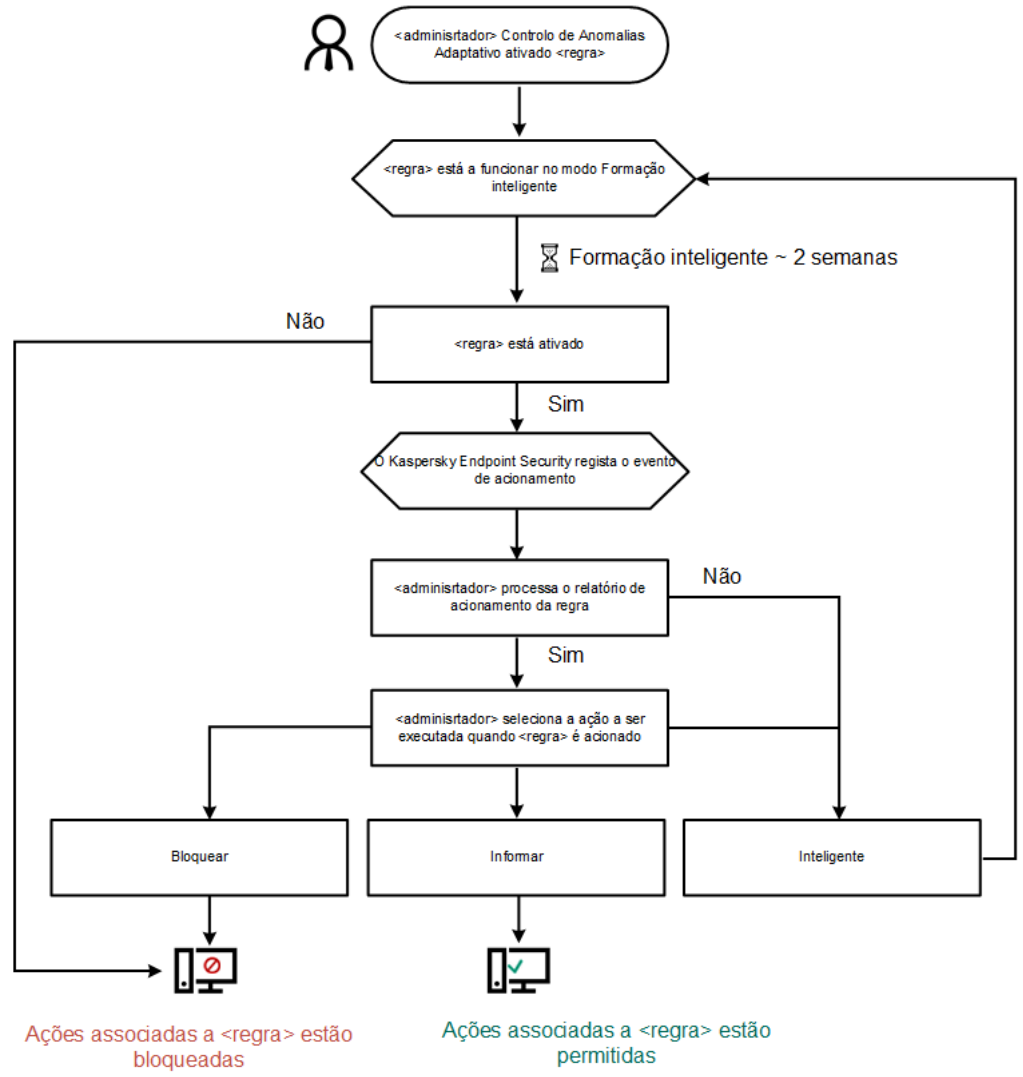
Quando uma aplicação maliciosa tentar realizar uma ação, o Kaspersky Endpoint Security irá bloquear a ação e exibir uma notificação (ver figura abaixo).



Notificação do Controlo de Anomalias Adaptativo

Algoritmo operacional do Controlo de Anomalias Adaptativo

O Kaspersky Endpoint Security decide se permite ou bloqueia uma ação associada a uma regra com base no seguinte algoritmo (ver figura abaixo).



Algoritmo operacional do Controlo de Anomalias Adaptativo

Definições do componente Controlo de Anomalias Adaptativo

Parâmetro	Descrição
Reportar o estado das regras do Controlo de Anomalias Adaptativo *(disponível apenas na Consola do Kaspersky Security Center)*	Este relatório contém informações sobre o estado das regras de deteção do Controlo de Anomalias Adaptativo (por exemplo, *Desativado* ou *Bloquear*). O relatório é gerado para todos os grupos de administração.
Reportar as regras acionadas do Controlo de Anomalias Adaptativo *(disponível apenas na Consola do Kaspersky Security Center)*	Este relatório contém informações sobre ações não típicas detetadas pelo Controlo de Anomalias Adaptativo. O relatório é gerado para todos os grupos de administração.

Parâmetro	Descrição
Regras	Tabela de regras do Controlo de Anomalias Adaptativo. As regras são criadas pelos especialistas da Kaspersky com base em cenários típicos de atividade maliciosa.
Modelos	**Mensagem sobre o bloqueio**. Modelo da mensagem apresentada a um utilizador quando uma regra do Controlo de Anomalias Adaptativo que bloqueia uma ação não típica é acionada. **Mensagem para o administrador**. Modelo da mensagem que um utilizador pode enviar para o administrador da rede empresarial local se considerar que o bloqueio foi um erro. Depois de o utilizador solicitar acesso, o Kaspersky Endpoint Security envia um evento ao Kaspersky Security Center: **Mensagem de bloqueio da atividade da aplicação para o administrador**. A descrição do evento contém uma mensagem para o administrador com variáveis substituídas. Pode visualizar estes eventos na consola do Kaspersky Security Center utilizando a seleção de eventos predefinida **User requests**. Se a sua organização não tiver o Kaspersky Security Center implementado ou não houver uma ligação ao Servidor de Administração, a aplicação irá enviar uma mensagem ao administrador para o endereço de e-mail especificado.

Monitorização da integridade do sistema

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para servidores. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para estações de trabalho.

A partir da versão 12.6, o Kaspersky Endpoint Security for Windows inclui o componente Monitorização da integridade do sistema, em vez do componente Monitor de integridade do ficheiro. O componente Monitorização da integridade do sistema inclui todas as funcionalidades do Monitor de integridade do ficheiro e, adicionalmente, permite monitorizar alterações de registo e conexão de dispositivos externos.

O componente Monitorização da integridade do sistema monitoriza as alterações no sistema operativo que podem indicar violações da segurança informática. Quando essas alterações são detetadas, o Kaspersky Endpoint Security gera eventos correspondentes e alerta o administrador. A Monitorização da integridade do sistema pode operar em tempo real e também realizar verificações de integridade do sistema mediante pedido.

Monitorização da integridade do sistema em tempo real

No modo de tempo real, a Monitorização da integridade do sistema rastreia alterações em objetos incluídos no âmbito do componente (o *âmbito de monitorização*). A Monitorização da integridade do sistema também permite bloquear o acesso não autorizado a esses objetos em tempo real.

Verificação de integridade do sistema mediante pedido

A Verificação de integridade do sistema mediante pedido é uma tarefa que pode realizar manualmente ou de forma programada. Para realizar a tarefa *Verificação de integridade do sistema*, tem de configurar o âmbito do componente (o *âmbito de monitorização*) e criar uma linha de base. A *linha de base* é um estado registado de objetos no sistema, que a aplicação usa como referência ao comparar com o estado atual.

Definições da Monitorização da integridade do sistema

Parâmetro	Descrição
Modo operativo das regras de bloqueio	• **Bloquear**. Neste modo, a Monitorização da integridade do sistema bloqueia ações com ficheiros e chaves de registo do âmbito de monitorização e gera um evento correspondente. • **Informar**. Neste modo, a Monitorização da integridade do sistema permite ações com ficheiros e chaves de registo do âmbito de monitorização e gera um evento correspondente.

Parâmetro	Descrição
Monitorização da integridade do sistema em tempo real	No modo de tempo real, a Monitorização da integridade do sistema rastreia alterações em objetos incluídos no âmbito do componente (o *âmbito de monitorização*). A Monitorização da integridade do sistema também permite bloquear o acesso não autorizado a esses objetos em tempo real.
Monitorizar dispositivos	A Monitorização da integridade do sistema monitoriza a ligação e desativação de dispositivos externos.
Monitorizar ficheiros e o registo	A Monitorização da integridade do sistema monitoriza alterações em ficheiros, pastas e registo.
Verificação de integridade do sistema	A Verificação de integridade do sistema mediante pedido é uma tarefa que pode realizar manualmente ou de forma programada. Para realizar a tarefa *Verificação de integridade do sistema*, tem de configurar o âmbito do componente (o *âmbito de monitorização*) e criar uma linha de base. A *linha de base* é um estado registado de objetos no sistema, que a aplicação usa como referência ao comparar com o estado atual.

Endpoint Sensor

O Endpoint Sensor não está incluído no Kaspersky Endpoint Security 11.4.0.

Pode gerir o Endpoint Sensor na Consola Web do Kaspersky Security Center e na Consola de Administração do Kaspersky Security Center. Não é possível gerir o Endpoint Sensor na Consola de Nuvem do Kaspersky Security Center.

O *Endpoint Sensor* foi concebido para interagir com Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* é uma solução criada para a deteção atempada de ameaças sofisticadas, como ataques direcionados, ameaças persistentes avançadas (APT), ataques de dia zero e outras. 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)*)

Pode adquirir todas as unidades funcionais ou unidades funcionais individuais separadamente. Para obter mais informações sobre a solução, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform.

A gestão do Endpoint Sensor possui as seguintes limitações:

- Pode configurar as definições do Endpoint Sensor numa política, desde que o Kaspersky Endpoint Security versão 11.0.0 a 11.3.0 esteja instalado no computador. Para obter mais informações sobre como configurar as definições do Endpoint Sensor com a política, consulte os artigos de ajuda das versões anteriores do Kaspersky Endpoint Security.
- Se o Kaspersky Endpoint Security versão 11.4.0 e posterior estiver instalado no computador, não é possível configurar as definições do Endpoint Sensor na política.

O Endpoint Sensor está instalado em computadores cliente. Nestes computadores, o componente monitoriza constantemente processos, ligações de rede ativas e ficheiros que são modificados. O Endpoint Sensor transmite informações para o servidor KATA.

A funcionalidade do componente está disponível nos seguintes sistemas operativos:

- 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 / Enterpris (64 bits);
- Windows Server 2012 R2 Foundation / Standard / Enterprise (64 bits);
- Windows Server 2016 Essentials / Standard (64 bits).

Para obter informações detalhadas sobre o funcionamento da KATA, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform.

Sandbox

O Kaspersky Endpoint Security for Windows inclui um agente integrado para integração com a solução Kaspersky Sandbox. O componente *Sandbox* deteta e bloqueia automaticamente ameaças avançadas em computadores. O Sandbox analisa o comportamento do objeto para detetar atividades maliciosas e atividades características de ataques direcionados à infraestrutura de TI da organização. O Sandbox analisa e verifica objetos em servidores especiais com imagens virtuais implementadas de sistemas operativos Microsoft Windows (servidores do Sandbox). Para obter mais informações 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 suporta o componente Sandbox que faz parte da solução Kaspersky Anti Targeted Attack Platform. Em contraste com a solução Kaspersky Sandbox, o componente KATA Sandbox apenas permite a verificação de ficheiros não só automaticamente, mas também manualmente a partir do menu de contexto do ficheiro.

O KATA Sandbox requer que o Kaspersky Anti Targeted Attack Platform 7.0 ou posterior seja implementado.

O componente só pode ser gerido através da Consola Web do Kaspersky Security Center. Não pode gerir este componente utilizando a Consola de Administração (MMC).

Definições do componente Sandbox

Parâmetro	Descrição
Integration mode	**Kaspersky Sandbox**. Integração com a solução Kaspersky Sandbox. A aplicação envia ficheiros para serem analisados no Kaspersky Sandbox apenas no modo automático. **KATA Sandbox**. Integração com o componente Sandbox da solução Kaspersky Anti Targeted Attack Platform. Pode selecionar o modo de envio de ficheiros para verificação: • **Manually**. O utilizador envia manualmente o ficheiro para verificação a partir do menu de contexto (**Enviar para Sandbox**). • **Automatically**. A aplicação deteta automaticamente os objetos e envia-os para o Sandbox para verificação. • **Combined**.
Server connection settings	**Timeout (msec)**. Tempo limite de ligação para o servidor do Sandbox (para Kaspersky Sandbox) ou servidor do Nó Central (para KATA). Depois de decorrido o tempo limite definido, o Kaspersky Endpoint Security envia um pedido ao próximo servidor. Pode aumentar o tempo limite de ligação do servidor se a velocidade da sua ligação for baixa ou instável. O tempo limite recomendado do pedido é de 0.5 segundos ou menos. **Request queue**. Tamanho da pasta da fila de pedidos. Ao enviar vários objetos para verificação no Sandbox, o Kaspersky Endpoint Security cria uma fila de pedidos. Por predefinição, o tamanho da pasta da fila de pedidos é limitado a 100 MB. Quando o tamanho máximo é atingido, o Sandbox para de adicionar novos pedidos à fila e envia o evento correspondente ao Kaspersky Security Center. Pode definir o tamanho da pasta da fila de pedidos consoante a configuração do seu servidor. **Server TLS certificate**. Para configurar uma ligação fiável ao servidor do Sandbox (para o Kaspersky Sandbox) ou ao servidor do Nó Central (para KATA), tem de preparar um certificado TLS. De seguida, tem de adicionar o certificado ao computador utilizando uma política. Também tem de adicionar o certificado ao servidor do Sandbox (para Kaspersky Sandbox) ou ao servidor do Nó Central (para KATA). **Use two-way authentication** (apenas para o KATA Sandbox). Autenticação bidirecional ao estabelecer uma ligação segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para utilizar a autenticação bidirecional, é necessário ativar a autenticação bidirecional nas definições do servidor do Central Node e, em seguida, obter um contentor criptográfico e definir uma password para proteger o contentor criptográfico. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform). Após configurar as definições do Central Node, é também necessário ativar a autenticação bidirecional nas definições do Kaspersky Endpoint Security e carregar um contentor criptográfico protegido por password.
Connection to Sandbox servers	**Kaspersky Sandbox**. Definições de ligação do servidor do Kaspersky. Os servidores utilizam imagens virtuais implementadas de sistemas operativos do Microsoft Windows para executar objetos que precisam de ser verificados. Pode inserir um endereço IP (IPv4 ou IPv6) ou um nome de domínio totalmente qualificado. **KATA Sandbox**. Definições de ligação do servidor do nó central. O Nó Central escolhe as definições ideais para verificação e equilibra a carga entre os servidores do Sandbox.
Action on threat detection	**Move copy to Quarantine, delete object**. Se esta opção for selecionada, o Kaspersky Endpoint Security elimina o objeto malicioso encontrado no computador. Antes de eliminar o objeto, o Kaspersky Endpoint Security cria uma cópia de segurança, caso o objeto precise de ser posteriormente restaurado. O Kaspersky Endpoint Security move a cópia de segurança para a Quarentena. **Run Critical Areas Scan**. Se esta opção for selecionada, o Kaspersky Endpoint Security executa a tarefa *Critical Areas Scan*. Por predefinição, o Kaspersky Endpoint Security verifica a memória Kernel, os processos em execução e os setores de inicialização do disco. **Create IOC Scan task**. Se esta opção for selecionada, o Kaspersky Endpoint Security cria automaticamente uma tarefa *IOC Scan (tarefa de verificação IOC autónoma)*. Para esta tarefa, pode configurar o modo de execução, âmbito de verificação e ação na deteção de IOC (*Move copy to Quarantine, delete object* ou *Run Critical Areas Scan*). Para modificar outras definições da tarefa *IOC Scan*, aceda às definições da tarefa.
IOC Scan scope	**Critical file areas**. Se esta opção for selecionada, o Kaspersky Endpoint Security fará uma verificação IOC apenas em áreas críticas do ficheiro do computador: memória kernel e setores de arranque. **File areas on system drive of the computer**. Se esta opção for selecionada, o Kaspersky Endpoint Security fará uma verificação IOC na unidade de sistema do computador.
Run IOC Scan task	**Manually**. Modo de execução, no qual pode iniciar a tarefa *IOC Scan* manualmente quando for conveniente para si. **Automatically**. Modo de execução no qual o Kaspersky Endpoint Security executa a tarefa *IOC Scan* automaticamente assim que uma ameaça é detetada. **Run only when the computer is idle**. Modo de execução no qual o Kaspersky Endpoint Security executa a tarefa *Verificação IOC* se a proteção de ecrã estiver ativa ou se o ecrã estiver bloqueado. Se o utilizador desbloquear o computador, o Kaspersky Endpoint Security pausa a tarefa. Tal significa que a tarefa pode demorar vários dias até ser concluída.

Managed Detection and Response

O Kaspersky Endpoint Security for Windows suporta a integração com a solução Managed Detection and Response. A solução *Kaspersky Managed Detection and Response (MDR)* deteta e analisa automaticamente os incidentes de segurança na sua infraestrutura. Para tal, o MDR utiliza dados de telemetria recebidos de terminais e aprendizagem automática. O MDR envia os dados de incidentes aos especialistas da Kaspersky. Os especialistas podem então processar o incidente e, por exemplo, adicionar uma nova entrada às bases de dados de antivírus. Em alternativa, os especialistas podem emitir recomendações sobre o processamento do incidente e, por exemplo, sugerir que o computador seja isolado da rede. Para obter mais informações sobre a utilização da solução, consulte a Ajuda do Kaspersky Managed Detection and Response.

Definições do Managed Detection and Response

Parâmetro	Descrição
Ficheiro de configuração MDR	O ficheiro BLOB contém a ID do cliente e informações sobre a licença do Kaspersky Managed Detection and Response. O ficheiro BLOB está localizado dentro do arquivo ZIP do ficheiro de configuração do MDR. Pode obter o arquivo ZIP na Consola do Kaspersky Managed Detection and Response. Para obter mais informações sobre ficheiros BLOB, consulte a Ajuda do Kaspersky Managed Detection and Response.

Endpoint Detection and Response

O Kaspersky Endpoint Security for Windows tem um agente integrado para a solução Kaspersky Endpoint Detection and Response Optimum (doravante também referida como "EDR Optimum"). A partir da versão 11.8.0, o Kaspersky Endpoint Security for Windows tem um agente integrado para a solução Kaspersky Endpoint Detection and Response Expert (doravante também referida como "EDR Expert"). O *Kaspersky Endpoint Detection and Response* é uma gama de soluções para proteger a infraestrutura de TI corporativa contra ciberameaças avançadas. A funcionalidade das soluções combina a deteção automática de ameaças com a capacidade de reagir a tais ameaças para neutralizar ataques avançados, incluindo novas explorações, ransomware, ataques sem ficheiros, bem como métodos que utilizam ferramentas legítimas do sistema. O EDR Expert oferece mais funcionalidades de monitorização de ameaças e de resposta do que o EDR Optimum. Para conhecer os detalhes das soluções, 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 verifica e analisa o desenvolvimento de ameaças e disponibiliza ao *pessoal de segurança* ou *Administrador* informações sobre o possível ataque que são necessárias para uma resposta atempada. O Kaspersky Endpoint Detection and Response apresenta as informações da deteção numa janela separada. Um *alerta* é um evento na infraestrutura de TI corporativa que a aplicação identificou como incomum ou suspeito e que pode representar uma ameaça à segurança da infraestrutura de TI corporativa. As *informações da deteção* é uma ferramenta para visualizar todas as informações recolhidas sobre uma ameaça detetada. As informações da deteção incluem, por exemplo, o histórico dos ficheiros que aparecem no computador. Para conhecer os detalhes sobre a gestão de deteção, consulte a Ajuda do Kaspersky Endpoint Detection and Response Optimum e a Ajuda do Kaspersky Endpoint Detection and Response Expert.

Pode configurar o componente Endpoint Detection and Response Optimum na Consola Web e na Cloud Console. As definições do componente Endpoint Detection and Response Expert (cloud) estão disponíveis apenas na Consola de Nuvem.

Parâmetro	Descrição
Enable advanced system activity logging	A telemetria estendida melhora a precisão da deteção de IOC, mas utiliza mais recursos do computador. Recomendamos ativar a telemetria estendida no computador para a verificação retrospetiva do IOC. A *Verificação retrospetiva dos IOC* é um modo da tarefa *IOC Scan* na qual o Kaspersky Endpoint Security verifica indicadores de comprometimento usando dados de um determinado período de tempo. Este modo destina-se à pesquisa de indicadores de comprometimento através dos dados de telemetria do computador protegido, tais como atividade de rede, processos, ficheiros e outros dados de telemetria. Se a telemetria estendida estiver desativada, o Kaspersky Endpoint Security poderá alternar as informações sobre os indicadores de comprometimento detetados.
Network Isolation	Isolamento automático do computador da rede em resposta às ameaças detetadas. Quando o isolamento da rede é ativado, a aplicação interrompe todas as ligações ativas e bloqueia todas as novas ligações TCP/IP no computador. A aplicação deixa apenas as seguintes ligações ativas: • Ligações listadas em Network isolation exclusions. • Ligações iniciadas pelos serviços do Kaspersky Endpoint Security. • Ligações iniciadas pelo Kaspersky Security Center Network Agent.
Automatically unlock isolated device in (hours)	O isolamento da rede pode ser desligado automaticamente após um tempo especificado ou manualmente. Por predefinição, o Kaspersky Endpoint Security desativa o isolamento da rede 5 horas após o início do isolamento.
Network isolation exclusions	Lista de regras para exclusões de isolamento da rede. Quando o isolamento da rede está ativado, as ligações de rede que correspondem às regras não são bloqueadas em computadores. Para configurar as exclusões de isolamento da rede, pode utilizar uma lista de *perfis de rede padrão*. Por predefinição, as exclusões incluem perfis de rede que contêm regras que garantem a operação ininterrupta de dispositivos com o servidor DNS/DHCP e funções de cliente DNS/DHCP. Também pode modificar as definições dos perfis de rede padrão ou definir exclusões manualmente. As exclusões especificadas nas propriedades da política são aplicáveis apenas se o isolamento da rede for ativado automaticamente em resposta a uma ameaça detetada. As exclusões especificadas nas propriedades do computador são aplicáveis apenas se o isolamento da rede for ativado manualmente nas propriedades do computador na Consola do Kaspersky Security Center ou nos detalhes do alerta.
Execution Prevention	Controlo da execução de ficheiros executáveis e scripts e abertura de ficheiros de formato do Office. Por exemplo, pode impedir a execução de aplicações consideradas não seguras no computador selecionado. A prevenção da execução suporta um conjunto de extensões de ficheiros Office e um conjunto de interpretadores de script. Para usar o componente Prevenção de execução, tem de adicionar regras de prevenção de execução. A *Regra de bloqueio de execução* é um conjunto de critérios que a aplicação tem em consideração ao reagir à execução de um objeto, por exemplo, ao bloquear a execução de um objeto. A aplicação identifica ficheiros pelos seus caminhos ou somas de verificação calculadas utilizando algoritmos hash MD5 e SHA256.
Action on execution or opening of forbidden object	**Block and add to event log**. Neste modo, a aplicação bloqueia a execução de objetos ou a abertura de documentos que correspondam aos critérios da regra de prevenção. A aplicação também publica um evento sobre tentativas de execução de objetos ou documentos abertos no Registo de Eventos do Windows e no Registo de Eventos do Kaspersky Security Center. **Add to event log**. Neste modo, o Kaspersky Endpoint Security publica um evento sobre tentativas de execução de objetos executáveis ou abrir documentos que correspondem aos critérios da regra de prevenção no Registo de Eventos do Windows e no Kaspersky Security Center, mas não bloqueia a tentativa de executar ou abrir o objeto ou documento. Esta modo está selecionado por predefinição.
Execution prevention rules	A *Regra de bloqueio de execução* é um conjunto de critérios que a aplicação tem em consideração ao reagir à execução de um objeto, por exemplo, ao bloquear a execução de um objeto. A aplicação identifica ficheiros pelos seus caminhos ou somas de verificação calculadas utilizando algoritmos hash MD5 e SHA256.

Parâmetro	Descrição
Cloud Sandbox	*Cloud Sandbox* é uma tecnologia que lhe permite detetar ameaças avançadas num computador. O Kaspersky Endpoint Security encaminha automaticamente ficheiros detetados para o Cloud Sandbox para análise. O Cloud Sandbox gere estes ficheiros num ambiente isolado para identificar atividades maliciosas e decidir sobre a sua reputação. Os dados sobre estes ficheiros são então enviados para a Kaspersky Security Network. Portanto, se o Cloud Sandbox tiver detetado um ficheiro malicioso, o Kaspersky Endpoint Security irá realizar a ação apropriada para eliminar esta ameaça em todos os computadores onde este ficheiro for detetado. A tecnologia Cloud Sandbox está permanentemente ativa e está disponível para todos os utilizadores da Kaspersky Security Network, independentemente do tipo de licença que estejam a utilizar. Se esta caixa de verificação estiver selecionada, o Kaspersky Endpoint Security irá ativar o contador de ameaças detetadas utilizando o Cloud Sandbox na janela principal da aplicação sob **Tecnologias de deteção de ameaças**. O Kaspersky Endpoint Security também irá indicar a tecnologia de deteção de ameaças do Cloud Sandbox em eventos da aplicação e no *Report on threats* na consola do Kaspersky Security Center.

Endpoint Detection and Response Expert (on-premises)

Endpoint Detection and Response Expert (on-premises)

O Kaspersky Endpoint Security for Windows suporta a integração com a solução Kaspersky Endpoint Detection and Response Expert (on-premises). O *Kaspersky Endpoint Detection and Response Expert (on-premises)* é uma solução de cibersegurança empresarial que inclui aplicações da Kaspersky que permitem a uma organização defender-se contra a maioria dos tipos de riscos cibernéticos e cobrir 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 numa única interface e permite integrar aplicações da Kaspersky com aplicações de terceiros num sistema de segurança abrangente.

Um dos elementos centrais da solução é o *SIEM*. O SIEM rastreia eventos provenientes de todos os componentes e correlaciona esses eventos entre si usando regras definidas pelo fornecedor e pelo utilizador. O EDR Expert (on-premises) analisa os registos e a telemetria recebidos da infraestrutura corporativa para detetar automaticamente ataques e permite investigar incidentes usando um gráfico de investigação unificado que combina todos os eventos recolhidos no EDR Expert (on-premises), incluindo eventos de aplicações da Kaspersky e produtos de segurança da informação de terceiros.

Para responder a incidentes avançados, o EDR Expert (on-premises) utiliza cenários predefinidos e definidos pelo utilizador. Também pode usar ações de resposta de aplicações de terceiros e cenários de resposta que envolvem várias aplicações.

Endpoint Detection and Response (KATA)

O Kaspersky Endpoint Security for Windows suporta o funcionamento com o 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 criada para a deteção atempada de ameaças sofisticadas, como ataques direcionados, ameaças persistentes avançadas (APT), ataques de dia zero e outras. 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)*)

Pode adquirir todas as unidades funcionais ou unidades funcionais individuais separadamente. Para obter mais informações sobre a solução, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform.

A Kaspersky Endpoint Security é instalada em computadores individuais na infraestrutura de TI corporativa e monitoriza continuamente os processos, as ligações de rede abertas e os ficheiros que estão a ser modificados. As informações sobre eventos no computador (dados de telemetria) são enviadas para o servidor Kaspersky Anti Targeted Attack Platform. Neste caso, o Kaspersky Endpoint Security também envia informações para o servidor Kaspersky Anti Targeted Attack Platform sobre ameaças detetadas pela aplicação, bem como informações sobre os resultados de processamento destas ameaças.

A integração do EDR (KATA) e NDR (KATA) é configurada na consola do Kaspersky Security Center. O agente integrado é então gerido usando a consola da Kaspersky Anti Targeted Attack Platform, incluindo a execução de tarefas, a gestão de objetos em quarentena, a exibição de relatórios e outras ações.

Definições do Endpoint Detection and Response Expert (on-premises)

Parâmetro	Descrição
Connection to telemetry collection servers	Um *servidor de recolha de telemetria* é um servidor que faz parte de uma solução SIEM e que recolhe, normaliza, correlaciona, analisa e armazena informações sobre eventos que ocorrem no computador. Configure o seguinte para conectar-se aos servidores de recolha de telemetria (KUMA): • **Timeout (sec)**. Tempo limite máximo de resposta do servidor. Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor diferente. • **Server certificate**. Certificado TLS para estabelecer uma ligação fiável com o servidor. Pode obter um certificado TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Use two-way authentication**. Autenticação bidirecional ao estabelecer uma ligação segura entre o Kaspersky Endpoint Security e o servidor. Para utilizar a autenticação bidirecional, é necessário ativar a autenticação bidirecional nas definições do servidor e, em seguida, obter um contentor criptográfico e definir uma password para proteger o contentor criptográfico. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). Após configurar as definições do servidor, é também necessário ativar a autenticação bidirecional nas definições do Kaspersky Endpoint Security e carregar um contentor criptográfico protegido por password. O cripto-contentor deve ser protegido por password. Não é possível adicionar um cripto-contentor com uma password em branco.
Address e **Port** (servidores de recolha de telemetria)	Definições para ligação a servidores de recolha de telemetria. Pode inserir um endereço IP (IPv4 ou IPv6). Pode adicionar vários endereços do servidor de recolha de telemetria. O Kaspersky Endpoint Security tenta ligar-se ao servidor utilizando o primeiro endereço IP. Se não for possível estabelecer uma ligação, o Kaspersky Endpoint Security tenta ligar-se utilizando o segundo endereço IP da lista e assim sucessivamente.
Send telemetry to telemetry collection servers	Esta funcionalidade permite desativar completamente o envio de telemetria para o servidor KATA. Se estiver a utilizar a Kaspersky Anti Targeted Attack Platform juntamente com outra solução que também usa telemetria, pode desativar o envio de telemetria para o KATA (EDR). Isto permite otimizar a carga do servidor para estas soluções. Por exemplo, se tiver a solução Managed Detection and Response e o KATA (EDR) implementado, pode utilizar a telemetria MDR e criar tarefas de Resposta à Ameaça no KATA (EDR). • **Send telemetry with IOA only**. Isto permite otimizar a telemetria e enviar apenas telemetria com IOA. *Indicador de Ataque (IOA)* é uma regra que contém uma descrição do comportamento suspeito no sistema que pode indicar um ataque direcionado. A aplicação compara o comportamento contínuo no sistema com essas regras e regista eventos que indicam um ataque direcionado. A aplicação utiliza a tecnologia de *análise em tempo real*, que permite o acompanhamento em tempo real desses eventos. • **Maximum event transmission delay (sec)**. A aplicação sincroniza com o servidor para enviar eventos após o término do intervalo de sincronização. A predefinição é 30 segundos. • **Limit the number of event packets per transmission**. A aplicação é sincronizada com o servidor quando a memória intermédia está cheia de eventos. A predefinição é 1024 eventos. Esta função permite desativar o armazenamento em memória intermédia de eventos antes da sincronização com o servidor.
Enable request throttling	Esta ação ajuda a otimizar a carga no servidor. Se esta funcionalidade estiver ativada, a aplicação restringe a transmissão de eventos. Se o número de eventos exceder os limites configurados, o Kaspersky Endpoint Security irá interromper o envio de eventos. Configurar as definições de telemetria: • **Maximum number of events per hour**. A aplicação analisa o fluxo de dados de telemetria e restringe o envio de eventos se o fluxo de eventos exceder o limite de eventos por hora configurado. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. A predefinição é 3000 eventos por hora. Se a aplicação estiver instalada num servidor, o fluxo de dados de telemetria é mais elevado. Para os servidores, recomenda-se que o valor seja aumentado para 60 000 eventos por hora. • **Percentage of event limit excess**. A aplicação ordena os eventos por tipo (por exemplo, eventos "alterações no registo") e restringe a transmissão de eventos se a proporção de eventos do mesmo tipo para o número total de eventos exceder o limite configurado em percentagem. O Kaspersky Endpoint Security retoma o envio de eventos quando a proporção de outros eventos para o número total de eventos se torna grande o suficiente novamente. A predefinição é 15%.
Send sync request to server every (min)	Frequência de pedidos de sincronização enviados ao servidor. Durante a sincronização, o Kaspersky Endpoint Security envia informações sobre as definições e tarefas modificadas da aplicação.

Parâmetro	Descrição
Connection to response servers	Um *servidor de resposta* é um servidor para receber e analisar dados, estudar o comportamento de objetos e publicar os resultados desses estudos. Configure o seguinte para a ligação dos servidores de resposta: • **Timeout (sec)**. Tempo limite máximo de resposta do servidor. Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor diferente. • **Server certificate**. Certificado TLS para estabelecer uma ligação fiável com o servidor. Pode obter um certificado TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Use two-way authentication**. Autenticação bidirecional ao estabelecer uma ligação segura entre o Kaspersky Endpoint Security e o servidor. Para utilizar a autenticação bidirecional, é necessário ativar a autenticação bidirecional nas definições do servidor e, em seguida, obter um contentor criptográfico e definir uma password para proteger o contentor criptográfico. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor TLS na Open Single Management Platform (consulte as instruções na Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises)). Após configurar as definições do servidor, é também necessário ativar a autenticação bidirecional nas definições do Kaspersky Endpoint Security e carregar um contentor criptográfico protegido por password.
Address e **Port** (servidores de resposta)	Definições para ligação a servidores de resposta. Pode inserir um endereço IP (IPv4 ou IPv6). Pode adicionar vários endereços do servidor de recolha de telemetria. O Kaspersky Endpoint Security tenta ligar-se ao servidor utilizando o primeiro endereço IP. Se não for possível estabelecer uma ligação, o Kaspersky Endpoint Security tenta ligar-se utilizando o segundo endereço IP da lista e assim sucessivamente.

Definições do Endpoint Detection and Response (KATA)

Parâmetro	Descrição
Send sync request to server every (min)	Frequência de pedidos de sincronização enviados ao servidor. Durante a sincronização, o Kaspersky Endpoint Security envia informações sobre as definições e tarefas modificadas da aplicação.
Connection to KATA servers	Configure o seguinte para a ligação do servidor do Central Node: • **Timeout (sec)**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor de Central Node diferente. • **Server certificate**. Certificado TLS para estabelecer uma ligação fiável com o servidor do Central Node. Pode obter um certificado TLS na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform). • **Use two-way authentication**. Autenticação bidirecional ao estabelecer uma ligação segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para utilizar a autenticação bidirecional, é necessário ativar a autenticação bidirecional nas definições do servidor do Central Node e, em seguida, obter um contentor criptográfico e definir uma password para proteger o contentor criptográfico. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform). Após configurar as definições do Central Node, é também necessário ativar a autenticação bidirecional nas definições do Kaspersky Endpoint Security e carregar um contentor criptográfico protegido por password. O cripto-contentor deve ser protegido por password. Não é possível adicionar um cripto-contentor com uma password em branco.
Address e **Port** (servidores KATA)	Definições para ligação aos servidores da Kaspersky Anti Targeted Attack Platform. Insira o endereço IP (IPv4 ou IPv6) e a porta do servidor do Central Node para se conectar. Pode adicionar vários endereços do servidor do Nó Central. O Kaspersky Endpoint Security tenta ligar-se ao servidor utilizando o primeiro endereço IP. Se não for possível estabelecer uma ligação, o Kaspersky Endpoint Security tenta ligar-se utilizando o segundo endereço IP da lista e assim sucessivamente.
Send telemetry to KATA	Esta funcionalidade permite desativar completamente o envio de telemetria para o servidor KATA. Se estiver a utilizar a Kaspersky Anti Targeted Attack Platform juntamente com outra solução que também usa telemetria, pode desativar o envio de telemetria para o KATA (EDR). Isto permite otimizar a carga do servidor para estas soluções. Por exemplo, se tiver a solução Managed Detection and Response e o KATA (EDR) implementado, pode utilizar a telemetria MDR e criar tarefas de Resposta à Ameaça no KATA (EDR). Configurar as definições de telemetria: • **Maximum event transmission delay (sec)**. A aplicação sincroniza com o servidor para enviar eventos após o término do intervalo de sincronização. A predefinição é 30 segundos. • **Maximum number of event packages**. A aplicação é sincronizada com o servidor quando a memória intermédia está cheia de eventos. A predefinição é 1024 eventos.

Parâmetro	Descrição
Enable request throttling	Esta ação ajuda a otimizar a carga no servidor. Se esta funcionalidade estiver ativada, a aplicação restringe a transmissão de eventos. Se o número de eventos exceder os limites configurados, o Kaspersky Endpoint Security irá interromper o envio de eventos. Configurar as definições de telemetria: • **Maximum number of events per hour**. A aplicação analisa o fluxo de dados de telemetria e restringe o envio de eventos se o fluxo de eventos exceder o limite de eventos por hora configurado. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. A predefinição é 3000 eventos por hora. Se a aplicação estiver instalada num servidor, o fluxo de dados de telemetria é mais elevado. Para os servidores, recomenda-se que o valor seja aumentado para 60 000 eventos por hora. • **Percentage of event limit excess**. A aplicação ordena os eventos por tipo (por exemplo, eventos "alterações no registo") e restringe a transmissão de eventos se a proporção de eventos do mesmo tipo para o número total de eventos exceder o limite configurado em percentagem. O Kaspersky Endpoint Security retoma o envio de eventos quando a proporção de outros eventos para o número total de eventos se torna grande o suficiente novamente. A predefinição é 15%.

Network Detection and Response (KATA)

O Kaspersky Endpoint Security for Windows suporta o funcionamento com o 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 criada para a deteção atempada de ameaças sofisticadas, como ataques direcionados, ameaças persistentes avançadas (APT), ataques de dia zero e outras. 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)*)

Pode adquirir todas as unidades funcionais ou unidades funcionais individuais separadamente. Para obter mais informações sobre a solução, consulte a Ajuda da Kaspersky Anti Targeted Attack Platform.

A Kaspersky Endpoint Security é instalada em computadores individuais na infraestrutura de TI corporativa e monitoriza continuamente os processos, as ligações de rede abertas e os ficheiros que estão a ser modificados. As informações sobre eventos no computador (dados de telemetria) são enviadas para o servidor Kaspersky Anti Targeted Attack Platform. Neste caso, o Kaspersky Endpoint Security também envia informações para o servidor Kaspersky Anti Targeted Attack Platform sobre ameaças detetadas pela aplicação, bem como informações sobre os resultados de processamento destas ameaças.

A integração do EDR (KATA) e NDR (KATA) é configurada na consola do Kaspersky Security Center. O agente integrado é então gerido usando a consola da Kaspersky Anti Targeted Attack Platform, incluindo a execução de tarefas, a gestão de objetos em quarentena, a exibição de relatórios e outras ações.

Parâmetro	Descrição
Definições de ligação do servidor	**Tempo limite (seg)**. Tempo limite máximo de resposta do servidor do Central Node. Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor de Central Node diferente. **Certificado TLS do servidor**. Certificado TLS para estabelecer uma ligação fiável com o servidor do Central Node. Pode obter um certificado TLS na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform). **Usar a autenticação bidirecional**. Autenticação bidirecional ao estabelecer uma ligação segura entre o Kaspersky Endpoint Security e o servidor do Central Node. Para utilizar a autenticação bidirecional, é necessário ativar a autenticação bidirecional nas definições do servidor do Central Node e, em seguida, obter um contentor criptográfico e definir uma password para proteger o contentor criptográfico. Um *cripto-contentor* é um arquivo PFX com um certificado e uma chave privada. Pode obter um cripto-contentor na consola da Kaspersky Anti Targeted Attack Platform (consulte as instruções na Ajuda da Kaspersky Anti Targeted Attack Platform). Após configurar as definições do Central Node, é também necessário ativar a autenticação bidirecional nas definições do Kaspersky Endpoint Security e carregar um contentor criptográfico protegido por password. O cripto-contentor deve ser protegido por password. Não é possível adicionar um cripto-contentor com uma password em branco.
Endereço e **Porta**	Definições para ligação aos servidores da Kaspersky Anti Targeted Attack Platform. Insira o endereço IP (IPv4 ou IPv6) e a porta do servidor do Central Node para se conectar. Pode adicionar vários endereços do servidor do Nó Central. O Kaspersky Endpoint Security tenta ligar-se ao servidor utilizando o primeiro endereço IP. Se não for possível estabelecer uma ligação, o Kaspersky Endpoint Security tenta ligar-se utilizando o segundo endereço IP da lista e assim sucessivamente.
Enviar pedido de sincronização ao servidor NDR a cada (min)	Frequência de pedidos de sincronização enviados ao servidor. Durante a sincronização, o Kaspersky Endpoint Security envia informações sobre as definições e tarefas modificadas da aplicação.
Atraso máximo de transmissão de eventos (seg)	A aplicação sincroniza com o servidor para enviar eventos após o término do intervalo de sincronização. A predefinição é 30 segundos.
Ativar limitação de pedidos	Esta ação ajuda a otimizar a carga no servidor. Se esta funcionalidade estiver ativada, a aplicação restringe a transmissão de eventos. Se o número de eventos exceder os limites configurados, o Kaspersky Endpoint Security irá interromper o envio de eventos.
Número máximo de eventos por hora	A aplicação analisa o fluxo de dados de telemetria e restringe o envio de eventos se o fluxo de eventos exceder o limite de eventos por hora configurado. O Kaspersky Endpoint Security retoma o envio de eventos após uma hora. A predefinição é 3000 eventos por hora. Se a aplicação estiver instalada num servidor, o fluxo de dados de telemetria é mais elevado. Para os servidores, recomenda-se que o valor seja aumentado para 60 000 eventos por hora.
Percentagem de excesso do limite de evento	A aplicação ordena os eventos por tipo (por exemplo, eventos "alterações no registo") e restringe a transmissão de eventos se a proporção de eventos do mesmo tipo para o número total de eventos exceder o limite configurado em percentagem. O Kaspersky Endpoint Security retoma o envio de eventos quando a proporção de outros eventos para o número total de eventos se torna grande o suficiente novamente. A predefinição é 15%.

Integração do KUMA

O Kaspersky Endpoint Security for Windows suporta a solução Kaspersky Unified Monitoring and Analysis Platform. O *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* é uma solução de gestão de eventos e informações de segurança (SIEM) para a infraestrutura informática das organizações. O KUMA permite detetar, analisar e atenuar as ameaças à segurança, antes que estas possam causar danos.

Parâmetro	Descrição
Maximum delay when sending events (sec)	A aplicação sincroniza com o servidor para enviar eventos após o término do intervalo de sincronização. A predefinição é 30 segundos.
Connection to KUMA servers	**Timeout (sec)**. Tempo máximo de espera por uma resposta do servidor KUMA (por predefinição, o valor é de 5 segundos). Quando o tempo limite acaba, o Kaspersky Endpoint Security tenta ligar-se a um servidor KUMA diferente. **Server certificate**. Certificado TLS para estabelecer uma ligação fiável com o servidor KUMA. Pode obter um certificado TLS na consola do Kaspersky Unified Monitoring and Analysis Platform (consulte as instruções na Ajuda do Kaspersky Unified Monitoring and Analysis Platform). Para estabelecer uma ligação de confiança, na consola KUMA, nas definições do conector tcp, tem de selecionar o modo TLS **With verification** (consulte as definições para o conetor de tipo tcp na Ajuda do Kaspersky Unified Monitoring and Analysis Platform). **Use two-way authentication**. Autenticação bidirecional ao estabelecer uma ligação segura entre o KES e o KUMA. Para utilizar a autenticação bidirecional, na consola KUMA, nas definições do conetor, tem de selecionar o modo TLS **Custom PFX with client authentication** (consulte as definições do conetor na Ajuda do Kaspersky Unified Monitoring and Analysis Platform). Em seguida, tem de transferir um certificado de servidor e definir uma password para proteger o contentor criptográfico. O cripto-contentor deve ser protegido por password. Não é possível adicionar um cripto-contentor com uma password em branco.
Servidores de KUMA	Definições de ligação aos servidores da Kaspersky Unified Monitoring and Analysis Platform. Pode inserir um endereço IP (IPv4 ou IPv6). Pode adicionar vários endereços do servidor KUMA. O Kaspersky Endpoint Security tenta ligar-se ao servidor utilizando o primeiro endereço IP. Se não for possível estabelecer uma ligação, o Kaspersky Endpoint Security tenta ligar-se utilizando o segundo endereço IP da lista e assim sucessivamente.

Encriptação de disco completa

Pode selecionar uma tecnologia de encriptação: Encriptação de disco Kaspersky ou Encriptação de Unidade BitLocker (aqui também referida simplesmente como "BitLocker").

Encriptação de disco Kaspersky

O Encriptação de disco Kaspersky não é compatível com computadores baseados em Arm.

Após a encriptação das unidades de disco rígido do sistema, no próximo arranque do computador, o utilizador tem de efetuar a autenticação utilizando o Agente de Autenticação antes de as unidades de disco rígido poderem ser acedidas e o sistema operativo ser carregado. Para tal é necessário introduzir a password do token ou smart card ligado ao computador ou o nome de utilizador e a password da conta do Agente de Autenticação criada pelo administrador da rede local utilizando a tarefa de *Gestão das contas de Agente de Autenticação*. Estas contas são baseadas em contas do Microsoft Windows com as quais os utilizadores iniciam sessão no sistema operativo. Pode também utilizar a tecnologia Single Sign-On (SSO) que permite iniciar sessão no sistema operativo automaticamente, utilizando o nome de utilizador e a password da conta do Agente de Autenticação.

A autenticação do utilizador no Agente de Autenticação pode ser efetuada de duas formas:

- Introduzindo o nome e a password da conta do Agente de Autenticação criada pelo administrador da rede da empresa utilizando as ferramentas do Kaspersky Security Center.
- Introduza a password de um token ou smart card ligado ao computador.

  A utilização de um token ou smart-card está disponível apenas se as unidades de disco rígido do computador tiverem sido encriptadas ao utilizar o algoritmo de encriptação AES256. Se os discos rígidos do computador foram encriptados através do algoritmo de encriptação AES56, a adição do ficheiro de certificado eletrónico ao comando será negada.

Encriptação de Unidade BitLocker

BitLocker é uma tecnologia de encriptação integrada nos sistemas operativos Windows. O Kaspersky Endpoint Security permite controlar e gerir o Bitlocker utilizando a infraestrutura do Kaspersky Next. O BitLocker encripta volumes lógicos. Não pode utilizar o BitLocker para a encriptação de unidades removíveis. Para obter mais informações sobre o BitLocker, consulte a documentação da Microsoft.

Ao criptografar o disco, o BitLocker coloca o carregador de inicialização e outros ficheiros auxiliares no system partition. Esta partição não está encriptada. O sistema operativo cria a partição do sistema automaticamente durante a instalação do Windows. Se o disco estiver totalmente particionado antes da instalação do Windows, o sistema operativo não poderá criar uma partição do sistema. Neste caso, quando inicia a encriptação de disco do BitLocker, o sistema operativo solicita que faça uma repartição do disco e crie uma partição do sistema. Depois de criar uma partição do sistema, o sistema operativo inicia a encriptação do BitLocker.

O BitLocker fornece armazenamento seguro de chaves de acesso ao utilizar um módulo de plataforma fiável. Um *Trusted Platform Module* (TPM) é um microchip desenvolvido para fornecer funções básicas relacionadas com segurança (por exemplo, para armazenar chaves de encriptação). Habitualmente, é instalado um Trusted Platform Module (TPM) na motherboard do computador e interage com todos os outros componentes do sistema através do barramento de hardware. Utilizar o TPM é a forma mais segura de armazenar chaves de acesso do BitLocker, uma vez que o TPM fornece verificação integrada do sistema antes do arranque. Ainda pode encriptar unidades num computador sem um TPM. Neste caso, a chave de acesso será encriptada com uma password. O BitLocker utiliza os seguintes métodos de autenticação:

- TPM.
- TPM e PIN.
- Password.

Depois de encriptar o disco rígido do sistema, o utilizador precisa passar pela autenticação do BitLocker para inicializar o sistema operativo. Após a autenticação, o BitLocker permite que o utilizador inicie sessão. O BitLocker não oferece suporte à tecnologia de início de sessão único (SSO).

Depois de encriptar uma unidade, o BitLocker cria uma chave de recuperação. O Kaspersky Endpoint Security envia a chave de recuperação ao Kaspersky Security Center para que possa restaurar o acesso ao disco, por exemplo, se um utilizador se esqueceu da password.

Se um utilizador encriptar um disco utilizando o BitLocker, o Kaspersky Endpoint Security enviará a chave de recuperação e informações sobre a encriptação do disco ao Kaspersky Security Center.

Se estiver a utilizar políticas de grupo do Windows, desative a gestão do BitLocker nas definições de política. As definições de política do Windows podem entrar em conflito com as definições de política do Kaspersky Endpoint Security. Ao encriptar uma unidade, podem ocorrer erros.

Definições do componente Encriptação de disco Kaspersky

Parâmetro	Descrição
Modo de encriptação	**Encriptar todas as unidades de discos rígido**. Se esta opção estiver selecionada, a aplicação encripta todas as unidades de disco rígido quando a política é aplicada. Se o computador tiver vários sistemas operativos instalados, após a encriptação apenas poderá carregar o sistema operativo com a aplicação instalada. **Desencriptar todas as unidades de discos rígido**. Se esta opção estiver selecionada, a aplicação desencripta todas as unidades de disco rígido previamente encriptadas quando a política é aplicada. **Manter inalterado**. Se este item estiver selecionado, a aplicação deixa as unidades no estado anterior quando a política é aplicada. Se a unidade foi encriptada, esta permanece encriptada. Se a unidade foi desencriptada, esta permanece desencriptada. Por predefinição, este item está selecionado.
Durante a encriptação, criar automaticamente contas do Agente de Autenticação para utilizadores do Windows	Se esta caixa de verificação estiver selecionada, a aplicação cria contas do Agente de Autenticação com base na lista de contas de utilizador do Windows no computador. Por predefinição, o Kaspersky Endpoint Security utiliza todas as contas locais e de domínio com as quais o utilizador iniciou a sessão no sistema operativo ao longo dos últimos 30 dias.
Definições 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 do 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 em algum momento. **Conta de serviço com uma password única**. A conta de serviço é necessária para obter acesso ao computador, por exemplo, quando o utilizador se esquece da password. Também pode utilizar a conta de serviço como uma conta de reserva. Tem de inserir o nome da conta (por defeito, `ServiceAccount`). O Kaspersky Endpoint Security cria uma password automaticamente. Pode encontrar a password na consola do Kaspersky Security Center. **Administrador local**. O Kaspersky Endpoint Security cria uma conta de utilizador do Agente de Autenticação para o administrador local do computador. **Gestor do computador**. O Kaspersky Endpoint Security cria uma conta de utilizador do Agente de Autenticação para a conta do gestor do computador. Pode ver qual é a conta que tem a função de gestor do computador nas propriedades do computador no Active Directory. Por defeito, a função de gestor do computador não está definida, ou seja, não corresponde a uma conta. **Conta ativa**. O Kaspersky Endpoint Security cria automaticamente uma conta do Agente de Autenticação para a conta que está ativa no momento da encriptação do disco.
Criar automaticamente contas do Agente de Autenticação para todos os utilizadores deste computador ao iniciar sessão	Se esta caixa de verificação estiver selecionada, a aplicação verifica as informações sobre as contas de utilizador do Windows no computador antes de iniciar o Agente de Autenticação. Se o Kaspersky Endpoint Security detetar uma conta de utilizador do Windows sem conta do Agente de Autenticação, a aplicação criará uma nova conta para aceder às unidades encriptadas. A nova conta do Agente de Autenticação terá as seguintes definições predefinidas: início de sessão protegido apenas por password e alteração da password na primeira autenticação. Como tal, não é necessário adicionar manualmente contas do Agente de Autenticação através da tarefa *Gestão das contas de Agente de Autenticação* para computadores com unidades já encriptadas.
Guardar o nome de utilizador introduzir no Agente de Autenticação	Se a caixa de verificação for selecionada, a aplicação guarda o nome da conta do Agente de Autenticação. Não será solicitada a introdução do nome da conta da próxima vez que tentar concluir a autorização no Agente de Autenticação com a mesma conta.

Parâmetro	Descrição
Encriptar apenas espaço utilizado do disco (reduz tempo de encriptação)	Esta caixa ativa/desativa a opção que limita a área de encriptação a setores ocupados do disco rígido. Este limite permite reduzir o tempo de encriptação. Ativar ou desativar a funcionalidade **Encriptar apenas espaço utilizado do disco (reduz tempo de encriptação)** após o início da encriptação não altera esta definição até que os discos rígidos sejam desencriptados. Tem de selecionar ou desmarcar a caixa de verificação antes de iniciar a encriptação. Se a caixa de verificação estiver selecionada, são encriptadas apenas as partes do disco rígido que estiverem ocupadas por ficheiros. O Kaspersky Endpoint Security encripta automaticamente dados novos quando são adicionados. Se a caixa de verificação estiver selecionada, é encriptado o disco rígido completo, incluindo os fragmentos residuais de ficheiros anteriormente eliminados e modificados. Recomenda-se esta opção para discos rígidos novos cujos dados não tenham sido modificados ou eliminados. Se estiver a aplicar encriptação num disco rígido que já esteja em utilização, recomenda-se encriptar o disco rígido completo. Dessa forma, assegura a proteção de todos os dados, mesmo os dados eliminados que sejam potencialmente recuperáveis. Por padrão, a caixa de verificação está desmarcada.
Utilizar Legacy USB Support (não recomendado)	Esta caixa de seleção ativa ou desativa a funcionalidade Legacy USB Support. O *Suporte de USB legado* **é** uma função BIOS/UEFI que permite usar dispositivos USB (como um token de segurança) durante a fase de inicialização do computador antes de iniciar o sistema operativo (modo BIOS). O Legacy USB Support não afeta o suporte para dispositivos USB após iniciar o sistema operativo. Se a caixa de verificação estiver selecionada, o suporte de dispositivos USB durante o arranque inicial do computador é ativado. Quando a função Legacy USB Support está ativa, o Agente de autenticação no modo BIOS não suporta trabalho com tokens via USB. Recomenda-se utilizar esta opção apenas quando existir um problema de compatibilidade de hardware e só para os computadores nos quais o problema ocorreu.
Definições de password	Definições de segurança da password da conta do Agente de Autenticação. Ao usar a tecnologia de autenticação única, o Agente de Autenticação ignora os requisitos de segurança da password especificados no Kaspersky Security Center. Pode definir os requisitos de segurança da password nas definições do sistema operativo.
Utilizar a tecnologia SSO (Single Sign-On)	A tecnologia SSO possibilita a utilização das mesmas credenciais de conta para aceder a unidades de disco rígido encriptadas e iniciar sessão no sistema operativo. Se a caixa de verificação estiver selecionada, tem de introduzir as credenciais para aceder a unidades de disco rígido encriptadas e, em seguida, iniciar sessão automaticamente no sistema operativo. Se a caixa de verificação estiver desmarcada, tem de introduzir em separado as credenciais de acesso a unidades encriptadas e as credenciais da conta de utilizador do sistema operativo para aceder a unidades de disco rígido encriptadas e, em seguida, iniciar sessão automaticamente no sistema operativo.
Envolver fornecedores de credenciais de terceiros	O Kaspersky Endpoint Security suporta o fornecedor de credenciais de terceiros ADSelfService Plus. Ao trabalhar com fornecedores de credenciais de terceiros, o Agente de Autenticação interceta a password antes de o sistema operativo ser carregado. Isto significa que um utilizador apenas precisa de introduzir uma password uma única vez ao iniciar sessão no Windows. Depois de iniciar sessão no Windows, o utilizador pode utilizar as capacidades de um fornecedor de credenciais de terceiros para realizar a autenticação em serviços empresariais, por exemplo. Os fornecedores de credenciais de terceiros também permitem aos utilizadores repor a sua própria password de forma independente. Neste caso, o Kaspersky Endpoint Security irá atualizar automaticamente a password do Agente de Autenticação. Se estiver a utilizar um fornecedor de credenciais de terceiros que não seja suportado pela aplicação, poderá encontrar algumas limitações no funcionamento da tecnologia de Início de Sessão Único.
Ajuda	**Autenticação**. Texto de ajuda que aparece na janela Agente de autenticação ao inserir as credenciais da conta. **Alterar password**. Texto de ajuda que aparece na janela Agente de autenticação ao alterar a password da conta do Agente de Autenticação. **Recuperar password**. Texto de ajuda que aparece na janela Agente de autenticação ao recuperar a password da conta do Agente de Autenticação.

Parâmetro	Descrição
Modo de encriptação	**Encriptar todas as unidades de discos rígido**. Se esta opção estiver selecionada, a aplicação encripta todas as unidades de disco rígido quando a política é aplicada. Se o computador tiver vários sistemas operativos instalados, após a encriptação apenas poderá carregar o sistema operativo com a aplicação instalada. **Desencriptar todas as unidades de discos rígido**. Se esta opção estiver selecionada, a aplicação desencripta todas as unidades de disco rígido previamente encriptadas quando a política é aplicada. **Manter inalterado**. Se este item estiver selecionado, a aplicação deixa as unidades no estado anterior quando a política é aplicada. Se a unidade foi encriptada, esta permanece encriptada. Se a unidade foi desencriptada, esta permanece desencriptada. Por predefinição, este item está selecionado.
Ativar utilização de autenticação BitLocker que exija introdução por teclado de pré-arranque em tablets	Utilizar a autenticação que requer a entrada de dados num ambiente de pré-arranque, mesmo que a plataforma não tenha a capacidade para a entrada de pré-arranque (por exemplo, no caso dos teclados táteis no ecrã nos tablets). O ecrã tátil dos tablets não está disponível no meio de pré-arranque. Para concluir a autenticação com BitLocker em tablets, o utilizador deve ligar, por exemplo, um teclado USB. Se a caixa de verificação estiver selecionada, é permitida a utilização da autenticação com entrada de pré-arranque. Recomendamos a utilização desta definição apenas para dispositivos que tenham ferramentas de entrada de dados alternativas num ambiente de pré-arranque como, por exemplo, um teclado USB adicionalmente aos teclados do ecrã tátil. Se a caixa de verificação estiver desmarcada, não é possível executar a Encriptação de Unidade BitLocker em tablets.
Utilizar encriptação de hardware (Windows 8 e versões mais recentes)	Se a caixa de verificação estiver selecionada, a aplicação aplica a encriptação de hardware. O que lhe permite aumentar a velocidade da encriptação e utilizar menos recursos do computador.
Encriptar apenas espaço utilizado do disco (Windows 8 e versões mais recentes)	Esta caixa ativa/desativa a opção que limita a área de encriptação a setores ocupados do disco rígido. Este limite permite reduzir o tempo de encriptação. Ativar ou desativar a funcionalidade **Encriptar apenas espaço utilizado do disco (reduz tempo de encriptação)** após o início da encriptação não altera esta definição até que os discos rígidos sejam desencriptados. Tem de selecionar ou desmarcar a caixa de verificação antes de iniciar a encriptação. Se a caixa de verificação estiver selecionada, são encriptadas apenas as partes do disco rígido que estiverem ocupadas por ficheiros. O Kaspersky Endpoint Security encripta automaticamente dados novos quando são adicionados. Se a caixa de verificação estiver selecionada, é encriptado o disco rígido completo, incluindo os fragmentos residuais de ficheiros anteriormente eliminados e modificados. Recomenda-se esta opção para discos rígidos novos cujos dados não tenham sido modificados ou eliminados. Se estiver a aplicar encriptação num disco rígido que já esteja em utilização, recomenda-se encriptar o disco rígido completo. Dessa forma, assegura a proteção de todos os dados, mesmo os dados eliminados que sejam potencialmente recuperáveis. Por padrão, a caixa de verificação está desmarcada.

Parâmetro	Descrição
Método de autenticação	**Apenas password (Windows 8 e versões mais recentes)** Se esta opção estiver selecionada, o Kaspersky Endpoint Security pede uma password ao utilizador quando este tenta aceder a unidade encriptada. Esta opção pode ser selecionada quando um Trusted Platform Module (TPM) não está a ser utilizado. **Trusted platform module (TPM)** Se esta opção estiver selecionada, o BitLocker utiliza um Trusted Platform Module (TPM). Um *Trusted Platform Module* (TPM) é um microchip desenvolvido para fornecer funções básicas relacionadas com segurança (por exemplo, para armazenar chaves de encriptação). Um Trusted Platform Module está normalmente instalado na placa principal (motherboard) e interage com todos os outros componentes de sistema através do hardware de barramento. No caso de computadores a executar o Windows 7 ou Windows Server 2008 R2, só está disponível encriptação utilizando um módulo TPM. Se um módulo TPM não estiver instalado, a encriptação do BitLocker não será possível. O uso de uma password nestes computadores não é suportado. Um dispositivo equipado com um Trusted Platform Module pode criar chaves de encriptação que apenas podem ser desencriptadas com o dispositivo. Um Trusted Platform Module encripta as chaves de encriptação com a sua própria chave de armazenamento de raiz. A chave de armazenamento de raiz está armazenada dentro do Trusted Platform Module. Isto fornece um nível adicional de proteção contra tentativas de penetração nas chaves de encriptação. Esta ação está selecionada por predefinição. Pode definir uma camada adicional de proteção para o acesso à chave de encriptação, e encriptar a chave com uma password ou um PIN: • **Utilizar PIN para TPM**. Se esta caixa de verificação estiver selecionada, um utilizador pode utilizar um código PIN para obter o acesso a uma chave de encriptação que esteja armazenada num Trusted Platform Module (TPM). Se esta caixa de verificação estiver desmarcada, os utilizadores estão proibidos de utilizar códigos PIN. Para aceder à chave de encriptação, um utilizador deverá introduzir a password. • **Trusted platform module (TPM) ou password se o TPM não estiver disponível**. Se esta opção estiver selecionada, o utilizador pode utilizar uma password para obter acesso a chaves de encriptação quando um Trusted Platform Module (TPM) não está disponível. Se a caixa de verificação não estiver selecionada e o TPM não estiver disponível, a encriptação de disco completa não é iniciada. O método de autenticação selecionado tem de ser configurado ao especificar os requisitos de password ou PIN: • **Comprimento mínimo do PIN (carateres)** (o valor predefinido é 6). • **Comprimento mínimo da password (carateres)** (o valor predefinido é 8). • **Número máximo de palavras-passe/PINs armazenados** (o valor predefinido é 5). • **Limitar período de validade de password/PIN para TPM (dias)** (desativado por predefinição). • **Utilizar PIN melhorado (letras e números)**. O *PIN avançado* permite a utilização de outros caracteres além dos caracteres numéricos: letras latinas maiúsculas e minúsculas, caracteres especiais e espaços. Desativado por predefinição.
Recriar automaticamente a chave de recuperação (dias)	Atualizar automaticamente a password para restaurar o acesso a uma unidade protegida por BitLocker. Se a caixa de verificação estiver selecionada, especifique o período de validade da password da chave de recuperação. Isto ajuda a evitar a reutilização da password da chave de recuperação.

Encriptação ao nível dos ficheiros

A encriptação de ficheiros não é suportada em computadores baseados em Arm.

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para estações de trabalho. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para servidores.

Pode compilar listas de ficheiros por extensão ou grupos de extensões e listas de pastas armazenadas em unidades de leitura locais e criar regras para encriptar ficheiros que são criados por aplicações específicas. Após a aplicação de uma política, o Kaspersky Endpoint Security encripta e desencripta os seguintes ficheiros:

- ficheiros adicionados individualmente a listas de encriptação e desencriptação;
- ficheiros armazenados em pastas adicionados a listas de encriptação e desencriptação;
- ficheiros criados por aplicações separadas.

A encriptação de ficheiros possui os seguintes recursos especiais:

- O Kaspersky Endpoint Security encripta/desencripta ficheiros em pastas predefinidas apenas para perfis de utilizadores locais do sistema operativo. O Kaspersky Endpoint Security não encripta ou desencripta ficheiros em pastas predefinidas de perfis de utilizadores em roaming, perfis de utilizador obrigatórios, perfis de utilizador temporários ou pastas redirecionadas.
- O Kaspersky Endpoint Security não encripta ficheiros cuja modificação possa prejudicar o sistema operativo e aplicações instaladas. Por exemplo, os seguintes ficheiros e pastas com todas as pastas imbricadas estão na lista de exclusões da encriptação:
  - %WINDIR%;
  - %PROGRAMFILES% e %PROGRAMFILES(X86)%;
  - Ficheiros de registo do Windows.

  A lista de exclusões de encriptação não pode ser visualizada nem editada. Embora os ficheiros e as pastas na lista de exclusões de encriptação possam ser adicionados à lista de encriptação, não serão encriptados durante encriptação de um ficheiro.

Definições do componente Encriptação ao nível dos ficheiros

Parâmetro	Descrição
Modo de encriptação	**Manter inalterado**. Se este item estiver selecionado, os ficheiros e as pastas permanecem inalterados pelo Kaspersky Endpoint Security, sem encriptação nem desencriptação. **De acordo com as regras**. Se este item for selecionado, o Kaspersky Endpoint Security encripta os ficheiros e pastas de acordo com as regras de encriptação, desencripta os ficheiros e pastas de acordo com as regras de desencriptação e regula o acesso das aplicações aos ficheiros encriptados de acordo com as regras da aplicação. **Desencriptar tudo**. Se este item estiver selecionado, o Kaspersky Endpoint Security desencripta todos os ficheiros e pastas desencriptados.

Parâmetro	Descrição
Encriptação	Este separador apresenta as regras de encriptação para ficheiros armazenados em unidades locais. Pode adicionar ficheiros da seguinte maneira: • **Pastas predefinidas**. O Kaspersky Endpoint Security permite adicionar as seguintes áreas: **Documentos**. Ficheiros na pasta *Documentos* padrão do sistema operativo e as respetivas subpastas. **Favoritos**. Ficheiros na pasta *Favoritos* padrão do sistema operativo e respetivas subpastas. **Ambiente de trabalho**. Ficheiros na pasta *Ambiente de trabalho* padrão do sistema operativo e respetivas subpastas. **Ficheiros temporários**. Ficheiros temporários relacionados com o funcionamento das aplicações instaladas no computador. Por exemplo, as aplicações do Microsoft Office criam ficheiros temporários que contêm cópias de segurança dos documentos. **Ficheiros do Outlook**. Ficheiros relacionados com o funcionamento do cliente de e-mail do Outlook: ficheiros de dados (PST), ficheiros de dados offline (OST), ficheiros do livro de endereços offline (OAB) e ficheiros do livro de endereços pessoal (PAB). • **Pasta predefinida**. Pode digitar o caminho até à pasta. Ao adicionar um caminho de pasta, cumpra as seguintes regras: Use uma variável de ambiente (por exemplo, `%FOLDER%\UserFolder\`). Pode usar uma variável de ambiente apenas uma vez e só no início do caminho. Não use caminhos relativos. Não use os carateres `*` e `?`. Não use caminhos UNC. Use `;` ou `,` como um caráter separador. • **Ficheiros por extensão**. Pode selecionar grupos de extensões da lista, como o grupo de extensões *Ficheiros*. Pode também adicionar manualmente a extensão do ficheiro.
Desencriptação	Este separador apresenta as regras de desencriptação para ficheiros armazenados em unidades locais.
Regras de aplicações	O separador apresenta uma tabela que contém regras de acesso ao ficheiro encriptado para as aplicações e regras de encriptação de ficheiros que são criados ou alterados por aplicações individuais.
Pacotes encriptados	Requisitos de segurança da password a serem cumpridos ao criar pacotes encriptados.

Encriptação de unidades amovíveis

A encriptação de unidades removíveis não é suportada em computadores baseados em Arm.

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para estações de trabalho. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Windows para servidores.

O Kaspersky Endpoint Security suporta a encriptação de ficheiros nos sistemas de ficheiros FAT32 e NTFS. Se uma unidade amovível com um sistema de ficheiros não suportado for ligada ao computador, a tarefa de encriptação desta unidade amovível termina com um erro e o Kaspersky Endpoint Security atribui o estado apenas de leitura à unidade amovível.

Para proteger dados em unidades amovíveis, pode usar os seguintes tipos de encriptação:

- Full Disk Encryption (FDE).

  Encriptação de toda a unidade amovível, incluindo o sistema de ficheiros.

  Não é possível aceder a dados encriptados fora da rede empresarial. Também é impossível aceder a dados encriptados dentro da rede empresarial se o computador não estiver ligado ao Kaspersky Security Center (ou seja, num computador convidado).

- File Level Encryption (FLE).

  Encriptação só de ficheiros numa unidade amovível. O sistema de ficheiros permanece inalterado.

  > A encriptação de ficheiros em unidades amovíveis fornece a capacidade de aceder a dados fora da rede empresarial através de um modo especial chamado *Modo portátil*.

Durante a encriptação, o Kaspersky Endpoint Security cria uma chave mestra. O Kaspersky Endpoint Security guarda a chave mestra nos seguintes repositórios:

- Kaspersky Security Center.
- Computador do utilizador.

  A chave mestra é encriptada com a chave secreta do utilizador.
- Unidade amovível.

  A chave mestra é encriptada com a chave pública do Kaspersky Security Center.

Após a conclusão da encriptação, os dados na unidade amovível podem ser acedidos na rede empresarial como se estivessem numa unidade amovível convencional não encriptada.

Aceder a dados encriptados

Quando uma unidade amovível com dados encriptados é ligada, o Kaspersky Endpoint Security executa as seguintes ações:

1. Verifica se há uma chave mestra no armazenamento local no computador do utilizador.

   Se a chave mestra for encontrada, o utilizador obterá acesso aos dados na unidade amovível.

   Se a chave mestra não for encontrada, o Kaspersky Endpoint Security executa as seguintes ações:

   a. Envia um pedido ao Kaspersky Security Center.

      Após receber o pedido, o Kaspersky Security Center envia uma resposta que contém a chave mestra.

   b. O Kaspersky Endpoint Security guarda a chave mestra no armazenamento local no computador do utilizador para operações subsequentes com a unidade amovível encriptada.
2. Desencripta os dados.

Recursos especiais de encriptação de unidade amovível

A encriptação de unidades amovíveis possui os seguintes recursos especiais:

- A política com predefinições para encriptação de unidades amovíveis é formada por um grupo específico de computadores geridos. Como tal, o resultado da aplicação da política do Kaspersky Security Center configurada para a encriptação/desencriptação de unidades amovíveis depende do computador ao qual a unidade amovível está ligada.
- O Kaspersky Endpoint Security não encripta/desencripta ficheiros apenas de leitura que estão armazenados em unidades amovíveis.
- Os seguintes tipos de dispositivos são suportados como unidades amovíveis:
  - Suportes de dados ligados pelo bus USB
  - unidades de disco rígido ligadas por bus USB e bus FireWire
  - unidades SSD ligadas por barramentos USB e FireWire

Definições do componente da encriptação de unidades amovíveis

Parâmetro	Descrição
Modo de encriptação	**Encriptar unidade amovível completa**. Se este item estiver selecionado, ao aplicar a política com as configurações de encriptação especificadas para unidades amovíveis, o Kaspersky Endpoint Security encripta unidades amovíveis setor a setor, incluindo os respetivos ficheiros de sistema. **Encriptar todos os ficheiros**. Se este item estiver selecionado, ao aplicar a política com as configurações de encriptação especificadas para unidades amovíveis, o Kaspersky Endpoint Security encripta todos os ficheiros que estão armazenados em unidades amovíveis. O Kaspersky Endpoint Security não encripta novamente os ficheiros que já estão encriptados. Os conteúdos do sistema de ficheiros de uma unidade amovível, incluindo nomes de estruturas de pastas e nomes de ficheiros encriptados, não são encriptados e permanecem acessíveis. **Encriptar apenas os ficheiros novos**. Se este item estiver selecionado, ao aplicar a política com as definições de encriptação especificadas para unidades amovíveis, o Kaspersky Endpoint Security encripta apenas os ficheiros que foram adicionados ou alterados nas unidades amovíveis após a última aplicação da política do Kaspersky Security Center. Este modo de encriptação é aconselhável quando uma unidade amovível é utilizada para fins pessoais e profissionais. Este modo de encriptação permite manter todos os ficheiros antigos inalterados e encriptar apenas os ficheiros que o utilizador cria num computador profissional com o Kaspersky Endpoint Security instalado e a funcionalidade de encriptação ativada. Deste modo, o acesso aos ficheiros pessoais está sempre disponível, independentemente de o Kaspersky Endpoint Security com a funcionalidade de encriptação estar ou não instalado no computador. **Desencriptar unidade amovível completa**. Se este item estiver selecionado, ao aplicar a política com as configurações de encriptação especificadas para unidades amovíveis, o Kaspersky Endpoint Security desencripta todos os ficheiros encriptados que estejam armazenados em unidades amovíveis, bem como todos os sistemas de ficheiros das unidades amovíveis, se tiverem sido encriptados anteriormente. **Manter inalterado**. Se este item estiver selecionado, a aplicação deixa as unidades no estado anterior quando a política é aplicada. Se a unidade foi encriptada, esta permanece encriptada. Se a unidade foi desencriptada, esta permanece desencriptada. Por predefinição, este item está selecionado.
Modo portátil	Esta caixa de verificação ativa/desativa a preparação de uma unidade amovível que possibilita o acesso a ficheiros guardados na unidade amovível, em computadores fora da rede da empresa. Se esta caixa de verificação estiver selecionada, o Kaspersky Endpoint Security solicita ao utilizador que especifique uma password antes da encriptação de ficheiros numa unidade amovível aquando da aplicação da política. A password é necessária para aceder a ficheiros encriptados numa unidade amovível, em computadores fora da rede da empresa. Pode configurar a segurança da password. O modo portátil está disponível para os modos **Encriptar todos os ficheiros** ou **Encriptar apenas os ficheiros novos**.

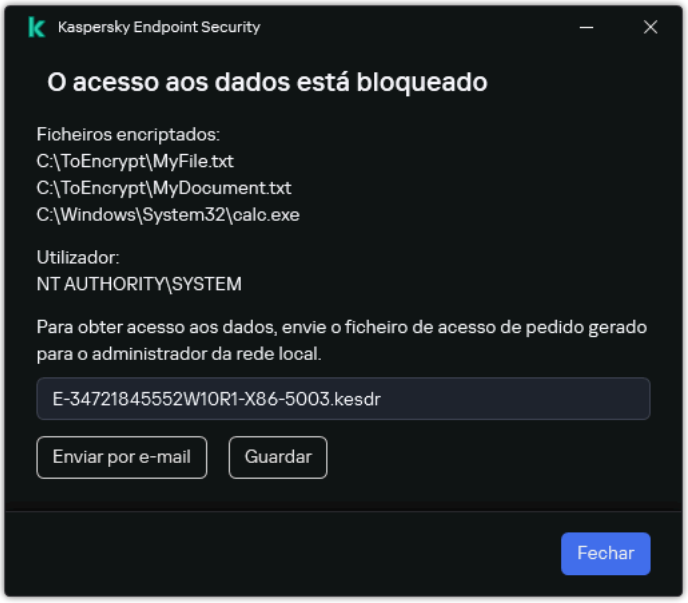
Parâmetro	Descrição
Encriptar apenas espaço de disco utilizado	Esta caixa de verificação ativa / desativa o modo de encriptação no qual apenas são encriptados os setores de disco ocupados. Este modo é recomendado para unidades novas cujos dados não tenham sido alterados ou eliminados. Se a caixa de verificação estiver selecionada, são encriptadas apenas as partes da unidade que estiverem ocupadas por ficheiros. O Kaspersky Endpoint Security encripta automaticamente dados novos quando são adicionados. Se a caixa de verificação estiver selecionada, é encriptada toda a unidade, incluindo fragmentos residuais de ficheiros anteriormente eliminados e modificados. A capacidade de encriptar apenas o espaço ocupado só está disponível para o modo **Encriptar unidade amovível completa**. Depois de a encriptação iniciar, ativar/desativar a função **Encriptar apenas espaço de disco utilizado** não alterará esta definição. Tem de selecionar ou desmarcar a caixa de verificação antes de iniciar a encriptação.

Regras personalizadas	Esta tabela contém dispositivos para os quais estão definidas regras de encriptação personalizadas. Pode criar regras de encriptação para unidades amovíveis individuais das seguintes maneiras:
	
	• Adicione uma unidade amovível da lista de dispositivos fiáveis para Controlo de Dispositivos.
	
	• Adicione manualmente uma unidade amovível:
	
	  • Por ID do dispositivo (Hardware ID ou HWID)
	
	  • Por modelo de dispositivo: Vendor ID (VID) e Product ID (PID)

Permitir encriptação de unidades amovíveis no modo offline	Se esta caixa de verificação estiver selecionada, o Kaspersky Endpoint Security encripta as unidades amovíveis mesmo quando não existe ligação ao Kaspersky Security Center. Nesse caso, os dados necessários para desencriptar as unidades amovíveis são armazenados no disco rígido do computador ao qual a unidade amovível está ligada, e não são transmitidos ao Kaspersky Security Center. Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security não encripta unidades amovíveis sem uma ligação ao Kaspersky Security Center.
Definições da password de encriptação/Gestor de ficheiros portátil	Definições da segurança da password para o Gestor de ficheiros portátil.

Modelos (encriptação de dados)

Após a encriptação 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 utilizador não tiver acesso aos dados encriptados, pode solicitar ao administrador acesso aos dados. Ou seja, o utilizador tiver de enviar um ficheiro de pedido de acesso ao administrador. O utilizador precisa de carregar então o ficheiro de resposta recebido do administrador no Kaspersky Endpoint Security. O Kaspersky Endpoint Security permite solicitar o acesso aos dados do administrador por e-mail (ver a figura abaixo).



Solicitar acesso a dados encriptados

É disponibilizado um modelo para relatar a falta de acesso a dados encriptados. Para conveniência do utilizador, pode preencher os seguintes campos:

- **Para**. Digite o endereço de e-mail do grupo de administradores com direitos sobre os recursos de encriptação de dados.
- **Assunto**. Introduza a assunto da mensagem de e-mail com o seu pedido de acesso a ficheiros encriptados. Pode, por exemplo, adicionar tags para filtrar mensagens.
- **Mensagem do utilizador**. Se necessário, altere o conteúdo da mensagem. Pode usar variáveis para obter os dados necessários (por exemplo, a variável `%USER_NAME%`).

Exclusões

Uma *zona fiável* consiste numa lista de objetos e aplicações, configurada pelo administrador do sistema, que o Kaspersky Endpoint Security não monitoriza quando está ativo.

O administrador cria a zona fiável de forma independente, tendo em consideração as características dos objetos processados e das aplicações instaladas no computador. Poderá ser necessário incluir objetos e aplicações na zona fiável quando o Kaspersky Endpoint Security bloqueia o acesso a um determinado objeto ou aplicação, caso o utilizador esteja seguro de que o objeto ou aplicação não constitui qualquer risco. Um administrador também pode permitir que um utilizador crie a sua própria zona fiável local para um computador específico. Desta forma, os utilizadores podem criar as suas próprias listas locais de exclusões e de aplicações fiáveis, além da zona fiável geral numa política.

A partir do Kaspersky Endpoint Security 12.5 for Windows, pode adicionar telemetria EDR à zona fiável. Isto permite otimizar os dados que a aplicação envia para o servidor de recolha de Telemetria para a solução do Kaspersky Anti Targeted Attack Platform (EDR).

A partir do Kaspersky Endpoint Security 12.6 para Windows, as exclusões de verificação e as aplicações fiáveis são adicionadas à zona fiável. Exclusões de verificação predefinidas e aplicações fiáveis ajudam a configurar rapidamente o Kaspersky Endpoint Security em servidores SQL, servidores Microsoft Exchange e System Center Configuration Manager. Isto significa que não é necessário configurar manualmente uma zona fiável para a aplicação nos servidores.

A partir do Kaspersky Endpoint Security 12.8 para Windows, pode instalar aplicação no modo Light Agent para proteger ambientes virtuais. As exclusões de verificação predefinidas e as aplicações fiáveis podem ajudá-lo a configurar rapidamente o Kaspersky Endpoint Security em ambientes virtuais Citrix e VMware.

Exclusões de verificação

Uma *exclusão de verificação* consiste num conjunto de condições que devem ser cumpridas para que o Kaspersky Endpoint Security não verifique a existência de vírus e outras ameaças num objeto específico. As exclusões de verificação possibilitam a utilização segura de software legítimo que pode ser explorado por criminosos para danificar o computador ou os dados do utilizador. Estas aplicações não têm necessariamente uma finalidade maliciosa, mas podem ser exploradas por hackers. Para obter informações detalhadas sobre aplicações legítimas que os intrusos podem utilizar para comprometer o computador ou os dados do utilizador, visite o site da Enciclopédia da Kaspersky.

Essas aplicações podem ser bloqueadas pelo Kaspersky Endpoint Security. Para impedir que sejam bloqueadas, pode configurar exclusões de verificação para as aplicações em utilização. Para tal, adicione o nome ou a máscara do nome indicada na Kaspersky IT Encyclopedia à zona fiável. Por exemplo, utiliza frequentemente a aplicação Radmin para a administração remota dos computadores. O Kaspersky Endpoint Security considera esta atividade como suspeita e pode bloqueá-la. Para impedir o bloqueio da aplicação, crie uma regra de exclusão de verificação com o nome ou a máscara do nome indicada na Kaspersky IT Encyclopedia.

Se uma aplicação que recolhe informação e a envia para ser processada estiver instalada no seu computador, o Kaspersky Endpoint Security pode classificar esta aplicação como software malicioso. Para evitar esta situação, pode excluir a aplicação da verificação, configurando o Kaspersky Endpoint Security como descrito neste documento.

As exclusões de verificação podem ser utilizadas pelos seguintes componentes e tarefas da aplicação, que são configurados pelo administrador do sistema:

- Deteção de comportamento.
- Prevenção de explorações.
- Prevenção contra invasões.
- Proteção contra ameaças de ficheiros.

- Proteção contra ameaças da Web.
- Proteção contra ameaças de correio.
- Tarefa de *Verificação de software malicioso*

A lista de aplicações confiáveis

A *lista de aplicações fiáveis* é uma lista de aplicações cujos ficheiros e atividade de rede (incluindo a atividade maliciosa) e o acesso ao registo do sistema não são monitorizados pelo Kaspersky Endpoint Security. Por predefinição, o Kaspersky Endpoint Security monitoriza objetos que sejam abertos, executados ou guardados por qualquer outro processo da aplicação e controla a atividade de todas as aplicações e tráfego de rede gerado pelos mesmos. Após uma aplicação ter sido adicionada à lista de aplicações fiáveis, o Kaspersky Endpoint Security para de monitorizar a atividade da aplicação.

A diferença entre exclusões de verificação e aplicações confiáveis é que, relativamente às exclusões, o Kaspersky Endpoint Security não verifica ficheiros, enquanto que em relação às aplicações confiáveis, não controla os processos iniciados. Se uma aplicação confiável criar um ficheiro malicioso numa pasta que não esteja incluída nas exclusões de verificação, o Kaspersky Endpoint Security detetará o ficheiro e eliminará a ameaça. Se a pasta for adicionada às exclusões, o Kaspersky Endpoint Security ignorará este ficheiro.

Por exemplo, se considerar como seguros objetos utilizados pela aplicação padrão Bloco de Notas do Microsoft Windows, o que significa que confia nesta aplicação, pode adicionar o Bloco de Notas do Microsoft Windows à lista de aplicações fiáveis para que os objetos utilizados por esta aplicação não sejam monitorizados. Esta ação aumentará o desempenho do computador, o que é especialmente importante quando se utiliza aplicações de servidor.

Além disso, algumas ações classificadas pelo Kaspersky Endpoint Security como suspeitas podem ser seguras no contexto da funcionalidade de um conjunto de aplicações. Por exemplo, a interceção de texto introduzido no teclado é um processo de rotina para alternadores de disposição do teclado (como o Punto Switcher). Para ter em consideração as especificidades destas aplicações e excluir a respetiva atividade da monitorização, recomendamos que adicione estas aplicações à lista de aplicações fiáveis.

As aplicações fiáveis ajudam a evitar problemas de compatibilidade entre o Kaspersky Endpoint Security e outras aplicações (por exemplo, o problema de dupla verificação do tráfego de rede de um computador de terceiros pelo Kaspersky Endpoint Security e por outra aplicação antivírus).

Simultaneamente, continua a ser efetuada a verificação da existência de vírus e outro software malicioso no ficheiro executável e no processo da aplicação fiável. Uma aplicação pode ser totalmente excluída da verificação do Kaspersky Endpoint Security com exclusões de verificação.

Parâmetro	Descrição

Tipos de objetos detetados

Independentemente das definições da aplicação configuradas, o Kaspersky Endpoint Security deteta e bloqueia sempre vírus, worms e Trojans. Estes podem causar danos significativos num computador.

- **Vírus e worms**

  Subcategoria: vírus e worms (Viruses_and_Worms)

  Nível de perigo: elevado

  Os vírus e worms clássicos executam ações não autorizadas pelo utilizador. Estes podem criar cópias de si próprios que são capazes de se auto-multiplicar.

  Vírus clássico

  Quando um vírus clássico se infiltra no computador, infeta um ficheiro, ativa-se, executa ações maliciosas e adiciona cópias de si próprio a outros ficheiros.

  Um vírus clássico multiplica-se apenas em recursos locais do computador; não conseguindo, por si só, penetrar noutros computadores. Só pode ser transmitido a outro computador se adicionar uma cópia de si próprio a um ficheiro armazenado numa pasta partilhada ou CD inserido ou se o utilizador reencaminhar uma mensagem de e-mail com um ficheiro infetado anexado.

  O código de um vírus clássico pode penetrar várias áreas dos computadores, sistemas operativos e aplicações. Dependendo do ambiente, os vírus dividem-se em *vírus de ficheiro*, *vírus de inicialização*, *vírus de script* e *vírus de macro*.

  Os vírus podem infetar ficheiros através de diversas técnicas. Os vírus *Overwriting* substituem o código do ficheiro infetado pelo seu próprio código, apagando, deste modo, o conteúdo do ficheiro. O ficheiro infetado deixa de funcionar e não pode ser restaurado. Os vírus *Parasitic* modificam ficheiros, deixando-os total ou parcialmente funcionais. Os *Companion* não modificam ficheiros, mas criam duplicados. Quando um ficheiro infetado é aberto, é iniciado um duplicado deste ficheiro (que é, na verdade, um vírus). São também detetados os seguintes tipos de vírus: o vírus *Link*, *vírus OBJ*, *vírus LIB*, *vírus em código fonte* e muitos outros.

  Worm

  Tal como um vírus clássico, o código de um worm é ativado e executa ações maliciosas após infiltrar-se num computador. O nome "worm" (verme) deve-se à sua capacidade de "rastejar" de um computador para outro e de disseminar cópias através de inúmeros canais de dados, sem a autorização do utilizador.

  A principal característica que permite diferenciar os vários tipos de worms é a forma como se disseminam. A tabela que se segue faculta uma descrição geral dos vários tipos de worms, que são classificados pela forma como se disseminam.

  Formas de disseminação de worms

Tipo	Name	Descrição
Worm de e-mail	Worm de e-mail	Disseminam-se por e-mail. Uma mensagem infetada contém um ficheiro anexado com uma cópia de um worm ou uma ligação a um ficheiro que é carregado para um site, o qual pode ter sido pirateado ou criado exclusivamente para esse fim. Quando o utilizador abre o ficheiro anexado, o worm é ativado. Quando o utilizador clica na ligação, transfere e, depois, abre o ficheiro, o worm começa também a executar as respetivas ações maliciosas. Depois disso, o worm continua a disseminar cópias de si próprio, a procurar outros endereços de e-mail e a enviar mensagens infetadas a esses endereços.
IM-Worm	Worms de cliente de MI	Estes disseminam-se através de clientes de MI. Normalmente, estes worms enviam mensagens que contêm uma ligação a um ficheiro com uma cópia do worm num site, utilizando a lista de contactos do utilizador. Quando o utilizador transfere e abre o ficheiro, o worm é ativado.
IRC-Worm	Worms de salas de conversação	Estes disseminam-se através de Internet Relay Chats (IRC), sistemas de serviços que permitem comunicar com outras pessoas, em tempo real, através da Internet. Estes worms publicam um ficheiro com uma cópia de si próprios ou uma ligação ao ficheiro numa sala de conversação na Internet. Quando o utilizador transfere e abre o ficheiro, o worm é ativado.
Net-Worm	Worms de rede	Estes worms disseminam-se através de redes de computadores. Ao contrário dos outros tipos de worms, um worm de rede típico dissemina-se sem a participação do utilizador. Este procura na rede local os computadores que contêm programas com vulnerabilidades. Para tal, envia um pacote de rede especialmente criado (exploit) que contém o código do worm ou uma parte desse código. Se existir um computador "vulnerável" na rede, este receberá o pacote de rede. O worm é ativado quando tiver penetrado completamente no computador.
P2P-Worm	Worms de rede de partilha de ficheiros	Disseminam-se em redes de partilha de ficheiros peer-to-peer. Para se infiltrar numa rede P2P, o worm copia-se a si próprio para uma pasta de partilha de ficheiros que, normalmente, está localizada no computador do utilizador. A rede P2P apresenta informação sobre este ficheiro, de forma a que o utilizador possa "encontrar" o ficheiro infetado na rede como qualquer outro ficheiro, transferi-lo e abri-lo. Os worms mais sofisticados imitam o protocolo de rede de uma rede P2P específica: devolvem respostas positivas a pedidos de pesquisa e disponibilizam cópias de si próprios para transferência.
Worm	Outros tipos de worms	Outros tipos de worms incluem: • Worms que disseminam cópias de si próprios através de recursos de rede. Utilizando as funções do sistema operativo, estes worms procuram pastas de rede disponíveis, estabelecem ligação a computadores na Internet e tentam obter acesso total às respetivas unidades de disco. Ao contrário dos tipos de worms descritos anteriormente, os outros tipos de worms não se ativam por si próprios, mas sim quando o utilizador abre um ficheiro que contém uma cópia do worm. • Os worms que não utilizam nenhum dos métodos descritos na tabela anterior para disseminar-se (por exemplo, aqueles que se disseminam por telemóveis).

- **Trojans (incluindo ransomware)**

  Subcategoria: Trojans

Nível de perigo: elevado

Ao contrário dos worms e dos vírus, os Trojans não se auto-multiplicam. Por exemplo, estes penetram num computador através do e-mail ou do navegador quando o utilizador visita uma página da Internet infetada. Os Trojans são iniciados com a participação do utilizador. Começam a efetuar as suas ações maliciosas assim que são executados.

Diferentes Trojans têm comportamentos diferentes nos computadores infetados. As principais funções dos "Trojans" incluem bloquear, modificar ou destruir informações, e desativar os computadores ou redes. Os Trojans também podem receber ou enviar ficheiros, executá-los, apresentar mensagens no ecrã, solicitar páginas da Internet, transferir e instalar programas e reiniciar o computador.

Muitas vezes, os hackers utilizam "conjuntos" de vários Trojans.

Os tipos de comportamento dos Trojan estão descritos na tabela seguinte.

Tipos de comportamento de Trojans num computador infetado

Tipo	Name	Descrição
Trojan-ArcBomb	Trojans – "arquivos bomba"	Uma vez descompactados, a dimensão destes arquivos aumenta de tal forma que o funcionamento do computador é afetado. Quando o utilizador tenta descompactar este arquivo, o computador pode começar a trabalhar de forma lenta ou bloquear e o disco pode ficar cheio de dados "vazios". Os "arquivos bomba" são especialmente perigosos para os servidores de ficheiros e de e-mails. Se o servidor utilizar um sistema automático para processar a informação recebida, um "arquivo bomba" pode parar o servidor.
Backdoor	Trojans para administração remota	São considerados o tipo de programa Trojan mais perigoso. Em termos de funções, são semelhantes às aplicações de administração remota instaladas nos computadores. Estes programas instalam-se no computador sem serem detetados pelo utilizador, permitindo ao intruso gerir remotamente o computador.
Trojan	Trojans	Estes incluem as seguintes aplicações maliciosas: • **Trojans clássicos**. Estes programas executam apenas as principais funções dos Trojans: bloquear, modificar ou destruir informações e desativar computadores ou redes. Não incluem quaisquer funções avançadas, ao contrário dos outros tipos de Trojans descritos na tabela. • **Trojans versáteis**. Estes programas têm as características avançadas típicas de vários tipos de Trojans.
Trojan-Ransom	Trojans de resgate	Estes "tomam como refém" a informação do utilizador, alterando-a ou bloqueando-a, ou perturbam o funcionamento do computador, de forma a que o utilizador não consiga utilizar a informação. O intruso exige um resgate ao utilizador, prometendo enviar uma aplicação que restaura o desempenho do computador e os dados que tinham sido armazenados na mesma.
Trojan-Clicker	Trojans de comandos	Estes acedem à página da Internet a partir do computador do utilizador, enviando comandos para um navegador ou alterando os endereços da Internet especificados nos ficheiros do sistema operativo. Ao utilizar estes programas, os intrusos efetuam ataques de rede e aumentam as visitas dos sites, aumentando o número de apresentações das faixas de publicidade (banners).
Trojan-Downloader	Trojans de transferências	Estes acedem à página da Internet do intruso, transferem outras aplicações maliciosas nessa localização e instalam-nas no computador do utilizador. Podem conter o nome do ficheiro da aplicação maliciosa a transferir ou recebê-lo a partir da página da Internet acedida.
Trojan-Dropper	Trojans instaladores	Estes contêm outros Trojans que instalam no disco rígido. Os intrusos podem utilizar programas do tipo Trojan Dropper com os objetivos seguintes: • Instalar uma aplicação maliciosa sem tal ser detetado pelo utilizador: Os programas do tipo Trojan Dropper não apresentam qualquer mensagem nem mensagens falsas, por exemplo, para notificar sobre um erro num arquivo ou sobre uma versão incompatível do sistema operativo. • Impedir que outra aplicação maliciosa conhecida seja detetada: nem todo o software antivírus consegue detetar aplicações maliciosas com uma aplicação do tipo Trojan Dropper.
Trojan-Notifier	Trojans notificadores	Estes informam um intruso de que um computador infetado está acessível, enviando-lhe informação sobre o computador: Endereço IP, número de uma porta aberta ou endereço de e-mail. Estes estabelecem ligação ao intruso por e-mail, por FTP, acedendo à página da Internet do intruso, ou de outra forma. Os programas do tipo Trojan Notifier são muitas vezes utilizados em conjuntos constituídos por vários Trojans. Estes notificam o intruso de que existem outros Trojans instalados com êxito no computador do utilizador.
Trojan-Proxy	Trojans proxies	Permitem ao intruso aceder a páginas de Internet de forma anónima, utilizando o computador do utilizador e são muitas vezes utilizados para enviar spam.
Trojan-PSW	Software de roubo de passwords	O software de roubo de passwords é um tipo de Trojan que rouba contas de utilizadores, por exemplo, dados de registo de software. Estes Trojans localizam dados confidenciais nos ficheiros do sistema e no registo e enviam-nos para o seu "atacante" por e-mail, por FTP, acedendo à página de Internet do intruso, ou de outra forma. Alguns destes programas Trojan estão categorizados em tipos separados descritos nesta tabela. Estes Trojans roubam contas bancárias (Trojan-Banker), dados de utilizadores de clientes de MI (Trojan-IM), e informações de utilizadores de jogos online (Trojan-GameThief).
Trojan-Spy	Trojans espiões	Estes espiam o utilizador, recolhendo informações sobre as ações do utilizador enquanto trabalha no computador. Estes podem intercetar os dados inseridos pelo utilizador através do teclado, tiram fotografias do ecrã ou recolhem listas de aplicações ativas. Depois de receberem esta informação, transferem-na para o intruso por e-mail, por FTP, acedendo à página de Internet do intruso, ou de outra forma.
Trojan-DDoS	Trojans de ataques de rede	Estes enviam numerosos pedidos a partir do computador do utilizador para um servidor remoto. O servidor não terá recursos suficientes para processar todos os pedidos, de tal forma que irá parar de funcionar (Recusa de Serviço ou simplesmente DoS). Muitas vezes, os hackers infetam vários computadores com estes programas para utilizarem os computadores para atacar em simultâneo um único servidor. Os programas DoS efetuam um ataque a partir de um único computador com o conhecimento do utilizador. Os programas DDoS (DoS Distribuído) efetuam ataques distribuídos a partir de diversos computadores, sem serem detetados pelo utilizador do computador infetado.
Trojan-IM	Trojans que roubam informações dos utilizadores de clientes de MI	Roubam números de contas e passwords de utilizadores de clientes de MI. Estes transferem informação para o intruso por e-mail, por FTP, acedendo à página de Internet do intruso, ou de outra forma.
Rootkit	Processos ocultos (Rootkits)	Estes ocultam outras aplicações maliciosas e as suas atividades e, assim, prolongam a existência dessas aplicações no sistema operativo. Também podem ocultar ficheiros, processos na memória de um computador infetado ou chaves de registo que executam aplicações maliciosas. Os rootkits podem ocultar o intercâmbio de dados entre aplicações no computador do utilizador e outros computadores da rede.

Trojan-SMS	Trojans sob a forma de mensagens SMS	Estes infetam os telemóveis e enviam mensagens SMS para números de valor acrescentado.
Trojan-GameThief	Trojans que roubam informações de utilizadores de jogos online	Estes roubam credenciais dos utilizadores de jogos online e, em seguida, enviam os dados para o intruso por e-mail, por FTP, acedendo à página de Internet do intruso, ou de outra forma.
Trojan-Banker	Trojans que roubam contas bancárias	Estes roubam dados de contas bancárias ou dados de sistemas de dinheiro eletrónico e enviam os dados para o intruso por e-mail, por FTP, acedendo à página de Internet do intruso, ou de outra forma.
Trojan-Mailfinder	Trojans que recolhem endereços de e-mail	Estes recolhem endereços de e-mail guardados num computador e transferem-nos para o intruso por e-mail, por FTP, acedendo à página de Internet do intruso, ou de outra forma. Os intrusos podem enviar spam para os endereços que recolheram.

- **Ferramentas maliciosas**

  Subcategoria: Ferramentas maliciosas

  Nível de perigo: médio

  Ao contrário de outros tipos de software malicioso, as ferramentas maliciosas não executam as suas ações assim que são iniciadas. Estas podem ser armazenadas e executadas em segurança no computador do utilizador. Os intrusos muitas vezes utilizam as funções destes programas para criarem vírus, worms e Trojans, organizarem ataques de rede em servidores remotos, para penetrarem em computadores ou efetuarem outras ações maliciosas.

  As diversas funções das ferramentas maliciosas estão agrupadas por tipo na tabela que se segue.

  Funções das ferramentas maliciosas

Tipo	Name	Descrição
Constructor	Construtores	Permitem criar novos vírus, worms e Trojans. Alguns construtores apresentam uma interface padrão baseada em janelas, na qual o utilizador pode selecionar o tipo de aplicação maliciosa a criar, o método para contornar os depuradores e outras características.
Dos	Ataques de rede	Estes enviam numerosos pedidos a partir do computador do utilizador para um servidor remoto. O servidor não terá recursos suficientes para processar todos os pedidos, de tal forma que irá parar de funcionar (Recusa de Serviço ou simplesmente DoS).
Exploit	Explorações de vulnerabilidades	A *exploração de vulnerabilidades (exploit)* é um conjunto de dados ou um código de programa, que utiliza as vulnerabilidades da aplicação, na qual é processado, para executar uma ação maliciosa num computador. Por exemplo, a exploração de vulnerabilidades pode escrever ou ler ficheiros ou solicitar páginas de Internet "infetadas". Os diferentes tipos de exploração utilizam as vulnerabilidades em diferentes aplicações ou serviços de rede. Disfarçado de um pacote de rede, a exploração é transferida através da rede para múltiplos computadores, procurando computadores com serviços de rede vulneráveis. Uma exploração de num ficheiro DOC utiliza as vulnerabilidades de um editor de texto. Quando o utilizador abre o ficheiro infetado, essa exploração de vulnerabilidades pode começar a executar ações pré-programadas por um hacker. Uma exploração de vulnerabilidades incorporada numa mensagem de e-mail procura vulnerabilidades em qualquer cliente de e-mail. Esta pode começar a executar uma ação maliciosa, assim que o utilizador abrir a mensagem infetada neste cliente de e-mail. Os worms de rede (Net-Worms) disseminam-se nas redes através da exploração de vulnerabilidades. O exploit Nuker é constituído por pacotes de rede que desativam os computadores.
FileCryptor	Encriptadores	Estes encriptam outras aplicações maliciosas, para os ocultarem das aplicações antivírus.
Flooder	Programas para "contaminar" redes	Estes enviam um elevado número de mensagens através de canais de rede. Este tipo de ferramentas inclui, por exemplo, programas que contaminam canais de salas de conversação (IRC). As ferramentas do tipo Flooder não incluem programas que "contaminam" os canais utilizados por clientes de e-mail, clientes de MI e sistemas de comunicação móvel. Estes programas são distinguidos como tipos separados, estando descritos na tabela (Email-Flooder, MI-Flooder e SMS-Flooder).
HackTool	Ferramentas de Hackers	Estes exploits permitem penetrar no computador onde estão instalados ou atacar outro computador (por exemplo, adicionando novas contas de sistema sem a autorização do utilizador, apagando os registos do sistema para ocultar quaisquer vestígios da sua presença no sistema operativo). Este tipo de ferramentas inclui alguns programas farejadores (sniffers), que possuem funções maliciosas, tais como a interceção de passwords. Os programas farejadores são programas que permitem visualizar o tráfego de rede.
Hoax	Programas de engodo (Hoaxes)	Estes surpreendem os utilizadores com mensagens semelhantes a vírus: podem "detetar um vírus" num ficheiro não infetado ou notificar o utilizador de que o disco foi formatado, embora, tal não tenha sucedido de facto.
Spoofer	Ferramentas de falsificação	Estas enviam mensagens e pedidos de rede com um endereço falso de um remetente. Os intrusos utilizam ferramentas de falsificação para se fazerem passar por remetentes legítimos, por exemplo.
VirTool	Ferramentas que modificam aplicações maliciosas	Estas permitem modificar outros programas de software malicioso, ocultando os mesmos das aplicações antivírus.
Email-Flooder	Programas que "contaminam" endereços de e-mail	Estes enviam numerosas mensagens para diversos endereços de e-mail, "contaminando-os". O elevado volume de mensagens recebidas impede que os utilizadores vejam as mensagens úteis nas suas caixas de correio.
IM-Flooder	Programas que "contaminam" o tráfego de clientes de MI	Enviam grandes quantidades de mensagens aos utilizadores de clientes de MI. O elevado volume de mensagens impede que os utilizadores vejam as mensagens úteis recebidas.
SMS-Flooder	Programas que "contaminam" o tráfego com mensagens SMS	Estes enviam numerosos SMS para telemóveis.

- **Adware**

  Subcategoria: software de publicidade (Adware)

Nível de perigo: médio

O adware apresenta informações de publicidade ao utilizador. Os programas de Adware apresentam faixas de publicidade (banners) nas interfaces de outros programas, redirecionando os pedidos de pesquisa para páginas da Internet com publicidade. Alguns destes programas recolhem e enviam ao seu criador informações de marketing sobre o utilizador: esta informação pode incluir os nomes dos sites visitados pelo utilizador ou o conteúdo dos pedidos de pesquisa do utilizador. Ao contrário dos programas Trojan espiões, os programas de Adware enviam esta informação ao programador com a permissão do utilizador.

- **Auto-dialers**

Subcategoria: software legal que pode ser utilizado por intrusos para danificar o computador ou os dados pessoais do utilizador.

Nível de perigo: médio

A maioria destas aplicações é útil, por isso muitos utilizadores executam-nas. Estas aplicações incluem clientes de IRC, auto-dialers, programas de transferências de ficheiros, monitores da atividade do sistema do computador, ferramentas de gestão de passwords, servidores de internet dos serviços FTP, HTTP, e Telnet.

Contudo, se os intrusos obtiverem acesso a estes programas ou se os implantarem no computador do utilizador, algumas das suas funcionalidades podem ser utilizadas para violação da segurança.

Estas aplicações diferem em termos de funções; os respectivos tipos são descritos na tabela seguinte.

Tipo	Name	Descrição
Client-IRC	Clientes de conversação na Internet	Os utilizadores instalam estes programas para comunicarem com pessoas através de salas de conversação. Os intrusos utilizam-nos para espalharem software malicioso.
Downloader	Programas para transferências	Estes conseguem transferir ficheiros a partir de páginas de Internet, de forma oculta.
Monitor	Programas para monitorização	Estes permitem monitorizar as atividades no computador onde estão instalados (verificando quais as aplicações que estão ativas e como estas trocam dados com aplicações instaladas noutros computadores).
PSWTool	Programas de restauro de passwords	Estes permitem visualizar e restaurar as passwords esquecidas. Os intrusos implantam estes programas, de forma secreta, nos computadores dos utilizadores, com esse mesmo propósito.
RemoteAdmin	Programas de administração remota	Estes programas são muito utilizados por administradores de sistema. Estes programas permitem obter acesso à interface de um computador remoto para o monitorizar e gerir. Os intrusos implantam estes programas, de forma secreta, nos computadores dos utilizadores, com esse mesmo propósito: monitorizar e gerir computadores remotos. Os programas legítimos de administração remota são diferentes dos Trojans do tipo backdoor para administração remota. Os Trojans conseguem penetrar no sistema operativo de forma independente e instalam-se no computador; os programas legais não o conseguem fazer.
Server-FTP	Servidores de FTP	Estes funcionam como servidores FTP. Os intrusos implantam-nos no computador do utilizador para abrirem o acesso remoto ao mesmo, através do protocolo FTP.
Server-Proxy	Servidores proxy	Estes funcionam como servidores de proxy. Os intrusos implantam-nos no computador do utilizador para enviarem spam em nome do utilizador.
Server-Telnet	Servidores Telnet	Estes funcionam como servidores Telnet. Os intrusos implantam-nos no computador do utilizador para abrirem o acesso remoto ao mesmo, através do protocolo Telnet.
Server-Web	Servidores da Internet	Estes funcionam como servidores de Internet. Os intrusos implantam-nos no computador do utilizador para abrirem o acesso remoto ao mesmo, através do protocolo HTTP.
RiskTool	Ferramentas para trabalhar num computador local	Estas fornecem ao utilizador opções adicionais quando trabalha no seu computador. As ferramentas permitem ao utilizador ocultar ficheiros ou janelas de aplicações ativas e terminar processos ativos.
NetTool	Ferramentas de risco	Estas fornecem ao utilizador opções adicionais quando trabalha com outros computadores na rede. Estas ferramentas permitem reiniciar esses computadores, detetar portas abertas e executar aplicações instaladas nos computadores.
Client-P2P	Programas de rede P2P	Estes permitem trabalhar em redes Peer-to-Peer. Podem ser utilizados pelos intrusos para espalhar software malicioso.
Client-SMTP	Clientes SMTP	Enviam mensagens de e-mail sem conhecimento do utilizador. Os intrusos implantam-nos no computador do utilizador para enviarem spam em nome do utilizador.
WebToolbar	Barras de ferramenta da Internet	Estes programas adicionam barras de ferramentas às interfaces de outras aplicações para utilizar motores de pesquisa.
FraudTool	Pseudo-programas	Estes programas fazem-se passar por outros programas. Por exemplo, existem programas pseudo-antivírus que apresentam mensagens sobre a deteção de software malicioso. Contudo, na verdade, não detetam nem desinfetam qualquer ameaça.

- **Software legítimo que pode ser utilizado por intrusos para danificar o seu computador ou dados pessoais**

Subcategoria: software legal que pode ser utilizado por intrusos para danificar o computador ou os dados pessoais do utilizador.

Nível de perigo: médio

A maioria destas aplicações é útil, por isso muitos utilizadores executam-nas. Estas aplicações incluem clientes de IRC, auto-dialers, programas de transferências de ficheiros, monitores da atividade do sistema do computador, ferramentas de gestão de passwords, servidores de internet dos serviços FTP, HTTP, e Telnet.

Contudo, se os intrusos obtiverem acesso a estes programas ou se os implantarem no computador do utilizador, algumas das suas funcionalidades podem ser utilizadas para violação da segurança.

Estas aplicações diferem em termos de funções; os respectivos tipos são descritos na tabela seguinte.

Tipo	Name	Descrição
Client-IRC	Clientes de conversação na Internet	Os utilizadores instalam estes programas para comunicarem com pessoas através de salas de conversação. Os intrusos utilizam-nos para espalharem software malicioso.
Downloader	Programas para transferências	Estes conseguem transferir ficheiros a partir de páginas de Internet, de forma oculta.
Monitor	Programas para monitorização	Estes permitem monitorizar as atividades no computador onde estão instalados (verificando quais as aplicações que estão ativas e como estas trocam dados com aplicações instaladas noutros computadores).
PSWTool	Programas de restauro de passwords	Estes permitem visualizar e restaurar as passwords esquecidas. Os intrusos implantam estes programas, de forma secreta, nos computadores dos utilizadores, com esse mesmo propósito.
RemoteAdmin	Programas de administração remota	Estes programas são muito utilizados por administradores de sistema. Estes programas permitem obter acesso à interface de um computador remoto para o monitorizar e gerir. Os intrusos implantam estes programas, de forma secreta, nos computadores dos utilizadores, com esse mesmo propósito: monitorizar e gerir computadores remotos. Os programas legítimos de administração remota são diferentes dos Trojans do tipo backdoor para administração remota. Os Trojans conseguem penetrar no sistema operativo de forma independente e instalam-se no computador; os programas legais não o conseguem fazer.
Server-FTP	Servidores de FTP	Estes funcionam como servidores FTP. Os intrusos implantam-nos no computador do utilizador para abrirem o acesso remoto ao mesmo, através do protocolo FTP.
Server-Proxy	Servidores proxy	Estes funcionam como servidores de proxy. Os intrusos implantam-nos no computador do utilizador para enviarem spam em nome do utilizador.
Server-Telnet	Servidores Telnet	Estes funcionam como servidores Telnet. Os intrusos implantam-nos no computador do utilizador para abrirem o acesso remoto ao mesmo, através do protocolo Telnet.
Server-Web	Servidores da Internet	Estes funcionam como servidores de Internet. Os intrusos implantam-nos no computador do utilizador para abrirem o acesso remoto ao mesmo, através do protocolo HTTP.
RiskTool	Ferramentas para trabalhar num computador local	Estas fornecem ao utilizador opções adicionais quando trabalha no seu computador. As ferramentas permitem ao utilizador ocultar ficheiros ou janelas de aplicações ativas e terminar processos ativos.
NetTool	Ferramentas de risco	Estas fornecem ao utilizador opções adicionais quando trabalha com outros computadores na rede. Estas ferramentas permitem reiniciar esses computadores, detetar portas abertas e executar aplicações instaladas nos computadores.
Client-P2P	Programas de rede P2P	Estes permitem trabalhar em redes Peer-to-Peer. Podem ser utilizados pelos intrusos para espalhar software malicioso.
Client-SMTP	Clientes SMTP	Enviam mensagens de e-mail sem conhecimento do utilizador. Os intrusos implantam-nos no computador do utilizador para enviarem spam em nome do utilizador.
WebToolbar	Barras de ferramenta da Internet	Estes programas adicionam barras de ferramentas às interfaces de outras aplicações para utilizar motores de pesquisa.
FraudTool	Pseudo-programas	Estes programas fazem-se passar por outros programas. Por exemplo, existem programas pseudo-antivírus que apresentam mensagens sobre a deteção de software malicioso. Contudo, na verdade, não detetam nem desinfetam qualquer ameaça.

- **Objetos comprimidos, cuja compactação pode ser utilizada para proteger um código malicioso**

  Subcategoria: ficheiros comprimidos que podem causar danos.

  Nível de perigo: médio.

  O ficheiro é comprimido utilizando um programa de compressão especial que é utilizado para comprimir software malicioso: vírus, worms, Trojans. O Kaspersky Endpoint Security verifica o módulo de descompressão com arquivos SFX (extração automática).

  Para esconder o software malicioso da deteção por um anti-vírus, os hackers comprimem-no utilizando programas de compressão especiais. Os especialistas da Kaspersky identificaram os programas de compressão mais populares entre os hackers.

- **Objetos multicomprimidos**

  Subcategoria: ficheiros comprimidos que podem causar danos.

  Nível de perigo: médio.

  O ficheiro é comprimido utilizando um programa de compressão especial que é utilizado para comprimir software malicioso: vírus, worms, Trojans. O Kaspersky Endpoint Security verifica o módulo de descompressão com arquivos SFX (extração automática).

  Para esconder o software malicioso da deteção por um anti-vírus, os hackers comprimem-no utilizando programas de compressão especiais. Os especialistas da Kaspersky identificaram os programas de compressão mais populares entre os hackers.

Exclusões

Esta tabela contém informações sobre as exclusões de verificação.

Recomendamos especificar caminhos relativos, em vez de caminhos absolutos. Isto permite excluir não apenas objetos do sistema de ficheiros, mas também objetos sem ficheiros. Por exemplo, `*\Program Files (x86)\Folder\Subfolder`.

	Pode excluir objetos de verificações utilizando os seguintes métodos:
	• Especifique o caminho para o ficheiro ou pasta.
	• Introduza o hash do objeto.
	• Usar máscaras:
	  • O carácter `*` (asterisco), o qual ocupa o lugar de qualquer conjunto de caracteres, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\*\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas na unidade C:, mas não nas subpastas.
	  • Dois caracteres `*` consecutivos ocupam o lugar de qualquer conjunto de caracteres (incluindo um conjunto vazio) no ficheiro ou nome de pasta, incluindo os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\**\*.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da `Folder`, exceto a própria `Folder`. A máscara deve incluir pelo menos um nível de aninhamento. A máscara `C:\**\*.txt` não é uma máscara válida.
	  • O carácter `?` (ponto de interrogação), o qual ocupa o lugar de qualquer carácter individual, exceto os caracteres `\` e `/` (delimitadores dos nomes de ficheiros e pastas nos caminhos dos ficheiros e pastas). Por exemplo, a máscara `C:\Folder\???.txt` incluirá caminhos para todos os arquivos que residem na pasta chamada `Folder` que tem a extensão TXT e um nome que consiste em três carateres.
	  Pode usar máscaras em qualquer lugar no caminho de um ficheiro ou pasta. Por exemplo, se quiser que o âmbito de verificação inclua a pasta Downloads para todas as contas de utilizador no computador, introduza a máscara `C:\Users\*\Downloads\`.
	  O Kaspersky Endpoint Security suporta variáveis de ambiente
	  > O Kaspersky Endpoint Security não suporta a variável do ambiente `%userprofile%` ao gerar uma lista de aplicações fiáveis na consola do Kaspersky Security Center. Para aplicar a entrada a todas as contas de utilizador, pode utilizar o caractere * (por exemplo, `C:\Users\*\Documents\File.exe`). Sempre que adiciona uma nova variável de ambiente, tem de reiniciar a aplicação.
	• Introduza o nome do tipo de objeto de acordo com a classificação da Enciclopédia Kaspersky (por exemplo, `Email-Worm`, `Rootkit` ou `RemoteAdmin`). Pode usar máscaras com o caráter `?` (substitui qualquer caráter único) e o caráter `*` (substitui qualquer número de caracteres). Por exemplo, se a máscara do `Client*` for especificada, a aplicação 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 de utilizador da aplicação se a configuração de exclusões de verificação for bloqueada pelo administrador na consola (símbolo de "cadeado fechado") e se as exclusões de verificação locais forem proibidas (a caixa de verificação **Permitir a utilização de exclusões locais** está desmarcada).

Aplicações fiáveis	Esta tabela indica as aplicações fiáveis cuja atividade não é monitorizada pelo Kaspersky Endpoint Security durante o seu funcionamento. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara. > O Kaspersky Endpoint Security não suporta a variável do ambiente `%userprofile%` ao gerar uma lista de aplicações fiáveis na consola do Kaspersky Security Center. Para aplicar a entrada a todas as contas de utilizador, pode utilizar o caractere * (por exemplo, `C:\Users\*\Documents\File.exe`). Sempre que adiciona uma nova variável de ambiente, tem de reiniciar a aplicação. O componente Controlo das Aplicações regula o arranque de cada uma das aplicações, independentemente de a aplicação estar incluída na tabela de aplicações fiáveis. > O Kaspersky Endpoint Security oculta a lista consolidada de aplicações fiáveis na interface de utilizador da aplicação se a configuração de aplicações fiáveis for bloqueada pelo administrador na consola (símbolo de "cadeado fechado") e se as aplicações fiáveis locais forem proibidas (a caixa de verificação **Permitir a utilização de aplicações fiáveis locais** está desmarcada).

Unir valores ao herdar *(disponível apenas na Consola do Kaspersky Security Center)*	Esta opção une a lista de exclusões de verificação e aplicações fiáveis nas políticas principal e subordinadas do Kaspersky Security Center. Para unir listas, a política subordinada tem de ser configurada para herdar as definições da política principal do Kaspersky Security Center. Se a caixa de verificação estiver selecionada, os itens da lista da política principal do Kaspersky Security Center serão apresentados nas políticas subordinadas. Deste modo, pode por exemplo, criar uma lista consolidada de aplicações fiáveis em toda a organização. Os itens de lista herdados numa política subordinada não podem ser eliminados nem editados. Os itens na lista de exclusões de verificação e na lista de aplicações fiáveis que são unidos durante a herança só podem ser eliminados e editados na política principal. Pode adicionar, editar ou eliminar itens de listas nas políticas de nível mais baixo. Se os itens nas listas das políticas subordinada e principal corresponderem, esses itens serão apresentados como o mesmo item da política principal. Se a caixa de verificação não estiver selecionada, os itens das listas não serão unidos ao herdar as definições das políticas do Kaspersky Security Center. Esta funcionalidade também permite unir listas em perfis de políticas. Para unir listas, no perfil de maior prioridade, ative a herança das definições de um perfil com menos prioridade. Para obter mais informações sobre as prioridades do perfil da política, consulte a Ajuda do Kaspersky Security Center.
Permitir a utilização de exclusões locais/Permitir a utilização de aplicações fiáveis locais *(disponível apenas na Consola do Kaspersky Security Center)*	*Exclusões locais e aplicações fiáveis locais (zona fiável local)* – lista definida pelo utilizador de objetos e aplicações no Kaspersky Endpoint Security para um computador específico. O Kaspersky Endpoint Security não monitoriza objetos e aplicações da zona fiável local. Desta forma, os utilizadores podem criar as suas próprias listas locais de exclusões e de aplicações fiáveis, além da zona fiável geral numa política. Se a caixa de verificação estiver selecionada, um utilizador pode criar uma lista local de exclusões de verificação e uma lista local de aplicações fiáveis. Um administrador pode usar o Kaspersky Security Center para ver, adicionar, editar ou eliminar itens da lista nas propriedades do computador. Se a caixa de verificação estiver desmarcada, um utilizador só pode aceder às listas gerais de exclusões de verificação e aplicações fiáveis geradas na política.
Telemetria do EDR (KATA)/NDR (KATA) *(disponível apenas na Consola do Kaspersky Security Center)*	Esta tabela contém informações sobre as exclusões de telemetria EDR.
Telemetria KUMA *(disponível apenas na Consola do Kaspersky Security Center)*	Lista de eventos a serem enviadas para a Kaspersky Unified Monitoring and Analysis Platform (KUMA). O Kaspersky Endpoint Security funciona nos seguintes modos: • **Enviar todos os eventos**. Neste modo, a aplicação envia todos os eventos do registo do Windows, exceto os eventos adicionados às regras de exclusão. • **Enviar apenas eventos selecionados**. Neste modo, a aplicação envia apenas eventos adicionados nas regras de inclusão.
Arquivo de certificados do sistema fiável	Se um dos armazenamentos de certificados de sistema fiável for selecionado, o Kaspersky Endpoint Security exclui as aplicações assinadas com uma assinatura digital fiável das verificações. O Kaspersky Endpoint Security atribui automaticamente essas aplicações ao grupo **Fiáveis**. Se a opção **Não utilizar** for selecionada, o Kaspersky Endpoint Security verifica as aplicações independentemente de terem ou não uma assinatura digital. O Kaspersky Endpoint Security coloca uma aplicação num grupo fiável, dependendo do nível de perigo que essa aplicação pode representar para o computador.

Definições da aplicação

Pode configurar as seguintes definições gerais da aplicação:

- Modo operacional
- Autodefesa
- Desempenho
- Informações de depuração
- Estado do computador quando são aplicadas definições

Parâmetro	Descrição
Iniciar a aplicação no arranque do computador (recomendado)	Quando esta opção está selecionada, o Kaspersky Endpoint Security é iniciado após o carregamento do sistema operativo, para proteger o computador durante toda a sessão. Quando esta opção está desmarcada, o Kaspersky Endpoint Security não é iniciado após o carregamento do sistema operativo, mas apenas quando for manualmente iniciado pelo utilizador. A proteção do computador está desativada e os dados do utilizador podem estar expostos a ameaças.
Utilizar a tecnologia de Desinfeção Avançada (requer recursos do computador consideráveis)	Normalmente, o Kaspersky Endpoint Security elimina o malware detetado antes que o computador seja infetado. A Tecnologia de desinfeção avançada protege o computador contra malware já ativo (infeção ativa), minimizando assim o risco de perda de dados e a propagação da ameaça. Se esta tecnologia estiver ativada, o Kaspersky Endpoint Security exibirá uma notificação pop-up quando uma atividade maliciosa for detetada. Nesta notificação, o Kaspersky Endpoint Security oferece ao utilizador a opção de executar a desinfeção Avançada do computador. Após a aprovação deste procedimento pelo utilizador, o Kaspersky Endpoint Security neutraliza a ameaça e depois reinicia o computador. A tecnologia de desinfeção avançada utiliza recursos consideráveis do computador, o que poderá tornar outras aplicações mais lentas. Quando a aplicação está a detetar uma infeção ativa, algumas funcionalidades do sistema operativo podem estar indisponíveis. A disponibilidade do sistema é restabelecida quando a Desinfeção Avançada for concluída e o computador reiniciado. Se o Kaspersky Endpoint Security for instalado num computador com o Windows para servidores, o Kaspersky Endpoint Security não apresenta a notificação. Como tal, não pode selecionar uma ação para desinfetar uma ameaça ativa. Para desinfetar uma ameaça, tem de Ativar Tecnologia de Desinfeção Avançada nas definições da aplicação e ativar a desinfeção avançada imediata nas definições da *Verificação de software malicioso*. Depois, tem de iniciar uma tarefa *Verificação de software malicioso*.
Utilizar o Kaspersky Security Center como servidor de proxy para ativação *(disponível apenas na Consola do Kaspersky Security Center)*	Se esta caixa de verificação estiver selecionada, a aplicação usa o Kaspersky Security Center Administration Server como um servidor proxy para se ligar a servidores de ativação. Isto é necessário quando utiliza um código de ativação para ativar a aplicação num segmento de rede isolado sem acesso à Internet. Se estiver a ativar a aplicação com um ficheiro-chave, o acesso à Internet não é necessário.
Ativar Autodefesa	Se esta funcionalidade estiver ativada, o Kaspersky Endpoint Security impede a alteração ou a eliminação dos ficheiros da aplicação no disco rígido, nos processos da memória e nas entradas do registo do sistema.
Bloquear a gestão externa dos serviços da aplicação	Se esta funcionalidade estiver ativada, o Kaspersky Endpoint Security não permite a gestão de serviços de aplicações ao usar aplicações de terceiros (como o CMD). Quando é efetuada uma tentativa de gerir serviços de aplicações através de aplicações de terceiros, é apresentada uma notificação na barra de tarefas do Microsoft Windows, acima do ícone da aplicação (exceto se o serviço de notificação tiver sido desativado pelo utilizador). Apenas pode permitir a gestão externa de serviços de aplicação em computadores que não suportem a tecnologia AM-PPL ou em computadores que tenham a tecnologia desativada.
Adiar as tarefas agendadas quando o computador estiver ligado com bateria	Se esta caixa de seleção estiver marcada, o modo de poupança de energia será ativado quando o computador estiver a funcionar com bateria. O Kaspersky Endpoint Security adia as tarefas agendadas. O utilizador pode iniciar as tarefas de verificação e de atualização manualmente, se necessário. Quando o modo de poupança de energia está ativado e o computador está ligado com bateria, as seguintes tarefas não são executadas, mesmo que estejam agendadas: • *Verificação completa*. • *Verificação de Áreas Críticas*. • *Verificação Personalizada*. • *Verificação de integridade da aplicação*. • *Verificação IOC*. • *Atualização das bases de dados e módulos da aplicação* (apenas correções) A aplicação ignora as atualizações programadas da base de dados apenas quando o portátil está a funcionar com a bateria e o nível de carga da bateria é inferior a 30% (valor predefinido). Pode alterar o nível mínimo de carga da bateria a partir do qual a aplicação começa a ignorar as atualizações agendadas das bases de dados de antivírus, editando o registo. Em todos os outros casos, o Kaspersky Endpoint Security atualiza as bases de dados de acordo com a programação, independentemente de o portátil estar ligado à corrente ou a funcionar com a bateria, ou de a aplicação se encontrar no modo de poupança de energia.

Parâmetro	Descrição
Ceder recursos a outras aplicações	O consumo de recursos do computador pelo Kaspersky Endpoint Security durante a verificação do computador pode aumentar a carga nos subsistemas da CPU e do disco rígido. Isto pode tornar as outras aplicações mais lentas. Para otimizar o desempenho, o Kaspersky Endpoint Security possui um *modo de transferência de recursos para outras aplicações*. Neste modo, o sistema operativo pode diminuir a prioridade das linhas de execução de tarefas de verificação do Kaspersky Endpoint Security quando a carga da CPU é elevada. Isto permite redistribuir os recursos do sistema operativo para outras aplicações. Desta forma, as tarefas de verificação irão receber menos tempo de CPU. Como resultado, o Kaspersky Endpoint Security irá demorar mais tempo a verificar o computador. Por predefinição, a aplicação está configurada para ceder recursos a outras aplicações.
Limitar a utilização da CPU para verificar tarefas	Para otimizar o desempenho do Kaspersky Endpoint Security, pode limitar a utilização da CPU através da tarefa *Verificação de software malicioso*. Se a caixa de verificação estiver selecionada, a carga média em todos os núcleos da CPU da tarefa *Verificação de software malicioso* aproxima-se do valor especificado. Por padrão, a caixa de verificação está desmarcada.
Ativar gravação de descarga	Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security grava ficheiros de descargas da memória em caso de falhas da aplicação. Se a caixa de seleção estiver desmarcada, o Kaspersky Endpoint Security não grava ficheiros de descarga da memória. A aplicação também elimina os ficheiros de descarga existentes da unidade de disco rígido do computador.
Ativar proteção de ficheiros de descarga e de rastreio	Se a caixa de verificação estiver selecionada, o acesso aos ficheiros de descarga é concedido ao administrador do sistema e ao administrador local, bem como ao utilizador que tenha ativado a função de escrita em ficheiros de descarga. Apenas os administradores de sistema e locais podem aceder a ficheiros de rastreio. Se a caixa de seleção estiver desmarcada, qualquer utilizador pode aceder a ficheiros de descarga e de rastreio.
Estado do computador quando são aplicadas definições *(disponível apenas na Consola do Kaspersky Security Center)*	As definições para apresentar os estados dos computadores do cliente com o Kaspersky Endpoint Security instalado na Consola Web quando ocorrem erros ao aplicar uma política ou executar uma tarefa. Estão disponíveis os seguintes estados *OK*, *Aviso* e *Crítica*.
Instalar as atualizações sem reiniciar o computador	A atualização da aplicação sem reiniciar o computador permite-lhe assegurar o funcionamento ininterrupto dos servidores. Pode atualizar a aplicação sem reiniciar a aplicação a partir da versão 11.10.0. Para atualizar uma versão anterior da aplicação, tem de reiniciar o computador. Desde a versão 11.11.0, pode executar as seguintes ações sem reiniciar um computador: • instalar patches • alterar o conjunto de componentes da aplicação • instalar o Kaspersky Endpoint Security sobre o Kaspersky Security for Windows Server O valor predefinido do parâmetro varia em função do tipo de sistema operativo. Se a aplicação for instalada numa estação de trabalho, a atualização da aplicação sem opção de reiniciar está desativada. Se a aplicação for instalada num servidor, a atualização da aplicação sem opção de reiniciar está ativada.
Compatibilidade com software de administração remota *(disponível apenas na Consola do Kaspersky Security Center)*	Se a utilização do Kaspersky Endpoint Security em conjunto com as Ferramentas de Administração Remota (RAT) causar problemas, pode ativar o modo de compatibilidade. Os problemas podem ser causados pela incompatibilidade dos RATs com a funcionalidade Secure Desktop da aplicação. O objetivo desta funcionalidade é confirmar ações que podem diminuir potencialmente o nível de segurança do computador. Esta funcionalidade permite que uma aplicação apresente uma caixa de diálogo de confirmação isolada de outros processos. Esta funcionalidade utiliza direitos superiores para proteger o pedido. Desta forma, apenas o utilizador poderá confirmar a ação e não o malware. Se esta opção estiver selecionada, o modo de compatibilidade de RAT está ativado. A aplicação apresenta uma caixa de diálogo de confirmação sem esta funcionalidade. Isto não afeta o nível de segurança do computador. Não recomendamos ativar o modo de compatibilidade se o Kaspersky Endpoint Security não causar problemas com o seu RAT. Se esta opção estiver desmarcada, o modo de compatibilidade de RAT estará desativado. Por padrão, a caixa de verificação está desmarcada. Exemplo: ao usar o navegador no modo RemoteApp, o Kaspersky Endpoint Security pode não apresentar uma janela de confirmação quando visita um Web site com um certificado não fiável porque o RemoteApp não suporta a funcionalidade de Secure Desktop da aplicação. Isto pode provocar o bloqueio do navegador. Para que o navegador funcione corretamente no modo RemoteApp, deve ativar o modo de compatibilidade. Pode também experimentar ativar o modo de compatibilidade se encontrar problemas com a funcionalidade Secure Desktop ao usar outro software de terceiros.

Relatórios e armazenamento

Relatórios

As informações sobre o funcionamento de cada componente do Kaspersky Endpoint Security, eventos de encriptação de dados, o desempenho de cada tarefa de verificação, tarefa de atualização e tarefa de verificação de integridade, bem como sobre o funcionamento geral da aplicação, são registadas nos relatórios.

Os relatórios são armazenados na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\Report`.

Cópia de segurança

A *cópia de segurança* armazena cópias de segurança de ficheiros que foram eliminados ou modificados durante a desinfeção. A *cópia de segurança* é a cópia de um ficheiro criada antes de o ficheiro ser desinfetado ou eliminado. As cópias de segurança dos ficheiros são armazenadas num formato especial e não constituem uma ameaça.

As cópias de segurança de ficheiros são armazenadas na pasta `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

Os utilizadores pertencentes aos grupos de administradores obtêm permissões completas de acesso a esta pasta. O utilizador cuja conta foi utilizada para instalar o Kaspersky Endpoint Security recebe direitos de acesso limitado para esta pasta.

O Kaspersky Endpoint Security não disponibiliza a capacidade de configurar as permissões de acesso do utilizador para a realização de cópias de segurança de ficheiros.

Quarentena

Quarentena é um armazenamento local especial no computador. O utilizador pode colocar em quarentena ficheiros que considere perigosos para o computador. Os ficheiros na quarentena são armazenados num estado encriptado e não põem em risco a segurança do dispositivo. O Kaspersky Endpoint Security utiliza a Quarentena apenas quando integrado com as soluções Kaspersky Detection and Response. Em todos os outros casos, o Kaspersky Endpoint Security coloca o ficheiro pertinentes na Cópia de Segurança. Para obter mais informações sobre a gestão da Quarentena como parte das soluções, consulte Ajuda do Kaspersky Sandbox, Ajuda do Kaspersky Endpoint Detection and Response Optimum e Ajuda do Kaspersky Endpoint Detection and Response Expert, Ajuda do Kaspersky Anti Targeted Attack Platform e Ajuda do Kaspersky Endpoint Detection and Response Expert (on-premises).

A quarentena só pode ser configurada através da Consola Web. Também pode utilizar a Consola Web para gerir objetos na quarentena (restaurar, eliminar, adicionar, etc). Pode restaurar objetos localmente no computador utilizando a Command line.

O Kaspersky Endpoint Security utiliza a conta de sistema (SYSTEM) para colocar os ficheiros na quarentena.

Definições de relatórios e armazenamento

Parâmetro	Descrição
Delete reports after (days)	Se a caixa de verificação estiver selecionada, o prazo máximo de armazenamento do relatório será limitado ao intervalo de tempo definido. O prazo máximo predefinido do armazenamento para relatórios é de 30 dias. Após esse período, o Kaspersky Endpoint Security apaga automaticamente as entradas mais antigas do ficheiro de relatório.
Limit the size of report file to (MB)	Se a caixa de verificação estiver selecionada, o tamanho do ficheiro do relatório será limitado ao valor definido. Por predefinição, o tamanho máximo do ficheiro é de 1024 MB. Para evitar exceder o tamanho máximo do ficheiro de relatórios o Kaspersky Endpoint Security apaga automaticamente as entradas mais antigas do ficheiro de relatórios quando o tamanho máximo do ficheiro de relatório é atingido.
Delete objects after (days)	Se a caixa de verificação estiver selecionada, o prazo máximo de armazenamento do ficheiro será limitado ao intervalo de tempo definido. O prazo máximo predefinido do armazenamento para ficheiros é de 30 dias. Após expirar o prazo máximo de armazenamento, o Kaspersky Endpoint Security elimina os ficheiros mais antigos da Cópia de segurança.
Limit the size of Backup to (MB)	Se a caixa de verificação estiver selecionada, o tamanho máximo de armazenamento será limitado ao valor definido. Por predefinição, o tamanho máximo é de 1024 MB. Para evitar exceder o tamanho máximo de armazenamento, o Kaspersky Endpoint Security elimina automaticamente os ficheiros mais antigos do ficheiro do armazenamento quando o tamanho máximo de armazenamento é atingido.
Limit the size of Quarantine	Se a caixa de verificação estiver selecionada, o tamanho máximo da Quarentena será limitado ao valor definido. Por predefinição, o tamanho máximo é de 1024 MB. Quando a Quarentena atinge o tamanho máximo, o Kaspersky Endpoint Security envia o evento *Espaço insuficiente no armazenamento da Quarentena* para o Kaspersky Security Center e publica-o no Registo de Eventos do Windows. Entretanto, a aplicação deixa de colocar novos objetos na quarentena. Tem de esvaziar manualmente a Quarentena.
Notify when the Quarantine storage reaches (%)	Valor limite da Quarentena. Por exemplo, pode definir o limite da quarentena para 50 %. Quando a Quarentena atinge o valor limite, o Kaspersky Endpoint Security envia o evento correspondente ao Kaspersky Security Center e publica-o no Registo de Eventos do Windows. Entretanto, a aplicação continua a colocar novos objetos na quarentena.
Transferência de dados para o Servidor de administração *(disponível apenas no Kaspersky Security Center)*	As categorias de eventos nos computadores do cliente cuja informação deve ser enviada para o Servidor de administração. Pode desativar a transferência de alguns dados para otimizar o espaço em disco no Servidor de Administração. A aplicação envia eventos das seguintes categorias: • **About Quarantine files**. Pode ver a lista de ficheiros em quarentena na consola do Kaspersky Security Center, na pasta **Advanced** → **Repositories** → **Quarantine**. O Kaspersky Endpoint Security utiliza a Quarentena apenas quando integrado com as soluções Kaspersky Detection and Response. • **About files in Backup**. Pode ver a lista de ficheiros na Cópia de segurança na consola do Kaspersky Security Center, na pasta **Advanced** → **Repositories** → **Backup**. • **About unprocessed files**. Pode ver a lista de ficheiros não processados na consola do Kaspersky Security Center, na pasta **Advanced** → **Repositories** → **Active threats**. • **About installed devices**. Pode ver a lista de dispositivos ligados no consola do Kaspersky Security Center na pasta **Advanced** → **Repositories** → **Hardware**. A lista de dispositivos também está disponível nas propriedades do computador e na política do Kaspersky Endpoint Security for Windows (secção **Controlo de Dispositivos**). • **About started applications**. Pode ver a lista de ficheiros executáveis na consola do Kaspersky Security Center, na pasta **Advanced** → **Application management** → **Executable files**. A lista de ficheiros executáveis também está disponível nas propriedades do computador. • **About file encryption errors**. Pode ver a lista erros de encriptação de ficheiros na consola do Kaspersky Security Center, na pasta **Advanced** → **Data encryption and protection** → **Encryption events**. A lista de erros também está disponível nas propriedades do computador. • **Report on Adaptive Anomaly Control rules state**. Pode ver o relatório na consola do Kaspersky Security Center no nó **Administration Server** no separador **Reports**. Este relatório também está disponível nas propriedades de política do Kaspersky Endpoint Security for Windows (secção **Controlo de Anomalias Adaptativo**). • **Report on triggered Adaptive Anomaly Control rules**. Pode ver o relatório na consola do Kaspersky Security Center no nó **Administration Server** no separador **Reports**. Este relatório também está disponível nas propriedades de política do Kaspersky Endpoint Security for Windows (secção **Controlo de Anomalias Adaptativo**). • **About a threat development chain**. Pode ver os detalhes da deteção na Consola Web do Kaspersky Security Center na secção **Monitoring** → **Alerts**. As informações sobre a cadeia de desenvolvimento de ameaças são utilizadas pelas soluções Kaspersky Endpoint Detection and Response.

Definições de Rede

Pode configurar o servidor proxy utilizado para estabelecer uma ligação à Internet e atualizar as bases de dados antivírus, selecionar o modo de monitorização da porta de rede e configurar verificações de ligações encriptadas.

Opções de rede

Parâmetro	Descrição
Limitar tráfego em ligações controladas	Se esta caixa de seleção estiver selecionada, a aplicação limita o próprio tráfego de rede quando a ligação à Internet tem limites. O Kaspersky Endpoint Security identifica uma ligação à Internet móvel de alta velocidade como uma ligação limitada e identifica uma ligação de Wi-Fi como uma ligação ilimitada. O Rede com Controlo de Custos funciona em computadores com o Windows 8 ou posterior.
Injetar script no tráfego de Internet para interagir com páginas de Internet	Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security injeta um script de interação de página de Internet no tráfego de Internet. Este script garante que o componente Controlo de Internet pode funcionar corretamente. O script permite o registo de eventos do Controlo de Internet. Sem este script, não é possível ativar a monitorização da atividade do utilizador na Internet. Os especialistas da Kaspersky recomendam injetar este script de interação de página da Internet no tráfego para garantir a operação correta do Controlo de Internet.
Definições do servidor de proxy	As definições do servidor de proxy utilizadas no acesso à internet de utilizadores dos computadores do cliente. O Kaspersky Endpoint Security utiliza estas definições para determinados componentes de proteção, incluindo a atualização de bases de dados e módulos da aplicação. Para a configuração automática de um servidor de proxy, o Kaspersky Endpoint Security utiliza o protocolo WPAD (Protocolo de Auto-descoberta de Proxy de Web). Se não for possível determinar o endereço IP do servidor de proxy através da utilização deste protocolo, a aplicação utiliza o endereço do servidor de proxy especificado nas definições do navegador Microsoft Internet Explorer.
Ignorar um servidor de proxy nos endereços locais	Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security não utiliza um servidor de proxy ao executar uma atualização a partir de uma pasta partilhada.
Definições de autenticação do servidor de proxy	Para autenticar a aplicação no servidor proxy para acesso à Internet, tem de introduzir as credenciais do utilizador. O Kaspersky Endpoint Security suporta autenticação automática no servidor proxy. Se a autenticação automática falhar, a aplicação pede-lhe que introduza as credenciais. **Não utilizar autenticação**. **Autenticação NTLM**. Autenticação NTLM com a conta de utilizador atual (predefinição). **Autenticação NTLM com nome de utilizador e password**. Autenticação NTLM com credenciais especificadas manualmente. **Nome de utilizador e password**. Autenticação com credenciais especificadas manualmente. **Autenticação automática**. **Autenticação Kerberos**. Autenticação Kerberos com a conta de utilizador atual. Para garantir que a autenticação Kerberos funciona corretamente quando se utilizam registos CNAME para o endereço do servidor proxy, tem de registar um Nome Principal de Serviço (SPN) para cada registo CNAME. **Autenticação Kerberos com nome de utilizador e password**. Autenticação Kerberos com credenciais especificadas manualmente. Se for selecionada a autenticação Kerberos, o Kaspersky Endpoint Security poderá, dependendo das definições do servidor proxy, efetuar a autenticação utilizando o protocolo Kerberos ou NTLM.

Parâmetro	Descrição
Portas monitorizadas	**Monitorizar todas as portas de rede**. Neste modo de monitorização de portas de rede, os componentes de proteção (Proteção contra ameaças de ficheiros, Proteção contra ameaças da Web e Proteção contra ameaças de correio) monitorizam fluxos de dados transmitidos através de qualquer porta de rede aberta no computador. **Monitorizar apenas as portas selecionadas**. Neste modo de monitorização de portas de rede, os componentes de proteção monitorizam as portas selecionadas do computador e a atividade de rede das aplicações selecionadas. A lista de portas de rede que são, normalmente, utilizadas para a transmissão de tráfego de e-mail e de rede é configurada de acordo com as recomendações dos peritos da Kaspersky. **Monitorizar todas as portas para as aplicações da lista recomendada pela Kaspersky**. Esta ação utiliza uma lista predefinida de aplicações cujas portas de rede são monitorizadas pelo Kaspersky Endpoint Security. Esta lista inclui, por exemplo, Google Chrome, Adobe Reader, Java e outras aplicações. **Monitorizar todas as portas das aplicações especificadas**. Esta ação utiliza uma lista de aplicações cujas portas de rede são monitorizadas pelo Kaspersky Endpoint Security.
Verificação de ligações encriptadas	O Kaspersky Endpoint Security verifica o tráfego de rede encriptada transmitido através dos seguintes protocolos: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. O Kaspersky Endpoint Security suporta os seguintes modos de verificação de ligação encriptada: • **Não verificar ligações encriptadas**. O Kaspersky Endpoint Security não terá acesso aos conteúdos de sites cujos endereços começam por `https://`. • **Verificar ligações encriptadas a pedido dos componentes de proteção**. O Kaspersky Endpoint Security só procederá à verificação de tráfego encriptado quando tal for solicitado pelos componentes Proteção Contra Ameaças da Web, Proteção Contra Ameaças de Correio e Controlo de Internet. • **Verificar sempre ligações encriptadas**. O Kaspersky Endpoint Security procederá à verificação do tráfego de rede encriptada ainda que os componentes de proteção estejam desativados. O Kaspersky Endpoint Security não verifica ligações encriptadas estabelecidas por aplicações fiáveis para as quais a verificação de tráfego está desativada. O Kaspersky Endpoint Security não verifica ligações encriptadas da lista predefinida de sites fiáveis. A lista predefinida de sites fiáveis é criada por especialistas da Kaspersky. Esta lista é atualizada com as bases de dados de antivírus da aplicação. Só pode ver a lista predefinida de sites fiáveis na interface do Kaspersky Endpoint Security. Não pode ver a lista na Consola do Kaspersky Security Center.
Certificados de raiz fiável	Lista de certificados de raiz fiável. O Kaspersky Endpoint Security permite-lhe instalar certificados de raiz fiáveis em computadores de utilizadores se, por exemplo, precisar de implementar um novo centro de certificação. A aplicação permite-lhe adicionar um certificado a uma loja especial de certificados do Kaspersky Endpoint Security. Neste caso, o certificado é considerado de confiança apenas para a aplicação do Kaspersky Endpoint Security. Por outras palavras, o utilizador pode ter acesso a um site com o novo certificado no navegador. Se outra aplicação tentar obter acesso ao site, pode obter um erro de ligação devido à emissão de um certificado. Para adicionar à loja de certificados do sistema, pode utilizar as políticas de grupo do Active Directory.
Visitar um domínio com um certificado não fiável	• **Permitir**. Quando visita um domínio com um certificado não fiável, o Kaspersky Endpoint Security permite a ligação à rede. Ao abrir um domínio com um certificado não fiável com um navegador, o Kaspersky Endpoint Security apresenta uma página HTML com um aviso e o motivo porque não é recomendável visitar esse domínio. Um utilizador pode clicar na ligação da página HTML de aviso para obter acesso ao recurso da Internet solicitado. Se uma aplicação ou serviço de terceiros estabelecer uma ligação com um domínio com um certificado não fiável, o Kaspersky Endpoint Security cria o seu próprio certificado para verificar o tráfego. O novo certificado tem o estado *Não fiável*. Isto é necessário para avisar a aplicação de terceiros sobre a ligação não fiável, uma vez que a página HTML não pode ser apresentada neste caso e a ligação pode ser estabelecida no modo de segundo plano. • **Bloquear**. Quando visita um domínio com um certificado não fiável, o Kaspersky Endpoint Security bloqueia a ligação à rede. Ao visitar um domínio com um certificado não fiável com um navegador, o Kaspersky Endpoint Security apresenta uma página HTML com o motivo porque o domínio específico está bloqueado.
Visitar um domínio com um erro de verificação de ligações encriptadas	• **Bloquear**. Se ocorrer um erro de verificação das ligações encriptadas, o Kaspersky Endpoint Security bloqueia a ligação de rede. • **Permitir e adicionar domínio às exclusões**. Se ocorrer um erro de verificação de ligações encriptadas, o Kaspersky Endpoint Security adiciona o domínio que resultou no erro à lista de domínios com erros de verificação e não monitoriza o tráfego de rede encriptado quando visita este domínio. Poder ver uma lista de domínios com erros de verificação de ligações encriptadas apenas na interface local da aplicação. Para limpar o conteúdo da lista, deve selecionar **Bloquear**. O Kaspersky Endpoint Security também gera um evento para o erro de verificação de ligações encriptadas.
Bloquear ligações SSL 2.0	Se a caixa de verificação estiver selecionada, a aplicação monitoriza e bloqueia as ligações de rede estabelecidas através do protocolo SSL 2.0. Se a caixa de verificação não estiver selecionada, a aplicação não bloqueia as ligações de rede estabelecidas através do protocolo SSL 2.0. No entanto, a aplicação não monitoriza o tráfego de rede através deste protocolo.

Parâmetro	Descrição
Bloquear ligações SSL 3.0	Se a caixa de verificação estiver selecionada, a aplicação bloqueia as ligações de rede estabelecidas através do protocolo SSL 3.0. Se a caixa de verificação não estiver selecionada, a aplicação não bloqueia as ligações de rede estabelecidas através do protocolo SSL 3.0. A aplicação não monitoriza o tráfego de rede através deste protocolo. Todos os componentes da aplicação funcionam sem restrições.
Bloquear ligações TLS 1.0	Se a caixa de verificação estiver selecionada, a aplicação bloqueia as ligações de rede estabelecidas através do protocolo TLS 1.0. Se a caixa de verificação não estiver selecionada, a aplicação não bloqueia as ligações de rede estabelecidas através do protocolo TLS 1.0. A aplicação não monitoriza o tráfego de rede através deste protocolo. Todos os componentes da aplicação funcionam sem restrições.
Desencriptar uma ligação encriptada com um site que utilize certificado EV	Certificados EV (Extended Validation Certificate) confirmam a autenticidade dos sites e melhoram a segurança da ligação. Os navegadores usam um ícone de cadeado na barra de endereços para indicar que um site tem um certificado EV. Os navegadores também podem colorir total ou parcialmente a barra de endereço a verde. Se a caixa de seleção estiver selecionada, a aplicação desencripta e monitoriza as ligações encriptadas com sites que utilizem um certificado EV. Se a caixa de seleção estiver desmarcada, a aplicação não terá acesso ao conteúdo do tráfego HTTPS. Por este motivo, a aplicação monitoriza o tráfego HTTPS apenas com base no endereço do site, por exemplo, `https://bing.com`. Se estiver a abrir um site com um certificado EV pela primeira vez, a ligação encriptada será desencriptada, independentemente de a caixa de seleção estar selecionada ou não.
Configurar endereços fiáveis	Esta ação utiliza uma lista de URL para os quais o Kaspersky Endpoint Security não verifica ligações de rede. Neste caso, o Kaspersky Endpoint Security não verifica o tráfego HTTPS de endereços da Internet fiáveis quando os componentes Proteção contra ameaças da web, Proteção contra ameaças de correio e Controlo de Internet estão a fazer o seu trabalho. Pode introduzir um nome de domínio ou endereço IP. O Kaspersky Endpoint Security suporta o caractere `*` para a introdução de uma máscara no nome de domínio. O Kaspersky Endpoint Security não suporta o símbolo `*` para endereços IP. Pode selecionar um intervalo de endereços IP com uma máscara de sub-rede (por exemplo, 198.51.100.0/24). Exemplos: • `domain.com` - o registo inclui os seguintes endereços: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. O registo não inclui subdomínios (por exemplo, `subdomain.domain.com`) • `subdomain.domain.com` - o registo inclui os seguintes endereços: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. O registo não inclui o domínio `domain.com`. • `*.domain.com` - o registo inclui os seguintes endereços: `https://movies.domain.com`, `https://images.domain.com/page123`. O registo não inclui o domínio `domain.com`.
Configurar aplicações fiáveis	Lista de aplicações cuja atividade não é monitorizada pelo Kaspersky Endpoint Security durante o seu funcionamento. Pode selecionar os tipos de atividade da aplicação que o Kaspersky Endpoint Security não irá monitorizar (por exemplo, não verificar o tráfego da rede). O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.
Para verificar as ligações encriptadas em aplicações com o armazenamento de certificados do mesmo, utilize *(disponível apenas na interface do Kaspersky Endpoint Security)*	Se esta caixa de verificação estiver selecionada, a aplicação verifica o tráfego encriptado no navegador Mozilla Firefox e no cliente de e-mail Thunderbird. O acesso a alguns sites através do protocolo HTTPS pode ser bloqueado. Para verificar tráfego no navegador Mozilla Firefox e no cliente de e-mail Thunderbird, tem de ativar a Verificação de ligações encriptadas. Se a Verificação de ligações encriptadas estiver desativada, a aplicação não verifica o tráfego no navegador Mozilla Firefox e no cliente de e-mail Thunderbird. A aplicação usa o certificado raiz da Kaspersky para desencriptar e analisar o tráfego encriptado. Pode selecionar o armazenamento de certificados que irá conter o certificado raiz da Kaspersky. • **Armazenamento de certificados do Windows (recomendado)**. O certificado raiz da Kaspersky é adicionado a este armazenamento durante a instalação do Kaspersky Endpoint Security. • **Armazenamento de certificados próprio**. O Mozilla Firefox e Thunderbird utilizam os seus próprios armazenamentos de certificados. Se o armazenamento de certificados Mozilla for selecionado, precisará de adicionar manualmente o certificado raiz da Kaspersky a este armazenamento através das propriedades do navegador.

Interface

Pode configurar as definições da interface da aplicação:

Definições da interface

Parâmetro	Descrição
Interação com o utilizador *(disponível apenas na Consola do Kaspersky Security Center)*	**Apresentar interface simplificada**. Num computador do cliente, a janela principal da aplicação está inacessível e apenas o ícone na área de notificação do Windows está disponível. No menu contextual do ícone, o utilizador pode realizar um número limitado de operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security também apresenta apenas as notificações que requerem uma ação do utilizador acima do ícone da aplicação. **Apresentar interface de utilizador**. Num computador do cliente, a janela principal do Kaspersky Endpoint Security e o ícone na área de notificação do Windows estão disponíveis. No menu contextual do ícone, o utilizador pode realizar operações com o Kaspersky Endpoint Security. O Kaspersky Endpoint Security apresenta também notificações acima do ícone da aplicação. **Secção Ocultar Monitor de Atividade das Aplicações**. No computador cliente, na janela principal do Kaspersky Endpoint Security, o botão **Monitor de Atividade das Aplicações** não está disponível. O *Monitor de Atividade das Aplicações* é uma ferramenta concebida para visualizar informações sobre a atividade das aplicações no computador de um utilizador em tempo real. **Não apresentar interface do utilizador**. Num computador do cliente, não são apresentados quaisquer sinais da operação do Kaspersky Endpoint Security. O ícone na área de notificação do Windows e as notificações não estão disponíveis.
Access to local tasks	Se a caixa de verificação estiver selecionada, as tarefas locais são apresentadas na interface local do Kaspersky Endpoint Security. Se não existirem restrições de política adicionais, o utilizador pode configurar e executar tarefas. Contudo, a configuração do agendamento de execução da tarefa permanece indisponível para o utilizador. O utilizador apenas pode executar tarefas manualmente. Se esta caixa de seleção estiver desmarcada, as tarefas locais ficam ocultas na interface da aplicação. Neste modo, as tarefas locais não são executadas executam conforme planeado. As Tarefas não podem ser iniciadas ou configuradas na interface local do Kaspersky Endpoint Security ou ao trabalhar com a command line. Um utilizador pode iniciar um verificação de um ficheiro ou pasta selecionando a opção **Verificar vírus** no menu de contexto do ficheiro ou pasta. A tarefa de verificação é iniciada com os valores predefinidos para a tarefa de verificação personalizada.
View group tasks	Se a caixa de verificação estiver selecionada, as tarefas do grupo são apresentadas na interface local do Kaspersky Endpoint Security. O utilizador pode visualizar a lista de todas as tarefas na interface da aplicação. Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security apresenta uma lista de tarefas vazia.
Manage group tasks	Se a caixa de seleção estiver marcada, os utilizadores podem iniciar e parar as tarefas de grupo especificadas na consola do Kaspersky Security Center. Os utilizadores podem iniciar e parar tarefas na interface da aplicação ou na interface simplificada da aplicação. Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security inicia tarefas agendadas automaticamente ou o administrador inicia as tarefas manualmente na consola do Kaspersky Security Center.
Configurar notificações	Uma tabela com as definições de notificações sobre eventos de diferentes níveis de importância que podem ocorrer durante a operação de um componente, tarefa ou toda a aplicação. O Kaspersky Endpoint Security mostra notificações sobre estes eventos no ecrã, envia-as por email ou regista-as.
Configurar notificações por e-mail	As definições do servidor SMTP para entrega de notificações sobre eventos registados durante a operação da aplicação. Por predefinição, o Kaspersky Endpoint Security usa as definições de notificação por e-mail do Kaspersky Security Center. Para obter mais informações sobre as definições de notificação por e-mail, consulte a Ajuda do Kaspersky Security Center. Se precisar configurar notificações de e-mail individuais, pode editar as seguintes definições: • **Endereço do remetente**. Endereço de e-mail do remetente. Usar um endereço inexistente não é recomendado. • **Servidor SMTP**. Um ou mais endereços de servidores de e-mail da sua organização (por exemplo, `mail.company.com`). Pode inserir um endereço IP (IPv4 ou IPv6). Para autenticar o utilizador no servidor SMTP, introduza as credenciais do remetente nos campos correspondentes. Para testar as notificações por e-mail, pode enviar uma mensagem de teste. • **Endereço de destino**. Endereços de e-mail de destinatários para os quais a aplicação 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; alternativamente, pode seguir uma programação pré-definida.

Parâmetro	Descrição
Mostrar o estado da aplicação na área de notificações	Categorias de eventos da aplicação que provocam a alteração do ícone do Kaspersky Endpoint Security na área de notificação da barra de tarefas do Microsoft Windows (ou) e resulte numa notificação pop-up.
Notificações de estado da base de dados local de anti-software malicioso	As definições de notificações sobre bases de dados de antivírus desatualizadas utilizadas pela aplicação.
Proteção por password	Se o botão estiver ativado, o Kaspersky Endpoint Security solicita uma password ao utilizador quando este tenta realizar uma operação no âmbito da Proteção por password. O âmbito da Proteção por password inclui operações proibidas (como desativar os componentes de proteção) e as contas de utilizador nas quais é aplicado o âmbito da Proteção por password. Depois de a Proteção por password estar ativada, o Kaspersky Endpoint Security solicita a configuração de uma password para a conta KLAdmin.
Suporte de utilizador/Ligações para recursos da Internet *(disponível apenas na Consola do Kaspersky Security Center)*	Lista de ligações para recursos da Internet que contêm informações sobre o suporte técnico do Kaspersky Endpoint Security. As ligações adicionadas serão apresentadas na janela **Suporte** da interface local do Kaspersky Endpoint Security em vez das ligações padrão.
Suporte de utilizador/Descrição *(disponível apenas na Consola do Kaspersky Security Center)*	A mensagem que é apresentada na janela **Suporte** da interface local do Kaspersky Endpoint Security.

Gerir definições

Pode guardar as definições atuais do Kaspersky Endpoint Security num ficheiro e utilizá-las para configurar rapidamente a aplicação num computador diferente. Também pode utilizar um ficheiro de configuração ao implementar a aplicação através do Kaspersky Security Center com um pacote de instalação. Pode restaurar as definições predefinidas a qualquer momento.

As definições de gestão da configuração da aplicação só estão disponíveis na interface do Kaspersky Endpoint Security.

Definições de gestão de configuração da aplicação

Definições	Descrição
Importar	Extrai as definições da aplicação de um ficheiro em formato CFG e aplicar as mesmas.
Exportar	Guarda as definições da aplicação atuais num ficheiro em formato CFG.
Restaurar	Pode restaurar as definições da aplicação recomendadas pela Kaspersky a qualquer momento. Quando as definições são restauradas, o nível de segurança **Recomendado** é definido para todos os componentes de proteção.

Atualização de bases de dados e módulos de software de aplicação

A atualização das bases de dados e dos módulos da aplicação do Kaspersky Endpoint Security garante a proteção atualizada do computador. Todos os dias surgem novos vírus e outros tipos de software malicioso a nível mundial. As bases de dados do Kaspersky Endpoint Security contêm informações sobre ameaças e formas de neutralizar as mesmas. Para detetar rapidamente ameaças, recomendamos que atualize regularmente as bases de dados e os módulos da aplicação.

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.

As atualizações regulares requerem uma licença válida. Se não existir uma licença atual, só poderá executar uma atualização uma vez.

O computador tem de estar ligado à Internet para transferir com êxito o pacote de atualização dos servidores de atualização da Kaspersky. Por predefinição, as definições da ligação à Internet são automaticamente determinadas. Se estiver a utilizar um servidor de proxy, terá de configurar as definições do servidor de proxy.

As atualizações são transferidas através do protocolo HTTPS. Também podem ser transferidas através do protocolo HTTP quando for impossível transferir as atualizações através do protocolo HTTPS.

Durante uma atualização, os seguintes objetos são transferidos e instalados no computador:

- Bases de dados do Kaspersky Endpoint Security. A proteção do computador é fornecida utilizando bases de dados com assinaturas de vírus e outras ameaças e informações sobre formas de neutralizar as mesmas. Os componentes de proteção utilizam estas informações durante a pesquisa e neutralização de ficheiros infetados no computador. As bases de dados são constantemente atualizadas com registos de novas ameaças e métodos de combate às mesmas. Por isso, recomendamos que atualize regularmente as bases de dados.

  Além das bases de dados do Kaspersky Endpoint Security, também são atualizados os controladores de rede que permitem que os componentes da aplicação intercetem o tráfego de rede.

- Módulos da aplicação. Além das bases de dados do Kaspersky Endpoint Security, também pode atualizar os módulos da aplicação. A atualização dos módulos da aplicação corrige vulnerabilidades no Kaspersky Endpoint Security, adiciona novas funções ou melhora as funções existentes.

Durante uma atualização, as bases de dados e os módulos da aplicação existentes no computador são comparados com a versão atualizada disponível na origem de atualização. Se as atuais bases de dados e módulos da aplicação diferirem das respetivas versões atualizadas, só será instalada no computador a parte das atualizações em falta.

Se as bases de dados estiverem obsoletas, o pacote de atualização pode ser extenso, o que pode implicar um tráfego adicional de internet (até várias dezenas de MB).

As informações sobre o estado atual das bases de dados do Kaspersky Endpoint Security são apresentadas na janela principal da aplicação ou na descrição que vê ao passar o cursor sobre o ícone da aplicação na área de notificação.

A informação sobre os resultados de atualização que ocorrem durante o desempenho da tarefa de atualização está registada no relatório do Kaspersky Endpoint Security.

Se a aplicação estiver a funcionar no modo Light Agent, são necessárias considerações especiais para atualizar as bases de dados e os módulos da aplicação.

Definições do módulo da aplicação e de atualização da base de dados

Parâmetro	Descrição
Agendamento da atualização das bases de dados	**Automaticamente**. Neste modo, a aplicação verifica a disponibilidade de novos pacotes de atualização na origem de atualização com uma determinada frequência. A frequência de verificação da disponibilidade de pacotes de atualização aumenta durante surtos de vírus e diminui quando não existem estes surtos. Após a deteção de um novo pacote de atualização, o Kaspersky Endpoint Security transfere-o e instala atualizações no computador. **Manually**. Este modo de execução da tarefa de atualização permite iniciar manualmente a tarefa de atualização. **By schedule**. Neste modo de execução da tarefa de atualização, o Kaspersky Endpoint Security executa a tarefa de atualização em conformidade com o agendamento especificado pelo utilizador. Se este modo de execução da tarefa de atualização estiver selecionado, pode também iniciar manualmente a tarefa de atualização do Kaspersky Endpoint Security.
Run missed tasks	Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security inicia a tarefa ignorada logo que possível. A tarefa pode ser ignorada, por exemplo, se o computador estiver desligado no momento de início da tarefa agendada. Quando a aplicação tem a oportunidade de executar tarefas ignoradas, inicia as tarefas aleatoriamente num determinado intervalo de tempo para distribuir a carga no computador. Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security não executa tarefas ignoradas. Em alternativa, executa a tarefa seguinte, em conformidade com o agendamento atual.
Origens da atualização	*Uma origem de atualização* é um recurso que contém atualizações para as bases de dados e os módulos da aplicação do Kaspersky Endpoint Security. As origens de atualização incluem o servidor do Kaspersky Security Center, os servidores de atualização da Kaspersky e as pastas de rede ou locais. No caso de os servidores de atualização da Kaspersky estarem indisponíveis, o Kaspersky Endpoint Security pode utilizar domínios alternativos para atualizar as suas bases de dados e módulos de software de aplicações. Para obter informações detalhadas, consulte a Base de Conhecimento de Apoio Técnico da Kaspersky. A lista predefinida de origens de atualização inclui o Kaspersky Security Center e os servidores de atualização da Kaspersky. Pode adicionar outras origens de atualização à lista. Pode especificar como origens de atualização servidores HTTP/FTP e pastas partilhadas. O Kaspersky Endpoint Security não suporta atualizações de servidores HTTPS, exceto se forem servidores de atualização da Kaspersky. Se forem selecionados vários recursos como origens de atualização, o Kaspersky Endpoint Security tentar estabelecer ligação aos mesmos, um após o outro, começando pelo topo da lista, e executa a tarefa de atualização recolhendo o pacote de atualização na primeira origem disponível. Por predefinição, o Kaspersky Endpoint Security usa o servidor Kaspersky Security Center como a primeira origem de atualização. Isto ajuda a conservar o tráfego durante a atualização. Se uma política não for aplicada ao computador, os servidores Kaspersky serão selecionados como a primeira origem de atualização nas definições da tarefa local *Atualização das bases de dados e módulos da aplicação* porque a aplicação pode não ter acesso ao servidor do Kaspersky Security Center. Se a aplicação estiver a ser executada no modo Light Agent, é selecionada uma pasta na SVM como origem de atualização.
Executar atualizações da base de dados como	Por predefinição, a tarefa de atualização do Kaspersky Endpoint Security é iniciada com a conta de utilizador utilizada para iniciar sessão no sistema operativo. Contudo, o Kaspersky Endpoint Security pode ser atualizado a partir de uma origem de atualização a que o utilizador não pode aceder por não ter os direitos necessários (por exemplo, uma pasta partilhada que contém um pacote de atualização) ou de uma origem de atualização para a qual a autenticação do servidor de proxy não está configurada. Nas definições da aplicação, pode especificar um utilizador que tenha esses direitos e iniciar a tarefa de atualização do Kaspersky Endpoint Security com essa conta de utilizador.

Parâmetro	Descrição
Transferir atualizações dos módulos da aplicação	A transferir atualizações do módulo da aplicação com atualizações da base de dados da aplicação. Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security notifica o utilizador sobre as atualizações dos módulos da aplicação disponíveis e inclui as atualizações do módulo da aplicação no pacote de atualização quando a tarefa de atualização é executada. A forma como as atualizações de módulo da aplicação são aplicadas é determinada pelas definições seguintes: • **Instalar atualizações críticas e aprovadas**. Se esta opção estiver selecionada, quando estão disponíveis atualizações de módulo da aplicação o Kaspersky Endpoint Security instala as atualizações críticas automaticamente e todas as outras atualizações de módulo da aplicação apenas após a sua instalação ser aprovada localmente através da interface da aplicação ou no Kaspersky Security Center. • **Instalar apenas atualizações aprovadas**. Se esta opção estiver selecionada, quando estão disponíveis atualizações de módulo da aplicação o Kaspersky Endpoint Security instala as mesmas apenas após a sua instalação ser aprovada localmente através da interface da aplicação ou no Kaspersky Security Center. Esta opção está selecionada por predefinição. Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security não notifica o utilizador sobre as atualizações dos módulos da aplicação disponíveis e não inclui as atualizações dos módulos da aplicação no pacote de atualização quando a tarefa de atualização é executada. Se as atualizações de módulo da aplicação necessitarem de verificação e aceitação dos termos do Contrato de Licença do Utilizador Final, a aplicação instala as atualizações após a aceitação dos termos do Contrato de Licença do Utilizador Final. A caixa de verificação está selecionada por predefinição.
Copiar atualizações para a pasta	Se esta caixa de verificação estiver selecionada, o Kaspersky Endpoint Security copia o pacote de atualização para a pasta partilhada especificada por baixo da caixa de verificação. Após esta ação, os restantes computadores da rede local podem receber o pacote de atualização a partir desta pasta partilhada. Este procedimento reduz o tráfego de Internet, uma vez que o pacote de atualização é transferido apenas uma vez. A pasta seguinte está especificada por defeito: `C:\ProgramData\Kaspersky Lab\KES.14.2\Update distribution\`.
Servidor de proxy para atualizações *(disponível apenas na interface do Kaspersky Endpoint Security)*	Definições do servidor de proxy para acesso à Internet de utilizadores de computadores clientes para atualizar módulos de aplicações e bases de dados. Para a configuração automática de um servidor de proxy, o Kaspersky Endpoint Security utiliza o protocolo WPAD (Web Proxy Auto-Discovery Protocol). Se não for possível determinar o endereço IP do servidor de proxy através da utilização deste protocolo, o Kaspersky Endpoint Security utiliza o endereço do servidor de proxy especificado nas definições do navegador Microsoft Internet Explorer.
Ignorar um servidor de proxy nos endereços locais *(disponível apenas na interface do Kaspersky Endpoint Security)*	Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security não utiliza um servidor de proxy ao executar uma atualização a partir de uma pasta partilhada.

Anexo 2. Grupos fiáveis da aplicação

O Kaspersky Endpoint Security categoriza todas as aplicações iniciadas no computador em grupos fiáveis. As aplicações são categorizadas em grupos fiáveis consoante o nível de ameaça que as aplicações representam para o sistema operativo.

Os grupos fiáveis são os seguintes:

- **Fiáveis**. Este grupo inclui aplicações para as quais se verificam uma ou mais das seguintes condições:
  - As aplicações são assinadas digitalmente por fornecedores fiáveis.
  - As aplicações são gravadas na base de dados de aplicações fiáveis da Kaspersky Security Network.
  - O utilizador adicionou a aplicação ao grupo *Fiáveis*.

Não existem operações interditas para estas aplicações.

- **Restrições baixas**. Este grupo inclui aplicações para as quais se verificam as condições seguintes:
  - As aplicações não são assinadas digitalmente por fornecedores fiáveis.
  - As aplicações não são gravadas na base de dados de aplicações fiáveis da Kaspersky Security Network.
  - O utilizador adicionou a aplicação ao grupo *Restrições baixas*.

  Tais aplicações estão sujeitas a restrições mínimas de acesso aos recursos do sistema operativo.
- **Restrições altas**. Este grupo inclui aplicações para as quais se verificam as condições seguintes:
  - As aplicações não são assinadas digitalmente por fornecedores fiáveis.
  - As aplicações não são gravadas na base de dados de aplicações fiáveis da Kaspersky Security Network.
  - O utilizador adicionou a aplicação ao grupo *Restrições altas*.

  Tais aplicações estão sujeitas a restrições elevadas de acesso aos recursos do sistema operativo.
- **Não fiáveis**. Este grupo inclui aplicações para as quais se verificam as condições seguintes:
  - As aplicações não são assinadas digitalmente por fornecedores fiáveis.
  - As aplicações não são gravadas na base de dados de aplicações fiáveis da Kaspersky Security Network.
  - O utilizador adicionou a aplicação ao grupo *Não fiáveis*.

  Todas as operações estão bloqueadas para essas aplicações.

Anexo 3. Extensões de ficheiro para verificação rápida de unidades removíveis

com – ficheiro executável de uma aplicação não superior a 64 KB

exe — ficheiro executável ou arquivo autoextraível

sys — ficheiro de sistema do Microsoft Windows

prg — texto de programa para dBase™, Clipper ou Microsoft Visual FoxPro®ou um programa WAVmaker

bin — ficheiro binário

bat — ficheiro de lote

cmd — ficheiro de comandos para o Microsoft Windows NT (semelhante a um ficheiro bat para DOS), OS/2

dpl — biblioteca Borland Delphi comprimida

dll — biblioteca de ligações dinâmicas

scr — ecrã inicial do Microsoft Windows

cpl — módulo do painel de controlo do Microsoft Windows

ocx — Objeto Microsoft OLE (Object Linking and Embedding)

tsp — programa em execução em modo parcial

drv — controlador de dispositivos

vxd — controlador de dispositivos do Microsoft Windows

pif — ficheiro de informação de programas

lnk — ficheiro de ligação do Microsoft Windows

reg — ficheiro-chave de registo do Microsoft Windows

ini — ficheiro de configuração que contém dados de configuração para o Microsoft Windows, Windows NT e algumas aplicações

cla — classe de Java

vbs — script Visual Basic®

vbe — extensão de vídeo da BIOS

js, jse — texto fonte do JavaScript

htm — documento de hipertexto

htt — cabeçalho de hipertexto do Microsoft Windows

hta — programa de hipertexto para o Microsoft Internet Explorer®

asp — script das Páginas do Servidor Ativo

o chm — ficheiro HTML compilado

pht — ficheiro HTML com scripts PHP integrados

php — script que está integrado em ficheiros HTML

wsh — ficheiro de script anfitrião do Microsoft Windows

wsf — script do Microsoft Windows

the - ficheiro de fundo de ecrã do ambiente de trabalho do Microsoft Windows 95

hlp — ficheiro de ajuda do Windows

msg — mensagem de e-mail do Microsoft Mail

plg — mensagem de e-mail

mbx — mensagem de e-mail guardada do Microsoft Office Outlook

doc* — documentos do Microsoft Office Word como, por exemplo: doc para documentos do Microsoft Office Word, docx para documentos do Microsoft Office Word 2007 com suporte de XML e docm para documentos do Microsoft Office Word 2007 com suporte para macros

dot* — modelos de documentos do Microsoft Office Word como, por exemplo: dot para modelos de documentos do Microsoft Office Word, dotx para modelos de documentos do Microsoft Office Word 2007, dotm para modelos de documentos do Microsoft Office Word 2007 com suporte para macros

fpm — programa de bases de dados, ficheiro de arranque do Microsoft Visual FoxPro

rtf — formato Rich Text Format

shs — fragmento Handler do Shell Scrap Object para Windows

dwg — base de dados de desenhos de AutoCAD®

msi — pacote do Microsoft Windows Installer

otm — projeto VBA para o Microsoft Office Outlook

pdf — documento do Adobe Acrobat

swf — objeto do pacote do Shockwave® Flash

jpg, jpeg — formato gráfico de imagens comprimidas

emf — ficheiro em formato de metaficheiro melhorado;

ico — ficheiro de ícones de objetos

ov? — Ficheiros executáveis de Microsoft Office Word

xl* — documentos e ficheiros do Microsoft Office Excel como, por exemplo: xla, extensão para o Microsoft Office Excel, xlc para diagramas, xlt para modelos de documentos, xlsx para livros do Microsoft Office Excel 2007, xltm para livros do Microsoft Office Excel 2007 com suporte de macros, xlsb para livros 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 para macros e xlam para plug-ins do Microsoft Office Excel 2007 com suporte para macros

pp* — documentos e ficheiros do Microsoft Office PowerPoint® como, por exemplo: pps para diapositivos 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 para macros, potx para modelos de apresentações do Microsoft Office PowerPoint 2007, potm para modelos de apresentações do Microsoft Office PowerPoint 2007 com suporte para macros, ppsx para apresentações de diapositivos do Microsoft Office PowerPoint 2007, ppsm para apresentações de diapositivos do Microsoft Office PowerPoint 2007 com suporte para macros e ppam para plug-ins do Microsoft Office PowerPoint 2007 com suporte para macros

md* — documentos e ficheiros do Microsoft Office Access® como, por exemplo: mda para grupos de trabalho e mdb para bases de dados

sldx — diapositivo do Microsoft PowerPoint 2007

sldm — diapositivo do Microsoft PowerPoint 2007 com suporte para macros

thmx — tema do Microsoft Office 2007

Anexo 4. Tipos de ficheiros para o filtro de anexo Proteção contra ameaças de correio

Note que o formato real de um ficheiro poderá não corresponder à sua extensão do nome de ficheiro.

Se tiver ativado a filtragem de anexos de mensagens de e-mail, o componente Proteção contra ameaças de correio pode renomear ou eliminar ficheiros com as seguintes extensões:

com – ficheiro executável de uma aplicação não superior a 64 KB

exe — ficheiro executável ou arquivo autoextraível

sys — ficheiro de sistema do Microsoft Windows

prg — texto de programa para dBase™, Clipper ou Microsoft Visual FoxPro®ou um programa WAVmaker

bin — ficheiro binário

bat — ficheiro de lote

cmd — ficheiro de comandos para o Microsoft Windows NT (semelhante a um ficheiro bat para DOS), OS/2

dpl — biblioteca Borland Delphi comprimida

dll — biblioteca de ligações dinâmicas

scr — ecrã inicial do Microsoft Windows

cpl — módulo do painel de controlo do Microsoft Windows

ocx — Objeto Microsoft OLE (Object Linking and Embedding)

tsp — programa em execução em modo parcial

drv — controlador de dispositivos

vxd — controlador de dispositivos do Microsoft Windows

pif — ficheiro de informação de programas

lnk — ficheiro de ligação do Microsoft Windows

reg — ficheiro-chave de registo do Microsoft Windows

ini — ficheiro de configuração que contém dados de configuração para o Microsoft Windows, Windows NT e algumas aplicações

cla — classe de Java

vbs — script Visual Basic®

vbe — extensão de vídeo da BIOS

js, jse — texto fonte do JavaScript

htm — documento de hipertexto

htt — cabeçalho de hipertexto do Microsoft Windows

hta — programa de hipertexto para o Microsoft Internet Explorer®

asp — script das Páginas do Servidor Ativo

o chm — ficheiro HTML compilado

pht — ficheiro HTML com scripts PHP integrados

php — script que está integrado em ficheiros HTML

wsh — ficheiro de script anfitrião do Microsoft Windows

wsf — script do Microsoft Windows

the - ficheiro de fundo de ecrã do ambiente de trabalho do Microsoft Windows 95

hlp — ficheiro de ajuda do Windows

msg — mensagem de e-mail do Microsoft Mail

plg — mensagem de e-mail

mbx — mensagem de e-mail guardada do Microsoft Office Outlook

doc* — documentos do Microsoft Office Word como, por exemplo: doc para documentos do Microsoft Office Word, docx para documentos do Microsoft Office Word 2007 com suporte de XML e docm para documentos do Microsoft Office Word 2007 com suporte para macros

dot* — modelos de documentos do Microsoft Office Word como, por exemplo: dot para modelos de documentos do Microsoft Office Word, dotx para modelos de documentos do Microsoft Office Word 2007, dotm para modelos de documentos do Microsoft Office Word 2007 com suporte para macros

fpm — programa de bases de dados, ficheiro de arranque do Microsoft Visual FoxPro

rtf — formato Rich Text Format

shs — fragmento Handler do Shell Scrap Object para Windows

dwg — base de dados de desenhos de AutoCAD®

msi — pacote do Microsoft Windows Installer

otm — projeto VBA para o Microsoft Office Outlook

pdf — documento do Adobe Acrobat

swf — objeto do pacote do Shockwave® Flash

jpg, jpeg — formato gráfico de imagens comprimidas

emf — ficheiro em formato de metaficheiro melhorado;

ico — ficheiro de ícones de objetos

ov? — Ficheiros executáveis de Microsoft Office Word

xl* — documentos e ficheiros do Microsoft Office Excel como, por exemplo: xla, extensão para o Microsoft Office Excel, xlc para diagramas, xlt para modelos de documentos, xlsx para livros do Microsoft Office Excel 2007, xltm para livros do Microsoft Office Excel 2007 com suporte de macros, xlsb para livros 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 para macros e xlam para plug-ins do Microsoft Office Excel 2007 com suporte para macros

pp* — documentos e ficheiros do Microsoft Office PowerPoint® como, por exemplo: pps para diapositivos 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 para macros, potx para modelos de apresentações do Microsoft Office PowerPoint 2007, potm para modelos de apresentações do Microsoft Office PowerPoint 2007 com suporte para macros, ppsx para apresentações de diapositivos do Microsoft Office PowerPoint 2007, ppsm para apresentações de diapositivos do Microsoft Office PowerPoint 2007 com suporte para macros e ppam para plug-ins do Microsoft Office PowerPoint 2007 com suporte para macros

md* — documentos e ficheiros do Microsoft Office Access® como, por exemplo: mda para grupos de trabalho e mdb para bases de dados

sldx — diapositivo do Microsoft PowerPoint 2007

sldm — diapositivo do Microsoft PowerPoint 2007 com suporte para macros

thmx — tema do Microsoft Office 2007

Anexo 5. Definições de rede para interação com serviços externos

O Kaspersky Endpoint Security e o Kaspersky Security Center utilizam um canal de comunicação encriptado com TLS (Transport Layer Security) para trabalhar com serviços externos da Kaspersky.

O Kaspersky Endpoint Security utiliza as seguintes definições de rede para interação com serviços externos.

Definições de Rede

Endereço	Descrição
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protocolo: `HTTPS` Port: `443`	Ativar a aplicação.

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`
Port: `443`
	Atualização de bases de dados e módulos de software de aplicação.

`downloads.upd.kaspersky.com` Protocolo: `HTTPS` Port: `443`	• Atualização de bases de dados e módulos de software de aplicação. • Verificar o acesso aos servidores da Kaspersky. Se o acesso aos servidores utilizando o DNS do sistema não for possível, a aplicação utiliza o DNS público. Isto é necessário para garantir que as bases de dados antivírus são atualizadas e que o nível de segurança do computador é mantido. O Kaspersky Endpoint Security utiliza a seguinte lista de servidores DNS públicos nesta ordem: 1. DNS público do Google (8.8.8.8). 2. DNS da Cloudflare (1.1.1.1). 3. DNS da Alibaba Cloud (223.6.6.6). 4. DNS da Quad9 (9.9.9.9). 5. CleanBrowsing (185.228.168.168). Os pedidos emitidos pela aplicação podem conter endereços de domínios e o endereço IP público do utilizador, porque a aplicação estabelece uma ligação TCP/UDP com o servidor DNS. Esta informação é necessária, por exemplo, para validar o certificado de um recurso da Web quando se utiliza HTTPS. Se o Kaspersky Endpoint Security estiver a utilizar um servidor DNS público, o processamento de dados será regido pela política de privacidade do serviço relevante. Se quiser impedir que o Kaspersky Endpoint Security utilize um servidor DNS público, entre em contacto com o Suporte Técnico para obter um patch privado.
`touch.kaspersky.com` Protocolo: `HTTP`	• Receber o tempo fiável para verificar o período de validade do certificado (ligação TLS). • Aviso sobre o acesso negado a um recurso da Internet no navegador quando a Proteção contra Ameaças da Web está 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`
Port: `80`
	Atualização de bases de dados e módulos de software de aplicação.

`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`
Port: `443`
	Utilização da 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`
Port: `443`, `1443`
	Utilização da Kaspersky Security Network.

`click.kaspersky.com`
 	
`redirect.kaspersky.com`
Protocolo: `HTTPS`
Port: `443`
	Seguir as ligações da interface.

Definições, utilizadas para encriptação

Endereço	Descrição

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protocolo: `HTTP`
Port: `80`
	Infraestrutura de chave pública (PKI).

Anexo 6. Eventos da aplicação

As informações sobre o funcionamento de cada componente do Kaspersky Endpoint Security, os eventos de encriptação de dados, a conclusão de cada tarefa de verificação de software malicioso, a tarefa de atualização e a tarefa de verificação de integridade, bem como sobre o funcionamento geral da aplicação, são registadas no registo de eventos do Kaspersky Security Center e no registo de eventos do Windows.

O Kaspersky Endpoint Security gera eventos dos seguintes tipos: eventos gerais e eventos específicos. Eventos específicos são criados apenas pelo Kaspersky Endpoint Security for Windows. Os eventos específicos têm um ID simples, como `000000cb`. Os eventos específicos contêm os seguintes parâmetros necessários:

- `GNRL_EA_DESCRIPTION` é o conteúdo do evento.
- `GNRL_EA_ID` é o ID do evento.
- `GNRL_EA_SEVERITY` é o estado do evento. `1` – *Info*, `2` – *Warning*, `3` – *Functional failure*, `4` – *Critical*.
- `EVENT_TYPE_DISPLAY_NAME` é o título do evento.
- `TASK_DISPLAY_NAME` é o nome do componente da aplicação que iniciou o evento.

Os eventos gerais podem ser criados pelo Kaspersky Endpoint Security for Windows, bem como outras aplicações da Kaspersky (por exemplo, o Kaspersky Security for Windows Server). Os eventos gerais têm um ID mais complexo, como `GNRL_EV_VIRUS_FOUND`. Para além das definições necessárias, os eventos gerais contêm definições avançadas.

Por quanto tempo os eventos são armazenados no servidor

Crítico

A licença expirou

Estado	⊗
Componente	Auditoria do Sistema
ID de evento do Windows	`201`
ID do evento do Kaspersky Security Center	`GNRL_EV_LICENSE_EXPIRATION`
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

A licença está prestes a expirar

Estado	⊗
Componente	Auditoria do Sistema
ID de evento do Windows	`203`
ID do evento do Kaspersky Security Center	`000000cb`

Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

As bases de dados estão em falta ou corrompidas

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	206
ID do evento do Kaspersky Security Center	000000ce
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Bases de dados estão muito desatualizadas

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	207
ID do evento do Kaspersky Security Center	000000cf
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

A inicialização automática da aplicação está desativada

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	209
ID do evento do Kaspersky Security Center	000000d1
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Erro de ativação

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	229
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Ameaça ativa detetada. A Desinfeção Avançada deve ser iniciada

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	231
ID do evento do Kaspersky Security Center	000000e7

Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Os servidores da KSN não estão disponíveis

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	2023
ID do evento do Kaspersky Security Center	000007e7
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Espaço insuficiente no armazenamento da Quarentena

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	343
ID do evento do Kaspersky Security Center	00000157
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Objeto não restaurado da Quarentena

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	346
ID do evento do Kaspersky Security Center	0000015a
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Objeto não eliminado da Quarentena

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	348
ID do evento do Kaspersky Security Center	0000015c
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

A aplicação estabeleceu uma ligação a um site com um certificado não fiável

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	57
ID do evento do Kaspersky Security Center	00000039

Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Não foi possível verificar uma ligação encriptada. O domínio foi adicionado à lista de exclusões

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	`60`
ID do evento do Kaspersky Security Center	`0000003c`
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Malicious object detected (local bases)

Estado	ⓘ
Componente	Proteção contra ameaças de ficheiros Proteção contra ameaças da Web Proteção contra ameaças de correio Proteção AMSI Prevenção contra invasões Deteção de comportamento Anti-Cryptor Prevenção de explorações Verificação de software malicioso
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 encriptação externa de pastas partilhadas é detetada, a aplicação mostra o caminho para o ficheiro alvo. • `GNRL_EA_PARAM_5` é o nome da ameaça de acordo com a classificação Kaspersky, por exemplo, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` é o nome do utilizador da sessão. • `GNRL_EA_PARAM_8` é o tipo de ameaça (`tipo`). • `GNRL_EA_PARAM_9` são informações adicionais sobre o objeto detetado: Componente da aplicação (`engine`). Tecnologia de deteção de ameaças (`method`). Ameaça detetada pela Kaspersky Private Security Network (`blacklist`): `true` ou `false`. Versão EDR. Identificador de ameaça no EDR. Hash MD5 do objeto.
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Malicious object detected (KSN)

Estado	ⓘ
Componente	Proteção contra ameaças de ficheiros Proteção contra ameaças da Web Proteção contra ameaças de correio Proteção AMSI Prevenção contra invasões Deteção de comportamento Anti-Cryptor Prevenção de explorações Verificação de software malicioso
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 Kaspersky, por exemplo, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` é o nome do utilizador da sessão. • `GNRL_EA_PARAM_8` é o tipo de ameaça (`tipo`). • `GNRL_EA_PARAM_9` são informações adicionais sobre o objeto detetado: Componente da aplicação (`engine`). Tecnologia de deteção de ameaças (`method`). Ameaça detetada pela Kaspersky Private Security Network (`blacklist`): `true` ou `false`. Versão EDR. Identificador de ameaça no EDR. Hash MD5 do objeto.
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Desinfeção impossível

Estado	ⓘ
Componente	Proteção contra ameaças de ficheiros Proteção contra ameaças de correio Prevenção contra invasões Deteção de comportamento Anti-Cryptor Verificação de software malicioso
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 Kaspersky, por exemplo, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` é o nome do utilizador da sessão. • `GNRL_EA_PARAM_8` é o tipo de ameaça (`tipo`). • `GNRL_EA_PARAM_9` são informações adicionais sobre o objeto detetado: Componente da aplicação (`engine`). Tecnologia de deteção de ameaças (`method`). Ameaça detetada pela Kaspersky Private Security Network (`blacklist`): `true` ou `false`. Versão EDR. Identificador de ameaça no EDR. Hash MD5 do objeto.
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Cannot be deleted

Estado	ⓘ
Componente	Proteção contra ameaças de ficheiros Prevenção contra invasões Deteção de comportamento Anti-Cryptor Verificação de software malicioso
ID de evento do Windows	313
ID do evento do Kaspersky Security Center	00000139
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Processing error

Estado	ⓘ
Componente	Proteção contra ameaças de ficheiros Proteção contra ameaças da Web Proteção contra ameaças de correio Prevenção contra invasões Proteção AMSI Verificação de software malicioso
ID de evento do Windows	317
ID do evento do Kaspersky Security Center	0000013d
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Process terminated

Estado	ⓘ
Componente	Proteção contra ameaças de ficheiros Prevenção contra invasões Deteção de comportamento Verificação de software malicioso
ID de evento do Windows	452
ID do evento do Kaspersky Security Center	000001c4
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Unable to terminate process

Estado	ⓘ
Componente	Proteção contra ameaças de ficheiros Prevenção contra invasões Deteção de comportamento Verificação de software malicioso
ID de evento do Windows	453
ID do evento do Kaspersky Security Center	000001c5
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Dangerous link blocked

Estado	ⓘ
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 do objeto. • GNRL_EA_PARAM_5 é o nome do objeto de acordo com a classificação Kaspersky. • GNRL_EA_PARAM_7 é o nome do utilizador da sessão. • GNRL_EA_PARAM_8 é o tipo de ameaça (tipo). • GNRL_EA_PARAM_9 são informações adicionais sobre o objeto detetado: Componente da aplicação (engine). Tecnologia de deteção de ameaças (method). Ameaça detetada pela KSN privada (blacklist): true ou false.
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Dangerous link opened

Estado	ⓘ
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 do objeto. • GNRL_EA_PARAM_5 é o nome do objeto de acordo com a classificação Kaspersky. • GNRL_EA_PARAM_7 é o nome do utilizador da sessão. • GNRL_EA_PARAM_8 é o tipo de ameaça (tipo). • GNRL_EA_PARAM_9 são informações adicionais sobre o objeto detetado: Componente da aplicação (engine). Tecnologia de deteção de ameaças (method). Ameaça detetada pela KSN privada (blacklist): true ou false.
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Previously opened dangerous link detected

Estado	ⓘ
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 do objeto. • GNRL_EA_PARAM_5 é o nome do objeto de acordo com a classificação Kaspersky. • GNRL_EA_PARAM_7 é o nome do utilizador da sessão. • GNRL_EA_PARAM_8 é o tipo de ameaça (tipo). • GNRL_EA_PARAM_9 são informações adicionais sobre o objeto detetado: Componente da aplicação (engine). Tecnologia de deteção de ameaças (method). Ameaça detetada pela KSN privada (blacklist): true ou false.

Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Process action blocked

Estado	⚠
Componente	Controlo de Anomalias Adaptativo
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 Controlo de Anomalias Adaptativo. • `GNRL_EA_PARAM_2` é o ID da regra heurística. • `GNRL_EA_PARAM_3` é o nome do utilizador da sessão. • `GNRL_EA_PARAM_4` é o processo original. • `GNRL_EA_PARAM_5` é o objeto de origem. • `GNRL_EA_PARAM_6` é o processo de destino. • `GNRL_EA_PARAM_7` é o objeto de destino. • `GNRL_EA_PARAM_8` são informações adicionais sobre o objeto detetado: Somas de verificação do processo/objeto original e processo/objeto de destino. Processo bloqueado (`verdict_type`): `true` ou `false`. ID de segurança do utilizador (SID).
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Teclado não autorizado

Estado	⚠
Componente	Prevenção de ataques BadUSB
ID de evento do Windows	`2051`
ID do evento do Kaspersky Security Center	`00000803`
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

AMSI request was blocked

Estado	⚠
Componente	Proteção AMSI
ID de evento do Windows	`2200`
ID do evento do Kaspersky Security Center	`00000898`
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Network activity blocked

Estado	⚠
Componente	Firewall
ID de evento do Windows	`602`
ID do evento do Kaspersky Security Center	`00000329`
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Ataque de rede detetado

Estado	ⓘ
Componente	Proteção contra ameaças de 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 de IP do computador que age como a origem do ataque de rede. O endereço de IP é indicado na ordem de bytes do anfitrião. 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 de IP do computador alvo do ataque de rede. O endereço de IP é indicado na ordem de bytes do anfitrião. Por exemplo, 2886729929 para 172.16.0.201.
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Inicialização da aplicação proibida

Estado	ⓘ
Componente	Controlo das aplicações
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 utilizador da sessão. • GNRL_EA_PARAM_3 é o identificador da categoria criado manualmente. • GNRL_EA_PARAM_4 é a ID da categoria da aplicação. • GNRL_EA_PARAM_5 é a informação relativa à assinatura digital da aplicação. • GNRL_EA_PARAM_6 é o nome do ficheiro executável da aplicação (por exemplo, chrome.exe). • GNRL_EA_PARAM_7 é o caminho do ficheiro executável. • GNRL_EA_PARAM_8 é o hash do objeto (SHA256). • GNRL_EA_PARAM_9 é a versão da aplicação que o utilizador está a tentar executar.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Prohibited process was started before Kaspersky Endpoint Security startup

Estado	ⓘ
Componente	Controlo das Aplicações
ID de evento do Windows	710
ID do evento do Kaspersky Security Center	000002c6
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Access denied (local bases)

Estado	ⓘ
Componente	Controlo de Internet

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 utilizador da sessão. • GNRL_EA_PARAM_3 é o nome da regra do Controlo de Internet.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Access denied (KSN)

Estado	!
Componente	Controlo de Internet
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 utilizador da sessão. • GNRL_EA_PARAM_3 é o nome da regra do Controlo de Internet.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Operation with the device prohibited

Estado	!
Componente	Controlo 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 a ID do hardware (HWID). • GNRL_EA_PARAM_2 é o nome do utilizador da sessão.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Network connection blocked

Estado	!
Componente	Controlo de Dispositivos
ID de evento do Windows	809
ID do evento do Kaspersky Security Center	00000329
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

A utilização do dispositivo é proibida até que o Kaspersky Endpoint Security seja iniciado

Estado	!
Componente	Controlo de Dispositivos
ID de evento do Windows	816
ID do evento do Kaspersky Security Center	00000330

Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

A ligação do dispositivo é proibida até que o Kaspersky Endpoint Security seja iniciado

Estado	ⓘ
Componente	Controlo de Dispositivos
ID de evento do Windows	817
ID do evento do Kaspersky Security Center	00000331
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Error updating component

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	1011
ID do evento do Kaspersky Security Center	000003f3
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Error distributing component updates

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	1012
ID do evento do Kaspersky Security Center	000003f4
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Local update error

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	1014
ID do evento do Kaspersky Security Center	000003f6
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Network update error

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	1015
ID do evento do Kaspersky Security Center	000003f7

Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Cannot start two tasks at the same time

Estado	⚠
Componente	Atualização
ID de evento do Windows	1017
ID do evento do Kaspersky Security Center	000003f9
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Erro ao verificar bases de dados e módulos da aplicação

Estado	⚠
Componente	Atualização
ID de evento do Windows	1018
ID do evento do Kaspersky Security Center	000003fa
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Erro na interação com o Kaspersky Security Center

Estado	⚠
Componente	Atualização
ID de evento do Windows	1019
ID do evento do Kaspersky Security Center	000003fb
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Nem todos os componentes foram atualizados

Estado	⚠
Componente	Atualização
ID de evento do Windows	1021
ID do evento do Kaspersky Security Center	000003fd
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Update completed successfully, update distribution failed

Estado	⚠
Componente	Atualização
ID de evento do Windows	1023
ID do evento do Kaspersky Security Center	000003ff

Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Internal task error

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	101
ID do evento do Kaspersky Security Center	00000065
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Patch installation failed

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	2153
ID do evento do Kaspersky Security Center	00000869
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Patch rollback failed

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	2156
ID do evento do Kaspersky Security Center	0000086c
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Error applying file encryption / decryption rules

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	904
ID do evento do Kaspersky Security Center	00000388
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

File encryption / decryption error

Estado	ⓘ
Componente	Encriptação 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 do ficheiro. • GNRL_EA_PARAM_2 é o nome do erro. • GNRL_EA_PARAM_3 é o tipo do dispositivo.
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

File access blocked

Estado	ⓘ
Componente	Encriptação 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 utilizador da sessão. • GNRL_EA_PARAM_3 é o nome do ficheiro executável da aplicação (por exemplo, chrome.exe), que está a tentar obter acesso ao ficheiro.
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Erro ao ativar o modo portátil

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	951
ID do evento do Kaspersky Security Center	000003b7
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Error disabling portable mode

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	953
ID do evento do Kaspersky Security Center	000003b9
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Error creating encrypted package

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	931
ID do evento do Kaspersky Security Center	000003a3
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Error encrypting / decrypting device

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1305
ID do evento do Kaspersky Security Center	00000519
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Could not load encryption module

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1311
ID do evento do Kaspersky Security Center	0000051f
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

The task for managing Authentication Agent accounts ended with an error

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1340
ID do evento do Kaspersky Security Center	0000053c
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Policy cannot be applied

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	1312
ID do evento do Kaspersky Security Center	00000520
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

FDE upgrade failed

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1342
ID do evento do Kaspersky Security Center	0000053e
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

FDE upgrade rollback failed (for more information, please refer to the Kaspersky Endpoint Security for Windows Online Help)

Estado	⚠
Componente	Encriptação de dados
ID de evento do Windows	1344
ID do evento do Kaspersky Security Center	00000540
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Kaspersky Anti Targeted Attack Platform server unavailable

Estado	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2100
ID do evento do Kaspersky Security Center	00000834
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Failed to delete object

Estado	⚠
Componente	Sandbox
ID de evento do Windows	2252
ID do evento do Kaspersky Security Center	000008cc
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Object not quarantined (Sandbox)

Estado	⚠
Componente	Sandbox
ID de evento do Windows	2603
ID do evento do Kaspersky Security Center	00000a2b
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

An internal error occurred

Estado	⚠
Componente	Sandbox
ID de evento do Windows	2607
ID do evento do Kaspersky Security Center	00000a2f
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Invalid Sandbox server certificate

Estado	ⓘ
Componente	Sandbox
ID de evento do Windows	2613
ID do evento do Kaspersky Security Center	00000a35
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

The Sandbox node is unavailable

Estado	ⓘ
Componente	Sandbox
ID de evento do Windows	2614
ID do evento do Kaspersky Security Center	00000a36
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Failed to process the object in Sandbox

Estado	ⓘ
Componente	Sandbox
ID de evento do Windows	2617
ID do evento do Kaspersky Security Center	00000a39
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Maximum load to Sandbox is exceeded

Estado	ⓘ
Componente	Sandbox
ID de evento do Windows	2618
ID do evento do Kaspersky Security Center	00000a3a
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

IOC found

Estado	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2651
ID do evento do Kaspersky Security Center	00000a5b
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Sandbox license verification failed

Estado	ⓘ
Componente	Sandbox
ID de evento do Windows	2620
ID do evento do Kaspersky Security Center	00000a3c
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Falha ao enviar a tarefa de verificação para o Sandbox por um utilizador

Estado	ⓘ
Componente	Sandbox
ID de evento do Windows	2623
ID do evento do Kaspersky Security Center	00000a3e
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Erro ao criar tarefa do Sandbox

Estado	ⓘ
Componente	Sandbox
ID de evento do Windows	2621
ID do evento do Kaspersky Security Center	00000a3d
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Object startup blocked

Estado	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2553
ID do evento do Kaspersky Security Center	000009f9
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Process startup blocked

Estado	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2551
ID do evento do Kaspersky Security Center	000009f7
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Script execution blocked

Estado	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2559
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Object not quarantined (Endpoint Detection and Response)

Estado	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2556
ID do evento do Kaspersky Security Center	000009fc
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Process startup is not blocked

Estado	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2561
ID do evento do Kaspersky Security Center	00000a01
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Object is not blocked

Estado	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2562
ID do evento do Kaspersky Security Center	00000a02
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Script execution is not blocked

Estado	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2563
ID do evento do Kaspersky Security Center	00000a03
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Error changing application components

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	1401
ID do evento do Kaspersky Security Center	00000579
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

There are patterns of a possible brute-force attack in the system

Estado	ⓘ
Componente	Inspeção de Registo
ID de evento do Windows	2800
ID do evento do Kaspersky Security Center	00000af0
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

There are patterns of a possible Windows Event Log abuse

Estado	ⓘ
Componente	Inspeção do Registo
ID de evento do Windows	2801
ID do evento do Kaspersky Security Center	00000af1
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Atypical actions detected on behalf of a new service installed

Estado	ⓘ
Componente	Inspeção do Registo
ID de evento do Windows	2802
ID do evento do Kaspersky Security Center	00000af2
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Atypical logon that uses explicit credentials detected

Estado	ⓘ
Componente	Inspeção de Registo
ID de evento do Windows	2803
ID do evento do Kaspersky Security Center	00000af3
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system

Estado	⚠
Componente	Inspeção de Registo
ID de evento do Windows	2804
ID do evento do Kaspersky Security Center	00000af4
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Suspicious changes detected in the privileged built-in Administrators group

Estado	⚠
Componente	Inspeção do Registo
ID de evento do Windows	2805
ID do evento do Kaspersky Security Center	00000af5
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

There is an atypical activity detected during a network logon session

Estado	⚠
Componente	Inspeção de Registo
ID de evento do Windows	2806
ID do evento do Kaspersky Security Center	00000af6
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Log Inspection rule triggered

Estado	⚠
Componente	Inspeção de Registo
ID de evento do Windows	2807
ID do evento do Kaspersky Security Center	00000af7
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Atypical event occurs too often. Event aggregation started

Estado	⚠
Componente	Inspeção do Registo
ID de evento do Windows	2808
ID do evento do Kaspersky Security Center	00000af8
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Report on an atypical event for the aggregation period

Estado	ⓘ
Componente	Inspeção do Registo
ID de evento do Windows	2809
ID do evento do Kaspersky Security Center	00000af9
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Error connecting to the EDR Expert server

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID de evento do Windows	2850
ID do evento do Kaspersky Security Center	00000b22
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Invalid certificate of the EDR Expert server

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID de evento do Windows	2851
ID do evento do Kaspersky Security Center	00000b23
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Invalid certificate of the agent on the EDR Expert server

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID de evento do Windows	2852
ID do evento do Kaspersky Security Center	00000b24
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Erro ao ligar ao servidor de resposta do EDR Expert

Estado	ⓘ
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
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Certificado inválido do servidor de resposta do EDR Expert

Estado	⚠
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
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Certificado inválido do agente no servidor de resposta do EDR Expert

Estado	⚠
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
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Erro de ligação do servidor de recolha de telemetria do EDR Expert

Estado	⚠
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
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Certificado inválido do servidor de recolha de telemetria do EDR Expert

Estado	⚠
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
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Certificado inválido do agente no servidor de recolha de telemetria do EDR Expert

Estado	⚠
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

Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Erro ao ligar ao servidor NDR

Estado	ⓘ
Componente	Network Detection and Response (KATA)
ID de evento do Windows	3080
ID do evento do Kaspersky Security Center	00000c08
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Certificado inválido do servidor NDR

Estado	ⓘ
Componente	Network Detection and Response (KATA)
ID de evento do Windows	3081
ID do evento do Kaspersky Security Center	00000c09
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Certificado inválido do agente no servidor NDR

Estado	ⓘ
Componente	Network Detection and Response (KATA)
ID de evento do Windows	3082
ID do evento do Kaspersky Security Center	00000c0a
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

O seu dispositivo está ligado a um Servidor de Administração não fiável. Contacte o administrador

Estado	ⓘ
Componente	Proteção da ligação do Servidor de Administração
ID de evento do Windows	3301
ID do evento do Kaspersky Security Center	00000ce5
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

File or folder change was detected

Estado	ⓘ / ⚠ / ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2950
ID do evento do Kaspersky Security Center	00000b86
Windows event log (padrão)	–

Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

Object changes too often. Event aggregation started

Estado	ⓘ / ⚠ / ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2955
ID do evento do Kaspersky Security Center	00000b8b
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Report on object modification for the aggregation period

Estado	ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2953
ID do evento do Kaspersky Security Center	00000b89
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Estado	ⓘ / ⚠ / ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2956
ID do evento do Kaspersky Security Center	00000b8c
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

Registry change was detected

Estado	ⓘ / ⚠ / ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2951
ID do evento do Kaspersky Security Center	00000b87
Windows event log (padrão)	–

Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

Device connection / disconnection is detected

Estado	ⓘ / ⚠ / ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2952
ID do evento do Kaspersky Security Center	00000b88
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

O âmbito da monitorização inclui objetos incorretos

Estado	ⓘ / ⚠ / ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2903
ID do evento do Kaspersky Security Center	00000b89
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

Attempts to perform the restricted operations with the object is too many. Event aggregation started

Estado	ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2963
ID do evento do Kaspersky Security Center	00000b93
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

An operation with the files of the monitoring scope was blocked

Estado	ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2959
ID do evento do Kaspersky Security Center	00000b8f

Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

Registry modification blocked

Estado	ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2960
ID do evento do Kaspersky Security Center	00000b90
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

Processing error

Estado	ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2954
ID do evento do Kaspersky Security Center	00000b8a
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

System Integrity Monitoring: rule triggering disabled for user accounts without matching security identifier (SID)

Estado	ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2964
ID do evento do Kaspersky Security Center	00000b94
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Application Control: rule triggering disabled for user accounts without matching security identifier (SID)

Estado	ⓘ
Componente	Controlo das aplicações
ID de evento do Windows	711
ID do evento do Kaspersky Security Center	000002c7
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Device Control: rule triggering disabled for user accounts without matching security identifier (SID)

Estado	ⓘ
Componente	Controlo de Dispositivos
ID de evento do Windows	810
ID do evento do Kaspersky Security Center	0000032a
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Web Control: rule triggering disabled for user accounts without matching security identifier (SID)

Estado	ⓘ
Componente	Controlo de Internet
ID de evento do Windows	757
ID do evento do Kaspersky Security Center	000002f5
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Adaptive Anomaly Control: rule triggering disabled for user accounts without matching security identifier (SID)

Estado	ⓘ
Componente	Controlo de Anomalias Adaptativo
ID de evento do Windows	504
ID do evento do Kaspersky Security Center	000001f8
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Log Inspection: rule triggering disabled for user accounts without matching security identifier (SID)

Estado	ⓘ
Componente	Inspeção de Registo
ID de evento do Windows	2810
ID do evento do Kaspersky Security Center	00000afa
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

SVM is unavailable

Estado	ⓘ
Componente	Light Agent
ID de evento do Windows	3151
ID do evento do Kaspersky Security Center	00000c4f
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Malicious object detected. Advanced Disinfection should be started on a virtual machine template

Estado	ⓘ
Componente	Light Agent
ID de evento do Windows	3182
ID do evento do Kaspersky Security Center	00000c6e
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

A ligação de rede estabelecida através do protocolo preterido foi bloqueada

Estado	ⓘ
Componente	Proteção
ID de evento do Windows	75
ID do evento do Kaspersky Security Center	0000004b
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Erro de ligação do servidor da KUMA

Estado	ⓘ
Componente	Integração KUMA
ID de evento do Windows	2854
ID do evento do Kaspersky Security Center	00000b26
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Certificado inválido do servidor da KUMA

Estado	ⓘ
Componente	Integração KUMA
ID de evento do Windows	2855
ID do evento do Kaspersky Security Center	00000b27
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Certificado inválido do agente no servidor da KUMA

Estado	ⓘ
Componente	Integração KUMA
ID de evento do Windows	2856
ID do evento do Kaspersky Security Center	00000b28
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

SIEM server connection error

Estado	ⓘ
Componente	Integração KUMA
ID de evento do Windows	3250
ID do evento do Kaspersky Security Center	00000cb2
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Invalid certificate of the SIEM server

Estado	ⓘ
Componente	Integração KUMA
ID de evento do Windows	3251
ID do evento do Kaspersky Security Center	00000cb3
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Invalid certificate of the agent on the SIEM server

Estado	ⓘ
Componente	Integração KUMA
ID de evento do Windows	3252
ID do evento do Kaspersky Security Center	00000cb4
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Falha funcional

Task cannot be performed

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	212
ID do evento do Kaspersky Security Center	000000d4
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Invalid task settings. Settings not applied

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	707
ID do evento do Kaspersky Security Center	000002c3

Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Aviso

Application crashed during previous session

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	237
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

License expires soon

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	204
ID do evento do Kaspersky Security Center	000000cc
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Databases are out of date

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	208
ID do evento do Kaspersky Security Center	000000d0
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Automatic updates are disabled

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	210
ID do evento do Kaspersky Security Center	000000d2
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Self-Defense is disabled

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	211
ID do evento do Kaspersky Security Center	000000d3
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Protection components are disabled

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	214
ID do evento do Kaspersky Security Center	000000d6
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Computer is running in safe mode

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	215
ID do evento do Kaspersky Security Center	000000d7
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

There are unprocessed files

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	216
ID do evento do Kaspersky Security Center	000000d8
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Group policy applied

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	219
ID do evento do Kaspersky Security Center	000000db
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Task stopped

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	222
ID do evento do Kaspersky Security Center	000000de
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Quit and reopen the application to complete updating

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	224
ID do evento do Kaspersky Security Center	0000057b
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Computer restart required

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	225
ID do evento do Kaspersky Security Center	000000e1
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

The license allows the use of components that have not been installed

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	226
ID do evento do Kaspersky Security Center	000000e2
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Advanced Disinfection started

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	232
ID do evento do Kaspersky Security Center	000000e8
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Advanced Disinfection completed

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	233
ID do evento do Kaspersky Security Center	000000e9
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Incorrect reserve key

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	230
ID do evento do Kaspersky Security Center	000000e6
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Subscription expires soon

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	240
ID do evento do Kaspersky Security Center	000000f0
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Bloqueado

Estado	⚠
Componente	Deteção de comportamento Anti-Cryptor Prevenção de explorações 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 encriptação externa de pastas partilhadas é detetada, a aplicação mostra o caminho para o ficheiro alvo. • GNRL_EA_PARAM_5 é o nome da ameaça de acordo com a classificação Kaspersky, por exemplo, EICAR-Test-File. • GNRL_EA_PARAM_7 é o nome do utilizador da sessão. • GNRL_EA_PARAM_8 é o tipo de ameaça (tipo). • GNRL_EA_PARAM_9 são informações adicionais sobre o objeto detetado: Componente da aplicação (engine). Tecnologia de deteção de ameaças (method). Ameaça detetada pela Kaspersky Private Security Network (blacklist): true ou false. Versão EDR. Identificador de ameaça no EDR. Hash MD5 do objeto.
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

The operating system settings do not allow to control access to Wi-Fi networks

Estado	⚠
Componente	Controlo de Dispositivos
ID de evento do Windows	249
ID do evento do Kaspersky Security Center	000000f9
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Object not restored from Backup

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	336
ID do evento do Kaspersky Security Center	00000150
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Suspicious network activity detected

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	2001
ID do evento do Kaspersky Security Center	000007d1
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Encrypted connection terminated

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	250
ID do evento do Kaspersky Security Center	000007d3
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Participation in KSN disabled

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	2021
ID do evento do Kaspersky Security Center	000007e5
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Processing of some OS functions is disabled

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	245
ID do evento do Kaspersky Security Center	000000f5
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Quarantine storage is almost out of space

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	344
ID do evento do Kaspersky Security Center	00000158
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Network connection blocked

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	809
ID do evento do Kaspersky Security Center	00000abe
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Cannot create a backup copy

Estado	⚠
Componente	Proteção contra ameaças de ficheiros Deteção de comportamento Anti-Cryptor Prevenção contra invasões Verificação de software malicioso
ID de evento do Windows	310
ID do evento do Kaspersky Security Center	00000136
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Object not processed

Estado	⚠
Componente	Proteção contra ameaças de ficheiros Proteção contra ameaças de correio Prevenção contra invasões Proteção AMSI Verificação de software malicioso
ID de evento do Windows	314
ID do evento do Kaspersky Security Center	0000013a
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Object encrypted

Estado	⚠
Componente	Prevenção contra invasões
ID de evento do Windows	320
ID do evento do Kaspersky Security Center	00000140
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Object corrupted

Estado	⚠
Componente	Proteção contra ameaças de ficheiros Proteção contra ameaças da Web Proteção contra ameaças de correio Proteção AMSI Prevenção contra invasões Verificação de software malicioso
ID de evento do Windows	321
ID do evento do Kaspersky Security Center	00000141
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Legitimate software that can be used by intruders to damage your computer or personal data was detected (local bases)

Estado	⚠
Componente	Proteção contra ameaças de ficheiros Proteção contra ameaças da Web Proteção contra ameaças de correio Prevenção contra invasões Proteção AMSI Deteção de comportamento Anti-Cryptor Anti-Cryptor Verificação de software malicioso
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 Kaspersky, por exemplo, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` é o nome do utilizador da sessão. • `GNRL_EA_PARAM_8` é o tipo de ameaça (`tipo`).
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Legitimate software that can be used by intruders to damage your computer or personal data was detected (KSN)

Estado	⚠
Componente	Proteção contra ameaças de ficheiros Proteção contra ameaças da Web Proteção contra ameaças de correio Prevenção contra invasões Proteção AMSI Deteção de comportamento Anti-Cryptor Anti-Cryptor Verificação de software malicioso
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 Kaspersky, por exemplo, `EICAR-Test-File`. • `GNRL_EA_PARAM_7` é o nome do utilizador da sessão. • `GNRL_EA_PARAM_8` é o tipo de ameaça (`tipo`).
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Object deleted

Estado	⚠
Componente	Proteção contra ameaças de ficheiros Proteção contra ameaças de correio Prevenção contra invasões Prevenção de explorações Deteção de comportamento Anti-Cryptor Verificação de software malicioso

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 Kaspersky, por exemplo, EICAR-Test-File. • GNRL_EA_PARAM_7 é o nome do utilizador da sessão. • GNRL_EA_PARAM_8 é o tipo de ameaça (tipo). • GNRL_EA_PARAM_9 são informações adicionais sobre o objeto detetado: Componente da aplicação (engine). Tecnologia de deteção de ameaças (method). Ameaça detetada pela Kaspersky Private Security Network (blacklist): true ou false. Versão EDR. Identificador de ameaça no EDR. Hash MD5 do objeto.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Object disinfected

Estado	⚠
Componente	Proteção contra ameaças de ficheiros Proteção contra ameaças de correio Prevenção contra invasões Verificação de software malicioso
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 Kaspersky, por exemplo, EICAR-Test-File. • GNRL_EA_PARAM_7 é o nome do utilizador da sessão. • GNRL_EA_PARAM_8 é o tipo de ameaça (tipo). • GNRL_EA_PARAM_9 são informações adicionais sobre o objeto detetado: Componente da aplicação (engine). Tecnologia de deteção de ameaças (method). Ameaça detetada pela Kaspersky Private Security Network (blacklist): true ou false. Versão EDR. Identificador de ameaça no EDR. Hash MD5 do objeto.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Object will be disinfected on restart

Estado	⚠
Componente	Prevenção contra invasões Proteção contra ameaças de ficheiros Verificação de software malicioso
ID de evento do Windows	324
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Object will be deleted on restart

Estado	⚠
Componente	Deteção de comportamento Anti-Cryptor Prevenção de explorações Prevenção contra invasões Proteção contra ameaças de ficheiros Verificação de software malicioso
ID de evento do Windows	323
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Object deleted according to settings

Estado	⚠
Componente	Proteção contra ameaças de correio
ID de evento do Windows	342
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Rollback completed

Estado	⚠
Componente	Proteção contra ameaças de ficheiros Deteção de comportamento Anti-Cryptor Prevenção de explorações Verificação de software malicioso
ID de evento do Windows	455
ID do evento do Kaspersky Security Center	000001c7
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Error removing the previous version of the application

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	246
ID do evento do Kaspersky Security Center	000000f6
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Object download was blocked

Estado	⚠
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 Kaspersky, por exemplo, EICAR-Test-File. • GNRL_EA_PARAM_7 é o nome do utilizador da sessão. • GNRL_EA_PARAM_8 é o tipo de ameaça (tipo). • GNRL_EA_PARAM_9 são informações adicionais sobre o objeto detetado: Componente da aplicação (engine). Tecnologia de deteção de ameaças (method). Ameaça detetada pela Kaspersky Private Security Network (blacklist): true ou false. Versão EDR. Identificador de ameaça no EDR. Hash MD5 do objeto.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Keyboard authorization error

Estado	⚠
Componente	Prevenção de ataques BadUSB
ID de evento do Windows	2052
ID do evento do Kaspersky Security Center	00000804
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

The object scan result has been sent to a third-party application

Estado	⚠
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 Kaspersky, por exemplo, EICAR-Test-File. • GNRL_EA_PARAM_7 é o nome do utilizador da sessão. • GNRL_EA_PARAM_8 é o tipo de ameaça (tipo). • GNRL_EA_PARAM_9 são informações adicionais sobre o objeto detetado: Componente da aplicação (engine). Tecnologia de deteção de ameaças (method). Ameaça detetada pela Kaspersky Private Security Network (blacklist): true ou false. Versão EDR. Identificador de ameaça no EDR. Hash MD5 do objeto.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Task settings applied successfully

Estado	⚠
Componente	Controlo das aplicações

ID de evento do Windows	708
ID do evento do Kaspersky Security Center	000002c4
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Warning about undesirable content (local bases)

Estado	⚠
Componente	Controlo de Internet
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 utilizador da sessão. • GNRL_EA_PARAM_3 é o nome da regra do Controlo de Internet.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Warning about undesirable content (KSN)

Estado	⚠
Componente	Controlo de Internet
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 utilizador da sessão. • GNRL_EA_PARAM_3 é o nome da regra do Controlo de Internet.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Undesirable content was accessed after a warning

Estado	⚠
Componente	Controlo de Internet
ID de evento do Windows	754
ID do evento do Kaspersky Security Center	000002f2
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Temporary access to the device activated

Estado	⚠
Componente	Controlo de Dispositivos
ID de evento do Windows	803
ID do evento do Kaspersky Security Center	000002f2
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Operation canceled by the user

Estado	⚠
Componente	Atualização
ID de evento do Windows	1016
ID do evento do Kaspersky Security Center	000003f8
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

User has opted out of the encryption policy

Estado	⚠
Componente	Encriptação de dados
ID de evento do Windows	1306
ID do evento do Kaspersky Security Center	0000051a
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Interrupted applying file encryption / decryption rules

Estado	⚠
Componente	Encriptação de dados
ID de evento do Windows	903
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

File encryption / decryption interrupted

Estado	⚠
Componente	Encriptação de dados
ID de evento do Windows	914
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Device encryption / decryption interrupted

Estado	⚠
Componente	Encriptação de dados
ID de evento do Windows	1303
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Failed to install or upgrade Kaspersky Disk Encryption drivers in the WinRE image

Estado	⚠
Componente	Encriptação de dados
ID de evento do Windows	1345
ID do evento do Kaspersky Security Center	00000541
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Module signature check failed

Estado	⚠
Componente	Verificação de integridade do sistema
ID de evento do Windows	2002
ID do evento do Kaspersky Security Center	000007d2
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Application startup was blocked

Estado	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2105
ID do evento do Kaspersky Security Center	00000839
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Document opening was blocked

Estado	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2106
ID do evento do Kaspersky Security Center	0000083a
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Process was terminated by the Kaspersky Anti Targeted Attack Platform server administrator

Estado	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2112
ID do evento do Kaspersky Security Center	00000840
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

The application was terminated by the Kaspersky Anti Targeted Attack Platform server administrator

Estado	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2113
ID do evento do Kaspersky Security Center	00000841
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

File or stream was deleted by the Kaspersky Anti Targeted Attack Platform server administrator

Estado	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2111
ID do evento do Kaspersky Security Center	0000083f
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

File was restored from quarantine on the Kaspersky Anti Targeted Attack Platform server by the administrator

Estado	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2110
ID do evento do Kaspersky Security Center	0000083e
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

File was quarantined on the Kaspersky Anti Targeted Attack Platform server by the administrator

Estado	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2109
ID do evento do Kaspersky Security Center	0000083d
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Network activity of all third-party applications is blocked

Estado	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2107
ID do evento do Kaspersky Security Center	0000083b
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Network activity of all third-party applications is unblocked

Estado	⚠
Componente	Endpoint Sensor
ID de evento do Windows	2108
ID do evento do Kaspersky Security Center	0000083c
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Object will be deleted after restart (Sandbox)

Estado	⚠
Componente	Sandbox
ID de evento do Windows	2605
ID do evento do Kaspersky Security Center	00000a2d
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Total size of scan tasks exceeded the limit

Estado	⚠
Componente	Sandbox
ID de evento do Windows	2612
ID do evento do Kaspersky Security Center	00000a34
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Object startup allowed, event logged

Estado	⚠
Componente	Endpoint Detection and Response
ID de evento do Windows	2553
ID do evento do Kaspersky Security Center	000009fa
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Process startup allowed, event logged

Estado	⚠
Componente	Endpoint Detection and Response
ID de evento do Windows	2554
ID do evento do Kaspersky Security Center	000009f8
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Object will be deleted after restart (Endpoint Detection and Response)

Estado	⚠
Componente	Endpoint Detection and Response
ID de evento do Windows	2558
ID do evento do Kaspersky Security Center	000009fe
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Network isolation

Estado	⚠
Componente	Endpoint Detection and Response
ID de evento do Windows	2700
ID do evento do Kaspersky Security Center	00000a8c
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Termination of network isolation

Estado	⚠
Componente	Endpoint Detection and Response
ID de evento do Windows	2701
ID do evento do Kaspersky Security Center	00000a8d
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Restart required to complete the task

Estado	⚠
Componente	Auditoria do Sistema
ID de evento do Windows	225
ID do evento do Kaspersky Security Center	0000057b
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Connection to a website with an untrusted certificate is established by user decision

Estado	⚠
Componente	Network Detection and Response (KATA)
ID de evento do Windows	70
ID do evento do Kaspersky Security Center	00000046
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Application startup blockage message to administrator

Estado	⚠
Componente	Controlo das aplicações
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 utilizador. • GNRL_EA_PARAM_2 é o nome do utilizador da sessão. • GNRL_EA_PARAM_6 é o nome do ficheiro executável da aplicação (por exemplo, chrome.exe). • GNRL_EA_PARAM_7 é o caminho do ficheiro executável. • GNRL_EA_PARAM_8 é o hash do objeto (SHA256). • GNRL_EA_PARAM_9 é a versão da aplicação que o utilizador está a tentar executar.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Device access blockage message to administrator

Estado	⚠
Componente	Controlo 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 utilizador. • GNRL_EA_PARAM_1 é a ID do hardware (HWID). • GNRL_EA_PARAM_2 é o nome do utilizador da sessão.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Web page access blockage message to administrator

Estado	⚠
Componente	Controlo de Internet
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 utilizador. • GNRL_EA_PARAM_1 é o URL. • GNRL_EA_PARAM_2 é o nome do utilizador da sessão.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Device connection blocked

Estado	⚠
Componente	Controlo 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 a ID do hardware (HWID). • GNRL_EA_PARAM_2 é o nome do utilizador da sessão.

Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Application activity blockage message to administrator

Estado	⚠
Componente	Controlo de Anomalias Adaptativo
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 utilizador. • `GNRL_EA_PARAM_1` é o nome da regra do Controlo de Anomalias Adaptativo. • `GNRL_EA_PARAM_2` é o ID da regra heurística. • `GNRL_EA_PARAM_3` é o nome do utilizador da sessão. • `GNRL_EA_PARAM_4` é o processo original. • `GNRL_EA_PARAM_5` é o objeto de origem. • `GNRL_EA_PARAM_6` é o processo de destino. • `GNRL_EA_PARAM_7` é o objeto de destino. • `GNRL_EA_PARAM_8` são informações adicionais sobre o objeto detetado: Hashes do processo/objeto original e processo/objeto de destino. Processo bloqueado (`verdict_type`): `true` ou `false`. ID de segurança do utilizador (SID).
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Starting the cloud service client application is blocked

Estado	⚠
Componente	Cloud Discovery
ID de evento do Windows	`2212`
ID do evento do Kaspersky Security Center	`000008a4`
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Access to the cloud service is blocked

Estado	⚠
Componente	Cloud Discovery
ID de evento do Windows	`2213`
ID do evento do Kaspersky Security Center	`000008a5`
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

File or folder change was detected

Estado	ⓘ / ⚠ / ⓔ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	`2950`
ID do evento do Kaspersky Security Center	`00000b86`
Windows event log (padrão)	–

Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

Object changes too often. Event aggregation started

Estado	ⓘ / ⚠ / ⓔ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2955
ID do evento do Kaspersky Security Center	00000b8b
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Report on object modification for the aggregation period

Estado	ⓘ / ⚠ / ⓔ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2956
ID do evento do Kaspersky Security Center	00000b8c
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

Registry change was detected

Estado	ⓘ / ⚠ / ⓔ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2951
ID do evento do Kaspersky Security Center	00000b87
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

Device connection / disconnection is detected

Estado	ⓘ / ⚠ / ⓔ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2952
ID do evento do Kaspersky Security Center	00000b88

Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

O âmbito da monitorização inclui objetos incorretos

Estado	ⓘ / ⚠ / ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2903
ID do evento do Kaspersky Security Center	00000b89
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

The prohibited operation was allowed in test mode

Estado	⚠
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2961
ID do evento do Kaspersky Security Center	00000b91
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Não foi possível ligar ao Servidor de Integração durante mais de 30 minutas. Verifique o estado do Servidor de Integração e as definições de rede

Estado	⚠
Componente	Light Agent
ID de evento do Windows	3102
ID do evento do Kaspersky Security Center	00000c1e
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Unable to connect to the Integration Server for more than 6 hours. Check Integration Server status and network settings

Estado	⚠
Componente	Light Agent
ID de evento do Windows	3103
ID do evento do Kaspersky Security Center	00000c1f

Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Não foi possível ligar ao Servidor de Integração. Verifique o estado do Servidor de Integração e as definições de rede

Estado	⚠
Componente	Light Agent
ID de evento do Windows	3101
ID do evento do Kaspersky Security Center	00000c1d
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

O modelo da máquina virtual precisa de ser atualizado

Estado	⚠
Componente	Light Agent
ID de evento do Windows	3181
ID do evento do Kaspersky Security Center	00000c6d
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

The Standard license is terminated. The application is running under the Enterprise license

Estado	⚠
Componente	Light Agent
ID de evento do Windows	3171
ID do evento do Kaspersky Security Center	00000c64
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Estado	⚠
Componente	Monitor de integridade de ficheiros
ID de evento do Windows	2901
ID do evento do Kaspersky Security Center	00000b55
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Estado	⚠
Componente	Monitor de integridade do ficheiro
ID de evento do Windows	2900
ID do evento do Kaspersky Security Center	00000b54
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Mensagens informativas

Application started

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	235
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Application stopped

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	236
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Self-Defense restricted access to the protected resource

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	213
ID do evento do Kaspersky Security Center	000000d5
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Report cleared

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	217
ID do evento do Kaspersky Security Center	000000d9
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Group policy disabled

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	220

ID do evento do Kaspersky Security Center	000000dc
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Application settings changed

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	218
ID do evento do Kaspersky Security Center	000000da
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Task started

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	221
ID do evento do Kaspersky Security Center	000000dd
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Task completed

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	223
ID do evento do Kaspersky Security Center	000000df
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

All application components that are defined by the license have been installed and run in normal mode

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	227
ID do evento do Kaspersky Security Center	000000e3
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Subscription settings have changed

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	238

ID do evento do Kaspersky Security Center	000000ee
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Subscription has been renewed

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	239
ID do evento do Kaspersky Security Center	000000ef
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Object restored from Backup

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	335
ID do evento do Kaspersky Security Center	0000014f
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

User name and password input

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	2000
ID do evento do Kaspersky Security Center	000007d0
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Participation in KSN enabled

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	2020
ID do evento do Kaspersky Security Center	000007e4
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

KSN servers available

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	2022

ID do evento do Kaspersky Security Center	000007e6
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

The application works and processes data under relevant laws and uses the appropriate infrastructure

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	2024
ID do evento do Kaspersky Security Center	000007e8
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Object restored from Quarantine

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	345
ID do evento do Kaspersky Security Center	00000159
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Object deleted from Quarantine

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	347
ID do evento do Kaspersky Security Center	0000015b
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

A backup copy of the object was created

Estado	ⓘ
Componente	Proteção contra ameaças de ficheiros Proteção contra ameaças de correio Deteção de comportamento Anti-Cryptor Prevenção contra invasões Sandbox Verificação de software malicioso
ID de evento do Windows	308
ID do evento do Kaspersky Security Center	00000134
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Overwritten by a copy that was disinfected earlier

Estado	ⓘ
Componente	Proteção contra ameaças de ficheiros Prevenção contra invasões Verificação de software malicioso
ID de evento do Windows	327
ID do evento do Kaspersky Security Center	00000147
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Password-protected archive detected

Estado	ⓘ
Componente	Proteção contra ameaças de ficheiros Proteção contra ameaças da Web Proteção contra ameaças de correio Proteção AMSI Prevenção contra invasões Verificação de software malicioso
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 utilizador da sessão. • GNRL_EA_PARAM_9 são informações adicionais sobre o objeto detetado: Componente da aplicação (engine). Tecnologia de deteção de ameaças (method). Ameaça detetada pela KSN Privada (denylist): true ou false.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Information about detected object

Estado	ⓘ
Componente	Proteção contra ameaças de ficheiros Proteção contra ameaças da Web Proteção contra ameaças de correio Proteção AMSI Prevenção contra invasões Verificação de software malicioso
ID de evento do Windows	332
ID do evento do Kaspersky Security Center	0000014c
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

The object is in the Kaspersky Private Security Network allowlist

Estado	ⓘ
Componente	Proteção contra ameaças de ficheiros Proteção contra ameaças da Web Proteção contra ameaças de correio Proteção AMSI Prevenção contra invasões Verificação de software malicioso
ID de evento do Windows	340

ID do evento do Kaspersky Security Center	00000154
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Object renamed

Estado	ⓘ
Componente	Proteção contra ameaças de correio Prevenção de explorações Deteção de comportamento Anti-Cryptor Verificação de software malicioso
ID de evento do Windows	329
ID do evento do Kaspersky Security Center	00000149
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Object processed

Estado	ⓘ
Componente	Prevenção contra invasões Proteção contra ameaças de ficheiros Proteção contra ameaças da Web Proteção contra ameaças de correio Verificação de software malicioso
ID de evento do Windows	301
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Object skipped

Estado	ⓘ
Componente	Prevenção contra invasões Proteção contra ameaças de ficheiros Proteção AMSI Verificação de software malicioso
ID de evento do Windows	315
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Archive detected

Estado	ⓘ
Componente	Prevenção contra invasões Proteção contra ameaças de ficheiros Proteção contra ameaças da Web Proteção contra ameaças de correio Proteção AMSI Verificação de software malicioso
ID de evento do Windows	318

ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Packed object detected

Estado	ⓘ
Componente	Prevenção contra invasões Proteção contra ameaças de ficheiros Proteção contra ameaças da Web Proteção contra ameaças de correio Proteção AMSI Verificação de software malicioso
ID de evento do Windows	319
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Link processed

Estado	ⓘ
Componente	Proteção contra ameaças da Web
ID de evento do Windows	361
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Application startup allowed

Estado	ⓘ
Componente	Controlo das Aplicações
ID de evento do Windows	701
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Update source is selected

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	1001
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

O servidor de proxy está selecionado

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	1002
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

The link is in the Kaspersky Private Security Network allowlist

Estado	ⓘ
Componente	Proteção contra ameaças da Web
ID de evento do Windows	370
ID do evento do Kaspersky Security Center	00000172
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Application placed in the trusted group

Estado	ⓘ
Componente	Prevenção contra invasões
ID de evento do Windows	401
ID do evento do Kaspersky Security Center	00000191
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Application placed in restricted group

Estado	ⓘ
Componente	Prevenção contra invasões
ID de evento do Windows	402
ID do evento do Kaspersky Security Center	00000192
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Host Intrusion Prevention was triggered

Estado	ⓘ
Componente	Prevenção contra invasões
ID de evento do Windows	403
ID do evento do Kaspersky Security Center	00000193
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

File restored

Estado	ⓘ
Componente	Deteção de comportamento Anti-Cryptor Prevenção de explorações Prevenção contra invasões
ID de evento do Windows	457
ID do evento do Kaspersky Security Center	000001c9
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Registry value restored

Estado	ⓘ
Componente	Deteção de comportamento Prevenção de explorações
ID de evento do Windows	458
ID do evento do Kaspersky Security Center	000001ca
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Registry value deleted

Estado	ⓘ
Componente	Deteção de comportamento Prevenção de explorações
ID de evento do Windows	459
ID do evento do Kaspersky Security Center	000001cb
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Process action skipped

Estado	ⓘ
Componente	Controlo de Anomalias Adaptativo
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 Controlo de Anomalias Adaptativo. • GNRL_EA_PARAM_2 é o ID da regra heurística. • GNRL_EA_PARAM_3 é o nome do utilizador da sessão. • GNRL_EA_PARAM_4 é o processo original. • GNRL_EA_PARAM_5 é o objeto de origem. • GNRL_EA_PARAM_6 é o processo de destino. • GNRL_EA_PARAM_7 é o objeto de destino. • GNRL_EA_PARAM_8 são informações adicionais sobre o objeto detetado: Hashes do processo/objeto original e processo/objeto de destino. Processo bloqueado (verdict_type): true ou false. ID de segurança do utilizador (SID).
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Keyboard authorized

Estado	ⓘ
Componente	Prevenção de ataques BadUSB
ID de evento do Windows	2050
ID do evento do Kaspersky Security Center	00000802
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Network activity allowed

Estado	ⓘ
Componente	Firewall
ID de evento do Windows	601
ID do evento do Kaspersky Security Center	00000259
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Application startup prohibited in test mode

Estado	ⓘ
Componente	Controlo das aplicações
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 utilizador da sessão. • GNRL_EA_PARAM_3 é o identificador da categoria criado manualmente. • GNRL_EA_PARAM_4 é o identificador de segurança da conta (SID). • GNRL_EA_PARAM_5 é a informação relativa à assinatura digital da aplicação. • GNRL_EA_PARAM_6 é o nome do ficheiro executável da aplicação (por exemplo, chrome.exe). • GNRL_EA_PARAM_7 é o caminho do ficheiro executável. • GNRL_EA_PARAM_8 é o hash do objeto (SHA256). • GNRL_EA_PARAM_9 é a versão da aplicação que o utilizador está a tentar executar.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Application startup allowed in test mode

Estado	ⓘ
Componente	Controlo das aplicações
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 utilizador da sessão. • GNRL_EA_PARAM_3 é o identificador da categoria criado manualmente. • GNRL_EA_PARAM_4 é o identificador de segurança da conta (SID). • GNRL_EA_PARAM_5 é a informação relativa à assinatura digital da aplicação.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

A page that is allowed was opened

Estado	
Componente	Controlo de Internet
ID de evento do Windows	751
ID do evento do Kaspersky Security Center	000002f4
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Operation with the device allowed

Estado	
Componente	Controlo de Dispositivos
ID de evento do Windows	801
ID do evento do Kaspersky Security Center	00000321
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

File operation performed

Estado	
Componente	Controlo 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 ficheiro (escrita ou eliminação). • GNRL_EA_PARAM_2 é o caminho do ficheiro. • GNRL_EA_PARAM_3 é o nome do dispositivo. • GNRL_EA_PARAM_4 é o nome do utilizador da sessão. • GNRL_EA_PARAM_5 é a ID do hardware (HWID).
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

No available updates

Estado	
Componente	Atualização
ID de evento do Windows	1020
ID do evento do Kaspersky Security Center	000003fc
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Update distribution completed successfully

Estado	
Componente	Atualização
ID de evento do Windows	1022
ID do evento do Kaspersky Security Center	000003fe

Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Downloading files

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	1003
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

File downloaded

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	1004
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

File installed

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	1005
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

File updated

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	1006
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

File rolled back due to update error

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	1007
ID do evento do Kaspersky Security Center	–

Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Updating files

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	1008
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Distributing updates

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	1009
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Rolling back files

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	1010
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Creating the list of files to download

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	1013
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Downloading patches

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	2150
ID do evento do Kaspersky Security Center	–

Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Installing patch

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	2151
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Patch installed

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	2152
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Rolling back patch

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	2154
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Patch rolled back

Estado	ⓘ
Componente	Atualização
ID de evento do Windows	2155
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Started applying file encryption / decryption rules

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	901
ID do evento do Kaspersky Security Center	00000385

Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Finished applying file encryption / decryption rules

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	902
ID do evento do Kaspersky Security Center	00000386
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Resumed applying file encryption / decryption rules

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	905
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

File encryption / decryption started

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	910
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

File encryption / decryption completed

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	911
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

File has not been encrypted because it is an exclusion

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	913
ID do evento do Kaspersky Security Center	–

Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Portable mode enabled

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	950
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Portable mode disabled

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	952
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Device encryption / decryption started

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1301
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Device encryption / decryption completed

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1302
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Device encryption / decryption resumed

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1304
ID do evento do Kaspersky Security Center	–

Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Device is not encrypted

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1307
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Device encryption / decryption process has been switched to active mode

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1308
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Device encryption / decryption process has been switched to passive mode

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1309
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Encryption module loaded

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1310
ID do evento do Kaspersky Security Center	0000051e
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

New Authentication Agent account created

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1330
ID do evento do Kaspersky Security Center	00000532

Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Authentication Agent account deleted

Estado	
Componente	Encriptação de dados
ID de evento do Windows	1331
ID do evento do Kaspersky Security Center	00000533
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Authentication Agent account password changed

Estado	
Componente	Encriptação de dados
ID de evento do Windows	1332
ID do evento do Kaspersky Security Center	00000534
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Successful Authentication Agent login

Estado	
Componente	Encriptação de dados
ID de evento do Windows	1333
ID do evento do Kaspersky Security Center	00000535
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Failed Authentication Agent login attempt

Estado	
Componente	Encriptação de dados
ID de evento do Windows	1334
ID do evento do Kaspersky Security Center	00000536
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Hard drive accessed using the procedure of requesting access to encrypted devices

Estado	
Componente	Encriptação de dados
ID de evento do Windows	1335
ID do evento do Kaspersky Security Center	00000537

Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Failed attempt to access the hard drive using the procedure of requesting access to encrypted devices

Estado	
Componente	Encriptação de dados
ID de evento do Windows	1336
ID do evento do Kaspersky Security Center	00000538
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Account was not added. This account already exists

Estado	
Componente	Encriptação de dados
ID de evento do Windows	1337
ID do evento do Kaspersky Security Center	00000539
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Account was not modified. This account does not exist

Estado	
Componente	Encriptação de dados
ID de evento do Windows	1338
ID do evento do Kaspersky Security Center	0000053a
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Account was not deleted. This account does not exist

Estado	
Componente	Encriptação de dados
ID de evento do Windows	1339
ID do evento do Kaspersky Security Center	0000053b
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

FDE upgrade successful

Estado	
Componente	Encriptação de dados
ID de evento do Windows	1341
ID do evento do Kaspersky Security Center	0000053d

Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

FDE upgrade rollback successful

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1343
ID do evento do Kaspersky Security Center	0000053f
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Failed to uninstall Kaspersky Disk Encryption drivers from the WinRE image

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1346
ID do evento do Kaspersky Security Center	00000542
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

BitLocker recovery key was changed

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1370
ID do evento do Kaspersky Security Center	0000055a
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

BitLocker password / PIN was changed

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1371
ID do evento do Kaspersky Security Center	0000055b
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

BitLocker recovery key was saved to a removable drive

Estado	ⓘ
Componente	Encriptação de dados
ID de evento do Windows	1372
ID do evento do Kaspersky Security Center	0000055c

Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Processing of tasks from the Kaspersky Anti Targeted Attack Platform server is inactive

Estado	ⓘ
Componente	Endpoint Sensor
ID de evento do Windows	2103
ID do evento do Kaspersky Security Center	00000837
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Endpoint Sensor connected to server

Estado	ⓘ
Componente	Endpoint Sensor
ID de evento do Windows	2101
ID do evento do Kaspersky Security Center	00000835
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Connection to the Kaspersky Anti Targeted Attack Platform server restored

Estado	ⓘ
Componente	Endpoint Sensor
ID de evento do Windows	2102
ID do evento do Kaspersky Security Center	00000836
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Tasks from the Kaspersky Anti Targeted Attack Platform server are being processed

Estado	ⓘ
Componente	Endpoint Sensor
ID de evento do Windows	2104
ID do evento do Kaspersky Security Center	00000838
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Object deleted

Estado	ⓘ
Componente	Eliminar dados
ID de evento do Windows	2251
ID do evento do Kaspersky Security Center	000008cb

Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	–

Wipe task statistics

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID de evento do Windows	2853
ID do evento do Kaspersky Security Center	00000b25
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Estado	ⓘ
Componente	Eliminar dados
ID de evento do Windows	2253
ID do evento do Kaspersky Security Center	000008cd
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Object quarantined (Sandbox)

Estado	ⓘ
Componente	Sandbox
ID de evento do Windows	2602
ID do evento do Kaspersky Security Center	00000a2a
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Object deleted (Sandbox)

Estado	ⓘ
Componente	Sandbox
ID de evento do Windows	2604
ID do evento do Kaspersky Security Center	00000a2c
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

IOC Scan started

Estado	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2652
ID do evento do Kaspersky Security Center	00000a5c
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

IOC Scan completed

Estado	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2653
ID do evento do Kaspersky Security Center	00000a5d
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Object quarantined (Endpoint Detection and Response)

Estado	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2555
ID do evento do Kaspersky Security Center	000009fb
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Object deleted (Endpoint Detection and Response)

Estado	ⓘ
Componente	Endpoint Detection and Response
ID de evento do Windows	2557
ID do evento do Kaspersky Security Center	000009fd
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Application components successfully changed

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	1402
ID do evento do Kaspersky Security Center	0000057a
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Estado	ⓘ
Componente	Sandbox
ID de evento do Windows	2606
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Estado	ⓘ
Componente	Sandbox
ID de evento do Windows	2609
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Estado	ⓘ
Componente	Sandbox
ID de evento do Windows	2610
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

Estado	ⓘ
Componente	Sandbox
ID de evento do Windows	2616
ID do evento do Kaspersky Security Center	–
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	–

O Servidor de Administração ao qual o seu dispositivo está ligado está definido como fidedigno

Estado	ⓘ
Componente	Proteção da ligação do Servidor de Administração
ID de evento do Windows	3300
ID do evento do Kaspersky Security Center	00000ce4
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

O seu dispositivo está ligado ao novo Servidor de Administração fiável

Estado	ⓘ
Componente	Proteção da ligação do Servidor de Administração
ID de evento do Windows	3302
ID do evento do Kaspersky Security Center	00000ce6
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

O Servidor de Administração ao qual o seu dispositivo está ligado já não está definido como fidedigno

Estado	ⓘ
Componente	Proteção da ligação do Servidor de Administração
ID de evento do Windows	3303

ID do evento do Kaspersky Security Center	00000ce7
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Asynchronous Sandbox detection

Estado	ⓘ
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 do componente Sandbox. • GNRL_EA_PARAM_2 é o caminho do objeto. • GNRL_EA_PARAM_3 é o ID do incidente. • GNRL_EA_PARAM_4 é o hash do objeto (SHA256).
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

The scan task has been successfully sent to Sandbox by a user

Estado	ⓘ
Componente	Sandbox
ID de evento do Windows	2622
ID do evento do Kaspersky Security Center	00000a3e
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Device is connected

Estado	ⓘ
Componente	Controlo 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 a ID do hardware (HWID). • GNRL_EA_PARAM_2 é o nome do utilizador da sessão.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Device is disconnected

Estado	ⓘ
Componente	Controlo 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 a ID do hardware (HWID). • GNRL_EA_PARAM_2 é o nome do utilizador da sessão.
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Successful connection to the EDR Expert server

Estado	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID de evento do Windows	2853
ID do evento do Kaspersky Security Center	00000b25
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Ligação ao servidor de resposta do EDR Expert efetuada com êxito

Estado	ⓘ
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
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Ligação ao servidor de recolha de telemetria do EDR Expert efetuada com êxito

Estado	ⓘ
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
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Ligação ao servidor NDR efetuada com êxito

Estado	ⓘ
Componente	Network Detection and Response (KATA)
ID de evento do Windows	3083
ID do evento do Kaspersky Security Center	00000c0b
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

Starting the cloud service client application is allowed

Estado	ⓘ
Componente	Cloud Discovery
ID de evento do Windows	2210
ID do evento do Kaspersky Security Center	000008a2

Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Access to the cloud service is allowed

Estado	ⓘ
Componente	Cloud Discovery
ID de evento do Windows	2211
ID do evento do Kaspersky Security Center	000008a3
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Acesso à área protegida

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	2004
ID do evento do Kaspersky Security Center	000007d4
Windows event log (padrão)	✓
Registo de evento do Kaspersky Security Center (padrão)	✓

File or folder change was detected

Estado	ⓘ / ⚠ / ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2950
ID do evento do Kaspersky Security Center	00000b86
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

Object changes too often. Event aggregation started

Estado	ⓘ / ⚠ / ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2955
ID do evento do Kaspersky Security Center	00000b8b
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Report on object modification for the aggregation period

Estado	/ /
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2956
ID do evento do Kaspersky Security Center	00000b8c
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

Registry change was detected

Estado	/ /
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2951
ID do evento do Kaspersky Security Center	00000b87
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

Device connection / disconnection is detected

Estado	/ /
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2952
ID do evento do Kaspersky Security Center	00000b88
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

O âmbito da monitorização inclui objetos incorretos

Estado	/ /
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2903
ID do evento do Kaspersky Security Center	00000b89
Windows event log (padrão)	–

Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

Baseline created

Estado	ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2957
ID do evento do Kaspersky Security Center	00000b8d
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Baseline updated

Estado	ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2958
ID do evento do Kaspersky Security Center	00000b8e
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

An operation is performed by the trusted user

Estado	ⓘ
Componente	Monitorização da integridade do sistema
ID de evento do Windows	2962
ID do evento do Kaspersky Security Center	00000b92
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Para configurar o período de retenção deste evento, aceda à secção **Event configuration** da política e defina o período de retenção para o evento geral de Monitorização da Integridade do Sistema – *File or folder change was detected*.

Connected to SVM

Estado	ⓘ
Componente	Light Agent
ID de evento do Windows	3152
ID do evento do Kaspersky Security Center	00000c50
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

A new temporary password was created

Estado	ⓘ
Componente	Auditoria do Sistema
ID de evento do Windows	265
ID do evento do Kaspersky Security Center	00000109
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Connected to the Integration Server

Estado	ⓘ
Componente	Light Agent
ID de evento do Windows	3105
ID do evento do Kaspersky Security Center	00000c21
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Restoring connection to the Integration Server

Estado	ⓘ
Componente	Light Agent
ID de evento do Windows	3104
ID do evento do Kaspersky Security Center	00000c20
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Ligação ao servidor da KUMA efetuada com êxito

Estado	ⓘ
Componente	Integração KUMA
ID de evento do Windows	2857
ID do evento do Kaspersky Security Center	00000b29
Windows event log (padrão)	–
Registo de evento do Kaspersky Security Center (padrão)	✓

Anexo 7. Extensões de ficheiros suportadas para a prevenção da execução

O Kaspersky Endpoint Security suporta a prevenção da abertura de ficheiros do formato do Office em determinadas aplicações. A informação sobre as aplicações e extensões de ficheiros suportadas encontra-se na seguinte tabela.

Extensões de ficheiros suportadas para a prevenção da execução

Nome da aplicação	Ficheiro executável	Estensão do ficheiro
Microsoft Word	winword.exe	rtf doc dot 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

Anexo 8. Interpretadores de script suportados para Prevenção da execução

A prevenção da execução suporta os seguintes interpretadores 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 da execução suporta o trabalho com aplicações Java no ambiente de tempo de execução Java (processos java.exe e javaw.exe).

Anexo 9. Âmbito de verificação IOC no registo (RegistryItem)

Quando adiciona o tipo de dados **Windows registry - RegistryItem** ao âmbito de verificação IOC, o Kaspersky Endpoint Security verifica as seguintes chaves de registo por defeito:

```
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
```

Anexo 10. Requisitos para IOC file

Ao criar tarefas de Verificação IOC, tenha em consideração os seguintes requisitos para IOC file e limitações:

- A aplicação suporta ficheiros IOC com as extensões IOC e XML nas versões 1.0 e 1.1 do padrão aberto OpenIOC para a descrição dos indicadores de comprometimento.
- Após carregar os ficheiros IOC, pode editá-los manualmente no editor integrado diretamente nas propriedades da tarefa. O Kaspersky Endpoint Security suporta a edição de ficheiros IOC compatíveis com o padrão OpenIOC 1.1. Não é possível modificar o conteúdo de ficheiros IOC compatíveis com a versão 1.0 do OpenIOC.
- Se durante a criação da tarefa *IOC Scan* na linha de comandos tiver carregado IOC files (alguns dos quais não são suportados), a aplicação utiliza apenas os IOC files suportados ao executar a tarefa. Se durante a criação da tarefa *IOC Scan* na linha de comandos, todos os IOC files que carregar se revelarem não serem suportados, a tarefa continuará a poder ser executada, mas não serão detetados quaisquer indicadores de compromisso. Não é possível carregar ficheiros IOC não suportados utilizando a Consola Web ou a Cloud Console.
- Os erros semânticos e as etiquetas e os termos IOC não suportados em IOC files não levam à falha na execução da tarefa. Em tais secções de IOC files, a aplicação não deteta qualquer correspondência.
- Os identificadores de todos os IOC files utilizados numa única tarefa Verificação IOC devem ser únicos. Se existirem IOC files com o mesmo identificador, tal pode afetar os resultados da execução da tarefa.
- Um único IOC file não deve exceder 2 MB. A utilização de ficheiros maiores irá fazer com que as tarefas Verificação IOC terminem com um erro. O tamanho total de todos os ficheiros adicionados à coleção IOC não deve exceder os 10 MB. Se o tamanho total de todos os ficheiros exceder 10 MB, terá de dividir a coleção IOC e criar várias tarefas *IOC Scan*.

- É recomendado criar um IOC file por ameaça. Tal facilita a análise dos resultados da tarefa *IOC Scan*.

O ficheiro que transfere através da ligação abaixo contém uma tabela com a lista completa dos termos IOC do padrão OpenIOC.

TRANSFERIR O FICHEIRO IOC_TERMS.XLSX

As funcionalidades e limitações de suporte da aplicação para o padrão OpenIOC são apresentadas na seguinte tabela.

Funcionalidades e limitações de suporte para OpenIOC versão 1.0 e 1.1.

Condições suportadas	OpenIOC 1.0:
	
	`is`
	`isnot` (como uma exceção do conjunto)
	`contains`
	`containsnot` (como uma exceção do conjunto)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	
	Para termos Email/*, são suportadas apenas as condições `contains` e `is`. Para que a Verificação retrospetiva dos IOC funcione corretamente ao usar a condição `is`, os endereços de e-mail nos ficheiros IOC têm de ser especificados no seguinte formato: `"name@example.org" <SMTP:name@example.org>`. Ao executar a tarefa *Verificação IOC* normalmente, basta especificar o endereço de e-mail no seguinte formato: `name@example.org`.

Atributos da condição suportados	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Operadores suportados	`AND` `OR`
Tipos de dados suportados	`"date"`: data (condições aplicáveis: `is`, `greater-than`, `less-than`) `"int"`: número inteiro (condições aplicáveis: `is`, `greater-than`, `less-than`) `"string"`: cadeia (condições aplicáveis: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: duração em segundos (condições aplicáveis: `is`, `greater-than`, `less-than`)

Funcionalidades da interpretação de tipos de dados	Os tipos de dados `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"` e `"base64Binary"` são interpretados como uma cadeia.
	
	A aplicação suporta a interpretação do campo `Content` para os tipos de dados `int` e `date` sempre que seja apresentado na forma de intervalos:
	
	OpenIOC 1.0:
	Utilizar o operador `TO` no campo `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	Utilizar as condições `greater-than` e `less-than`
	Utilizar o operador `TO` no campo `Content`
	A aplicação suporta a interpretação dos tipos de dados `date` e `duration`, se os indicadores estiverem definidos no formato `ISO 8601, Zulu time zone, UTC`.

Anexo 11. API para Resposta a Ameaças EDR

O Kaspersky Endpoint Security 12.9 for Windows apresenta suporte de ações de Resposta a Ameaças EDR (EDR responses) utilizando uma OpenAPI do Kaspersky Security Center. Ou seja, pode invocar métodos OpenAPI para automatizar a resposta a ameaças de EDR utilizando o Python. Pode invocar estes métodos quando integrados com soluções SIEM. A *Kaspersky Unified Monitoring and Analysis Platform*, a solução Kaspersky SIEM, suporta a OpenAPI de Resposta a Ameaças 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, tem de criar um pedido e enviá-lo utilizando a KSC Open API (`AddIncident`). Após o processamento do pedido, é criada uma tarefa especial na consola do Kaspersky Security Center.

Para criar tarefas ao responder a ameaças EDR, tem de estabelecer uma ligação em segundo plano entre o Servidor de Administração e a Consola Web do Kaspersky Security Center. O serviço de ligação em segundo plano está disponível no Kaspersky Security Center Windows 14.2 ou posterior e no Kaspersky Security Center Linux 15.2 ou posterior. Não são suportadas outras consolas, incluindo consolas de soluções do Kaspersky Detection and Response.

Para o EDR Threat Response, tem de especificar parâmetros básicos de pedido, por exemplo, no formato JSON:

- `task` é o tipo da tarefa (veja abaixo).
- `targetHost` é o ID do computador no qual o script tem de ser executado. Argumento obrigatório. O script obtém este argumento do evento.
- `responseEventIncidentArea` é o nome da aplicação que executou o script (por exemplo, `KUMA`). Este parâmetro é adicionado ao nome da tarefa criada.

Para configurar a Resposta à Ameaça EDR, tem de especificar as definições da tarefa no formato JSON no parâmetro `"KLINCDT_BODY": json.dumps(data)`. Como resultado, a aplicação cria o `[Response][KUMA] <task type> - <Date> <Time> - <ID>` na consola do Kaspersky Security Center.

Ligação à OpenAPI do Kaspersky Security Center

Como parte do EDR Threat Response, a aplicação cria tarefas especiais na consola do Kaspersky Security Center. A criação destas tarefas requer o estabelecimento de uma ligação entre o computador e o Kaspersky Security Center. Para o fazer, os parâmetros de ligação do Kaspersky Security Center têm de ser especificados no pedido.

Na versão 2.1 do Kaspersky XDR, o método de autorização de pedidos foi alterado. O Kaspersky XDR utiliza tokens PAT, em vez de autenticação por nome de utilizador e password. Portanto, não é possível executar scripts no Kaspersky XDR. Para obter mais informações sobre a autorização de pedidos, consulte a Ajuda do Kaspersky XDR.

Parâmetros de ligação do Kaspersky Security Center

Parâmetro	Tipo	Descrição
`kscHost`	`string`	Endereço do Servidor de Administração do Kaspersky Security Center. Parâmetro obrigatório.
`kscPort`	`int`	Porta da ligação do Servidor de Administração. Parâmetro obrigatório.
`kscCert`	`string`	Caminho para um ficheiro de certificado para ligação ao Servidor de Administração do Kaspersky Security Center. Por defeito, o parâmetro está definido para `False`.
`kscUser`	`string`	Credenciais da conta do utilizador. Parâmetro obrigatório.
`kscPassword`	`string`	Password da conta do utilizador. 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 utilizador não estão protegidos, pelo que precisa de dedicar um utilizador separado que será utilizado apenas para executar estas ações.

Obter ficheiro – getFile

Definições de tarefa Obter ficheiro

Parâmetro	Tipo	Descrição
md5hash	string	Hash MD5 do ficheiro que deseja obter.
sha256hash	string	Hash SHA256 do ficheiro que deseja obter.
path	string	Caminho para o ficheiro que 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;
};
```

Eliminar ficheiro – deleteFile

Definições de tarefa Eliminar ficheiro

Parâmetro	Tipo	Descrição
md5hash	string	Hash MD5 do ficheiro que deseja eliminar.
sha256hash	string	Hash SHA256 do ficheiro que deseja eliminar.
path	string	Caminho para o ficheiro que deseja eliminar.
searchInSubfolders?	boolean	Procure o ficheiro que deseja eliminar 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 ficheiro para a Quarentena – quarantineFile

Definições de tarefa Mover ficheiro para a Quarentena

Parâmetro	Tipo	Descrição
md5hash	string	Hash MD5 do ficheiro que deseja colocar em quarentena.
sha256hash	string	Hash SHA256 do ficheiro que deseja colocar em quarentena.
path	string	Caminho para o ficheiro que 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 IOC – iocScan

Definições de tarefa Verificação IOC

Parâmetro	Tipo	Descrição
ioc	string	Caminho para o Arquivo Zip com um ficheiro IOC que deseja utilizar para a verificação.
isolateHost	boolean	Isole o computador da rede quando um indicador de comprometimento for detetado para evitar que a ameaça se espalhe.
scanCriticalAreas	boolean	Execute a tarefa *Verificação de Áreas Críticas* quando um indicador de comprometimento for detetado.
quarantineObject	boolean	Elimine o objeto malicioso quando um indicador de comprometimento for detetado. Antes de eliminar o objeto, o Kaspersky Endpoint Security cria uma cópia de segurança, caso o objeto precise de ser posteriormente restaurado. O Kaspersky Endpoint Security move a cópia de segurança 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

Definições de tarefa Iniciar processo

Parâmetro	Tipo	Descrição
executablePath	string	Caminho para o ficheiro 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;
};
```

Terminar processo – terminateProcess

Definições de tarefa Terminar processo

Parâmetro	Tipo	Descrição
md5hash	string	Hash MD5 do ficheiro cujo processo deseja encerrar.
sha256hash	string	Hash SHA256 do ficheiro cujo processo deseja encerrar.
path	string	Caminho para o ficheiro que deseja eliminar.
caseSensitive	boolean	Diferenciação de maiúsculas e minúsculas ao pesquisar o ficheiro.

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 da rede do computador – isolateHost

Definições do isolamento da rede do computador

Parâmetro	Tipo	Descrição
`action`	`string`	Modo de funcionamento de Isolamento da rede.

Exemplo

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

Prevenção da execução – preventExecution

Definições da prevenção da execução

Parâmetro	Tipo	Descrição
`hash`	`string`	Hash MD5 do ficheiro cuja execução deseja impedir.
`path`	`string`	Caminho para o ficheiro cuja execução deseja impedir.
`caseSensitive`	`boolean`	Diferenciação de maiúsculas e minúsculas ao pesquisar o ficheiro.

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 software malicioso – onDemandScan

Definições de tarefa Verificação de software malicioso

Parâmetro	Tipo	Descrição
`path`	`string`	Lista delimitada por espaços de ficheiros e pastas para Verificação Personalizada.
`recursive`	`boolean`	Modo de verificação recursiva.

Parâmetro	Tipo	Descrição
type	number	Âmbito de 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;
};
```

Anexo 12. Contas de utilizador em regras de componentes de aplicação

Para configurar alguns componentes da aplicação, tem de adicionar regras especiais. Por exemplo, para o Controlo de Internet, tem de adicionar uma regra com uma lista de endereços da Internet que pretende que a aplicação bloqueie. Nas regras de componentes da aplicação, também pode configurar um calendário para o componente ou selecionar utilizadores para os quais a aplicação tem de aplicar a regra.

Têm de ser adicionadas regras para configurar os seguintes componentes da aplicação:

- Controlo das aplicações.
- Controlo de Internet.
- Controlo de Dispositivos.
- Inspeção do Registo.
- Controlo de Anomalias Adaptativo.
- Monitorização da integridade do sistema.

A partir do Kaspersky Endpoint Security for Windows 12.5, pode selecionar utilizadores não só a partir do Active Directory, mas também a partir da lista de utilizadores no Kaspersky Security Center. Também pode introduzir manualmente os dados da conta de utilizador local. Isto significa que pode adicionar utilizadores das seguintes formas:

- Active Directory (recomendado)
- Lista de utilizadores no Kaspersky Security Center
- Conta de utilizador local

Para empregar corretamente todos os métodos de seleção de utilizadores, tem de atualizar a aplicação Kaspersky Endpoint Security e o plug-in de gestão para a versão 12.5 ou superior.

A Kaspersky recomenda o uso de contas de utilizador locais apenas em casos especiais, quando não é possível utilizar contas de utilizador do domínio. Para obter detalhes sobre os riscos de segurança da utilização de contas locais, consulte a Base de Dados de Conhecimento da Microsoft. O utilizador é totalmente responsável pela segurança de um computador se forem usadas contas de utilizador locais; em particular, isto inclui a responsabilidade de controlar e restringir o acesso às definições do Kaspersky Endpoint Security.

A aplicação utiliza o SID (Identificador de Segurança) do utilizador para identificar os utilizadores. Ao usar contas de utilizador do Active Directory ou da lista de utilizadores do Kaspersky Security Center, a aplicação determina o SID no Servidor de Administração. Isto significa que a aplicação não coloca carga adicional no computador para identificar um utilizador. Se tiver adicionado mais de 1000 contas de utilizador locais a uma regra de aplicação, as aplicações contactam o controlador de domínio para identificar o utilizador. Isto significa que a carga no computador é maior. Para otimizar o impacto do desempenho no computador, recomendamos a utilização de contas de utilizador do Active Directory ou da lista de utilizadores do Kaspersky Security Center.

A aplicação utiliza nomes NetBIOS para identificação de contas de utilizador 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, a aplicação não consegue identificar o utilizador. Então a aplicação desativa a regra e gera um erro, por exemplo, *Web Control: rule triggering disabled for user accounts without matching security identifier (SID)*. Para que a regra funcione, deve encurtar manualmente o nome do computador. Pode adicionar contas de utilizador do Active Directory ou do Kaspersky Security Center. Neste caso, a aplicação encurta automaticamente o nome do computador.

O Kaspersky Endpoint Security também suporta utilizadores e grupos integrados (como o grupo "Todos") em regras. Devido à forma como o SID de um utilizador é determinado, a aplicação permite utilizar apenas contas de utilizador integradas adicionadas a partir do Active Directory ou da lista de utilizadores no Kaspersky Security Center. Regras nas quais uma conta de utilizador interna é adicionada localmente não funcionam.

Informações legais

Fornecimento de dados

Esta secção contém informações sobre os dados que a aplicação do Kaspersky Endpoint Security pode armazenar no dispositivo e transmitir automaticamente à Kaspersky durante o seu funcionamento.

A informação recebida está protegida pela Kaspersky conforme a lei e os requisitos, bem como as regulamentações aplicáveis da Kaspersky. Os dados são transmitidos através der canais de comunicação encriptados.

Fornecimento de dados ao abrigo do Contrato de Licença do Utilizador Final

Se for aplicado um código de ativação para ativar o Kaspersky Endpoint Security, o utilizador aceita transmitir, periodicamente, a seguinte informação, de forma automática, para efeitos de verificar a utilização correta da aplicação:

- 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 operativo, e nome do ambiente virtual (se o Kaspersky Endpoint Security estiver instalado num ambiente virtual);
- ID do pedido exclusivo para os serviços do Titular dos Direitos;
- ID dos componentes do Kaspersky Endpoint Security que estejam ativos quando a informação é transmitida.

A Kaspersky também pode utilizar esta informação para criar estatísticas sobre a disseminação e utilização de software da Kaspersky.

Com a utilização de um código de ativação, aceita transmitir automaticamente os dados indicados acima. Se não aceitar transmitir esta informação à Kaspersky, deve utilizar um ficheiro-chave para ativar o Kaspersky Endpoint Security.

Ao aceitar os termos do Contrato de Licença do Utilizador Final, aceita transmitir automaticamente a seguinte informação:

- Quando atualizar o Kaspersky Endpoint Security:
  - versão do Kaspersky Endpoint Security;
  - ID do Kaspersky Endpoint Security;

- chave ativa;
- ID única do início da tarefa de atualização;
- ID única da instalação do Kaspersky Endpoint Security.

- Ao seguir ligações a partir da interface do Kaspersky Endpoint Security:
  - versão do Kaspersky Endpoint Security;
  - versão do sistema operativo;
  - Data de ativação do Kaspersky Endpoint Security;
  - data de validade da licença;
  - data de criação da chave;
  - Data de instalação do Kaspersky Endpoint Security;
  - ID do Kaspersky Endpoint Security;
  - ID da vulnerabilidade detetada no sistema operativo;
  - ID da última atualização instalada do Kaspersky Endpoint Security;
  - hash do ficheiro detetado com uma ameaça, de acordo com a classificação da Kaspersky;
  - Categoria do erro de ativação do Kaspersky Endpoint Security;
  - Código de erro de ativação do Kaspersky Endpoint Security;
  - número de dias até expiração da chave;
  - número de dias decorridos desde o acréscimo da chave;
  - número de dias decorridos desde que a licença expirou;
  - número de computadores em que a licença atual é aplicada;
  - chave ativa;
  - Validade da licença do Kaspersky Endpoint Security;
  - estado atual da licença;
  - tipo de licença atual;
  - tipo de aplicação;
  - ID única do início da tarefa de atualização;
  - ID única da instalação do Kaspersky Endpoint Security no computador;
  - Idioma da interface do Kaspersky Endpoint Security.

A informação recebida está protegida pela Kaspersky conforme a lei e os requisitos, bem como as regulamentações aplicáveis da Kaspersky. Os dados são transmitidos através der canais de comunicação encriptados.

Leia o Contrato de Licença do Utilizador Final e visite o site da Kaspersky para obter mais informações sobre a recebe, processamento, armazenamento e eliminação de informações sobre a utilização das aplicações, após aceitar o Contrato de Licença do Utilizador Final e aceitar a Declaração de Recolha de Dados da KSN. Os ficheiros license.txt e ksn_<ID do idioma>.txt contêm o texto do Contrato de Licença do Utilizador Final e a Declaração de Recolha de Dados da KSN está incluída no kit de distribuição da aplicação.

Fornecimento de dados ao utilizar a Kaspersky Security Network

O conjunto de dados que o Kaspersky Endpoint Security envia à Kaspersky depende do tipo de licença e das definições de utilização da Kaspersky Security Network.

Utilização da KSN sob licença num máximo de 4 computadores

Ao aceitar a Declaração de Recolha de Dados da KSN, aceita transmitir automaticamente a seguinte informação:

- informação sobre as atualizações da configuração KSN: identificador da configuração ativa, identificador da configuração recebida, código de erro da atualização da configuração;
- informação sobre os ficheiros e endereços URL a verificar: somas de verificação do ficheiro verificado (MD5, SHA2-256, SHA1) e padrões de ficheiro (MD5), o tamanho do padrão, tipo de ameaça detetada e o seu nome de acordo com a classificação do Titular do Direito, identificador para as bases de dados de antivírus, endereço URL para o qual está a ser solicitada a reputação, bem como o endereço URL da referência, o identificador do protocolo da ligação e o número da porta que está a ser utilizada;
- ID da tarefa de verificação que detetou a ameaça;
- informação sobre certificados digitais que estão a ser utilizados, necessária para verificar a sua autenticidade: as somas de verificação (SHA256) do certificado utilizado para assinar o objeto verificado e a chave pública do certificado;
- identificador do componente do software que está a realizar a verificação;
- IDs das bases de dados de antivírus e os registos nestas bases de dados de antivírus;
- informação sobre a ativação do software no computador: cabeçalho assinado do pedido do serviço de ativação (identificador do centro de ativação regional, soma de verificação do código de ativação, soma de verificação do pedido, data de criação do pedido, identificador único do pedido, versão do pedido, estado da licença, data e hora de início/fim da validade do pedido, identificador único da licença, versão da licença), identificador do certificado utilizado para assinar o cabeçalho do pedido, soma de verificação (MD5) do ficheiro-chave;
- informação sobre o Software do Titular do Direito: versão completa, tipo, versão do protocolo utilizado para estabelecer a ligação aos serviços da Kaspersky.

Uso da KSN sob licença em 5 ou mais computadores

Ao aceitar a Declaração de Recolha de Dados da KSN, aceita transmitir automaticamente a seguinte informação:

Se a caixa de verificação **Kaspersky Security Network** estiver selecionada e a caixa de verificação **Ativar o modo KSN alargado** for desmarcada, a aplicação envia as seguintes informações:

- informação sobre as atualizações da configuração KSN: identificador da configuração ativa, identificador da configuração recebida, código de erro da atualização da configuração;
- informação sobre os ficheiros e endereços URL a verificar: somas de verificação do ficheiro verificado (MD5, SHA2-256, SHA1) e padrões de ficheiro (MD5), o tamanho do padrão, tipo de ameaça detetada e o seu nome de acordo com a classificação do Titular do Direito, identificador para as bases de dados de antivírus, endereço URL para o qual está a ser solicitada a reputação, bem como o endereço URL da referência, o identificador do protocolo da ligação e o número da porta que está a ser utilizada;
- ID da tarefa de verificação que detetou a ameaça;
- informação sobre certificados digitais que estão a ser utilizados, necessária para verificar a sua autenticidade: as somas de verificação (SHA256) do certificado utilizado para assinar o objeto verificado e a chave pública do certificado;
- identificador do componente do software que está a realizar a verificação;
- IDs das bases de dados de antivírus e os registos nestas bases de dados de antivírus;
- informação sobre a ativação do software no computador: cabeçalho assinado do pedido do serviço de ativação (identificador do centro de ativação regional, soma de verificação do código de ativação, soma de verificação do pedido, data de criação do pedido, identificador único do pedido, versão do pedido, estado da licença, data e hora de início/fim da validade do pedido, identificador único da licença, versão da licença), identificador do certificado utilizado para assinar o cabeçalho do pedido, soma de verificação (MD5) do ficheiro-chave;
- informação sobre o Software do Titular do Direito: versão completa, tipo, versão do protocolo utilizado para estabelecer a ligação aos serviços da Kaspersky.

Se a caixa de verificação **Ativar o modo KSN alargado** estiver selecionada juntamente com a caixa de verificação **Kaspersky Security Network**, além da informação indicada acima, a aplicação enviará também as seguintes informações:

- informação sobre os resultados da categorização dos recursos Web solicitados, que contém o URL processado e o endereço IP do anfitrião, a versão do componente do software que realizou a categorização, o método de categorização e o conjunto de categorias definidas para o recurso Web;
- informação sobre o software instalado no computador: nome das aplicações do software e fornecedores de software, chaves de registo e os seus valores, informação sobre os ficheiros dos componentes do software instalado (somas de verificação(MD5, SHA2-256, SHA1), nome, caminho até ao ficheiro no computador, tamanho, versão e assinatura digital);
- informação sobre o estado da proteção antivírus do Computador: as versões e os carimbos de data/hora de lançamento das bases de dados de antivírus utilizadas, a ID da tarefa e a ID do Software que executa a verificação;

- informação sobre os ficheiros que estão a ser transferidos pelo Utilizador Final: os endereços URL e IP da transferência e as páginas de transferência, identificador do protocolo da transferência e o número da porta de ligação, o estado dos URL como sendo maliciosos ou não, atributos do ficheiro, tamanho e somas de verificação (MD5, SHA2-256, SHA1), informação sobre o processo que transferiu o ficheiro, (somas de verificação (MD5, SHA2-256, SHA1), data e hora de criação/compilação, estado da reprodução automática, atributos, nomes dos packers, informação sobre as assinaturas, sinalizador do ficheiro executável, identificador do formato e entropia), nome do ficheiro e o seu caminho no computador, a assinatura digital do ficheiro e o carimbo de data/hora da sua geração, o endereço URL onde ocorreu a deteção, o número do script na página que parece ser suspeito ou malicioso, informação sobre os pedidos HTTP gerados e a resposta aos mesmos;

- informação sobre as aplicações em execução e os seus módulos: dados sobre os processos em execução no sistema (ID do processo (PID), nome do processo, informação sobre a conta onde foi iniciado o processo, a aplicação e comando que iniciaram o processo, o sinal do programa ou processo fiável, o caminho completo até aos ficheiros do processo e às suas somas de verificação (MD5, SHA2-256, SHA1), e a linha inicial do comando, nível de integridade do processo, uma descrição do produto ao qual pertence o processo (o nome do produto e informação sobre o editor), bem como certificados digitais que estão a ser utilizados e informação necessária para verificar a sua autenticidade ou informação sobre a ausência da assinatura digital de um ficheiro) e informação sobre os módulos carregados nos processos (os seus nomes, tamanhos, tipos, datas de criação, atributos, somas de verificação (MD5, SHA2-256, SHA1), os caminhos até eles no computador), informação do cabeçalho do ficheiro PE, nomes dos packers (se o ficheiro tiver sido empacotado);

- informação sobre todos os objetos e atividades potencialmente maliciosos: nome do objeto detetado e caminho completo para o objeto no computador, somas de verificação de ficheiros processados (MD5, SHA2-256, SHA1), data e hora da deteção, nomes e tamanhos dos ficheiros infetados e respetivos caminhos, código do modelo do caminho, sinal de ficheiro executável, indicador de se o objeto é um contentor, nomes do programa de compressão (caso o ficheiro tenha sido comprimido), código do tipo de ficheiro, ID do formato do ficheiro, lista de ações realizadas pelo software malicioso e a decisão tomada pelo software e utilizador em resposta, ID das bases de dados de antivírus e dos registros nesses bases de dados de antivírus utilizadas para tomar a decisão, indicador de um objeto potencialmente malicioso, o nome da ameaça detetada de acordo com a classificação do titular dos direitos, o nível de perigo, o estado e método de deteção, motivo para inclusão no contexto analisado e número de sequência do ficheiro no contexto, somas de verificação (MD5, SHA2-256, SHA1), o nome e atributos do ficheiro executável da aplicação através da qual a mensagem ou ligação infetada foi transmitida, endereços IP despersonalizados (IPv4 e IPv6) do anfitrião do objeto bloqueado, entropia do ficheiro, indicador de execução automática do ficheiro, hora a que o ficheiro foi detetado pela primeira vez no sistema, o número de vezes que o ficheiro foi executado desde o envio das últimas estatísticas, informação sobre o nome, somas de verificação (MD5, SHA2-256, SHA1) e tamanho do cliente de e-mail através do qual o objeto malicioso foi recebido, ID da tarefa do software que realizou a verificação, indicador de se a reputação ou assinatura do ficheiro foi verificada, resultado do processamento do ficheiro, soma de verificação (MD5) do padrão recolhido para o objeto, o tamanho do padrão em bytes e as especificações técnicas das tecnologias de deteção aplicadas;

- informação sobre os objetos verificados: o grupo fiável atribuído no qual e/ou a partir do qual o ficheiro foi colocado, o motivo pelo qual o ficheiro foi colocado nessa categoria, identificador da categoria, informação sobre a origem das categorias e a versão da base de dados da categoria, o sinalizador do certificado fiável do ficheiro, nome do fornecedor do ficheiro, versão do ficheiro, nome e versão da aplicação do software que inclui o ficheiro;

- informação sobre vulnerabilidades detetadas: a ID da vulnerabilidade na base de dados de vulnerabilidades, a classe de perigo da vulnerabilidade;

- informação sobre a emulação do ficheiro executável: tamanho do ficheiro e as suas somas de verificação (MD5, SHA2-256, SHA1), a versão do componente de emulação, profundidade de emulação, um conjunto de propriedades de blocos lógicos e funções nos blocos lógicos obtidas durante a emulação, dados dos cabeçalhos PE do ficheiro executável;

- os endereços IP do computador atacante (IPv4 e IPv6), o número da porta no computador à qual está direcionado o ataque de rede, identificador do protocolo do pacote IP que contém o ataque, o alvo do ataque (nome da organização, site), sinalizador para a reação ao ataque, o peso do ataque, nível de fiabilidade;

- informação sobre ataques associados a recursos da rede falsificados, os endereços DNS e IP (IPv4 ou IPv6) de sites visitados.

- Endereços DNS e IP (IPv4 ou IPv6) do recurso da Internet solicitado, informação sobre o ficheiro e/ou cliente Web que acede ao recurso da Internet, nome, tamanho e somas de verificação (MD5, SHA2-256 e SHA1) do ficheiro, caminho completo do ficheiro e código do modelo do ficheiro, resultado da verificação da assinatura digital e respetivo estado na KSN;

- informação sobre a reversão de ações de software malicioso: dados sobre o ficheiro cuja atividade foi revertida [nome do ficheiro, caminho completo do ficheiro, respetivo tamanho e somas de verificação (MD5, SHA2-256 e SHA1)], dados sobre ações bem e malsucedidas para eliminar, mudar o nome e copiar ficheiros e restaurar os valores no registo (nomes das chaves de registo e respetivos valores), e informação sobre os ficheiros do sistema modificados pelo software malicioso, antes e depois da reversão;

- informação sobre as exclusões definidas para o componente do Controlo de Anomalias Adaptativo: a ID e o estado da regra que foi acionada, a ação realizada pelo software quando a regra foi acionada, o tipo de conta de utilizador ao abrigo da qual o processo ou thread realiza a atividade suspeita, informação sobre o processo que realizou ou foi sujeito à atividade suspeita (ID do script ou nome do ficheiro do processo, caminho completo para o ficheiro do processo, código do modelo do caminho, somas de verificação (MD5, SHA2-256, SHA1) do ficheiro do processo); informação sobre o objeto que realizou as ações suspeitas bem como sobre o objeto que foi sujeito às ações suspeitas (nome da chave de registo ou nome do ficheiro, caminho completo até ao ficheiro, código do modelo do caminho e as somas de verificação (MD5, SHA2-256, SHA1) do ficheiro).

- informação sobre módulos de software carregados: nome, tamanho e somas de verificação (MD5, SHA2-256, SHA1) do ficheiro do módulo, caminho completo do mesmo e o código do modelo do caminho, definições da assinatura digital do ficheiro do módulo, data e hora da criação da assinatura, nome do sujeito e organização que assinaram o ficheiro do módulo, ID do processo em que o módulo foi carregado, nome do fornecedor do módulo e o número da sequência do módulo na fila para carregamento;

- informação sobre a qualidade da interação do software com os serviços KSN: data e hora de início e fim do período no qual foram geradas as estatísticas, informação sobre a qualidade dos pedidos e ligação a cada um dos serviços KSN utilizados (ID do serviço KSN, número de pedidos com êxito, número de pedidos com respostas da memória intermédia, número de pedidos sem êxito (problemas da rede, KSN desativado nas definições do software, encaminhamento incorreto), propagação do tempo dos pedidos com êxito, propagação do tempo dos pedidos cancelados, propagação do tempo dos pedidos com limite de tempo excedido, número de ligações a KSN retiradas da memória intermédia, número de ligações com êxito ao KSN, número de ligações sem êxito ao KSN, número de transações com êxito; Número de transações sem êxito, propagação do tempo das ligações com êxito ao KSN, propagação do tempo das ligações sem êxito ao KSN, propagação do tempo das transações com êxito, propagação do tempo as transações sem êxito);

- se for detetado um objeto potencialmente malicioso, a informação é fornecida sobre os dados na memória dos processos: elementos da hierarquia do objeto do sistema (ObjectManager), dados na memória UEFI BIOS, nomes das chaves de registo e os seus valores;

- informação sobre eventos nos registos de sistemas: data e hora do evento, nome do início de sessão em que o evento foi detetado, tipo e categoria do evento, nome da origem do evento e respetiva descrição;

- informação sobre ligações de rede: versão e somas de verificação (MD5, SHA2-256, SHA1) do ficheiro a partir do qual foi iniciado um processo que abriu a porta, caminho do ficheiro do processo e respetiva assinatura digital, endereços IP local e remoto, números das portas de ligação local e remota, estado da ligação e data e hora de abertura da porta;

- informação sobre a data de instalação e ativação do software no computador: a ID do parceiro que vendeu a licença, o número de série da licença, o cabeçalho assinado do pedido do serviço de ativação (a ID de um centro de ativação regional, a soma de verificação do código de ativação, a soma de verificação do pedido, a data de criação do pedido, a ID única do pedido, a versão do pedido, o estado da licença, a data e hora de início/fim do pedido, a ID única da licença, a versão da licença), a ID do certificado utilizado para assinar o cabeçalho do pedido, a soma de verificação (MD5) do ficheiro de chave, a ID única de instalação do software no computador, o tipo e ID da aplicação que é atualizada, a ID da tarefa de atualização;

- informação sobre o conjunto de todas as atualizações instaladas e o conjunto das atualizações mais recentemente instaladas/removidas, o tipo de evento que originou o envio da informação da atualização, duração desde a instalação da última atualização, informação sobre as bases de dados de antivírus atualmente instaladas;

- informação sobre o funcionamento do software no computador: dados sobre a utilização da CPU, dados sobre a utilização da memória (bytes privados, bloco não paginado, bloco paginado), número de threads ativos no processo do software e de threads pendentes, e a duração do funcionamento do software antes do erro;

- número de descargas do software e do sistema (BSOD) desde que o software foi instalado e desde a última atualização, o identificador e a versão do módulo do software em que a anomalia ocorreu, a pilha de memória no processo do software e informação sobre as bases de dados de antivírus quando a anomalia ocorreu;

- dados na descarga do sistema (BSOD): um sinalizador a indicar a ocorrência do BSOD o computador, o nome do controlador que causou o BSOD, o endereço e pilha de memória no controlador, um sinalizador a indicar a duração da sessão OS antes da ocorrência do BSOD, pilha de memória do controlador que teve a anomalia, tipo de descarga de memória armazenado, sinalizador da sessão OS antes do BSOD ter durado mais de 10 minutos, identificador único da descarga, carimbo de data e hora do BSOD;

- informação sobre erros ou problemas de desempenho que tenham ocorrido durante a operação dos componentes do software: a ID do estado do software, tipo de erro, código e causa bem como a hora à qual o erro ocorreu, as IDs do componente, módulo e processo do produto no qual o erro ocorreu, a ID da tarefa ou categoria da atualização durante a qual o erro ocorreu, registos (logs) de controladores utilizados pelo software (código do erro, nome do módulo, nome do ficheiro fonte e a linha na qual o erro ocorreu);

- informação sobre as atualizações das bases de dados de antivírus e componentes do software: o nome, data e hora dos ficheiros de índice durante a última atualização e que estão a ser transferidos durante a atual atualização;

- informação sobre a terminação anómala da operação do software: o carimbo de data e hora da descarga, o seu tipo, o tipo de evento que causou a terminação anómala da operação do software (desativação inesperada, anomalia de uma aplicação de terceiros), data e hora da desativação inesperada;

- informação sobre a compatibilidade dos controladores do software com hardware e software: informação sobre propriedades do SO que restringem a funcionalidade dos componentes do software (Secure Boot, KPTI, WHQL Enforce, BitLocker, Case Sensitivity), tipo de software de transferência instalado (UEFI, BIOS), identificador do Módulo da Plataforma fiável (TPM), versão de especificação do TPM, informação sobre a CPU instalada no computador, modo operacional e parâmetros do Code Integrity e Device Guard, modo operacional dos controladores e motivo da utilização do modo atual, versão dos controladores do software, estado do suporte da virtualização do software e hardware do computador;

- informação sobre aplicações de terceiros que causaram o erro: nome, versão e localização, código do erro e informação sobre o mesmo proveniente do registo de aplicações do sistema, endereço do erro e pilha de memória da aplicação de terceiros, sinalizador a indicar a ocorrência do erro no componente do software, período de tempo em que a aplicação de terceiros funcionou antes do erro, somas de verificação (MD5, SHA2-256, SHA1) da imagem do processo da aplicação em que o erro ocorreu, caminho para a imagem do processo da aplicação e código do modelo do caminho, informação proveniente do registo do sistema com uma descrição do erro associado à aplicação, informação sobre o módulo da aplicação em que o erro ocorreu (identificador da exceção, endereço da memória da anomalia como um desvio no módulo da aplicação, nome e versão do módulo, identificador da anomalia da aplicação no plug-in do Titular do Direito e pilha de memória da anomalia, duração da sessão da aplicação antes da anomalia);

- versão do componente atualizador do software, número de anomalias do componente atualizador enquanto estava a executar as tarefas de atualização ao longo da vida útil do componente, ID do tipo de tarefa de atualização, número de tentativas falhas do componente atualizador para completar as tarefas de atualização;

- informação sobre a operação dos componentes de monitorização do sistema do software: versões completas dos componentes, data e hora às quais os componentes foram iniciados, código do evento que transbordou da fila de eventos e o número de tais eventos, o número total de transbordos da fila de eventos, informação sobre o ficheiro do processo que iniciou o evento (nome do ficheiro e respetivo caminho no computador, código do modelo do caminho, somas de verificação (MD5, SHA2-256, SHA1) do processo associado ao ficheiro, versão do ficheiro), identificador da interceção do evento que ocorreu, a versão completa do filtro de interceção, identificador do tipo de evento intercetado, tamanho da fila de eventos e o número de eventos entre o primeiro evento na fila e o evento atual, número de eventos em atraso na fila, informação sobre o ficheiro do processo do iniciador do evento atual (nome do ficheiro e o seu caminho no computador, código modelo do caminho do ficheiro, somas de verificação (MD5, SHA2-256, SHA1) do processo associado ao ficheiro), duração do processamento do evento, duração máxima do processamento do evento, probabilidade do envio de estatísticas, informação sobre eventos do SO para o qual foi excedido o limite de tempo de processamento (data e hora do evento, número de inicializações repetidas de bases de dados de antivírus, data e hora da última inicialização repetida das bases de dados de antivírus depois da sua atualização, tempo de atraso do processamento do evento para cada componente de monitorização do sistema, número de eventos na fila, número de eventos processados, número de eventos atrasados do tipo atual, tempo de atraso total para os eventos do tipo atual, tempo de atraso total para todos os eventos);

- informação da ferramenta de rastreio de eventos do Windows (Event Tracing for Windows, ETW) na eventualidade de problemas de desempenho do software, fornecedores de eventos de SysConfig / SysConfigEx / WinSATAssessment da Microsoft: informação sobre o computador (modelo, fabricante, fator de forma do invólucro, versão), informação sobre a métrica de desempenho do Windows (WinSAT assessments, índice de desempenho do Windows), nome do domínio, informação sobre os processadores físicos e lógicos (número de processadores físicos e lógicos, fabricante, modelo, nível de grau, número de núcleos, frequência do relógio, CPUID, características da memória intermédia, características do processador lógico, indicadores dos modos suportados e instruções), informação sobre módulos RAM (tipo, fator de forma, fabricante, modelo, capacidade, granularidade da alocação de memória), informação sobre interfaces de rede (endereços IP e MAC, nome, descrição, configuração das interfaces de rede, decomposição do número e tamanho dos pacotes de rede por tipo, velocidade da troca de rede, divisão do número de erros da rede por tipo), configuração do controlador IDE, endereços IP dos servidores DNS, informação sobre a placa de vídeo (modelo, descrição, fabricante, compatibilidade, capacidade de memória vídeo, permissão do ecrã, número de bits por pixel, versão da BIOS), informação sobre dispositivos plug-and-play (nome, descrição, identificador do dispositivo [PnP, ACPI], informação sobre discos e dispositivos de armazenamento (número de discos ou unidades flash, fabricante, modelo, capacidade do disco, número de cilindros, número de faixas por cilindro, número de setores por faixa, capacidade do setor, características da memória intermédia, número sequencial, número de partições, configuração do controlador SCSI), informação sobre discos lógicos (número sequencial, capacidade da partição, capacidade do volume, letra do volume, tipo de partição, tipo de sistema de ficheiros, número de clusters, tamanho do cluster, número de setores por cluster, número de clusters vazios e ocupados, letra do volume de arranque, endereço de desvio da partição em relação ao arranque do disco), informação sobre a motherboard da BIOS (fabricante, data de lançamento, versão), informação sobre a motherboard (fabricante, modelo, tipo), informação sobre a memória física (capacidade partilhada e livre), informação sobre serviços do sistema operativo (nome, descrição, estado, sinalizador), informação sobre os processos [nome e PIDI], parâmetros de consumo de energia para o computador, configuração do controlador de interrupção, caminho para as pastas do sistema Windows (o Windows e System32), informação sobre o SO (versão, compilação, data de lançamento, nome, tipo, data de instalação), tamanho do ficheiro da página, informação sobre os monitores (número, fabricante, permissão do ecrã, capacidade de resolução, tipo), informação sobre o controlador da placa de vídeo (fabricante, data de lançamento, versão);

- informação de ETW, fornecedores de eventos de EventTrace / EventMetadata da Microsoft: informação sobre a sequência dos eventos do sistema (tipo, hora, data, fuso horário), metadados sobre o ficheiro com resultados de rastreio (nome, estrutura, parâmetros do rastreio, divisão do número de operações de rastreio por tipo), informação sobre o SO (nome, tipo, versão, compilação, data de lançamento, hora de início);

- informação de ETW, fornecedores de eventos do Process / Microsoft Windows Kernel Process / Microsoft Windows Kernel Processor Power da Microsoft: informação sobre os processos iniciados e concluídos (nome, PID, parâmetros de arranque, linha de comando, código de retorno, parâmetros de gestão energética, hora de início e conclusão, tipo de token de acesso, SID, SessionID, número de descritores instalados), informação sobre alterações nas prioridades do thread (TID, prioridade, hora), informação sobre operações do disco do processo (tipo, hora, capacidade, número), histórico de alterações à estrutura e capacidade dos processos de memória utilizáveis;

- informação de ETW, fornecedores de eventos de StackWalk / Perfinfo da Microsoft: informação sobre os contadores do desempenho (o desempenho das secções do código individual, sequência de chamadas de função, PID, TID, endereços e atributos de ISRs e DPCs);

- informação do ETW, fornecedor de eventos de KernelTraceControl-ImageID da Microsoft: informação sobre ficheiros executáveis e bibliotecas dinâmicas (nome, tamanho da imagem, caminho completo), informação sobre ficheiros PDB (nome, identificador), dados do recurso VERSIONINFO para ficheiros executáveis (nome, descrição, criador, localização, versão e identificador da aplicação, versão e identificador do ficheiro);

- informação de ETW, fornecedores de eventos de FileIo / DiskIo / Image / Windows Kernel Disk da Microsoft: informação sobre as operações de ficheiros e do disco (tipo, capacidade, hora de início, hora de conclusão, duração, estado de conclusão, PID, TID, endereços da chamada da função do controlador, I/O Request Packet (IRP), atributos do objeto do ficheiro do Windows), informação sobre os ficheiros envolvidos nas operações de ficheiros e do disco (nome, versão, tamanho, caminho completo, atributos, desvio, soma de verificação da imagem, opções de abertura e acesso);

- informação de ETW, fornecedor de eventos de PageFault da Microsoft: informação sobre erros de acesso à página de memória (endereço, hora, capacidade, PID, TID, atributos do objeto do ficheiro do Windows, parâmetros de alocação de memória);

- informação de ETW, fornecedor de eventos de Thread da Microsoft: informação sobre a criação/conclusão do thread, informação sobre os threads iniciados (PID, TID, tamanho da pilha, prioridades e alocação dos recursos CPU, recursos I/O, páginas de memória entre threads, endereço da pilha, endereço da função de inicialização, endereço de Thread Environment Block (TEB), etiqueta do serviço do Windows);

- informação de ETW, fornecedor de eventos de Microsoft Windows Kernel Memory da Microsoft: informação sobre as operações de gestão da memória (estado de conclusão, hora, quantidade, PID), estrutura de alocação da memória (tipo, capacidade, SessionID, PID);

- informação sobre a operação do software na eventualidade de problemas de desempenho: identificador de instalação do software, tipo e valor da queda do desempenho, informação sobre a sequência de eventos no software (hora, fuso horário, tipo, estado de conclusão, identificador do componente do software, identificador do cenário operacional do software, TID, PID, endereços da chamada da função), informação sobre as ligações de rede a verificar (URL, direção da ligação, tamanho do pacote de rede), informação sobre os ficheiros PDB (nome, identificador, tamanho da imagem do ficheiro executável), informação sobre ficheiros a verificar (nome, caminho completo, soma de verificação), parâmetros de monitorização do desempenho do software;

- informação sobre o último reinício malsucedido do SO: o número de reinícios malsucedidos desde a instalação do SO, dados sobre a descarga do sistema (código de erro e parâmetros, nome, versão e soma de verificação (CRC32) do módulo que provocou o erro no funcionamento do SO, endereço do erro como desvio no módulo e somas de verificação (MD5, SHA2-256, SHA1) da descarga do sistema);

- informação para verificar a autenticidade dos certificados digitais utilizados para assinar os ficheiros: a impressão digital do certificado, o algoritmo da soma de verificação, a chave pública e o número de série do certificado, o nome do emissor do certificado, o resultado da validação do certificado e o identificador da base de dados do certificado;

- informação sobre o processo que está a executar o ataque contra a autodefesa do software: nome e tamanho do ficheiro do processo, respetivas somas de verificação (MD5, SHA2-256, SHA1), caminho completo do ficheiro do processo e código do modelo do caminho do ficheiro, carimbos de data e hora de criação/compilação, sinalizador do ficheiro executável, atributos do ficheiro do processo, informação sobre o certificado utilizado para assinar o ficheiro do processo, código da conta utilizada para iniciar o processo, ID das operações realizadas para aceder ao processo, tipo de recurso com o qual a operação foi realizada (processo, ficheiro, objeto de registo, função de pesquisa FindWindow), nome do recurso com o qual a operação foi realizada, sinalizador que indica o sucesso da operação, o estado do ficheiro do processo e a respetiva assinatura na KSN;

- informações sobre o software do Titular do Direito: versão completa, tipo, localização e estado de operação do software utilizado, versões dos componentes de software instalados e o seu estado de operação, informações sobre as atualizações de software instaladas, o valor do filtro TARGET, a versão do protocolo utilizado para a ligação aos serviços do Titular do Direito;

- informação sobre o hardware instalado no computador: tipo, nome, o nome do modelo, versão de firmware, parâmetros de dispositivos integrados e ligados, o identificador único do computador com o software instalado;

- informações sobre as versões do sistema operativo e atualizações instaladas, o tamanho da palavra, edição e parâmetros do modo de execução do SO, versão e somas de verificação (MD5, SHA2-256, SHA1) do ficheiro kernel do SO e data e hora do arranque do SO;

- ficheiros executáveis e não executáveis, total ou parcialmente;

- partes da RAM do Computador;

- setores envolvidos no processo de arranque do SO;
- pacotes de dados de tráfego de rede;
- páginas da Internet e e-mails que contenham objetos suspeitos e maliciosos;
- descrições das classes e das ocorrências das classes do repositório WMI;
- relatórios de atividade das aplicações:
  - o nome, o tamanho e a versão do ficheiro enviado, a respetiva descrição e as somas de verificação (MD5, SHA2-256, SHA1), o identificador do formato do ficheiro, o nome do fornecedor do ficheiro, o nome do produto ao qual pertence o ficheiro, o caminho completo no Computador, o código do modelo do caminho, os carimbos de data/hora da criação e modificação do ficheiro;
  - a data e hora de início e fim do período de validade do certificado (se o ficheiro tiver uma assinatura digital), a data e hora da assinatura, o nome do emissor do certificado, as informações relativas ao titular do certificado, a impressão digital, a chave pública do certificado e os algoritmos adequados, bem como o número de série do certificado;
  - o nome da conta a partir da qual o processo está a ser executado;
  - as somas de verificação (MD5, SHA2-256, SHA1) do nome do Computador no qual o processo está a ser executado;
  - os títulos das janelas do processo;
  - o identificador para as bases de dados de antivírus, o nome da ameaça detetada de acordo com a classificação do Titular do Direito;
  - os dados sobre a licença instalada, o respetivo identificador, tipo e data de validade;
  - hora local do Computador no momento do fornecimento de informações;
  - nomes e caminhos dos ficheiros que foram acedidos pelo processo;
  - os nomes das chaves de registo e os respetivos valores acedidos pelo processo;
  - os endereços URL e IP acedidos pelo processo;
  - os endereços URL e IP a partir dos quais o ficheiro em execução foi transferido.

Fornecimento de dados ao usar soluções de Detection and Response

Nos computadores com o Kaspersky Endpoint Security instalado, são armazenados os dados preparados para envio automático para os servidores Kaspersky Endpoint Detection and Response, Kaspersky Sandbox e Kaspersky Anti Targeted Attack Platform. Os ficheiros são armazenados em computadores de forma simples e não encriptada.

O conjunto específico de dados depende da solução em que o Kaspersky Endpoint Security é utilizado.

Kaspersky Endpoint Detection and Response

Todos os dados que a aplicação armazena localmente no computador, são eliminados do computador quando o Kaspersky Endpoint Security for desinstalado.

Dados recebidos como resultado da execução da tarefa IOC Scan (tarefa padrão)

O Kaspersky Endpoint Security envia dados automaticamente nos resultados da execução da tarefa *Verificação IOC* para o Kaspersky Security Center.

Os dados nos resultados da execução da tarefa *Verificação IOC* podem conter as seguintes informações:

- Endereço IP da tabela ARP
- Morada física da tabela ARP
- Tipo e nome do registo DNS
- Endereço IP do computador protegido
- Endereço físico (endereço MAC) do computador protegido
- Identificador na entrada do registo de eventos
- Nome da origem de dados no registo
- Nome do registo
- Hora do evento
- Hashes MD5 e SHA256 do ficheiro
- Nome completo do ficheiro (incluindo caminho)
- Tamanho do ficheiro
- Endereço IP remoto e porta ao qual a ligação 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 ficheiro do processo
- Identificador do Windows (PID) do processo
- Identificador do Windows (PID) do processo principal
- Conta do utilizador que iniciou o processo
- Data e hora em que o processo foi iniciado
- Nome do serviço
- Descrição do serviço
- Caminho e nome do serviço DLL (para svchost)
- Caminho e nome do ficheiro executável do serviço
- Identificador do Windows (PID) do serviço
- Tipo de serviço (por exemplo, um controlador ou adaptador de kernel)
- Estado do serviço
- Modo de inicialização do serviço
- Credenciais da conta do utilizador.
- Nome do volume
- Letra do volume
- Tipo do volume
- Valor de registo do Windows
- Valor do ramo de registo
- Caminho da chave do registo (sem ramo e nome do valor)
- Configuração do registo
- Sistema (ambiente)
- Nome e versão do sistema operativo que está instalado no computador
- Nome da rede do computador protegido
- Domínio ou grupo a que o computador protegido pertence
- Nome do navegador de Internet
- Versão do navegador de Internet
- Hora em que o recurso da web foi acedido pela última vez

- URL da solicitação HTTP
- Nome da conta usada para a solicitação HTTP
- Nome do ficheiro do processo que fez a solicitação HTTP
- Caminho completo para o ficheiro do processo que fez a solicitação HTTP
- Identificador do Windows (PID) do processo que fez a solicitação HTTP
- Referenciador HTTP (URL de origem da solicitação HTTP)
- URI do recurso solicitado por HTTP
- Informações sobre o agente do utilizador HTTP (a aplicação que fez a solicitação HTTP)
- Tempo de execução da solicitação HTTP
- Identificador exclusivo do processo que fez a consulta HTTP

Dados para criar uma cadeia de desenvolvimento de ameaças

Os dados para criar uma cadeia de desenvolvimento de ameaças são armazenados durante sete dias por predefinição. Os dados são enviados automaticamente para o Kaspersky Security Center.

Os dados para criar uma cadeia de desenvolvimento de ameaças podem conter as seguintes informações:

- Data e hora do incidente
- Nome da deteção
- Modo de verificação
- Estado da última ação relacionada com a deteção
- Razão pela qual o processamento de deteção falhou
- Tipo de objeto detetado
- Nome do objeto detetado
- Estado 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 único do processo
  - Identificador exclusivo do processo principal

- Identificador exclusivo do ficheiro do processo
- Identificador do processo do Windows (PID)
- Linha de comandos do processo
- Conta do utilizador que iniciou o processo
- Código da sessão de início de sessão em que o processo está em execução
- Tipo da sessão em que o processo está a ser executado
- Nível de integridade do processo que está a ser executado
- Associação da conta de utilizador 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 ficheiro local ou endereço da Internet do ficheiro transferido)
- Hash MD5 ou SHA256 do objeto processado
- Tipo de 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 Internet da transferência do objeto processado (apenas para ficheiros em disco)
- Nome da aplicação que transferiu o ficheiro
- Hashes MD5 e SHA256 da aplicação que transferiu o ficheiro
- Nome da aplicação que modificou o ficheiro pela última vez
- Hashes MD5 e SHA256 da aplicação que modificou o ficheiro pela última vez
- Número de inicializações de objetos processados

- Data e hora em que o objeto processado foi iniciado pela primeira vez
- Identificadores exclusivos do ficheiro
- Nome completo do ficheiro (nome do ficheiro local ou endereço da Internet do ficheiro transferido)
- Caminho para a variável de registo do Windows processada
- Nome da variável de registo do Windows processada
- Valor da variável de registo do Windows processada
- Tipo da variável de registo do Windows processada
- Indicador da associação da chave de registo processada no ponto de execução automática
- Endereço da Internet do pedido Web processado
- Origem da ligação do pedido Web processado
- Agente do utilizador do pedido Web processado
- Tipo do pedido Web processado (`GET` ou `POST`)
- Porta IP local do pedido Web processado
- Porta IP remota do pedido Web processado
- Direção da ligação (entrada ou saída) do pedido Web processado
- Identificador do processo em que o código malicioso foi integrado

Kaspersky Sandbox

Todos os dados que a aplicação armazena localmente no computador, são eliminados do computador quando o Kaspersky Endpoint Security for desinstalado.

Dados de serviço

O Kaspersky Endpoint Security armazena os seguintes dados processados durante a resposta automática:

- Ficheiros processados e dados introduzidos pelo utilizador durante a configuração do agente integrado do Kaspersky Endpoint Security:
  - Ficheiros em 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 na cache
  - Hash MD5 da tarefa de verificação
  - Identificador da tarefa de verificação
  - Resultado da verificação para o objeto
- Fila de pedidos de verificação de objeto:
  - ID do objeto na fila
  - Hora em que o objeto foi colocado na fila
  - Estado de processamento do objeto na fila
  - ID da sessão do utilizador no sistema operativo onde a tarefa de verificação do objeto foi criada
  - Identificador do sistema (SID) do utilizador do sistema operativo cuja conta foi usada para criar a tarefa
  - Hash MD5 da tarefa de verificação do objeto
- Informação sobre as tarefas para as quais o agente integrado do Kaspersky Endpoint Security está à espera dos resultados da verificação do Kaspersky Sandbox:
  - Hora em que a tarefa de verificação do objeto foi recebida
  - Estado de processamento do objeto
  - ID da sessão do utilizador no sistema operativo onde a tarefa de verificação do objeto foi criada
  - Identificador da tarefa de verificação do objeto
  - Hash MD5 da tarefa de verificação do objeto
  - Identificador do sistema (SID) do utilizador do sistema operativo 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 ficheiros relacionados

Dados recebidos como resultado da execução da tarefa IOC Scan (tarefa autónoma)

O Kaspersky Endpoint Security envia dados automaticamente nos resultados da execução da tarefa *Verificação IOC* para o Kaspersky Security Center.

Os dados nos resultados da execução da tarefa *Verificação IOC* podem conter as seguintes informações:

- Endereço IP da tabela ARP
- Morada física da tabela ARP
- Tipo e nome do registo DNS
- Endereço IP do computador protegido
- Endereço físico (endereço MAC) do computador protegido
- Identificador na entrada do registo de eventos
- Nome da origem de dados no registo
- Nome do registo
- Hora do evento
- Hashes MD5 e SHA256 do ficheiro
- Nome completo do ficheiro (incluindo caminho)
- Tamanho do ficheiro
- Endereço IP remoto e porta ao qual a ligação 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 ficheiro do processo
- Identificador do Windows (PID) do processo
- Identificador do Windows (PID) do processo principal
- Conta do utilizador que iniciou o processo
- Data e hora em que o processo foi iniciado
- Nome do serviço
- Descrição do serviço
- Caminho e nome do serviço DLL (para svchost)
- Caminho e nome do ficheiro executável do serviço
- Identificador do Windows (PID) do serviço
- Tipo de serviço (por exemplo, um controlador ou adaptador de kernel)
- Estado do serviço
- Modo de inicialização do serviço
- Credenciais da conta do utilizador.
- Nome do volume
- Letra do volume
- Tipo do volume
- Valor de registo do Windows
- Valor do ramo de registo
- Caminho da chave do registo (sem ramo e nome do valor)
- Configuração do registo
- Sistema (ambiente)
- Nome e versão do sistema operativo que está instalado no computador
- Nome da rede do computador protegido
- Domínio ou grupo a que o computador protegido pertence
- Nome do navegador de Internet

- Versão do navegador de Internet
- Hora em que o recurso da web foi acedido pela última vez
- URL da solicitação HTTP
- Nome da conta usada para a solicitação HTTP
- Nome do ficheiro do processo que fez a solicitação HTTP
- Caminho completo para o ficheiro do processo que fez a solicitação HTTP
- Identificador do Windows (PID) do processo que fez a solicitação HTTP
- Referenciador HTTP (URL de origem da solicitação HTTP)
- URI do recurso solicitado por HTTP
- Informações sobre o agente do utilizador HTTP (a aplicação que fez a solicitação HTTP)
- Tempo de execução da solicitação HTTP
- Identificador exclusivo do processo que fez a consulta HTTP

Kaspersky Endpoint Detection and Response Expert (on-premises)

Todos os dados que a aplicação armazena localmente no computador, são eliminados do computador quando o Kaspersky Endpoint Security for desinstalado.

Dados de serviço

O agente integrado do Kaspersky Endpoint Security armazena os seguintes dados localmente:

- Dados necessários para integração com o componente EDR Expert (on-premises):
  - Endereço e porta para ligação ao servidor KATA Central Node
  - Endereço e porta para ligação ao servidor de transmissão de telemetria
  - Endereço e porta para ligação ao servidor de respostas
  - Informações sobre os certificados utilizados para a integração com o KATA Central Node
  - Informações sobre os certificados utilizados para integração com o servidor de transmissão de telemetria
  - Informações sobre os certificados utilizados para a integração com o servidor de respostas
- Ficheiros em quarentena

Dados de eventos de telemetria transmitidos

- **Dados de telemetria**
  - Dados nos ficheiros:
    - Identificadores exclusivos do ficheiro
    - Tipo de ficheiro
    - Caminho completo do ficheiro
    - Tamanho do ficheiro
    - Atributos do ficheiro
    - Identificador de zona
    - Data e hora em que o ficheiro foi criado
    - Data e hora em que o ficheiro foi modificado pela última vez
    - Nome do ficheiro original
    - Nome da aplicação
    - Versão da aplicação.
    - Fornecedor de aplicações
    - Descrição do ficheiro
    - Versão do ficheiro.
    - Hashes MD5 e SHA256 do objeto
    - Resultado da verificação da assinatura do ficheiro
    - Nome do emissor do 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 passado para o AMSI
    - Conteúdo do objeto passado para o AMSI

- Nome do objeto
- Hashes MD5 e SHA256 do objeto

- Dados sobre o bloqueio de aplicações:
  - Identificador exclusivo do processo que iniciou o bloqueio da aplicação
  - Identificador exclusivo do processo principal
  - Identificador único do sistema do processo
  - Comando usado para iniciar um processo
  - ID da sessão de início de sessão
  - Nível de integridade do processo
  - Estado do processo
  - Identificador exclusivo do ficheiro do processo
  - Linha de comandos do processo
  - Lista de identificadores únicos de ficheiros interpretados
- Dados sobre aberturas de ficheiros bloqueadas:
  - Identificador exclusivo do processo que iniciou a abertura do ficheiro
  - Identificadores exclusivos do ficheiro
- Dados sobre a carga do controlador:
  - Identificador único do controlador carregado
- Dados sobre eventos:
  - Identificador único do evento
  - Data e hora do evento
- Dados sobre a modificação do ficheiro:
  - Identificador exclusivo do processo que iniciou a modificação do ficheiro
  - Identificadores exclusivos do ficheiro
  - Tipo de operação de modificação
  - Sinalizador a indicar que o ficheiro será eliminado após o reinício do computador
  - Identificador exclusivo do ficheiro modificado
  - Identificador exclusivo do ficheiro antes da modificação

    - Conjunto de sinalizadores de bits que determinam como o ficheiro foi aberto
    - Dados sobre operações na lista de controlo de acesso
    - Dados sobre alterações na propriedade ou no grupo principal do ficheiro
- Dados sobre o início de sessão:
    - ID da sessão de início de sessão
    - Nome do utilizador que iniciou sessão
    - Tipo de conta do utilizador
    - Tipo de sessão
- Dados sobre as ligações de rede:
    - Identificador exclusivo do processo que iniciou a ligação
    - Endereço IP local usado para iniciar a ligação
    - Endereço IP remoto do ponto final da ligação
    - Direção da ligação
    - Protocolo de transferência de dados
    - Método HTTP
    - Caminho sem o nome do anfitrião
    - Nome do anfitrião
    - Estado dinâmico do processo no momento da ligação
    - Sinalizador a indicar que a ligação está aberta no nível do socket bruto
    - Versão TLS usada na sessão de ligação
    - Nome do servidor TLS
    - Hashes MD5 e SHA1 do certificado do servidor TLS
    - Lista de Nomes Alternativos do Assunto (SAN) do certificado
    - Nome do emissor do certificado TLS
    - Número de série do certificado
    - Algoritmo de encriptação utilizado
    - Datas de início e término do certificado

    - Impressão digital JA3 do cliente TLS
    - Impressão digital JA3S do servidor
- Dados capturados durante a escuta numa porta de rede:
    - Identificador exclusivo do processo que iniciou a ligação
- Dados de entrada da linha de comandos:
    - Identificador exclusivo do processo que iniciou a entrada da consola
    - Tipo de entrada da consola
    - Texto inserido por um utilizador ou um processo
- Dados sobre a criação do processo:
    - Identificador único do processo
    - Identificador exclusivo do processo principal
    - Identificador único do sistema do processo
    - Comando usado para iniciar um processo
    - ID da sessão de início de sessão
    - Nível de integridade do processo
    - Identificador exclusivo do ficheiro do processo
    - Lista de identificadores únicos de ficheiros interpretados
    - Tipo de processo
- Dados sobre o módulo carregado pelo processo:
    - Identificador exclusivo do processo que iniciou a transferência
    - Caminho completo para o ficheiro que foi carregado no processo
    - Identificador exclusivo do ficheiro do módulo
    - Nome totalmente qualificado do conjunto .NET, caso o ficheiro carregado seja um módulo .NET
    - Sinalizadores do conjunto .NET definidos no seu manifesto
- Dados sobre o término do processo:
    - Identificador exclusivo do processo terminado

- Dados sobre a modificação do registo:
  - Identificador exclusivo do processo que iniciou a modificação do registo
  - Tipo de operação de registo
  - Caminho completo para a chave de registo
  - Nome do valor dentro de uma chave de registo
  - Tipo de dados armazenados no valor da chave de registo
  - Dados especificados no valor da chave de registo
  - Nome da chave antes da alteração do nome
  - Informações sobre uma alteração na titularidade da chave ou do grupo de chaves primárias
  - Lista de alterações na lista de controlo de acesso (ACL) da chave
- Dados sobre a ameaça detetada e o seu processamento:
  - Sinalizador a indicar que a deteção de ameaças foi executada em segundo plano
  - Veredicto de ameaça
  - Nome do veredicto
  - Identificador único do registo da base de dados
  - Hora em que o registo da ameaça foi guardado na base de dados
  - Modo de processamento da ameaça
  - Tipo de objeto infetado
  - Nome do objeto infetado
  - Hashes MD5 e SHA256 do objeto
  - Identificador único do objeto infetado
  - Identificador único do processo que transferiu o objeto infetado da internet
  - URL de onde o objeto infetado foi transferido
  - Endereço de e-mail do remetente que enviou o objeto infetado
  - Protocolo de rede através do qual o objeto infetado foi recebido
  - Endereço local de onde o objeto infetado foi recebido
  - Endereço externo de onde o objeto infetado foi recebido

- Tipo de conteúdo do objeto
- Conteúdo do objeto

- Dados sobre o acesso aos processos:
  - Identificador exclusivo do processo que tentou o acesso
  - Identificador exclusivo do processo de destino que foi acedido
  - Conjunto de direitos solicitados do processo de destino
  - Tipo de operação
  - Conjunto de chamadas no momento de acesso a um processo
  - Descritor do processo de origem
  - Descritor do processo de destino
- Dados sobre DNS:
  - Identificador exclusivo do processo que iniciou a consulta DNS
  - Endereço IP do servidor DNS
  - Sinalizadores que gerem o comportamento de uma consulta DNS
  - Estado de conclusão do pedido
  - 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 único do processo que tentou injetar código
  - Método de acesso utilizado
  - Conjunto de chamadas no momento em que o código injetado foi detetado
  - Identificador único do processo de destino para o 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 ficheiro DDL

- Dados sobre operações com canais nomeados:
  - Identificador único do processo que criou ou se conectou ao canal
  - Nome completo do canal mencionado
  - Tipo de operação (criação ou ligação)
- Dados sobre consultas WMI:
  - Identificador exclusivo do processo que iniciou a operação WMI
  - Tipo de operação WMI
  - Nome do dispositivo de destino para a consulta WMI
  - Conta de utilizador que iniciou a consulta WMI
  - Texto da consulta WMI
  - Espaço de nomes no qual a consulta WMI é realizada
  - Nome do filtro WMI
  - Nome do objeto de consumo
  - Texto que descreve a ação do objeto de consumo
- Dados sobre consultas LDAP:
  - Identificador exclusivo do processo que fez a consulta LDAP
  - Âmbito de pesquisa das consultas LDAP
  - Filtro LDAP
  - Parâmetro que especifica a partição do Active Directory para a qual a consulta foi direcionada
  - Atributos de pesquisa LDAP
- Dados sobre dispositivos USB conectados:
  - Tipo de operação do dispositivo USB
  - Tipo de dispositivo USB
  - Identificador do dispositivo USB
  - Nome do dispositivo USB
  - Caminho para o dispositivo USB
  - Sinalizador a indicar que o dispositivo USB é uma unidade de sistema
- Dados sobre a criação, eliminação e modificação de uma tarefa agendada

    - Dados sobre a criação, eliminação e modificação de serviços
    - Dados sobre a montagem/desmontagem do sistema de ficheiros
    - Dados sobre o funcionamento 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 término do agente
        - Código de término do processo do agente
- Definições de filtro de eventos:
    - Nomes dos módulos
    - Caminhos completos para os objetos
    - Hashes MD5 e SHA256 dos objetos
    - Identificadores das entradas no registo de eventos do Windows
    - Definições de certificado digital
    - Direção do tráfego, endereços IP, portas, protocolos, caminhos completos para ficheiros executáveis
    - Nomes de utilizador
    - Tipos de inícios de sessão do utilizador
    - Tipos de eventos de telemetria em que os filtros são aplicados

Dados dos pedidos do componente EDR Expert ao agente integrado do Kaspersky Endpoint Security

- Definições gerais da tarefa:
    - Tipo de tarefa
    - Definições de agendamento da tarefa
    - Nomes e passwords das contas em que as tarefas podem ser executadas
    - Versões das definições

- Identificadores de objetos em quarentena
- Caminhos para os objetos
- Hashes MD5 e SHA256 dos objetos
- Linha de comandos para iniciar o processo com os argumentos
- Sinalizadores das ações adicionais realizadas após a conclusão das tarefas
- Identificadores do ficheiro IOC a serem recuperados do servidor
- IOC files
- Nome do serviço
- Tipo de inicialização do serviço
- Pastas em que os resultados da tarefa *Obter informações forenses* têm de ser recebidos
- Máscaras dos nomes de objeto e extensões para a tarefa *Obter informações forenses*

- Definições de isolamento de rede:
  - Tipos de definições
  - Versões das definições
  - Listas de exclusões de isolamento de rede e definições de exclusão: direção do tráfego, endereços IP, portas, protocolos e caminhos completos para os ficheiros executáveis
  - Sinalizadores das ações adicionais
  - Tempo de desativação do isolamento automático
- Definições da prevenção da execução:
  - Tipos de definições
  - Versões das definições
  - Listas de regras de prevenção de execução e definições de regras: caminhos para objetos, tipos de objetos, hashes MD5 e SHA256 de objetos
  - Sinalizadores das ações adicionais

Dados de pedidos enviados pelo Kaspersky Endpoint Security para o componente EDR Expert

Ao integrar com a solução EDR Expert (on-premises), os seguintes dados são armazenados localmente nos computadores.

- Em pedidos de sincronização:
  - ID único
  - Parte básica do endereço da Internet do servidor
  - Nome do computador
  - Endereço IP do computador
  - Endereço MAC do computador
  - Hora local no computador
  - Estado de autodefesa do Kaspersky Endpoint Security
  - Nome e versão do sistema operativo que está instalado no computador
  - Versão do Kaspersky Endpoint Security
  - Versões das definições das aplicações e definições da tarefa
  - Estado da tarefa: identificadores das tarefas, estado de execução, códigos de erro
- Nos pedidos para obter ficheiros do servidor:
  - Identificadores exclusivos dos ficheiros
  - Identificador exclusivo do Kaspersky Endpoint Security
  - Identificadores exclusivos dos certificados
  - Parte básica do endereço da Internet do servidor com o componente do Central Node instalado
  - Endereço IP do anfitrião
- Nos relatórios sobre os resultados da execução da tarefa:
  - Endereço IP do anfitrião
  - Informações sobre os objetos detetados durante uma verificação IOC ou verificação YARA
  - Sinalizadores das ações adicionais realizadas após a conclusão das tarefas
  - Erros de execução de tarefas e códigos de retorno
  - Estados da conclusão da tarefa

- Tempo de conclusão da tarefa
- Versões das definições usadas para a execução das tarefas
- Informações sobre os objetos enviados para o 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 num computador a pedido do servidor: PID e UniquePID, código de erro, hashes MD5 e SHA256 dos objetos
- Informações sobre os serviços iniciados ou interrompidos num computador a pedido do servidor: nome do serviço, tipo de inicialização, código de erro, hashes MD5 e SHA256 das imagens do ficheiro dos serviços
- Informações sobre os objetos para os quais foi efetuada uma informação de memória para uma verificação YARA (caminhos, identificador do ficheiro de informação)
- Ficheiros solicitados pelo servidor

- Dados sobre processos em execução:
  - Nome do ficheiro executável, incluindo caminho completo e extensão
  - Parâmetros de execução automática do processo
  - ID do processo
  - ID da sessão de início de sessão
  - Nome da sessão de início de sessão
  - Data e hora em que o processo foi iniciado
  - Hashes MD5 e SHA256 do objeto
- Dados nos ficheiros:
  - Caminho do ficheiro
  - Nome do ficheiro.
  - Tamanho do ficheiro
  - Atributos do ficheiro
  - Data e hora em que o ficheiro foi criado
  - Data e hora em que o ficheiro foi modificado pela última vez
  - Descrição do ficheiro
  - Nome da empresa
  - Hashes MD5 e SHA256 do objeto
  - Chave de registo (para pontos de execução automática)

- Dados em erros que ocorrem quando as informações sobre os objetos foram recuperadas:
  - Nome completo do objeto que foi processado quando ocorreu um erro
  - Código de 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 desenvolvimento de ameaças.

  Os dados são temporariamente armazenados localmente na fila para enviar os resultados da execução da tarefa para o servidor Kaspersky Anti Targeted Attack Platform. Os dados são eliminados do armazenamento temporário após serem enviados.
  - Hashes MD5 e SHA256 do ficheiro
  - Nome completo do ficheiro
  - Caminho do ficheiro
  - Tamanho do ficheiro
  - Nome do processo
  - Argumentos do processo
  - Caminho para o ficheiro do processo
  - Identificador do Windows (PID) do processo
  - Identificador do Windows (PID) do processo principal
  - Conta do utilizador que iniciou o processo
  - Data e hora em que o processo foi iniciado
- Dados nos resultados da verificação IOC:
  - Endereço IP da tabela ARP
  - Morada física da tabela ARP
  - Nome de registo DNS
  - Tipo de registo DNS
  - Nome do anfitrião
  - Endereço IP
  - ID do evento no registo
  - Nome da origem de dados no registo
  - Nome do registo

- Nome do utilizador
- Data e hora em que o evento foi gerado, no formato ISO
- Hashes MD5 e SHA256 do ficheiro
- Nome completo do ficheiro
- Tamanho do ficheiro
- Endereço IP remoto e porta ao qual a ligação foi estabelecida durante a verificação
- Endereço IP e porta do adaptador local
- Protocolo
- Nome do processo
- Argumentos do processo
- Caminho para o ficheiro do processo
- Identificador do Windows (PID) do processo
- Identificador do Windows (PID) do processo principal
- Conta do utilizador que iniciou o processo
- Data e hora em que o processo foi iniciado
- Caminho para a chave do registo
- Nome da chave de registo
- Valor de texto da chave de registo
- Nome do serviço
- Descrição do serviço
- Caminho e nome do serviço DLL
- Caminho e nome do ficheiro executável do serviço
- Identificador do Windows (PID) do serviço
- Tipo de serviço
- Estado do serviço
- Modo de inicialização do serviço
- Nome do sistema operativo
- Versão do sistema operativo

- Nome de rede de computadores sem domínio
- Domínio ou grupo de trabalho
- Nome do utilizador
- Nome do volume
- Letra do volume
- Tipo do volume

Kaspersky Network Detection and Response (KATA)

Todos os dados que a aplicação armazena localmente no computador, são eliminados do computador quando o Kaspersky Endpoint Security for desinstalado.

Dados de telemetria

- **Dados sobre ficheiros**
  - Identificadores exclusivos do ficheiro
  - Tipo de ficheiro
  - Caminho completo do ficheiro
  - Tamanho do ficheiro
  - Atributos do ficheiro
  - Identificador de zona
  - Data e hora em que o ficheiro foi criado
  - Data e hora em que o ficheiro foi modificado pela última vez
  - Nome do ficheiro original
  - Nome da aplicação
  - Versão da aplicação.
  - Fornecedor de aplicações
  - Descrição do ficheiro
  - Versão do ficheiro.

- Hashes MD5 e SHA256 do objeto
- Resultado da verificação da assinatura do ficheiro
- Data e hora em que a assinatura do ficheiro foi criada
- Cadeias de certificados usadas no ficheiro de assinatura
- Tipo de cadeia de certificado
- Certificados na cadeia
- Nome do emissor do 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 o início de sessão**
  - ID da sessão de início de sessão
  - Nome da conta do utilizador que iniciou sessão
  - Tipo de conta do utilizador
  - Tipo de sessão
  - Endereço IP da máquina a partir da qual a tentativa de início de sessão foi feita
  - Endereço IP da máquina local na qual a tentativa de início de sessão foi feita
  - Sinalizador a indicar que a sessão representada por este evento possui privilégios elevados e direitos de administrador
  - Parâmetro que indica se outras sessões estão vinculadas a este início de sessão
  - Protocolo usado para a sessão do terminal
  - Protocolo IPv4 usado para a sessão do terminal
- **Dados sobre comunicação em rede**
  - Início e fim do intervalo de tempo durante o qual os dados foram recolhidos
  - 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 de rede através da qual a comunicação foi capturada

- **Dados sobre a ligação de rede**
  - Identificador exclusivo do processo que iniciou a ligação
  - Protocolo de transferência de dados
  - Endereço IP local usado para iniciar a ligação
  - Endereço IP remoto do ponto final da ligação
  - Método HTTP
  - Caminho sem o nome do anfitrião
  - Nome do anfitrião
  - Estado dinâmico do processo no momento da ligação
  - Direção da ligação
  - Estado do processo dinâmico
  - Campo EtherType do quadro Ethernet
- **Dados capturados durante a escuta numa porta de rede**
  - Identificador exclusivo do processo que iniciou a ligação
  - Protocolo de transferência de dados
  - Endereço local
  - Estado dinâmico do processo no momento da ligação

- **Resultado da verificação de ligação**
  - Definições da rede do anfitrião
  - Descrição da interface de rede
  - Nome de domínio DNS
  - Endereço MAC local do computador
  - Número da métrica de ligação IP
  - Lista de endereços IP
  - Endereço IP
  - Máscara de rede
  - Endereço IP do gateway
  - Endereço MAC do gateway
  - Lista de correções instaladas
  - Número da correção
  - Data de instalação da correção
  - Modelo do dispositivo
  - Fornecedor do dispositivo
  - ID do anfitrião 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 da base de dados do componente do antivírus da Kaspersky instalado
  - Data da última atualização da base de dados do componente de antivírus da Kaspersky instalado
  - Estado dos componentes do antivírus da Kaspersky instalado
  - Lista de chaves de licença
  - Número de série da chave
  - Tipo de chave

- Data de validade da chave
- Estado da chave

- **Dados sobre a criação de processos no anfitrião**
  - Identificador único do processo
  - Identificador exclusivo do processo principal
  - Identificador único do sistema do processo
  - Comando usado para iniciar um processo
  - ID da sessão de início de sessão
  - ID da sessão do terminal
  - Identificador exclusivo do ficheiro do processo
  - Nível de integridade do processo
  - Lista de tokens de direitos de processo
  - Direitos de atributos
  - Lista de identificadores únicos de ficheiros interpretados
  - Estado do processo
  - Comando usado para iniciar um processo
- **Dados sobre o término do processo**
  - Identificador único do processo
- **Dados sobre ameaças detetadas**
  - Informações sobre ameaças
  - Veredicto de ameaça
  - Número de registo AMR
  - Versão da base de dados de antivírus
  - Modo de deteção de ameaças
  - Identificador único da ameaça
  - Tecnologia de proteção
  - Informações sobre o objeto infetado
  - Tipo de objeto infetado

- Nome do objeto infetado
- Hashes MD5 e SHA256 do objeto
- Identificador único do processo infetado
- Identificador único do objeto infetado
- Identificador único do processo que transferiu o objeto infetado da internet
- URL de onde o objeto infetado foi transferido
- Endereço de e-mail do remetente que enviou o objeto infetado
- Protocolo de rede através do qual o objeto infetado foi recebido
- Endereço local de onde o objeto infetado foi recebido
- Endereço externo de onde o objeto infetado foi recebido
- Tipo de conteúdo do objeto
- Contexto da ameaça detetada
- Conteúdo do objeto
- Sinalizador a indicar que a deteção de ameaças foi executada em segundo plano

- **Dados sobre o processamento de ameaças**
  - Informações sobre ameaças
  - Veredicto de ameaça
  - Número de registo AMR
  - Versão da base de dados de antivírus
  - Modo de deteção de ameaças
  - Nome do objeto infetado
  - Hashes MD5 e SHA256 do objeto
  - Identificador único do processo infetado
  - Identificador único do objeto infetado
  - Protocolo de rede através do qual o objeto infetado foi recebido
  - Endereço local de onde o objeto infetado foi recebido
  - Endereço externo de onde o objeto infetado foi recebido
  - Estado de processamento da ameaça

- Motivo pelo qual a ameaça não pôde ser resolvida
- Endereço físico local

- **Dados sobre utilizadores**
  - SID do utilizador
  - ID do utilizador
  - Nome do utilizador
  - Nome completo do utilizador
  - Descrição do utilizador
  - Se a conta está ativa ou bloqueada
  - Se a password expirou
  - Se é necessário alterar a password
  - Se é permitido alterar a password
  - Tipo de conta do utilizador
  - Se o início de sessão automático está ativado para esta conta
  - Lista de grupos aos quais o utilizador pertence

Integração com Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Todos os dados que a aplicação armazena localmente no computador, são eliminados do computador quando o Kaspersky Endpoint Security for desinstalado.

Ao integrar com a Kaspersky Unified Monitoring and Analysis Platform (KUMA), são transferidos os dados das definições de ligação, bem como todos os eventos registados nos registos do Windows.

Os principais registos de eventos do Windows são: Sistema, Segurança, Aplicações, ForwardedEvents e HardwareEvents. Os utilizadores também podem criar e trabalhar com registos personalizados para satisfazer as suas necessidades específicas.

Conformidade com a legislação da União Europeia (RGPD)

O Kaspersky Endpoint Security pode transmitir dados para a Kaspersky nas seguintes situações:

- Utilização da Kaspersky Security Network.
- Ativar a aplicação com um código de ativação.

- Atualizar módulos de aplicações e bases de dados de antivírus.
- Seguir ligações na interface da aplicação.

Independentemente da classificação de dados e do território a partir do qual os dados são recebidos, a Kaspersky cumpre altos padrões de segurança de dados e emprega várias medidas legais, organizacionais e técnicas para proteger os dados dos utilizadores, de modo a garantir a segurança e confidencialidade dos dados e também para garantir o cumprimento dos direitos dos utilizadores garantidos pela legislação aplicável. O texto da Política de Privacidade está incluído no kit de distribuição da aplicação e está disponível no site da Kaspersky.

Antes de utilizar o Kaspersky Endpoint Security, leia com atenção a descrição dos dados transmitidos no Contrato de Licença do Utilizador Final e na Declaração da Kaspersky Security Network. Se alguns dados específicos transmitidos a partir do Kaspersky Endpoint Security em qualquer um dos cenários descritos puderem ser classificados como dados pessoais de acordo com a legislação ou as normas locais, deve certificar-se de que esses dados são processados legalmente e obter o consentimento dos utilizadores finais para a recolha e transmissão dos mesmos.

Leia o Contrato de Licença do Utilizador Final e visite o site da Kaspersky para obter mais informações sobre a recebe, processamento, armazenamento e eliminação de informações sobre a utilização das aplicações, após aceitar o Contrato de Licença do Utilizador Final e aceitar a Declaração de Recolha de Dados da KSN. Os ficheiros license.txt e ksn_<ID do idioma>.txt contêm o texto do Contrato de Licença do Utilizador Final e a Declaração de Recolha de Dados da KSN está incluída no kit de distribuição da aplicação.

Se não quiser transmitir dados para a Kaspersky, pode desativar o fornecimento de dados.

Utilização da Kaspersky Security Network

Ao utilizar a Kaspersky Security Network, aceita fornecer automaticamente os dados listados na Declaração da Kaspersky Security Network. Se não aceitar fornecer esses dados à Kaspersky, utilize a Kaspersky Private Security Network (KPSN) ou desative a utilização da KSN. Para obter mais informações detalhadas sobre o KPSN, consulte a documentação sobre a Kaspersky Private Security Network.

Ativar a aplicação com um código de ativação

Ao utilizar um código de ativação, aceita fornecer automaticamente os dados listados no Contrato de Licença do Utilizador Final. Se não aceitar fornecer esses dados à Kaspersky, utilize um ficheiro-chave para ativar o Kaspersky Endpoint Security.

Atualizar módulos de aplicações e bases de dados de antivírus

Ao utilizar os servidores da Kaspersky, aceita fornecer automaticamente os dados listados no Contrato de Licença do Utilizador Final. O Kaspersky solicita estas informações para verificar se o Kaspersky Endpoint Security está a ser utilizado de forma legítima. Se não aceitar fornecer essas informações à Kaspersky, utilize o Kaspersky Security Center para atualizações da base de dados ou a Kaspersky Update Utility.

Seguir ligações na interface da aplicação

Ao utilizar ligações na interface da aplicação, aceita fornecer automaticamente os dados listados no Contrato de Licença do Utilizador Final. A lista precisa de dados transmitidos em cada ligação específica depende de onde a ligação está localizada na interface da aplicação e qual o problema que a mesma pretende resolver. Se não aceitar fornecer esses dados à Kaspersky, utilize a interface simplificada da aplicação ou oculte a interface da aplicação.

Gravação de descarga

Se tiver habilitado a gravação de descarga, o Kaspersky Endpoint Security criará um ficheiro de descarga que conterá todos os dados da memória provenientes dos processos da aplicação no momento em que este ficheiro de descarga foi criado.

Avisos de marcas comerciais

As marcas comerciais registadas e de serviço são propriedade dos seus respetivos proprietários.

Adobe, Acrobat, Flash, Reader e Shockwave são marcas comerciais registadas ou marcas comerciais de Adobe nos Estados Unidos e/ou noutros países.

Amazon, Amazon Web Services e AWS são marcas comerciais da Amazon.com, Inc. ou das suas filiais.

Apple, FireWire, iTunes, Mac e Safari são marcas comerciais da Apple Inc.

Arm é uma marca comercial registada da Arm Limited (ou as suas subsidiárias) nos EUA e/ou noutros países.

AutoCAD é uma marca comercial ou marca comercial registada de Autodesk, Inc. e/ou das suas subsidiárias e/ou filiais nos Estados Unidos e/ou noutros países.

A palavra, marca e logótipos Bluetooth são propriedade de Bluetooth SIG, Inc.

Borland é marca comercial ou marca comercial registada da Borland Software Corporation.

Cisco, Cisco AnyConnect e IOS são marcas comerciais registadas ou marcas comerciais da Cisco Systems, Inc. e/ou das 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 comerciais registadas ou marcas comerciais da Cloud Software Group, Inc. e/ou das suas subsidiárias nos Estados Unidos e/ou noutros países.

Cloudflare, Cloudflare Workers e o logótipo da Cloudflare são marcas comerciais e/ou marcas registadas da Cloudflare, Inc. nos Estados Unidos e outras jurisdições.

Core é uma marca comercial da Intel Corporation ou das suas subsidiárias.

o dBase é uma marca comercial da dataBased Intelligence, Inc.

Dell Technologies, Dell, EMC e outras marcas comerciais são marcas comerciais da Dell Inc. ou das suas subsidiárias.

Docker e o logótipo da Docker são marcas comerciais e/ou marcas registadas da Docker, Inc. nos Estados Unidos e/ou noutros países. Docker, Inc. e outras partes também podem ter direitos de marca comercial noutros termos aqui usados.

ESET é uma marca comercial ou marca registada da ESET spol. s r.o. ou da respetiva entidade ESET.

Foxit é uma marca registada 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 registadas da Huawei Technologies Co., Ltd.

ICQ é uma marca comercial e/ou marca de serviço da ICQ LLC.

Intel é uma marca comercial da Intel Corporation ou das suas subsidiárias.

IBM é uma marca comercial de International Business Machines Corporation, registada em várias jurisdições em todo o mundo.

Lenovo e Lenovo ThinkPad são marcas comerciais da Lenovo nos Estados Unidos e/ou noutras localidades.

Linux é uma marca comercial registada de Linus Torvalds nos EUA e noutros países.

Logitech é uma marca comercial registada ou marca comercial da Logitech nos Estados Unidos e/ou noutros países.

LogMeIn Pro e Remotely Anywhere são marcas comerciais de LogMeIn, Inc.

Mail.ru é uma marca comercial da Mail.ru, LLC.

McAfee é marca comercial ou marca registrada da McAfee LLC ou das suas subsidiárias nos Estados Unidos e/ou noutros 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 comerciais do grupo de empresas Microsoft.

Mozilla, Firefox e Thunderbird são marcas comerciais da Mozilla Foundation nos Estados Unidos e noutros países.

NetApp é uma marca comercial ou marca comercial registada da NetApp, Inc. nos Estados Unidos e/ou noutros países.

OpenSSL é uma marca registada detida pela OpenSSL Software Foundation.

OpenStack é uma marca comercial registada da OpenStack Foundation nos EUA e noutros países.

Oracle, Java e JavaScript são marcas comerciais registadas de Oracle Corporation e/ou das suas filiais.

Python é uma marca comercial ou marca comercial registada da Python Software Foundation.

Realtek é uma marca registada da Realtek Semiconductor Corporation.

SAMSUNG é uma marca comercial da SAMSUNG nos Estados Unidos ou noutros países.

Thawte é uma marca comercial ou marca comercial registada da Symantec Corporation ou das suas filiais nos EUA e noutros países.

Trend Micro é uma marca comercial ou marca comercial registada da Trend Micro Incorporated.

VERISIGN é uma marca comercial registada ou não registada da VeriSign, Inc. e das suas subsidiárias nos Estados Unidos e noutros países.

VMware, VMware ESXi, VMware Horizon, VMware Workstation, VMware Tools e VMware vSphere são marcas comerciais registadas ou marcas comerciais da VMware, Inc. nos Estados Unidos e outros países.

Informação acerca de código de terceiros

As informações sobre o código de terceiros encontram-se no ficheiro legal_notices.txt localizado na pasta de instalação da aplicação.