

kaspersky

Kaspersky Endpoint Security for Windows 11.8.0

© 2023 AO Kaspersky Lab

Conteúdos

[Perguntas frequentes](#)

[O que há de novo](#)

[Kaspersky Endpoint Security for Windows](#)

[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](#)

[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](#)

[Change application components](#)

[Atualização a partir de uma versão anterior da aplicação](#)

[Remover a aplicação](#)

[Desinstalar através do Kaspersky Security Center](#)

[Desinstalar a aplicação utilizando o Assistente](#)

[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](#)

[Ativar a aplicação através do Kaspersky Security Center](#)

[Utilizar o Assistente de Ativação para ativar a aplicação](#)

[Ver informação sobre a licença](#)

[Comprar uma licença](#)

[Renovar a subscrição](#)

[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](#)

[Conformidade com a legislação da União Europeia \(RGPD\)](#)

[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](#)

[Como Começar](#)

[Gerir políticas](#)

[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](#)

[Verificação de vírus do computador](#)

[Verificar o computador](#)

[Verificar unidades amovíveis quando forem ligadas ao computador](#)

[Verificação de fundo](#)

[Verificar a partir do menu de contexto](#)

[Controlo da 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](#)

[Configurar atualizações a partir de uma pasta partilhada](#)

[Atualizar módulos de aplicação](#)

[Utilizar um servidor proxy para atualizações](#)

[Reverter última atualização](#)

[Trabalhar com ameaças ativas](#)

[Desinfeção de ameaças ativas em computadores](#)

[Desinfeção de ameaças ativas em servidores](#)

[Ativar ou desativar a Tecnologia de Desinfeção Avançada](#)

[Processamento de ameaças ativas](#)

[Proteção do computador](#)

[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](#)

[Proteção contra ameaças da Web](#)

[Ativar e desativar a Proteção contra ameaças da Web](#)
[Alterar a ação a executar em objetos maliciosos de tráfego de Internet](#)
[Verificar URL por comparação com bases de dados de endereços Web de phishing e maliciosos](#)
[Utilizar a análise heurística no funcionamento do componente Proteção contra ameaças da Web](#)
[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](#)

[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 ataques de rede por tipo](#)

[Firewall](#)

[Ativar ou desativar a Firewall](#)
[Alterar o estado 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](#)
[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 ataques BadUSB](#)

[Ativar e desativar Prevenção de ataques BadUSB](#)
[Utilizar o teclado no ecrã para autorização de dispositivos USB](#)

[Proteção AMSI](#)

[Ativar e desativar a Proteção AMSI](#)

[Utilizar a Proteção AMSI para verificar ficheiros compostos](#)

[Prevenção de explorações](#)

[Ativar e desativar a prevenção de explorações](#)

[Selecionar uma ação a executar quando é detetada uma exploração](#)

[Proteção da memória de processos do sistema](#)

[Deteção de comportamento](#)

[Ativar e desativar a Deteção de comportamento](#)

[Selecionar a ação a ser executada ao detetar atividade de software malicioso](#)

[Proteção de pastas partilhadas contra encriptação externa](#)

[Ativar ou desativar a proteção de pastas partilhadas contra encriptação externa](#)

[Selecionar a ação a executar ao detetar encriptação externa de pastas partilhadas](#)

[Criar uma exclusão para proteção de pastas partilhadas contra encriptação externa](#)

[Configurar endereços das exclusões da proteção de pastas partilhadas contra encriptação externa](#)

[Exportar e importar uma lista de exclusões da proteção de pastas partilhadas contra encriptação externa](#)

[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](#)

[Motor de remediação](#)

[Kaspersky Security Network](#)

[Ativar e desativar a utilização da Kaspersky Security Network](#)

[Limitações do KSN privado](#)

[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](#)

[Configurar as definições da verificação de ligações encriptadas](#)

[Verificar ligações encriptadas no Firefox e no Thunderbird](#)

[Excluir ligações encriptadas da verificação](#)

[Eliminar dados](#)

[Controlo de computador](#)

[Controlo de Internet](#)

[Ativar e desativar o Controlo de Internet](#)

[Ações com regras de acesso a recursos da Internet](#)

[Adicionar uma regra de acesso a recursos da Internet](#)

[Atribuir prioridades a regras de acesso a recursos da Internet](#)

[Ativar e desativar uma regra de acesso a recursos da Internet](#)

[Exportar e importar a lista de endereços Web fiáveis](#)

[Testar regras de acesso a recursos da Internet](#)

[Exportar e importar a lista de endereços de recursos da Internet](#)

[Monitorizar atividade da Internet do utilizador](#)

[Editar modelos de mensagens de Controlo de Internet](#)

[Editar máscaras para endereços de recursos da Internet](#)

[Migrar as regras de acesso de recursos da Internet de versões anteriores da aplicação](#)

[Controlo de Dispositivos](#)

[Ativar e desativar o Controlo de Dispositivos](#)

[Sobre as regras de acesso](#)

[Editar uma regra de acesso a dispositivos](#)

[Editar uma regra de acesso a barramentos de ligação](#)

[Adicionar uma rede Wi-Fi à lista fiável](#)

[Monitorizar o uso de unidades amovíveis](#)

[Alterar a duração da cache](#)

[Ações com dispositivos fiáveis](#)

[Adicionar um dispositivo à lista fiável a partir da interface da aplicação](#)

[Adicionar um dispositivo à lista fiável do Kaspersky Security Center](#)

[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](#)

[Ativar e desativar o 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](#)

[Visualizar relatórios de Controlo Adaptativo de Anomalia](#)

[Controlo das Aplicações](#)

[Limitações da funcionalidade de Controlo das Aplicações](#)

[Ativar e desativar o Controlo das Aplicações](#)

[Selecionar o modo de Controlo das Aplicações](#)

[Trabalhar com regras de controlo das aplicações na interface da aplicação](#)

[Adicionar uma Regra de Controlo das Aplicações](#)

[Adicionar uma condição de ativação para uma Regra de Controlo das aplicações](#)

[Alterar o estado de uma Regra de Controlo das aplicações](#)

[Gerir Regras de Controlo das Aplicações no Kaspersky Security Center](#)

[Receber informações sobre as aplicações instaladas nos computadores dos utilizadores](#)

[Criar categorias de aplicações](#)

[Adicionar ficheiros executáveis da pasta de Ficheiros executáveis à categoria de aplicações](#)

[Adicionar ficheiros executáveis relacionados a eventos à categoria de aplicações](#)

[Adicionar e modificar uma Regra de Controlo das aplicações utilizando o Kaspersky Security Center](#)

[Alterar o estado de uma Regra de Controlo das aplicações utilizando o Kaspersky Security Center](#)

[Exportar e importar Regras de Controlo das Aplicações](#)

[Testar Regras de Controlo das Aplicações utilizando o Kaspersky Security Center](#)

[Ver eventos que resultam de operação de teste do componente de Controlo das Aplicações](#)

[Ver um relatório sobre as aplicações bloqueadas no modo de teste](#)

[Ver eventos que resultam da operação do componente de Controlo das Aplicações](#)

[Ver um relatório sobre aplicações bloqueadas](#)

[Testar Regras 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](#)

[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](#)

[Proteção por password](#)

[Ativar proteção por password](#)

[Conceder permissões a utilizadores ou grupos individuais](#)

[Usar uma password temporária para conceder permissões](#)

[Aspetos especiais de permissões de proteção por password](#)

[Zona fiável](#)

[Criar uma exclusão de verificação](#)

[Ativar e desativar a exclusão de verificação](#)

[Selecionar tipos de objetos detetáveis](#)

[Editar a lista de aplicações fiáveis](#)

[Ativar e desativar as regras da zona fiável para uma aplicação da lista de aplicações fiáveis](#)

[Utilizar o armazenamento de certificados de sistema fiável](#)

[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](#)

[Ativar e desativar a defesa de gestão externa](#)

[Disponibilizar apoio para aplicações de administração remota](#)

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](#)

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](#)

[Encriptação de disco completa utilizando a tecnologia de 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](#)

[Atualizar o sistema operativo](#)

[A eliminar erros da atualização da funcionalidade de encriptação](#)

[Selecionar o nível de rastreio do 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](#)

[Kaspersky Endpoint Agent](#)

[Migração de Política e Tarefa para o Kaspersky Endpoint Agent](#)

[Migrar a configuração \[KES+KEA\] para a configuração \[KES+agente incorporado\]](#)

[Managed Detection and Response](#)

[Integração com o MDR](#)

[Migração do Kaspersky Endpoint Agent](#)

[Endpoint Detection and Response](#)

[Integração com o Kaspersky Endpoint Detection and Response](#)

[Migração do Kaspersky Endpoint Agent](#)

[Verificar os indicadores de compromisso \(tarefa padrão\)](#)

[Mover ficheiro para Quarentena](#)

[Obter ficheiro](#)

[Delete file](#)

[Início do Processo](#)

[Terminação de Processo](#)

[Prevenção da execução](#)

[Isolamento da rede do computador](#)

[Anexo 1. Extensões de ficheiros suportadas para a prevenção da execução](#)

[Anexo 2. Interpretadores de script suportados](#)

[Anexo 3. Âmbito de verificação IOC no registo \(RegistryItem\)](#)

[Anexo 4. Requisitos para IOC file](#)

[Kaspersky Sandbox](#)

[Integração com o Kaspersky Sandbox](#)

[Migração do Kaspersky Endpoint Agent](#)

[Adição de um certificado TLS](#)

[Adicionar servidores do Kaspersky Sandbox](#)

[Verifique se há indicadores de compromisso \(tarefa autónoma\)](#)

[Gerir a Quarentena](#)

[Configurar o tamanho máximo da Quarentena](#)

[Enviar dados sobre ficheiros da Quarentena para o Kaspersky Security Center](#)

[Kaspersky Security for Windows Server](#)

[Instalar o KES sobre o KSWs](#)

[Ativar o KES com uma chave KSWs](#)

[Gerir a aplicação a partir da command line](#)

[Instalar a aplicação](#)

[Ativar a aplicação](#)

[Remover a aplicação](#)

[Comandos AVP](#)

[SCAN. Scan de vírus](#)

[UPDATE. Atualização de bases de dados e módulos de software de aplicação](#)

[ROLLBACK. Reverter última atualização](#)

[TRACES. Rastreamento](#)

[START. Iniciar o 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. Detecção de spyware](#)

[KSN. Transição do KSN Privado/Global](#)

[Comandos KESCLI](#)

[Scan. Scan de vírus](#)

[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. Determinar a hora de conclusão atualizada](#)

[EnableRTP. Ativar proteção](#)

[GetRealTimeProtectionState. Estado da Proteção contra ameaças de ficheiros](#)

[Versão. Identificar a versão da aplicação](#)

[Comandos Managed Detection and Response](#)

[SANDBOX. Gerir o Kaspersky Sandbox](#)

[PREVENÇÃO. Gestão de prevenção de execução](#)

[ISOLAMENTO. Gerir o isolamento da rede](#)

[RESTORE. Restaurar ficheiros a partir da Quarentena](#)

[IOCSCAN. Verificar indicadores de comprometimento \(IOC\)](#)

[MDRLICENSE. Ativação MDR](#)

[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 rastreamento](#)

[Rastreamento da operação da aplicação](#)

[Rastreamento de desempenho da aplicação](#)

[Gravação de descarga](#)

[Proteger ficheiros de descarga e ficheiros de rastreio](#)

[Limitações e avisos](#)

[Glossário](#)

[Agente de Autenticação](#)

[Agente de Rede](#)

[Âmbito de Proteção](#)

[Âmbito de verificação](#)

[Arquivo](#)

[Base de dados de endereços de phishing](#)

[Base de dados de endereços web maliciosos](#)

[Bases de dados de antivírus](#)

[Certificado de licença](#)

[Chave adicional](#)

[Chave ativa](#)

[Desinfecção](#)

[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](#)

[Máscara](#)

[Objeto OLE](#)

[OpenIOC](#)

[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](#)

[Controlo de Internet](#)

[Controlo de Dispositivos](#)

[Controlo das Aplicações](#)

[Controlo de Anomalias Adaptativo](#)

[Endpoint Sensor](#)

[Kaspersky Sandbox](#)
[Endpoint Detection and Response](#)
[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 no Registo de eventos do Windows](#)
[Anexo 7. Eventos da aplicação no Registo de eventos do Kaspersky Security Center](#)
[Informação acerca de código de terceiros](#)
[Avisos de marcas comerciais](#)

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 excludo um ficheiro fiável das verificações?](#)

[Como é que protejo um computador contra vírus de unidades USB?](#)

[Como é que executo uma verificação de vírus 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?](#)



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?](#)

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

O que há de novo

Atualização 11.8.0

O Kaspersky Endpoint Security for Windows 11.8.0 disponibiliza as seguintes funcionalidades e melhorias:

1. [Foi adicionado o agente integrado para suportar a operação da solução Kaspersky Endpoint Detection and Response Expert](#). O *Kaspersky Endpoint Detection and Response Expert* é uma solução para proteger a infraestrutura de TI corporativa contra ciberameaças avançadas. A funcionalidade da solução combina a detecção 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 obter mais informações sobre a solução, consulte a [Ajuda do Kaspersky Endpoint Detection and Response Expert](#).
2. A interface do [Monitor de Rede](#) foi melhorada. O Monitor de Rede mostra agora o protocolo UDP além do TCP.
3. A tarefa de [Verificação de vírus](#) foi melhorada: Se reiniciou o computador durante a verificação, o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que a verificação foi interrompida.
4. Agora pode definir um limite para o tempo de execução da tarefa. Pode limitar o tempo de execução para as tarefas *Verificação de vírus* e *Verificação IOC*. Após o período especificado, o Kaspersky Endpoint Security interrompe a tarefa. Para reduzir o tempo de execução da tarefa *Verificação de vírus*, pode, por exemplo, [configurar o âmbito de verificação](#) ou [otimizar a verificação](#).
5. As limitações das plataformas de servidores são levantadas para a aplicação instalada no Windows 10 Enterprise multi-sessão. O Kaspersky Endpoint Security agora considera o Windows 10 Enterprise multi-sessão como um sistema operativo de estação de trabalho, e não um sistema operativo de servidores. Da mesma forma, as [limitações da plataforma do servidor](#) já não se aplicam à aplicação no Windows 10 Enterprise multi-sessão. A aplicação usa também uma chave de licença de estação de trabalho, em vez de uma chave de licença de servidor.

Atualização 11.7.0

O Kaspersky Endpoint Security for Windows 11.7.0 disponibiliza as seguintes funcionalidades e melhorias:

1. A [interface do Kaspersky Endpoint Security for Windows](#) está atualizada.
2. [Suporte para Windows 11, Windows 10 21H2 e Windows Server 2022](#).
3. Novos componentes adicionados:
 - Foi adicionado [um agente integrado para o Kaspersky Sandbox](#). A *solução Kaspersky Sandbox* deteta e bloqueia automaticamente ameaças avançadas em computadores. O Kaspersky Sandbox analisa o comportamento do objeto para detetar atividades maliciosas e atividades características de ataques direcionados à infraestrutura de TI da organização. O Kaspersky Sandbox analisa e verifica objetos em servidores especiais com imagens virtuais implementadas de sistemas operativos Microsoft Windows (servidores do Kaspersky Sandbox). Para obter mais informações sobre a solução, consulte a [Ajuda do Kaspersky Sandbox](#).

Já não é preciso o Kaspersky Endpoint Agent para usar o Kaspersky Sandbox. O Kaspersky Endpoint Security pode executar todas as funções do Kaspersky Endpoint Agent. Para migrar as políticas do Kaspersky Endpoint Agent, utilize o [Assistente de migração](#). Precisa do Kaspersky Security Center 13.2 para que todas as funções do Kaspersky Sandbox funcionem. Para obter detalhes sobre a migração do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows, consulte a [ajuda da aplicação](#).

- [Foi adicionado o agente integrado para suportar a operação da solução Kaspersky Endpoint Detection and Response Optimum](#). O *Kaspersky Endpoint Detection and Response Optimum* é uma solução para proteger a infraestrutura de TI da organização contra ciberameaças avançadas. A funcionalidade da solução combina a detecção 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](#).

Já não é preciso o Kaspersky Endpoint Agente para usar o Kaspersky Endpoint Detection and Response. O Kaspersky Endpoint Security pode executar todas as funções do Kaspersky Endpoint Agent. Para migrar as políticas e tarefas do Kaspersky Endpoint Agent, utilize o [Assistente de migração](#). Para usar todas as funções, o Kaspersky Endpoint Detection and Response Optimum exige o Kaspersky Security Center 13.2. Para obter detalhes sobre a migração do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows, consulte a [ajuda da aplicação](#).

4. Foi adicionado o [Assistente de migração](#) das políticas e tarefas do Kaspersky Endpoint Agent. O Assistente de migração cria novas tarefas e políticas combinadas do Kaspersky Endpoint Security for Windows. O assistente permite mudar as soluções do Detection and Response do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security. As soluções Detection and Response incluem o Kaspersky Sandbox, o Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) e o Kaspersky Managed Detection and Response (MDR).

5. O [Kaspersky Endpoint Agent](#), incluído no kit de distribuição, foi atualizado para a versão 3.11.

Ao atualizar o Kaspersky Endpoint Security, a aplicação deteta a versão e o fim estabelecido do Kaspersky Endpoint Agent. Se o Kaspersky Endpoint Agent for designado para o funcionamento do Kaspersky Sandbox, Kaspersky Managed Detection and Response (MDR) e Kaspersky Endpoint Detection and Response Optimum (EDR Optimum), o Kaspersky Endpoint Security muda o funcionamento destas soluções para o agente integrado da aplicação. Para o Kaspersky Sandbox e EDR Optimum, a aplicação desinstala automaticamente o Kaspersky Endpoint Agent. Para o MDR, pode desinstalar o Kaspersky Endpoint Agent manualmente. Se a aplicação for designada para o funcionamento do Kaspersky Endpoint Detection and Response Expert (EDR Expert), o Kaspersky Endpoint Security atualiza a versão do Kaspersky Endpoint Agent. Para obter mais informações sobre a aplicação, consulte a documentação das soluções Kaspersky que suportam o Kaspersky Endpoint Agent.

6. A funcionalidade de encriptação de BitLocker foi melhorada:

- O PIN avançado pode agora ser utilizado com a [Encriptação de Unidade BitLocker](#). O *PIN avançado* permite a utilização de outros caracteres além dos caracteres numéricos: letras latinas maiúsculas e minúsculas, caracteres especiais e espaços.
- Foi adicionada uma funcionalidade para [desativar a autenticação BitLocker para a atualização do sistema operativo ou instalação de pacotes de atualização](#). A instalação de atualizações pode exigir reiniciar o computador várias vezes. Para instalar as atualizações corretamente, pode desativar temporariamente a autenticação do BitLocker e reativar a mesma após a instalação das atualizações.
- Agora pode [definir um tempo de expiração para a password ou PIN de encriptação de BitLocker](#). Quando a password ou PIN expira, o Kaspersky Endpoint Security solicita uma nova password ao utilizador.

7. Agora pode definir o número máximo de tentativas de autorização de teclado para prevenção de ataques BadUSB. Quando [é atingido o número definido de tentativas falhadas para a introdução do código de autorização](#), o dispositivo USB é temporariamente bloqueado.

8. A funcionalidade da firewall foi melhorada:

- Agora pode configurar um intervalo de endereços IP para [Regras de pacote da Firewall](#). Pode introduzir um intervalo de endereços no formato IPv4 ou IPv6. Por exemplo, 192.168.1.1-192.168.1.100 ou 12:34::2-12:34::99.
 - Agora pode introduzir nomes DNS para [Regras de pacote da Firewall](#) em vez de endereços 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.
9. A pesquisa de [regra de Controlo de Internet](#) foi melhorada. Para procurar uma regra de acesso a recurso da Internet, além do nome da regra, pode usar o URL do website, um nome de utilizador, uma categoria de conteúdo ou um tipo de dados.
10. A tarefa de *Verificação de vírus* foi melhorada:
- A tarefa de [Verificação de vírus](#) em inatividade foi melhorada. Se reiniciou o computador durante a verificação, o Kaspersky Endpoint Security executa a tarefa automaticamente, continuando a partir do ponto em que a verificação foi interrompida.
 - A tarefa de [Verificação de vírus](#) foi otimizada. Por predefinição, só o Kaspersky Endpoint Security executa a verificação quando o computador está inativo. Pode configurar o momento da execução da verificação do computador nas propriedades da tarefa.
11. Agora pode restringir o acesso do utilizador aos dados fornecidos pelo [Monitor de atividade das aplicações](#). 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 administrador pode ocultar o Monitor de Atividade das Aplicações do utilizador nas propriedades da política da aplicação.
12. [Maior segurança de gestão da aplicação através da API REST](#). O Kaspersky Endpoint Security agora valida a assinatura das solicitações enviadas através da API REST. Para gerir o programa, precisa de instalar um certificado para identificação de solicitação.

[Atualização 11.6.0](#)

O Kaspersky Endpoint Security for Windows 11.6.0 disponibiliza as seguintes funcionalidades e melhorias:

1. [Suporte para Windows 10 21H1](#). Para obter detalhes sobre o suporte do sistema operativo do Microsoft Windows 10, por favor refira-se ao [Conhecimento de Suporte Técnico](#).
2. [O componente Managed Detection and Response foi adicionado](#). Este componente facilita a interação com a solução conhecida como Kaspersky Managed Detection and Response. O Kaspersky Managed Detection and Response (MDR) fornece proteção 24 horas por dia contra um número cada vez maior de ameaças capazes de contornar os mecanismos de proteção automática para organizações com dificuldades em encontrar especialistas altamente qualificados ou com recursos internos limitados. Para obter mais informações sobre a utilização da solução, consulte a Ajuda do Kaspersky Managed Detection and Response.
3. O [Kaspersky Endpoint Agent](#), incluído no kit de distribuição, foi atualizado para a versão 3.10. O Kaspersky Endpoint Agent 3.10 fornece novas funcionalidades, resolve alguns problemas anteriores e dispõe de maior estabilidade. Para obter mais informações sobre a aplicação, consulte a documentação das soluções Kaspersky que suportam o Kaspersky Endpoint Agent.
4. Agora, oferece a capacidade de fazer a gestão da proteção contra ataques, como, por exemplo, saturação de redes e mapeamento de portas nas [definições de Proteção contra ameaças de Rede](#).
5. Adicionado novo método de criação de regras de rede para a Firewall. Pode adicionar [regras de pacotes](#) e [regras de aplicações](#) para as ligações que forem apresentadas na janela [Monitor de Rede](#). Contudo, as definições de ligação da regra de rede serão configuradas automaticamente.
6. A interface do [Monitor de Rede](#) foi melhorada. Adicionadas as informações sobre a atividade de rede: ID do processo que iniciou a atividade de rede; tipo de rede (rede local ou Internet); portas locais. Por predefinição, as informações sobre o tipo de rede estão ocultas.
7. Agora, passa a estar disponível a capacidade de criar automaticamente contas do Agente de Autenticação para novos utilizadores do Windows. O Agente permite a um utilizador concluir a autenticação para aceder a unidades que foram [encriptadas através da tecnologia Encriptação de disco Kaspersky](#) e para iniciar o sistema operativo. A aplicação verifica as informações sobre as contas de utilizador do Windows no computador. 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. Como tal, não é necessário [adicionar manualmente contas do Agente de Autenticação](#) para computadores com unidades já encriptadas.
8. Agora, passa a estar disponível a capacidade de monitorizar o processo de encriptação de disco na interface da aplicação, nos computadores dos utilizadores (Encriptação de disco Kaspersky e BitLocker). Pode executar a ferramenta Monitor de Encriptação na [janela principal da aplicação](#).

[Atualização 11.5.0](#)





O Kaspersky Endpoint Security for Windows 11.5.0 disponibiliza as seguintes funcionalidades e melhorias:

1. [Suporte para Windows 10 20H2](#). Para obter detalhes sobre o suporte do sistema operativo do Microsoft Windows 10, por favor refira-se ao [Conhecimento de Suporte Técnico](#).
2. [Interface da aplicação](#) atualizada. Também atualizou o [ícone da aplicação na área da notificação](#), notificações da aplicação e caixas de diálogo.
3. Interface melhorada do plug-in da Web do Kaspersky Endpoint Security para os componentes Controlo de Aplicações, Controlo de Dispositivos e Controlo de Anomalias Adaptativo.
4. Funcionalidade adicionada para importar e exportar listas de regras e exclusões no formato XML. O formato XML permite editar listas depois de serem exportadas. Pode gerir listas apenas na Consola do Kaspersky Security Center. As listas que se seguem estão disponíveis para exportação/importação:
 - [Deteção de comportamento \(lista de exclusões\)](#).
 - [Proteção contra ameaças da Web \(Lista de endereços da Internet fiáveis\)](#).
 - [Proteção contra ameaças de correio \(lista de extensões de filtro de anexos\)](#).
 - [Proteção contra ameaças de Rede \(lista de exclusões\)](#).
 - [Firewall \(lista de regras de pacotes de rede\)](#).
 - [Controlo das Aplicações \(lista de regras\)](#).
 - [Controlo de Internet \(lista de regras\)](#).
 - [Monitorização de portas de rede \(listas de portas e aplicações monitorizadas pelo Kaspersky Endpoint Security\)](#).
 - [Encriptação de Disco Kaspersky \(lista de exclusões\)](#).
 - [Encriptação de unidades amovíveis \(lista de regras\)](#).
5. As informações do objeto MD5 foram adicionadas ao [relatório de deteção de ameaças](#). Nas versões anteriores da aplicação, o Kaspersky Endpoint Security mostrava apenas o SHA256 de um objeto.
6. Adicionada capacidade para [atribuir a prioridade para regras de acesso de dispositivos](#) nas definições de Controlo de Dispositivos. A atribuição de prioridades permite uma configuração mais flexível do acesso do utilizador aos dispositivos. 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. 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 0 ao grupo de administradores e atribua uma prioridade de 1 ao grupo Todos. Pode configurar a prioridade apenas para dispositivos que dispõem de um sistema de ficheiros. Isso inclui discos rígidos, unidades amovíveis, disquetes, unidades de CD/DVD e dispositivos portáteis (MTP).
7. Nova funcionalidade adicionada:
 - [Gerir notificações sonoras](#).
 - O Kaspersky Endpoint Security na Rede com Controlo de Custos limita o seu próprio tráfego de rede se a ligação à Internet for limitada (por exemplo, através de uma ligação móvel).

- [Faça a gestão das definições do Kaspersky Endpoint Security através de aplicações de administração remota fiáveis](#) (como TeamViewer, LogMeIn Pro e Remotely Anywhere). Pode usar aplicações de administração remota para iniciar o Kaspersky Endpoint Security e gerir as definições na interface da aplicação.
 - [Faça a gestão das definições de verificação de tráfego seguro no Firefox e Thunderbird](#). Pode seleccionar o armazenamento de certificados que será utilizado pelo Mozilla: o armazenamento de certificados do Windows ou o armazenamento de certificados do Mozilla. Esta funcionalidade está disponível apenas para computadores que não têm uma política aplicada. Se estiver a ser aplicada uma política a um computador, o Kaspersky Endpoint Security ativa automaticamente o uso do armazenamento de certificados do Windows no Firefox e no Thunderbird.
8. Adicionada capacidade para [configurar o modo de verificação de tráfego seguro](#): verifica sempre o tráfego, mesmo que os componentes de proteção estejam desativados, ou verifica o tráfego quando solicitado pelos componentes de proteção.
 9. Procedimento revisto para [eliminação de informações de relatórios](#). Um utilizador só pode eliminar todos os relatórios. Nas versões anteriores da aplicação, um utilizador podia seleccionar componentes específicos da aplicação cujas informações seriam eliminadas dos relatórios.
 10. Procedimento revisto para [importar um ficheiro de configuração contendo definições do Kaspersky Endpoint Security](#) e procedimento revisto para [restaurar as definições da aplicação](#). Antes de importar ou restaurar, o Kaspersky Endpoint Security apresenta apenas um aviso. Nas versões anteriores da aplicação, era possível visualizar os valores das novas definições antes de serem aplicadas.
 11. [Procedimento simplificado para restaurar o acesso a uma unidade encriptada pelo BitLocker](#). Depois de concluir o procedimento de recuperação de acesso, o Kaspersky Endpoint Security solicita ao utilizador que defina uma nova password ou código PIN. Depois de definir uma nova password, o BitLocker encriptará a unidade. Na versão anterior da aplicação, o utilizador tinha de redefinir manualmente a password nas definições do BitLocker.
 12. Os utilizadores agora têm a capacidade de 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](#), além da zona fiável geral numa política. Um administrador pode permitir ou bloquear o uso de exclusões locais ou aplicações fiáveis locais. Um administrador pode usar o Kaspersky Security Center para ver, adicionar, editar ou eliminar itens da lista nas propriedades do computador.
 13. Adicionada capacidade para [introduzir comentários nas propriedades de aplicações fiáveis](#). Os comentários ajudam a simplificar as pesquisas e a classificação das aplicações fiáveis.
 14. [Gestão da aplicação através da API REST](#):
 - Agora existe a capacidade de configurar as definições da extensão Proteção Contra Ameaças de Correio para Outlook.
 - É proibido desativar a deteção de vírus, worms e Trojans.

[Atualização 11.4.0](#)

O Kaspersky Endpoint Security for Windows 11.4.0 disponibiliza as seguintes funcionalidades e melhorias:

1. Novo design do [ícone da aplicação na área de notificação da barra de tarefas](#). O novo ícone  é agora apresentado em vez do antigo . Se o utilizador tiver de executar uma ação (por exemplo, reiniciar o computador depois de atualizar a aplicação), o ícone muda para . Se os componentes de proteção da aplicação estiverem desativados ou apresentarem um funcionamento incorreto, o ícone muda para  ou . Se colocar o rato sobre o ícone, o Kaspersky Endpoint Security apresenta uma descrição do problema na proteção do computador.
2. O Kaspersky Endpoint Agent, incluído no kit de distribuição, foi atualizado para a versão 3.9. O Kaspersky Endpoint Agent 3.9 suporta a integração com novas soluções Kaspersky. Para obter mais informações sobre a aplicação, consulte a documentação das soluções Kaspersky que suportam o Kaspersky Endpoint Agent.
3. Adicionado o estado *Não suportado pela licença* aos componentes do Kaspersky Endpoint Security. Pode visualizar o estado dos componentes na lista de componentes na [janela principal da aplicação](#).
4. Foram adicionados novos eventos da [Prevenção de explorações](#) aos [relatórios](#).
5. Os controladores da [tecnologia Kaspersky Disk Encryption](#) agora são adicionados automaticamente ao Windows Recovery Environment (WinRE) quando a encriptação da unidade é iniciada. A versão anterior do Kaspersky Endpoint Security adicionou controladores ao instalar a aplicação. Adicionar controladores ao WinRE pode melhorar a estabilidade da aplicação ao restaurar o sistema operativo em computadores protegidos pela tecnologia Kaspersky Disk Encryption.

O componente Endpoint Sensor foi removido do Kaspersky Endpoint Security. Ainda 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.

Kaspersky Endpoint Security for Windows

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


Tecnologias de deteção de ameaças

 <h3>Aprendizagem automática</h3> <p>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).</p>	 <h3>Análise comportamental</h3> <p>O Kaspersky Endpoint Security analisa a atividade de um objeto em tempo real.</p>
 <h3>Análise da nuvem</h3> <p>O Kaspersky Endpoint Security recebe dados sobre ameaças da Kaspersky Security Network. A <i>Kaspersky Security Network (KSN)</i> 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.</p>	 <h3>Análise automática</h3> <p>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.</p>
 <h3>Análise especializada</h3> <p>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.</p>	 <h3>Kaspersky Sandbox</h3> <p>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.</p>

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.

Árvore de seleções

Secção	Componente
Proteção essencial contra ameaças 	Proteção contra ameaças de ficheiros <p>O componente Proteção contra ameaças de ficheiros permite prevenir a infeção do sistema de ficheiros do computador. Por predefinição, o componente Proteção contra ameaças de ficheiros reside permanentemente na RAM do computador. O componente verifica ficheiros em todas as unidades do computador, bem como nas unidades ligadas. 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.</p> Proteção contra ameaças da Web

O componente Proteção contra Ameaças da Web impede a transferência de ficheiros maliciosos da Internet e também bloqueia 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 também verifica as mensagens em busca de hiperligações maliciosas e phishing. Por predefinição, o componente Proteção contra ameaças de correio reside permanentemente na RAM do computador e verifica todas as mensagens recebidas ou enviadas usando os protocolos POP3, SMTP, IMAP ou NNTP ou o cliente de correio do Microsoft Office Outlook (MAPI). 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 Rede

O componente Proteção contra ameaças de Rede verifica o tráfego de rede de entrada quanto à existência de atividades típicas de ataques de rede. Quando o Kaspersky Endpoint Security deteta uma tentativa de ataque à rede no computador do utilizador, bloqueia a ligação da rede a o computador atacante. As bases de dados do Kaspersky Endpoint Security 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

A Firewall bloqueia ligações não autorizadas ao computador enquanto trabalha na Internet ou na 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.

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 categoria e reputação dos ficheiros verificados bem como informações sobre a reputação dos endereços da Web verificados.

Deteção de comportamento

O componente Detecção 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 Detecção 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 com base em assinaturas de fluxos de comportamento proporciona defesa proativa ao computador.

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.

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 Motor de remediação permite que o Kaspersky Endpoint Security reverta ações que foram executadas por software malicioso no sistema operativo.

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 dos utilizadores 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 do *Início do Microsoft PowerShell a partir de uma aplicação do escritório*). 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.

Tarefas

Scan de vírus



O Kaspersky Endpoint Security verifica o computador à procura de vírus e outras ameaças. A Verificação de vírus 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

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

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 seleccionar pastas predefinidas para encriptação, seleccionar uma pasta manualmente ou seleccionar 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).

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](#).

Kaspersky Sandbox

Agente integrado para a solução Kaspersky Sandbox. A *solução Kaspersky Sandbox* deteta e bloqueia automaticamente ameaças avançadas em computadores. O Kaspersky Sandbox analisa o comportamento do objeto para detetar atividades maliciosas e atividades características de ataques direcionados à infraestrutura de TI da organização. O Kaspersky Sandbox analisa e verifica objetos em servidores especiais com imagens virtuais implementadas de sistemas operativos Microsoft Windows (servidores do Kaspersky Sandbox). Para obter mais informações sobre a solução, consulte a [Ajuda do Kaspersky Sandbox](#).

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](#).

Funções de serviço da aplicação

O Kaspersky Endpoint Security inclui um conjunto de funções de serviço. As funções de serviço são disponibilizadas a manter a aplicação atualizada, expandir a sua funcionalidade e auxiliar o utilizador na sua utilização.

- **Relatórios.** Durante o seu funcionamento, a aplicação gera um relatório de cada componente da aplicação. Também pode utilizar relatórios para monitorizar os resultados das tarefas concluídas. Os relatórios contêm listas de eventos que ocorreram durante a operação do Kaspersky Endpoint Security e todas as operações realizadas pela aplicação. Em caso de um incidente, pode enviar relatórios para o Kaspersky, onde o problema será verificado em pormenor por especialistas de Suporte Técnico.
- **Cópia de segurança.** Se a aplicação detetar ficheiros infetados ao verificar a existência de vírus e outras ameaças no computador, esses ficheiros são bloqueados. O Kaspersky Endpoint Security armazena cópias de ficheiros desinfetados e apagados na *Cópia de segurança*. O Kaspersky Endpoint Security move os ficheiros que, por alguma razão, não foram processados para a *lista de ameaças ativas*. Pode verificar ficheiros, repor ficheiros nas pastas originais e apagar todos os conteúdos do armazenamento de dados.
- **Notificações.** O serviço de notificação ajuda o utilizador a acompanhar os eventos que influenciam o estado da proteção do computador e a operação do Kaspersky Endpoint Security. As notificações podem ser apresentadas no ecrã ou enviadas por e-mail.
- **Kaspersky Security Network.** A participação dos utilizadores na Kaspersky Security Network melhora a eficiência da proteção informática através da utilização em tempo real de informações sobre a reputação de ficheiros, recursos da Internet e software recebido de utilizadores em todo o mundo.
- **Licença.** Adquirir uma licença desbloqueia todas as funcionalidades da aplicação, fornece acesso a atualizações da base de dados e módulos da aplicação e a suporte telefónico ou por e-mail para questões relacionadas com a instalação, configuração e utilização da aplicação.
- **Suporte.** Todos os utilizadores registados da Kaspersky Endpoint Security podem contactar os especialistas do Suporte Técnico para obter assistência. Pode enviar um pedido ao Suporte Técnico da Kaspersky através do portal Kaspersky CompanyAccount ou contactar o Suporte Técnico por telefone.

Kit de distribuição

O kit de distribuição inclui os seguintes pacotes de distribuição:

- **Encriptação forte (AES256)**

Este pacote de distribuição contém ferramentas criptográficas que implementam o algoritmo de encriptação AES (Padrão de Encriptação Avançado) com um comprimento de chave de 256 bits.

- **Encriptação leve (AES56)**

Este pacote de distribuição contém ferramentas criptográficas que implementam o algoritmo de encriptação AES com um comprimento de chave de 56 bits.

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 de plug-in de gestão de Kaspersky Endpoint Security do Kaspersky Security Center.
bases.cab	Os ficheiros do pacote de atualização que são usados durante a instalação.
cleaner.cab	Ficheiros para remover o software incompatível.
incompatible.txt	Ficheiro que contém uma lista do software incompatível.
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.
endpointagent.msi	Pacote de instalação do Kaspersky Endpoint Agent , que é necessário para integração com outras soluções Kaspersky (por exemplo, Kaspersky Sandbox).
NDP<versão>-<propriedades do pacote>	Pacote de instalação do Microsoft .NET Framework.
keswin_web_plugin.zip	Arquivo que contém os ficheiros necessários para instalar o plug-in da Web do Kaspersky Endpoint Security .

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

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

Requisitos gerais mínimos:

- 2 GB de espaço disponível no disco rígido;
- CPU:
 - Estação de trabalho: 1 GHz;
 - Servidor: 1.4 GHz;
 - Suporte para o conjunto de instruções SSE2.
- RAM:
 - Estação de trabalho (x86): 1 GB;
 - Estação de trabalho (x64): 2 GB;
 - Servidor: 2 GB.

Estações de trabalho

Sistemas operativos suportados para as estações de trabalho:

- Windows 7 Home/Professional/Ultimate/Enterprise Service Pack 1 ou posterior;
- Windows 8 Professional/Enterprise;
- Windows 8.1 Professional/Enterprise;
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-sessão;
- Windows 11.

O algoritmo de assinatura do módulo SHA-1 foi preterido pela Microsoft. A atualização KB4474419 é necessária para a instalação bem-sucedida do Kaspersky Endpoint Security num computador com o sistema operativo Microsoft Windows 7. Para obter mais detalhes sobre esta atualização, visite o [site de suporte técnico da Microsoft](#).

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 11.8.0 traz suporte para os principais componentes da aplicação em computadores com o sistema operativo Windows para servidores. Agora pode usar o Kaspersky Endpoint Security for Windows em vez do Kaspersky Security for Windows Server em servidores e clusters da sua organização. O Modo Central é suportado com [limitações](#).

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 / Datacenter Service Pack 1 ou posterior;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation/Essentials/Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

O algoritmo de assinatura do módulo SHA-1 foi preterido pela Microsoft. A atualização KB4474419 é necessária para a instalação bem-sucedida do Kaspersky Endpoint Security num computador com o sistema operativo Microsoft Windows Server 2008 R2. Para obter mais detalhes sobre esta atualização, visite o [site de suporte técnico da Microsoft](#).

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](#).

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.

Plataformas virtuais

Plataformas virtuais suportadas:

- VMware Workstation 16.1.2;
- VMware ESXi 7.0 Update 3;
- Microsoft Hyper-V Server 2019;
- Citrix Virtual Apps and Desktops 7 2106;
- Citrix Provisioning 2109;
- Citrix Hypervisor 8.2 (Hotfix XS82E033).

O Kaspersky Endpoint Security suporta o funcionamento com as seguintes versões do Kaspersky Security Center:

- Kaspersky Security Center 11;
- Kaspersky Security Center 12;
- Kaspersky Security Center 12 Patch A;
- Kaspersky Security Center 12 Patch B;
- Kaspersky Security Center 13;
- Kaspersky Security Center 13.1;
- Kaspersky Security Center 13.2;
- Kaspersky Security Center 13.2.2.

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).

Comparação das funcionalidades do Kaspersky Endpoint Security

Funcionalidade	Estação de trabalho	Servidor
Proteção avançada contra ameaças		
Kaspersky Security Network	✓	✓
Deteção de comportamento	✓	✓

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		
Controlo das Aplicações	✓	✓
Controlo de Dispositivos	✓	✓
Controlo de Internet	✓	✓
Controlo de Anomalias Adaptativo	✓	–
Encriptação de dados		
Encriptação de disco Kaspersky	✓	–
Encriptação de Unidade BitLocker	✓	✓
Encriptação ao nível dos ficheiros	✓	–
Encriptação de unidades amovíveis	✓	–
Detection and Response		
Kaspersky Endpoint Agent	✓	✓
Endpoint Detection and Response Optimum	✓	✓
Endpoint Detection and Response Expert	✓	✓
Kaspersky Sandbox	✓	✓
Managed Detection and Response	✓	✓

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 Consola da Web com navegador em qualquer computador com acesso ao Servidor de Administração.

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](#).

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	✓	✓	✓
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			
Controlo das Aplicações	✓	✓	✓
Controlo de Dispositivos	✓	✓	✓
Controlo de Internet	✓	✓	✓
Controlo de Anomalias Adaptativo	✓	✓	✓
Encriptação de dados			
Encriptação de disco Kaspersky	✓	✓	–
Encriptação de Unidade BitLocker	✓	✓	✓
Encriptação ao nível dos ficheiros	✓	✓	–
Encriptação de unidades amovíveis	✓	✓	–

Detection and Response			
Kaspersky Endpoint Agent	✓	✓	✓
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert	–	–	✓
Kaspersky Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
Tarefas			
Adicionar chave	✓	✓	✓
Change application components	✓	✓	✓
Inventário	✓	✓	✓
Atualização	✓	✓	✓
Reverter atualização	✓	✓	✓
Scan de vírus	✓	✓	✓
Verificação de integridade	✓	✓	–
Eliminar dados	✓	✓	✓
Gestão de contas do Agente de Autenticação (Kaspersky Disk Encryption)	✓	✓	–
Verificação IOC (EDR)	–	✓	✓
Mover ficheiro para Quarentena (EDR)	–	✓	✓
Obter ficheiro (EDR)	–	✓	✓
Delete file (EDR)	–	✓	✓
Início do processo (EDR)	–	✓	✓
Terminação de processo (EDR)	–	✓	✓

Compatibilidade com outras aplicações

Antes da instalação, o Kaspersky Endpoint Security verifica se existem outras aplicações da Kaspersky no computador. A aplicação também verifica se o computador contém software incompatível. A lista de softwares incompatíveis está disponível no ficheiro incompatible.txt que está incluído no [kit de distribuição](#).



[TRANSFERIR O FICHEIRO INCOMPATIBLE.TXT](#)

O Kaspersky Endpoint Security não é compatível com as seguintes aplicações da Kaspersky:

- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.

- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Kaspersky Anti Targeted Attack Platform (incluindo o componente Endpoint Sensor).
- Kaspersky Sandbox (incluindo o Kaspersky Endpoint Agent).
- Kaspersky Endpoint Detection and Response (incluindo o componente Endpoint Sensor).

Se o componente Endpoint Agent for instalado num computador com as ferramentas de implementação de outras aplicações Kaspersky, o componente será automaticamente removido durante a instalação do Kaspersky Endpoint Security. O Kaspersky Endpoint Security também pode incluir o componente Endpoint Sensor / Kaspersky Endpoint Agent se selecionar o Endpoint Agent na lista de componentes da aplicação.

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

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](#).

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

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. 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](#).

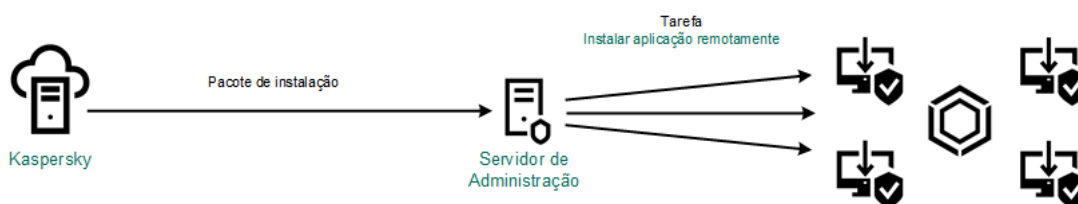
Instalação padrão da aplicação

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. Na Consola de Administração, aceda à pasta **Administration Server** → **Additional** → **Remote installation**.

2. 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 seleccionar 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 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 3. 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.** 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 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 seleccionar 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 seleccionar 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.** Seleccionar 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 Directório Ativo. Para instalar o Agente de Rede, a tarefa de instalação remota deve ser executada com privilégios de administrador de domínio.

Passo 4. Seleccionar 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 5. Seleccionar a definição de reinicialização do sistema operativo

Selecione a ação que deve ser executada se for necessário um reinício de computador. Reinício não é necessário ao instalar o Kaspersky Endpoint Security. O reinício 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. 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 7. Seleccionar 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 seleccionar uma conta se instalar o Kaspersky Endpoint Security utilizando ferramentas do Agente de Rede.

Passo 8. Iniciar a instalação

Sair do 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, seleccione **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 seleccionar 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.** Selecione o método de instalação da aplicação:
 - **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 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 seleccionar 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 seleccionar 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 Directório 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. Reinício não é necessário ao instalar o Kaspersky Endpoint Security. O reinício 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 seleccionar um grupo de administração, os computadores serão adicionados ao grupo de **Dispositivos não atribuídos**.

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 seleccionar uma conta se instalar o Kaspersky Endpoint Security utilizando ferramentas do Agente de Rede.

Passo 10. Iniciar instalação

Sair do 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, dirija-se à pasta **Administration Server** → **Additional** → **Remote installation** → **Installation packages**.

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

2. Clique no botão **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 11.8.0*.

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 também selecionar os componentes da aplicação e configurar as definições da instalação da aplicação (consulte a tabela abaixo). O pacote de instalação inclui bases de dados de antivírus do repositório do Servidor de Administração. Pode [update the databases in the installation package](#) 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 Consola da Web e na Consola da Nuvem](#) 

1. Na janela principal da Consola Web, seleccione **Discovery & Deployment** → **Deployment & Assignment** → **Installation packages**.

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

2. Clique no botão **Add**.

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**.

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.

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.

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 também seleccionar os componentes da aplicação e configurar as definições da instalação da aplicação (consulte a tabela abaixo). O pacote de instalação inclui bases de dados de antivírus do repositório do Servidor de Administração. Pode [update the databases in the installation package](#) para reduzir o consumo de tráfego quando atualizar as bases de dados depois de instalar o Kaspersky Endpoint Security.

Definições do pacote de instalação

Secção	Descrição
Componentes de proteção	<p>Nesta secção, pode seleccionar os componentes da aplicação que estarão disponíveis. Pode alterar o conjunto de componentes da aplicação mais tarde utilizando a tarefa <i>Change application components</i>. Por predefinição, o componente Prevenção de ataques BadUSB, o componente Detection and Response e os componentes de Encriptação de dados não são instalados. Estes componentes podem ser adicionados nas definições do pacote de instalação.</p> <p>Se precisar de instalar os componentes Detection and Response components, o Kaspersky Endpoint Security suporta as seguintes configurações:</p> <ul style="list-style-type: none">• Apenas Endpoint Agent• Apenas Endpoint Detection and Response Optimum• Apenas Endpoint Detection and Response Expert• Apenas Kaspersky Sandbox

	<ul style="list-style-type: none"> • Endpoint Detection and Response Optimum e Kaspersky Sandbox • Endpoint Detection and Response Expert e Kaspersky Sandbox. <p>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.</p>
Chave da licença	<p>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.</p>
Aplicações incompatíveis	<p>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.</p>
Definições de instalação	<p>Add application location to environment variable %PATH%. Pode adicionar o caminho de instalação à variável %PATH% para utilização conveniente da interface da linha de comando.</p> <p>Do not 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.</p> <p>Garanta a compatibilidade com Citrix PVS (esta opção apenas é necessária com Citrix PVS). Pode ativar o suporte dos Citrix Provisioning Services para instalar o Kaspersky Endpoint Security numa máquina virtual.</p> <p>Caminho para a pasta de instalação da aplicação. Pode alterar o caminho de instalação do Kaspersky Endpoint Security num computador de cliente. Por predefinição, a aplicação é instalada na pasta %ProgramFiles%\Kaspersky Lab\Kaspersky Endpoint Security for Windows.</p> <p>Ficheiro de configuração. Pode carregar um ficheiro que define as definições do Kaspersky Endpoint Security. Pode criar um ficheiro de configuração na interface local da aplicação.</p>

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 *Transferir atualizações para do repositório do Servidor de Administração* 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. Na Consola de Administração, dirija-se à pasta **Administration Server** → **Additional** → **Remote installation** → **Installation packages**.

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

2. Abra as propriedades do pacote de instalação.
3. Na secção **General**, clique no botão **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 concebida 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. Na Consola de Administração, dirija-se à pasta **Administration Server** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **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 seleccionar 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 seleccionada 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.** Seleccionar o método de instalação da aplicação:
 - **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 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 seleccionar 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 seleccionar 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. Reinício não é necessário ao instalar o Kaspersky Endpoint Security. O reinício 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 11.8.0*.

Passo 10. Concluir a criação da tarefa

Sair do 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 de Web, seleccione **Devices** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **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**, seleccione **Kaspersky Security Center**.

2. Na lista pendente **Task type**, seleccione **Install application remotely**.

3. No campo **Task name**, introduza uma breve descrição, por exemplo, *Installation of Kaspersky Endpoint Security for Managers*.

4. Na secção **Select devices to which the task will be assigned**, seleccione o âmbito de tarefa.

Passo 2. Selecionar computadores para instalação

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

Passo 3. Configurar um pacote de instalação

Neste passo, configure o pacote de instalação:

1. Seleccione o pacote de instalação do Kaspersky Endpoint Security for Windows (11.8.0).

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

A versão seleccionada 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. Na secção **Force installation package download** section, seleccione o método de instalação de aplicação:

- **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 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 seleccionar 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 na secção **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 múltiplas 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 **Concluir**. 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 **k** será adicionado à área de notificação do computador do utilizador. Se o ícone tiver o seguinte aspeto **k**, 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.

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:

- Presença de software incompatível instalado (a lista de software incompatível 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 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.

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 11.8.0 for Windows, e a versão anterior da aplicação é automaticamente removida. Isto aplica-se às seguintes versões da aplicação:

- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows (compilação 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 for Windows (compilação 10.3.3.304).
- Kaspersky Endpoint Security 11.0.0 for Windows (compilação 11.0.0.6499).
- Kaspersky Endpoint Security 11.0.1 for Windows (compilação 11.0.1.90).
- Kaspersky Endpoint Security 11.0.1 for Windows SF1 (compilação 11.0.1.90).
- Kaspersky Endpoint Security 11.1.0 for Windows (compilação 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 for Windows (compilação 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 for Windows (compilação 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 for Windows CF1 (compilação 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 for Windows (compilação 11.3.0.773).

- Kaspersky Endpoint Security 11.4.0 for Windows (compilação 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 for Windows (compilação 11.5.0.590).
- Kaspersky Endpoint Security 11.6.0 for Windows (compilação 11.6.0.394).
- Kaspersky Endpoint Security 11.7.0 for Windows (compilação 11.7.0.669).

Componentes do Kaspersky Endpoint Security

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

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

- [Prevenção de ataques BadUSB](#).
- [Componentes da encriptação de dados](#).
- Componentes Detection and Response.

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:

- Apenas Endpoint Agent
- Apenas Endpoint Detection and Response Optimum
- Apenas Endpoint Detection and Response Expert
- Apenas Kaspersky Sandbox
- Endpoint Detection and Response Optimum e Kaspersky Sandbox
- Endpoint Detection and Response Expert e Kaspersky Sandbox.

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.

Definições avançadas

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 (esta opção apenas é necessária com Citrix PVS). Pode ativar o suporte dos Citrix Provisioning Services para instalar o Kaspersky Endpoint Security numa máquina virtual.

Add application location to environment variable %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, na secção **Gestão de aplicações**, seleccione **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**, seleccione 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** seleccionado.
 - d. Na secção **Requisitos**:
 - Seleccione a caixa de verificação **Executar primeiro outro programa** se pretender que seja iniciada uma aplicação diferente antes de instalar o Kaspersky Endpoint Security.
Seleccione 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** na secção **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.



[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. 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. O componente Managed Detection and Response também não se encontra

neste bloco. Para instalar este componente, tem de [ativar o Managed Detection and Response na Consola do Kaspersky Security Center](#).

- [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 `sim`, `ativado`, `ativar` e `ativado`.

As alternativas ao valor 0 são os valores `não`, `desativado`, `desativar` e `desativado`.

Configurações do ficheiro setup.ini

Secção	Parâmetro	Descrição
[Setup]	InstallDir	Caminho para a pasta de instalação da aplicação.
	ActivationCode	Código de ativação do Kaspersky Endpoint Security.
	EULA=1	<p>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.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>É necessário aceitar os termos do Contrato de Licença do Utilizador Final para instalar a aplicação ou para atualizar a versão da aplicação.</p> </div>
	PrivacyPolicy=1	<p>Aceitação da Política de Privacidade. O texto da Privacy Policy encontra-se incluído no kit de distribuição do Kaspersky Endpoint Security.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Para instalar a aplicação ou atualizar a versão da aplicação, tem de aceitar a Privacy Policy.</p> </div>
	KSN	<p>Aceitar ou recusar participar na Kaspersky Security Network. 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:</p> <ul style="list-style-type: none"> • 1 - acordo para participar na KSN. • 0 – Recusar participar na KSN (valor predefinido). <p>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.</p>

	Entrar	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 Início de sessão, 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 Iniciar sessão e Password). Utilize o carácter ";" para especificar vários valores. Valores disponíveis: <ul style="list-style-type: none"> • 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.
	Autoproteção	Ativação ou desativação do mecanismo de proteção de instalação da aplicação. Valores disponíveis: <ul style="list-style-type: none"> • 1 – o mecanismo de proteção de instalação de aplicação é ativado (valor predefinido). • 0 – o mecanismo de proteção de instalação de aplicação é desativado.

		<p>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.</p>
	Reboot=1	<p>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.</p> <p>Reinício não é necessário ao instalar o Kaspersky Endpoint Security. O reinício é necessário apenas se precisar de remover aplicações incompatíveis antes da instalação. Reinício pode também ser necessário ao atualizar a versão da aplicação.</p>
	AddEnvironment	<p>Complementar a variável de sistema %PATH% com o caminho para os ficheiros executáveis localizados na pasta de instalação do Kaspersky Endpoint Security. Valores disponíveis:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>A tecnologia AM-PPL está disponível para os sistemas operacionais Windows 10 versão 1703 (RS2) ou posterior e Windows Server 2019.</p> <p>Valores disponíveis:</p> <ul style="list-style-type: none"> • 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.
	SetupReg	<p>Ativa a escrita das chaves de registo do ficheiro setup.reg para o registo. Valor do parâmetro SetupReg: setup.reg.</p>
	EnableTraces	<p>Ativar ou desativar os rastreios da aplicação. Depois de</p>

		<p>iniciado, o Kaspersky Endpoint Security guarda os ficheiros de rastreio na pasta %ProgramData%\Kaspersky Lab\KES\Traces. Valores disponíveis:</p> <ul style="list-style-type: none"> • 1 – os rastreios estão ativados. • 0 – os rastreios estão desativados (valor padrão).
	TracesLevel	<p>Nível de detalhe do rastreio. Valores disponíveis:</p> <ul style="list-style-type: none"> • 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	<p>Gestão da aplicação com API REST. Para gerir a aplicação com API REST, deve especificar o nome do utilizador (parâmetro RESTAPI_User).</p> <p>Valores disponíveis:</p> <ul style="list-style-type: none"> • 1 - a gestão com API REST é permitida. • 0 - a gestão com API REST é bloqueada (valor predefinido). <p>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.</p>
	RESTAPI_User	<p>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 seleccionar um utilizador para trabalhar com API REST.</p> <p>Adicionar um nome de utilizador é um pré-requisito para gerir a aplicação com API REST.</p>
	RESTAPI_Port	<p>Porta usada para gerir a aplicação com API REST. A porta 6782 é usada por defeito.</p>
		<p>Certificado de identificação de solicitações (por</p>

	RESTAPI_Certificate	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.
[Components]	ALL	<p>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.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Devido ao modo como as soluções Detection and Response são suportadas, os componentes Endpoint Detection and Response Optimum e Kaspersky Sandbox são instalados no computador. Os componentes Endpoint Detection and Response Expert e Endpoint Agent não são compatíveis com esta configuração.</p> </div>
	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.
	FileEncryption	Bibliotecas de encriptação ao nível dos ficheiros.
	DiskEncryption	Bibliotecas de Encriptação Completa do Disco.
	BadUSBAttackPrevention	Prevenção de ataques BadUSB.
	AntiAPT	<p>Agente de Endpoint. O Endpoint Agent instala o Kaspersky Endpoint Agent. O Kaspersky Endpoint Agent suporta soluções de Detection and Response para deteção de ameaças avançada (por exemplo, Kaspersky Sandbox).</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>O componente não é compatível com os componentes do EDR Optimum (EDR), do EDR Expert (EDRCloud) e do Kaspersky Sandbox (SB).</p> </div>

	EDR	Endpoint Detection and Response Optimum (EDR Optimum). O componente não é compatível com os componentes do Endpoint Agent (AntiAPT) e do EDR Expert (EDRCloud).
	EDRCloud	Endpoint Detection and Response Expert (EDR Expert). O componente não é compatível com os componentes do Endpoint Agent (AntiAPT) e do EDR Optimum (EDR).
	SB	Kaspersky Sandbox. O componente é incompatível com o componente Endpoint Agent (AntiAPT).
	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: <ul style="list-style-type: none"> • 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.
[Tasks]	ScanMyComputer	Tarefa de Verificação Completa. Valores disponíveis: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.
	Atualização	Tarefa de atualização. Valores disponíveis:

- | | | |
|--|--|---|
| | | <ul style="list-style-type: none">• 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. |
|--|--|---|

Change application components

Durante a instalação da aplicação, pode seleccionar 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.

- Remotamente, utilizando o Kaspersky Security Center.

A tarefa *Alterar os componentes de 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, descripte 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.

[Como adicionar ou remover componentes de aplicações na Consola de Administração \(MMC\)](#) 

1. Na Consola de Administração, dirija-se à pasta **Administration Server** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **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 (11.8.0)** → **Change application components**.

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

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

Selecione a caixa de verificação **Remover aplicações de terceiros incompatíveis**. A lista de aplicações incompatíveis pode ser consultada em `incompatible.txt`, incluída no [kit de distribuição](#). Se forem instaladas aplicações incompatíveis no computador, a instalação do Kaspersky Endpoint Security termina com um erro.

Se necessário, ative [proteção por palavra-passe](#) para desempenho do tarefas:

1. Clique no botão **Adicional**.

2. Selecione a caixa de verificação **Utilizar password para modificar um conjunto de componentes da aplicação**.

3. Introduza as credenciais da conta do utilizador do KLAdmin.

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, por exemplo, *Adicionar o componente Controlo das Aplicações*.

Passo 6. Completar a criação da tarefa

Sair do 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.

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.

[Como adicionar ou remover componentes de aplicações na Consola da Web e Consola da Nuvem](#) 

1. Na janela principal da Consola de Web, seleccione **Devices** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **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 suspensa **Application**, seleccione **Kaspersky Endpoint Security for Windows (11.8.0)**.

2. Na lista pendente **Task type**, seleccione **Change application components**.

3. No campo **Task name**, introduza uma breve descrição, por exemplo, *Add the Application Control component*.

4. No bloco **Select devices to which the task will be assigned**, seleccione 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, seleccione um grupo de administração separado ou compile uma selecção.

Passo 3. Completar a criação da tarefa

Selecione a caixa de verificação **Open task details when creation is complete** e termine o Assistente. Nas propriedades da tarefa, seleccione o separador **Definições da Aplicação** e seleccione os componentes da aplicação que estarão disponíveis.

Se necessário, ative [proteção por palavra-passe](#) para desempenho do tarefas:

1. No bloco **Definições avançadas**, seleccione a caixa de verificação **Utilizar password para modificar um conjunto de componentes da aplicação**.

2. Introduza as credenciais da conta do utilizador do KLAdmin.

Guarde as alterações e execute a tarefa.

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.

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.
- Se o computador tiver discos rígidos encriptados a utilizar a [Encriptação de disco completa \(FDE\)](#), será necessário descriptar todos os discos rígidos encriptados para atualizar o Kaspersky Endpoint Security da versão 10 até à versão 11.0.0 ou posterior.

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.

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

- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows (compilação 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 for Windows (compilação 10.3.3.304).
- Kaspersky Endpoint Security 11.0.0 for Windows (compilação 11.0.0.6499).
- Kaspersky Endpoint Security 11.0.1 for Windows (compilação 11.0.1.90).
- Kaspersky Endpoint Security 11.0.1 for Windows SF1 (compilação 11.0.1.90).
- Kaspersky Endpoint Security 11.1.0 for Windows (compilação 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 for Windows (compilação 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 for Windows (compilação 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 for Windows CF1 (compilação 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 for Windows (compilação 11.3.0.773).
- Kaspersky Endpoint Security 11.4.0 for Windows (compilação 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 for Windows (compilação 11.5.0.590).
- Kaspersky Endpoint Security 11.6.0 for Windows (compilação 11.6.0.394).
- Kaspersky Endpoint Security 11.7.0 for Windows (compilação 11.7.0.669).

Ao atualizar o Kaspersky Endpoint Security 10 Service Pack 2 for Windows para o Kaspersky Endpoint Security 11.8.0 for Windows, os ficheiros que tinham sido colocados na Cópia de segurança ou em Quarentena na versão anterior da aplicação são transferidos para a Cópia de segurança na nova versão da aplicação. Para versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows, os ficheiros que tenham sido colocados na Cópia de segurança e de Quarentena numa versão anterior da aplicação não são migrados para a versão mais recente.

O Kaspersky Endpoint Security pode ser atualizado no 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](#).

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

- Consola Web do Kaspersky Security Center ou Consola de Nuvem 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 de componentes predefinidos, por exemplo, a Prevenção de ataques BadUSB será removida do computador, pois 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](#).

Remover a aplicação

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

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

- localmente, usando o [Assistente de Configuração](#);
- localmente a partir da [command line](#);
- remotamente, utilizando o Kaspersky Security Center (consulte a [Ajuda do Kaspersky Security Center](#) para obter informações adicionais);
- remotamente, através do Microsoft Windows Group Policy Management Editor (para obter mais detalhes, visite o [Website de Suporte Técnico da Microsoft](#)).

Se tiver selecionado o componente agente Endpoint durante a instalação da aplicação, serão instaladas no computador as duas aplicações que se seguem: Kaspersky Endpoint Security e Kaspersky Endpoint Agent. Após a desinstalação do Kaspersky Endpoint Security, o Kaspersky Endpoint Agent também será desinstalado automaticamente.

Desinstalar 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. Na Consola de Administração, dirija-se à pasta **Administration Server** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **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** → **Additional** → **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 (11.8.0)**.

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 seleccionar 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 seleccionar 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. Clique no botão **Editar**.

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 seleccionar 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 11.8.0*.

Passo 10. Concluir a criação da tarefa

Sair do 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.

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

A lista de tarefas é aberta.

2. Clique no botão **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, *Uninstall Kaspersky Endpoint Security from Technical Support computers*.

4. Na secção **Select 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 **Uninstall managed application**.

2. Selecione **Kaspersky Endpoint Security for Windows (11.8.0)**.

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 seleccionar 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 seleccionar 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 seleccionar 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 **Concluir**. Será apresentada uma nova tarefa na lista de tarefas.

Para executar uma tarefa, selecione a caixa de selecção 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 [protegido 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 Desinstalar aplicação remotamente:

1. Na janela principal da Consola de Web, selecione **Devices** → **Tasks**.
A lista de tarefas é aberta.
2. Clique na tarefa do Kaspersky Security Center **Uninstall application remotely**.
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.

Desinstalar a aplicação utilizando o Assistente

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.

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.

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.

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\Kaspersky Endpoint Security for Windows\Doc\

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.
- *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:

- Chave 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 caracteres alfanuméricos. Introduce 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.

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 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
Proteção avançada contra ameaças						
Kaspersky Security Network	✓	✓	✓	✓	✓	✓
Deteção de comportamento	✓	✓	✓	✓	✓	✓
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						
Controlo das Aplicações	✓	✓	✓	✓	✓	✓
Controlo de Dispositivos	✓	✓	✓	✓	✓	✓
Controlo de Internet	✓	✓	✓	✓	✓	✓
Controlo de Anomalias Adaptativo	–	✓	✓	✓	✓	✓
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 <i>(A licença do Kaspersky Sandbox tem de ser comprada em separado)</i>	✓	✓	✓	✓	✓	✓

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 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
Proteção avançada contra ameaças						
Kaspersky Security Network	✓	✓	✓	✓	✓	✓
Deteção de comportamento	✓	✓	✓	✓	✓	✓
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						
Controlo das Aplicações	-	✓	✓	✓	✓	✓
Controlo de Dispositivos	-	✓	✓	✓	✓	✓
Controlo de Internet	-	✓	✓	✓	✓	✓
Controlo de Anomalias Adaptativo	-	-	-	-	-	-
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)

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 a partir da interface da aplicação, utilizando o [Assistente de Ativação](#) pode adicionar tanto a chave ativa como a chave de reserva deste modo.
- Remotamente com o [software do Kaspersky Security Center](#) criando e depois iniciando uma tarefa de inclusão da chave de licença. É possível adicionar a chave ativa e a chave de reserva desta forma.
- Remotamente, através da distribuição de ficheiros de chave e códigos de ativação armazenados no armazenamento de chaves do Servidor de Administração do Kaspersky Security Center para computadores cliente. Para obter mais informações sobre a distribuição de chaves, consulte a [Ajuda do Kaspersky Security Center](#). É possível adicionar a chave ativa e a chave de reserva desta forma.

O código de ativação adquirido com subscrição é distribuído em primeiro lugar.

- Utilização da [Command line](#).

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.

Ativar a aplicação através do Kaspersky Security Center

Pode ativar a aplicação remotamente através do Kaspersky Security Center das seguintes maneiras:

- 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.

- 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](#).


- 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.

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](#)².

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.

Pode monitorizar a utilização de licenças dos seguintes modos:

- Ver o *Relatório de utilização de chaves* para a infraestrutura da organização (**Monitoring and reporting** → **Relatórios**).
- Ver os estados dos computadores no separador **Devices** → **Managed 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 as propriedades da chave (**Operações** → **Licenciamento**).

[Como ativar a aplicação na Consola de administração \(MMC\)](#)²

1. Na Consola de Administração, dirija-se à pasta **Administration Server** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **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 (11.8.0)** → **Add key**.

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

Sair do 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.

1. Na janela principal da Consola de Web, seleccione **Devices** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **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 suspensa **Application**, seleccione **Kaspersky Endpoint Security for Windows (11.8.0)**.

2. Na lista pendente **Task type**, seleccione **Add key**.

3. No campo **Task name**, introduza uma breve descrição, por exemplo, *Activation of Kaspersky Endpoint Security for Windows*.

4. Na secção **Select devices to which the task will be assigned**, seleccione 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.
- Seleccione 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 **Concluir**. Será apresentada uma nova tarefa na lista de tarefas. Para executar uma tarefa, seleccione a caixa de selecção em frente da tarefa e clique no botão **Start**. Como resultado, o Kaspersky Endpoint Security será ativado nos computadores dos utilizadores no modo silencioso.

Nas propriedades da tarefa *Add key*, pode adicionar uma chave de reserva ao computador. Uma *chave de reserva* é ativada quando a chave ativa expira ou é eliminada. 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 **Administration Server** → **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 distributed license key**.

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, seleccione **Operations** → **Licensing** → **Kaspersky Licenses**.

Uma lista de chaves de licença surge.

2. Abra as propriedades da chave de licença.

3. No separador **General**, ative o botão **Deploy license key automatically**.

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**.

Utilizar o Assistente de Ativação para ativar a aplicação

Para ativar o Kaspersky Endpoint Security através do Assistente de Ativação:

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

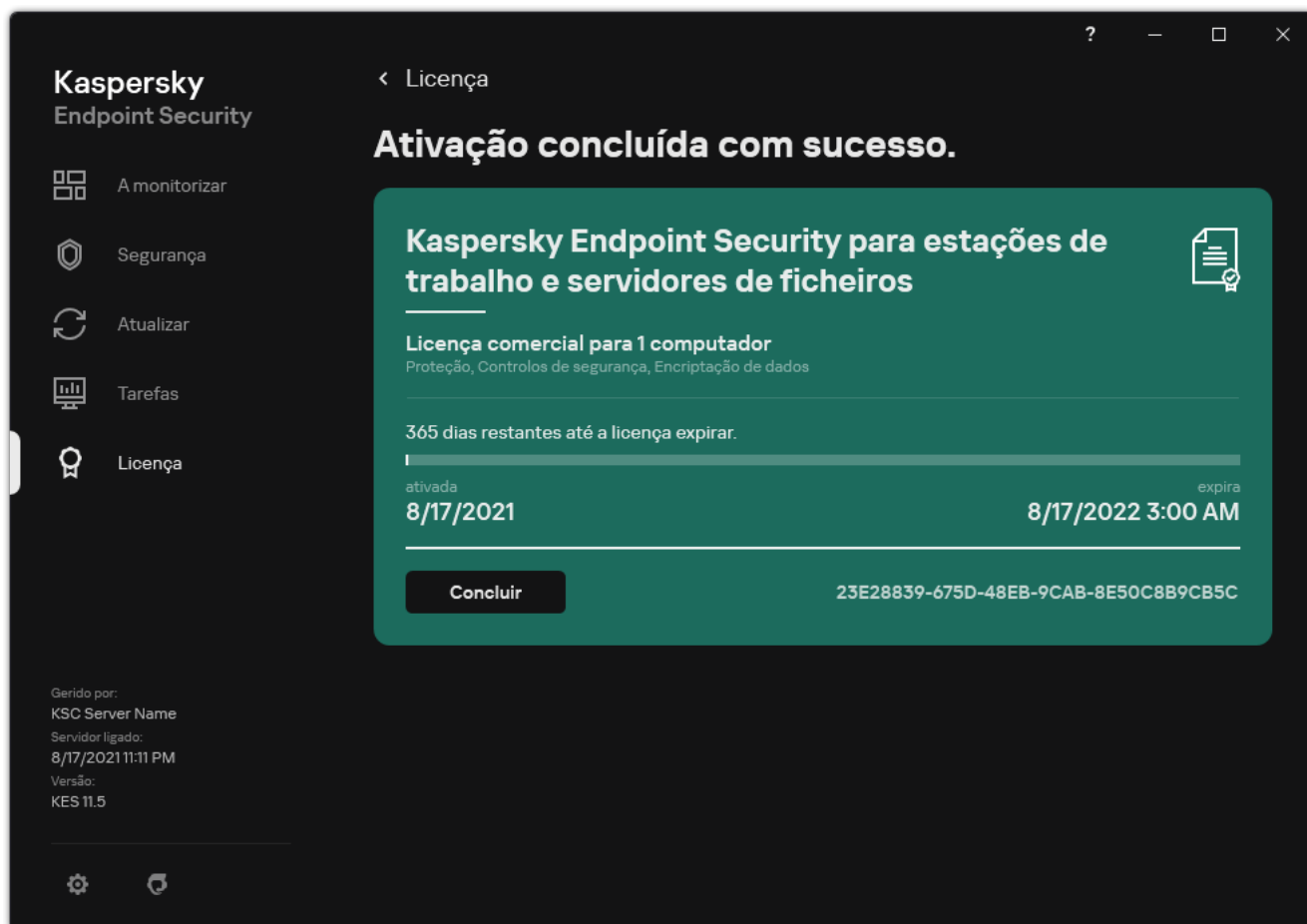
2. Seleccione o botão **Ativar a aplicação com uma licença nova**.

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

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 de 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 no botão **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.

Fornecimento de dados

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 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 ativa é aplicada;
- chave ativa;
- Validade da licença do Kaspersky Endpoint Security;
- estado atual da licença;
- tipo de licença ativa;
- 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 de canais de comunicação encriptados.

Leia o Contrato de Licença do Utilizador Final e visite o [site da Kaspersky](#) para obter mais informações sobre a receção, 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 (somadas 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 somadas de verificação (MD5, SHA2-256, SHA1), informação sobre o processo que transferiu o ficheiro, (somadas 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 somadas 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, somadas 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, somadas 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 registos nessas 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, CUID, 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 PID], 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](#) e [Kaspersky Sandbox](#). 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 Verificação IOC (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 solicitação 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 Verificação IOC (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 solicitação HTTP

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.
- Gravação de descarga.

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 receção, 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 KSN Privada ou [desative a utilização da KSN](#). Para obter mais informações detalhadas sobre o KSN Privado, 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.

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

A Consola Web do Kaspersky Security Center (doravante também referido como *Consola Web*) é uma aplicação Web para executar centralmente as tarefas principais para gerir e manter o sistema de segurança da rede de uma organização. A Consola de Web é um componente do Kaspersky Security Center que disponibiliza uma interface de utilizador. 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. Ao contrário do Management Plug-in da Consola de Administração do Kaspersky Security Center, que é instalada na estação de trabalho de um administrador, o plug-in Web deve ser instalado num computador com o Kaspersky Security Center Web Console instalado. 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**. Para obter mais informações sobre a compatibilidade das versões do plug-in Web e da Consola Web, consulte a [Ajuda do Kaspersky Security Center](#) ².

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 Web do Kaspersky Security Center, consulte a [Ajuda do Kaspersky Security Center](#) ².

- 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.

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.

Atualizar o plug-in de gestão do Kaspersky Endpoint Security 10 for Windows

Se o plug-in de gestão do Kaspersky Endpoint Security 10 for Windows for instalado na Consola de Administração, considere o seguinte ao instalar o plug-in de gestão do Kaspersky Endpoint Security 11 for Windows:

- O plug-in de gestão do Kaspersky Endpoint Security 10 for Windows não será removido e permanecerá disponível para funcionamento. Como tal, terá acesso a dois plug-ins de gestão para trabalhar com as versões da aplicação 10 e 11.
- O plug-in de gestão do Kaspersky Endpoint Security 11 for Windows não é compatível com a gestão de suporte do Kaspersky Endpoint Security 10 for Windows em computadores.


- O plug-in de gestão do Kaspersky Endpoint Security 11 for Windows não é compatível com itens (por exemplo, políticas ou tarefas) que foram criados recorrendo ao plug-in de gestão do Kaspersky Endpoint Security 10 for Windows.

Pode utilizar o Assistente de Conversão de Políticas e Tarefas em Lote para converter políticas e tarefas da versão 10 para a versão 11. Para obter mais informações sobre conversão de políticas e tarefas, consulte a [Ajuda do Kaspersky Security Center](#).



Atualizar o plug-in de gestão do Kaspersky Endpoint Security 11 for Windows

Se o plug-in de gestão do Kaspersky Endpoint Security 11 for Windows for instalado na Consola de Administração, considere o seguinte quando instalar uma nova versão do plug-in de gestão do Kaspersky Endpoint Security 11 for Windows:

- A versão anterior do plug-in de gestão do Kaspersky Endpoint Security 11 for Windows será removida.
- A nova versão do plug-in de gestão do Kaspersky Endpoint Security 11 for Windows suporta a gestão da versão anterior do Kaspersky Endpoint Security 11 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.
- Quando atualizar o Management Plug-in para a versão 11.2.0, tem de abrir uma política para que seja convertida automaticamente. No final, o Kaspersky Endpoint Security irá solicitar-lhe uma confirmação de participação na KSN. Se já tiver atualizado a aplicação para a versão 11.2.0 nos computadores da sua empresa, a participação na KSN será desativada até que aceite os termos de participação na KSN.

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 infraestrutura de chave pública (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 certificados autoassinados. 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 categoria e reputação dos ficheiros verificados bem como informações sobre a reputação dos endereços da Web verificados.*
- **Monitor de atividade das aplicações.** Visualize informações sobre a operação das aplicações instaladas. A Monitorização do Sistema 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.

	<ul style="list-style-type: none"> • 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.
Atualização	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 scan de vírus 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.

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.

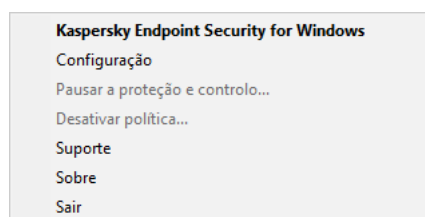
- **Pausar proteção/Retomar proteção.** Pausa a operação de todos os componentes de proteção e controlo que não estejam assinalados por um cadeado (🔒) na política. Antes de executar esta operação, recomenda-se a desativação da política do Kaspersky Security Center.

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 seleccionar 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. A aplicação continua também a utilizar o Kaspersky Security Network.

- **Desativar política/Ativar política.** Desativa 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.** Desativa 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.**
 - **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:

- **With simplified interface.** 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 apresenta também notificações acima do ícone da aplicação.
- **With full interface.** 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.
- **No 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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Definições gerais** → **Interface**.
6. No bloco **Interação com o utilizador**, execute uma das seguintes ações:
 - Selecione a caixa de verificação **Apresentar interface de utilizador** se pretender que os seguintes elementos da interface sejam apresentados no computador cliente:
 - A pasta que contém o nome da aplicação no menu **Iniciar**
 - [Ícone do Kaspersky Endpoint Security](#) na área de notificação da barra de tarefas do Microsoft Windows
 - Notificações pop-up
 - Se esta caixa de verificação for seleccionada, o utilizador pode visualizar e, consoante os direitos disponíveis, alterar as definições da aplicação a partir da interface da aplicação.
 - Desmarque a caixa de verificação **Apresentar interface de utilizador** se pretender ocultar todos os vestígios do Kaspersky Endpoint Security no computador cliente.
7. Na secção **Interação com o utilizador**, selecione a caixa de verificação **Apresentar interface simplificada** se pretender que a [interface simplificada da aplicação](#) seja apresentada num computador cliente que tenha o Kaspersky Endpoint Security instalado.

[Como configurar o modo de apresentação da interface da aplicação na Consola de Administração e Consola de Nuvem](#) 

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Definições gerais** → **Interface**.
5. Na secção **Interaction with user**, configure como a interface da aplicação será apresentada:
 - **With simplified interface.** 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 apresenta também notificações acima do ícone da aplicação.
 - **With full interface.** 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.
 - **No 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.
6. Guarde as suas alterações.

Como Começar

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 tarefas de *Atualização* e *Verificação de vírus*.

A tarefa de *Atualização* 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 *Update* é criada automaticamente pelo Quick Start Wizard do Kaspersky Security Center. Para criar a tarefa *Update*, instale o plug-in Web do Kaspersky Endpoint Security for Windows enquanto executa o Assistente.

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

[Como criar uma tarefa de Verificação de Vírus na Consola de Administração \(MMC\)](#) 

1. Na Consola de Administração, dirija-se à pasta **Administration Server** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **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 (11.8.0)** → **Verificação de vírus**.

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, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção falhar, o Kaspersky Endpoint Security apaga os ficheiros.
- **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 não for possível, 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.

Configure o modo de execução da tarefa utilizando a caixa de verificação **Executar apenas quando o computador está inativo**. Esta caixa de verificação ativa/desativa a função que suspende a tarefa de *Verificação de vírus* quando os recursos do computador são limitados. O Kaspersky Endpoint Security pausa a tarefa de *Verificação de vírus* se a proteção de ecrã estiver desativada e o computador estiver desbloqueado.

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 vírus*. 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

Sair do 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 Scan de vírus será executada nos computadores do utilizador de acordo com o calendário especificado.

[Como criar uma tarefa de Verificação de Vírus na Consola Web ?](#)

1. Na janela principal da Consola de Web, seleccione **Devices** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **Add**.

O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

a. Na lista suspensa **Application**, seleccione **Kaspersky Endpoint Security for Windows (11.8.0)**.

b. Na lista pendente **Task type**, seleccione **Virus Scan**.

c. No campo **Task name**, introduza uma breve descrição, por exemplo, *Weekly scan*.

d. Na secção **Select devices to which the task will be assigned**, seleccione o âmbito de tarefa.

4. Seleccione os dispositivos de acordo com a opção do âmbito da tarefa seleccionada. Avance para o passo seguinte.

5. Sair do Assistente.

Será apresentada uma nova tarefa na lista de tarefas.

6. 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.

7. Seleccione a caixa de verificação junto à tarefa.

8. Clique no botão **Run**.

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 Scan de vírus será executada nos computadores do utilizador de acordo com o calendário especificado.

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.

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.

Política ativa e inativa

Uma política destina-se a um grupo de computadores geridos e pode estar ativa ou inativa. 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.



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.

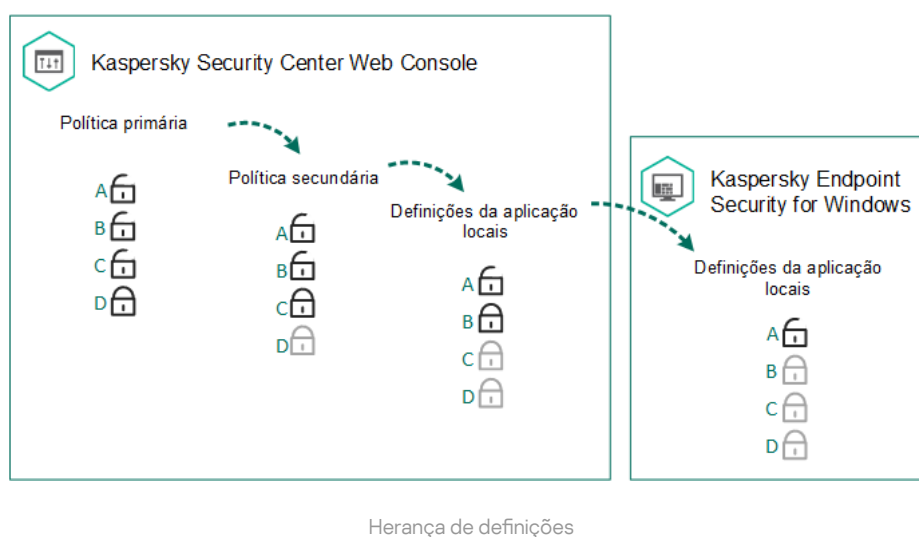
Política fora do escritório

Uma política fora do escritório é ativada quando um computador abandona o perímetro de rede da organização.

Herança de definições

Políticas, como grupos de administração, são organizadas em hierarquia. Por predefinição, a política secundária herda as definições da política principal. *Política secundária* é uma política para níveis de hierarquia imbricados, ou seja, uma política para grupos de administração aninhados e servidores de administração secundários. Pode desativar a herança de definições da política principal.

Cada definição da política tem o atributo , que indica se as definições podem ser modificadas nas políticas secundárias ou nas [definições da aplicação local](#). O atributo  só é aplicável se a herança de definições da política principal estiver ativada para a política secundária. As políticas relativas a um estado fora do escritório não afetam outras políticas na hierarquia de grupos de administração.






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 **Segurança** da janela de propriedades do Servidor de Administração do Kaspersky Security Center.



Criar uma 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 no botão **New policy**.
O Assistente de Política é iniciado.
5. Siga as instruções do Assistente de Política.

[Como criar uma política na Consola Web e na Consola de Nuvem](#) 

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no botão **Add**.
O Assistente de Política é iniciado.
3. Seleccione 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. No separador **General**, pode executar as seguintes ações:
 - Mudar o nome de política.
 - Seleccione o estado da política:
 - **Ativado**. Depois seguinte sincronização, a política será utilizada como a política ativa do computador.
 - **Inactive**. Política de reserva. Se necessário, uma política inativa pode mudar para o estado ativo.
 - **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.
6. No separador **Definições da aplicação**, pode configurar as [definições da política do Kaspersky Endpoint Security](#).
7. Guarde as suas alterações.

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](#) .

Indicador de nível de segurança

O indicador do nível de segurança é apresentado na parte superior da janela **Propriedades: <Nome 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.
 - Detecção de comportamento.
 - Prevenção de explorações.
 - Motor de remediação.
 - **Importante.** Esta categoria inclui os seguintes componentes:
 - Kaspersky Security Network.
 - Proteção contra ameaças da Web.
 - Proteção contra ameaças de correio.
 - Prevenção contra invasões.
- **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.

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 vírus.** 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 vírus* 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](#)**. O Kaspersky Endpoint Security atualiza as bases de dados e módulos da aplicação. A tarefa *Atualizar* 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](#)**. 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.

As tarefas apenas são executadas num computador se o [Kaspersky Endpoint Security estiver em execução](#).


Adicionar uma nova tarefa

[Como criar uma tarefa na Consola de Administração \(MMC\)](#) ²


1. Abra a Consola de Administração do Kaspersky Security Center.
2. Selecione a pasta **Tarefas** na árvore da Consola de Administração.
3. Clique no botão **Nova tarefa**.
O Assistente de Tarefas é iniciado.
4. Siga as instruções do Assistente de Tarefas.

1. Na janela principal da Consola de Web, seleccione **Devices** → **Tasks**.
A lista de tarefas é aberta.
2. Clique no botão **Adicionar**.
O Assistente de Tarefas é iniciado.
3. Configurar as definições de tarefas:
 - a. Na lista suspensa **Aplicação**, seleccione **Kaspersky Endpoint Security for Windows (11.8.0)**.
 - b. Na lista pendente **Tipo de tarefa**, seleccione a tarefa que pretende executar nos computadores dos utilizadores.
 - c. No campo **Task name**, introduza uma breve descrição.
 - d. No bloco **Select devices to which the task will be assigned**, seleccione o âmbito de tarefa.
4. Seleccione os dispositivos de acordo com a opção do âmbito da tarefa seleccionada. Avance para o passo seguinte.
5. Sair do 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 seleccionar a caixa de verificação oposta à tarefa e clicar no botão **Iniciar**. 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 and reporting** → **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](#).

Controlo de acesso à tarefa

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 **Segurança** 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. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivo geridos** 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 **Políticas**.
4. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Tarefas locais** → **Gestão de tarefas**.
6. Configure o modo de gestão de tarefas (consulte a tabela abaixo).
7. 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 **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Selecione o separador **Definições da aplicação**.
4. Aceda a **Tarefas locais** → **Gestão de tarefas**.
5. Configure o modo de gestão de tarefas (consulte a tabela abaixo).
6. Guarde as suas alterações.

Definições de gestão de tarefas

Parâmetro	Descrição
Permitir utilização de tarefas locais	<p>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.</p> <p>Se a caixa de verificação estiver desmarcada, a utilização de tarefas locais é parada. 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 linha de comandos.</p> <p>Um utilizador pode ainda iniciar um scan de vírus de um ficheiro ou pasta selecionando a opção Verificar a presença de 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.</p>
Permitir que as tarefas sejam apresentadas	<p>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.</p>

	Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security apresenta uma lista de tarefas vazia.
Permitir a gestão de tarefas de grupo	<p>Se a caixa de seleção estiver marcada, os utilizadores podem iniciar e parar as tarefas de grupo especificadas no Kaspersky Security Center. Os utilizadores podem iniciar e parar tarefas na interface da aplicação ou na interface simplificada da aplicação.</p> <p>Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security inicia tarefas agendadas automaticamente ou o administrador inicia as tarefas manualmente no Kaspersky Security Center.</p>

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 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. Selecione o computador para o qual pretende configurar as definições do Kaspersky Endpoint Security.
5. No menu de contexto do computador cliente, selecione **Propriedades**.
É aberta uma janela de propriedades do computador cliente.
6. Na janela de propriedades do computador cliente, selecione a secção **Aplicações**.
Uma lista de aplicações da Kaspersky instaladas no computador cliente é apresentada na parte direita da janela de propriedades do computador cliente.
7. Selecione o Kaspersky Endpoint Security.
8. Clique no botão **Propriedades** na lista de aplicações da Kaspersky.
Tal abre a janela **Kaspersky Endpoint Security for Windows application settings**.
9. Na secção **Definições gerais**, configure o Kaspersky Endpoint Security, bem como os Relatórios e Armazenamento.
As restantes secções da janela **Definições da aplicação Kaspersky Endpoint Security for Windows** são as mesmas das secções padrão do 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**.

10. Guarde as suas alterações.

1. Na janela principal da Consola Web, seleccione **Devices** → **Managed devices**.
2. Seleccione um computador para o qual quer configurar definições da aplicação locais.
As propriedades do computador são apresentadas.
3. Seleccione o separador **Aplicações**.
4. Clique em **Kaspersky Endpoint Security for Windows**.
As definições da aplicação locais são apresentadas.
5. Seleccione o separador **Application settings**.
6. Configure as definições da aplicação locais.
7. 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.

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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela da política, selecione **Definições gerais** → **Definições da aplicação**.
6. Utilize a caixa de seleção **Start Kaspersky Endpoint Security for Windows on computer startup** para configurar o arranque da aplicação.
7. Guarde as suas alterações.

[Como configurar o arranque do Kaspersky Endpoint Security na Consola Web](#)

1. Na janela principal da Consola Web, selecione **Devices** → **Policies & Profiles**.
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 **Definições gerais** → **Definições da aplicação**.
5. Utilize a caixa de seleção **Iniciar o Kaspersky Endpoint Security no arranque do computador (recomendado)** 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 de definições da aplicação, selecione **Definições gerais** → **Definições da aplicação**.
3. Utilize a caixa de seleção **Start Kaspersky Endpoint Security for Windows on computer startup** 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 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, seleccione o separador **Devices**.
4. Seleccione o computador no qual pretende iniciar ou parar a aplicação.
5. Clique com o botão direito do rato para visualizar o menu de contexto do computador cliente e seleccione **Propriedades**.
6. Na janela de propriedades do computador cliente, seleccione a secção **Aplicações**.
Uma lista de aplicações da Kaspersky instaladas no computador cliente é apresentada na parte direita da janela de propriedades do computador cliente.
7. Seleccione o Kaspersky Endpoint Security.
8. Execute as seguintes ações:

- 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, seleccione **Devices** → **Managed 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. Seleccione o separador **Aplicações**.
4. Seleccione a caixa de verificação no lado contrário a **Kaspersky Endpoint Security for Windows**.
5. Clique no botão **Início** ou **Parar**.

Como iniciar ou parar o Kaspersky Endpoint Security a partir da command line

Para parar a aplicação a partir da command line, [ative a gestão externa dos serviços do sistema](#).



O ficheiro klpsm.exe, incluído no kit de distribuição do Kaspersky Endpoint Security, é utilizado para iniciar ou parar a aplicação 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. 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`.

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 ativas.

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, seleccione **Pausar proteção** (consulte a figura abaixo).

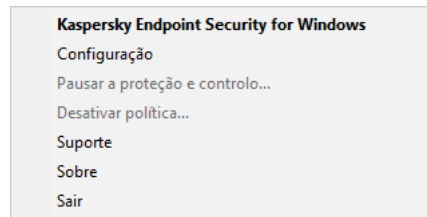
Este item do menu contextual está disponível se a [proteção por password estiver ativada](#).

3. Seleccione 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 no botão **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.
Para tal, deve guardar o ficheiro de configuração na mesma pasta onde está localizado o pacote de distribuição.
- Executar a instalação remota do Kaspersky Endpoint Security através das configurações predefinidas do Kaspersky Security Center.
- Migrar as definições do Kaspersky Endpoint Security de um computador para o outro.


Para criar um ficheiro de configuração:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Definições gerais** → **Gerir definições**.
3. Clique no botão **Export**.
4. 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`.

5. Guardar o ficheiro.

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 de definições da aplicação, selecione **Definições gerais** → **Gerir definições**.
3. Clique no botão **Importar**.
4. Na janela que se abre, introduza o caminho para o ficheiro de configuração.
5. Abrir o ficheiro.

Todos os valores de definições do Kaspersky Endpoint Security serão estabelecidos de acordo com o ficheiro de configuração selecionado.

Restaurar as predefinições da aplicação

Pode restaurar as definições recomendadas pela Kaspersky para o Kaspersky Endpoint Security 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 de definições da aplicação, selecione **Definições gerais** → **Gerir definições**.
3. Clique no botão **Restaurar**.
4. Guarde as suas alterações.

Verificação de vírus do computador

Um scan de vírus é essencial para a segurança do computador. Executar verificações de vírus 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 da tarefa de *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 da tarefa de *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

- Caixa de correio do Microsoft Outlook
- Unidades de disco rígido, amovíveis e de rede
- Qualquer ficheiro selecionado

Verificação de fundo

A *Verificação de fundo* 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

O Kaspersky Endpoint Security verifica se os módulos de aplicação foram corrompidos ou modificados.

Verificar o computador

Um scan de vírus é essencial para a segurança do computador. Executar verificações de vírus 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 tarefas padrão predefinidas *Verificação Completa*, *Verificação de Áreas Críticas*, *Verificação Personalizada*. Se a sua organização tiver o sistema de administração do Kaspersky Security Center implementado, pode [criar uma tarefa Verificação de vírus](#) e configurar a verificação. A tarefa [Verificação em segundo plano](#) também está disponível no Kaspersky Security Center. Não é possível configurar a verificação em segundo plano.

[Como executar uma verificação de vírus 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 **Tarefas**.
4. Selecione a tarefa de verificação e clique duas vezes para abrir as propriedades da tarefa.
Se necessário, [crie uma tarefa de Verificação de vírus](#).
5. Na janela de propriedades da tarefa, selecione a secção **Definições**.
6. Configure a tarefa de verificação (consulte a tabela abaixo).
Se necessário, [configure o agendamento da tarefa de verificação](#).
7. Guarde as suas alterações.
8. 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 verificação de vírus na Consola Web e na Cloud Console](#)

1. Na janela principal da Consola de Web, selecione **Devices** → **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 verificação de vírus 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. 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**. Se a tarefa de verificação não for apresentada, tal significa que o administrador [proibiu a utilização de tarefas locais na política](#).

Definições de verificação

Parâmetro	Descrição
Nível de segurança	<p>O Kaspersky Endpoint Security pode utilizar diferentes grupos de definições para executar uma verificação. Estes grupos de definições armazenados na aplicação chamam-se <i>níveis de segurança</i>.</p> <ul style="list-style-type: none"> • Alto. O Kaspersky Endpoint Security verifica todos os tipos de ficheiros. Ao verificar os ficheiros compostos, o Kaspersky Endpoint Security também verifica os ficheiros de formato de e-mail. • Recomendado. O Kaspersky Endpoint Security verifica apenas os formatos de ficheiros especificados, em todos os discos rígidos, unidades de rede e meios de armazenamento removíveis do computador, bem como os objetos OLE incorporados. O Kaspersky Endpoint Security não verifica arquivos nem pacotes de instalação. • Baixo. O Kaspersky Endpoint Security verifica apenas ficheiros novos ou modificados com as extensões especificadas em todos os discos rígidos, unidades amovíveis e unidades de rede do computador. O Kaspersky Endpoint Security não verifica ficheiros compostos. <p>Pode seleccionar 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.</p>
Ação após deteção de ameaças	<p>Desinfetar; eliminar se a desinfeção falhar. Se esta opção estiver seleccionada, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção falhar, o Kaspersky Endpoint Security apaga os ficheiros.</p> <p>Desinfetar; bloquear se a desinfeção falhar. Se esta opção estiver seleccionada, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção não for possível, o Kaspersky Endpoint Security adiciona a informação sobre os ficheiros infetados que são detetados à lista de ameaças ativas.</p> <p>Notificar. Se esta opção for seleccionada, o Kaspersky Endpoint Security adiciona a informação sobre ficheiros infetados à lista de ameaças ativas na deteção destes ficheiros.</p>

	<p>Antes de tentar desinfetar ou eliminar um ficheiro infetado, o Kaspersky Endpoint Security 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.</p>
	<p>Ao detetar ficheiros infetados que fazem parte da aplicação Loja Windows, o Kaspersky Endpoint Security tenta eliminar esses ficheiros.</p>
<p>Executar a Desinfeção Avançada imediatamente</p> <p><i>(disponível apenas na Consola do Kaspersky Security Center)</i></p>	<p>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.</p> <p>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.</p> <p>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.</p>
<p>Âmbito de verificação</p>	<p>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, bases de dados de correio, discos rígidos, unidades amovíveis ou unidades de rede, uma pasta ou um ficheiro.</p>
<p>Agendamento de verificações</p>	<p>Manualmente. Modo de execução, no qual pode iniciar a verificação manualmente quando for conveniente para si.</p> <p>Por agendamento. Neste modo de execução da tarefa, o Kaspersky Endpoint Security 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.</p>
<p>Adiar execução, após o início da aplicação durante N minutos</p>	<p>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.</p>
<p>Executar tarefas ignoradas</p>	<p>Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security inicia a tarefa de verificação ignorada logo que possível. A tarefa de verificação pode ser ignorada, por exemplo, se o computador estiver desligado no momento de início da tarefa de verificação agendada. Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security não executa tarefas de verificação ignoradas. Em alternativa, executa a tarefa de verificação seguinte, em conformidade com o agendamento atual.</p>
<p>Executar apenas quando o</p>	<p>Início adiado da tarefa de verificação 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</p>

computador está inativo	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.
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 do Kaspersky Endpoint Security e executar a tarefa de verificação com a conta deste utilizador.
Tipos de ficheiros	<div style="border: 1px solid black; padding: 10px; margin-bottom: 10px;"> <p>O Kaspersky Endpoint Security considera os ficheiros sem extensão como sendo ficheiros executáveis. O Kaspersky Endpoint Security verifica sempre ficheiros executáveis, independentemente dos tipos de ficheiros selecionados para verificação.</p> </div> <p>Todos os ficheiros. Se esta definição estiver ativada, o Kaspersky Endpoint Security verifica todos os ficheiros sem exceção (todos os formatos e extensões).</p> <p>Ficheiros verificados por formato. Se esta configuração estiver ativada, o Kaspersky Endpoint Security 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.</p> <p>Ficheiros verificados por extensão. Se esta configuração estiver ativada, o Kaspersky Endpoint Security verifica apenas ficheiros infetáveis. O formato do ficheiro é então determinado com base na extensão do ficheiro.</p> <p>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)</p>
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 objetos verificados durante mais de N segundos	Limita a duração da verificação de um único objeto. Após o período especificado, o Kaspersky Endpoint Security interrompe a verificação de um ficheiro. Isto ajuda a reduzir a duração de uma verificação.
Verificar arquivos	A verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros formatos de arquivo.
Verificar pacotes de distribuição	Esta caixa de verificação ativa/desativa a verificação de pacotes de distribuição 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.
Analisar formatos de e-	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

<p>mail</p>	<p>Mail/Outlook Express, bem como ficheiros EML.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>O Kaspersky Endpoint Security não suporta a versão de 64 bits do cliente de e-mail MS Outlook. Significa que o Kaspersky Endpoint Security não analisa ficheiros do MS Outlook (ficheiros PST e ST) se no computador estiver instalada uma versão de 64 bits do MS Outlook, mesmo que o e-mail esteja incluído no âmbito da análise.</p> </div> <p>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.</p> <p>Se esta caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security verifica o ficheiro de formato de e-mail como um ficheiro único.</p>
<p>Verificar arquivos protegidos por password</p>	<p>Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security verifica os arquivos protegidos por password. Para que seja possível verificar os ficheiros num arquivo ser-lhe-á pedido que introduza a password.</p> <p>Se a caixa de verificação estive desmarcada, o Kaspersky Endpoint Security ignora a verificação dos arquivos protegidos por password.</p>
<p>Não descompactar ficheiros compostos extensos</p>	<p>Se esta caixa de verificação estiver selecionada, o Kaspersky Endpoint Security não verifica ficheiros compostos se o tamanho destes exceder o valor especificado.</p> <p>Se esta caixa de verificação for desmarcada, o Kaspersky Endpoint Security verifica ficheiros compostos de todos os tamanhos.</p> <p>O Kaspersky Endpoint Security verifica ficheiros grandes que são extraídos dos arquivos, independentemente de a caixa de verificação estar marcada ou não.</p>
<p>Aprendizagem automática e análise de assinaturas</p>	<p>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.</p> <p>Com base nas recomendações dos especialistas da Kaspersky, a aprendizagem automática e a análise de assinaturas estão sempre ativadas.</p>
<p>Análise heurística</p>	<p>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.</p> <p>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.</p>
<p>Tecnologia iSwift</p> <p><i>(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)</i></p>	<p>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 considera a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições da verificação. A tecnologia iSwift é um avanço da tecnologia iChecker para o sistema de ficheiros NTFS.</p>

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 (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 desinfecção 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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Tarefas locais** → **Verificação das unidades amovíveis**.
6. Na lista pendente **Ação ao ligar uma unidade amovível**, selecione **Verificação detalhada** ou **Verificação Rápida**.
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 Consola Web e na Cloud Console](#)

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Tarefas locais** → **Verificação das unidades amovíveis**.
5. Na lista pendente **Ação ao ligar uma unidade amovível**, seleccione **Verificação detalhada** ou **Verificação Rápida**.
6. Configure opções avançadas para a verificação de unidades amovíveis (consulte a tabela abaixo).
7. 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, seleccione 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
Ação ao ligar uma unidade amovível	<p>Verificação detalhada. Se esta opção estiver seleccionada, quando uma unidade removível é ligada, o Kaspersky Endpoint Security verifica todos os ficheiros na unidade amovível, 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 palavra-passe.</p> <p>Verificação Rápida. Se esta opção estiver seleccionada, 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.</p>
Tamanho máximo da unidade amovível	<p>Se esta caixa de verificação estiver seleccionada, o Kaspersky Endpoint Security executa a ação seleccionada na lista pendente Ação ao ligar uma unidade amovível nas unidades amovíveis com um tamanho inferior ao tamanho máximo da unidade especificado.</p> <p>Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security executa a ação seleccionada na lista pendente Ação ao ligar uma unidade amovível nas unidades amovíveis com qualquer tamanho.</p>

Mostrar progresso da verificação	<p>Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security apresenta o progresso das verificações de unidades amovíveis numa janela separada e na secção Tarefas.</p> <p>Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security executa uma verificação em 2.º plano das unidades amovíveis.</p>
Bloquear a interrupção da tarefa de verificação	<p>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.</p>

Verificação de fundo

A *Verificação de fundo* 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. 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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Tarefas locais** → **Verificação em segundo plano**.
6. Use a caixa de verificação **Ativar Verificação em segundo plano** para ativar ou desativar as verificações em segundo plano.
7. 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 **Devices** → **Policies & Profiles**.
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 **Tarefas locais** → **Verificação em segundo plano**.
5. Use a caixa de verificação **Ativar Verificação em segundo plano** para ativar ou desativar as verificações em segundo plano.
6. Guarde as suas alterações.

[Como ativar verificações em segundo plano na interface da aplicação](#)

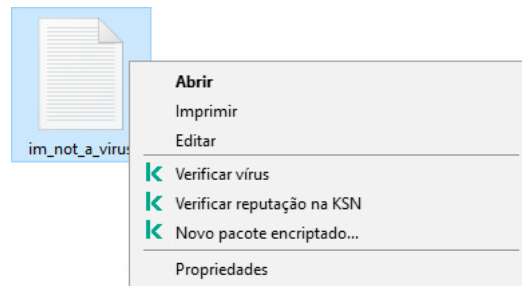
1. Na janela principal da aplicação, aceda à secção **Tarefas**.
2. Na lista de tarefas, selecione a tarefa de verificação e clique em .
3. Use o botão de alternar **Verificação em segundo plano** para ativar ou desativar as verificações em segundo plano.
4. Guarde as suas alterações.

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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Tarefas locais** → **Verificar a partir do menu de contexto**.
6. Configurar as verificações a partir do menu de contexto (consulte a tabela abaixo).
7. 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, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Tarefas Locais** → **Verificar a partir do menu de contexto**.
5. Configurar as verificações 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, seleccione 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 *Verificar 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	<p>O Kaspersky Endpoint Security pode utilizar diferentes grupos de definições para executar uma verificação. Estes grupos de definições armazenados na aplicação chamam-se <i>níveis de segurança</i>.</p> <ul style="list-style-type: none"> • Alto. O Kaspersky Endpoint Security verifica todos os tipos de ficheiros. Ao verificar os ficheiros compostos, o Kaspersky Endpoint Security também verifica os ficheiros de formato de e-mail. • Recomendado. O Kaspersky Endpoint Security verifica apenas os formatos de ficheiros especificados, em todos os discos rígidos, unidades de rede e meios de armazenamento removíveis do computador, bem como os objetos OLE incorporados. O Kaspersky Endpoint Security não verifica arquivos nem pacotes de instalação. • Baixo. O Kaspersky Endpoint Security verifica apenas ficheiros novos ou modificados com as extensões especificadas em todos os discos rígidos, unidades amovíveis e unidades de rede do computador. O Kaspersky Endpoint Security não verifica ficheiros compostos.
Ação após deteção de ameaças	<p>Desinfetar; eliminar se a desinfeção falhar. Se esta opção estiver seleccionada, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção falhar, o Kaspersky Endpoint Security apaga os ficheiros.</p>

	<p>Desinfetar; bloquear se a desinfeção falhar. Se esta opção estiver selecionada, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção não for possível, o Kaspersky Endpoint Security adiciona a informação sobre os ficheiros infetados que são detetados à lista de ameaças ativas.</p> <p>Notificar. Se esta opção for selecionada, o Kaspersky Endpoint Security adiciona a informação sobre ficheiros infetados à lista de ameaças ativas na deteção destes ficheiros.</p>
<p>Tipos de ficheiros</p>	<div style="border: 1px solid #ccc; padding: 10px; margin-bottom: 10px;"> <p>O Kaspersky Endpoint Security considera os ficheiros sem extensão como sendo ficheiros executáveis. O Kaspersky Endpoint Security verifica sempre ficheiros executáveis, independentemente dos tipos de ficheiros selecionados para verificação.</p> </div> <p>Todos os ficheiros. Se esta definição estiver ativada, o Kaspersky Endpoint Security verifica todos os ficheiros sem exceção (todos os formatos e extensões).</p> <p>Ficheiros verificados por formato. Se esta configuração estiver ativada, o Kaspersky Endpoint Security 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.</p> <p>Ficheiros verificados por extensão. Se esta configuração estiver ativada, o Kaspersky Endpoint Security verifica apenas ficheiros infetáveis . O formato do ficheiro é então determinado com base na extensão do ficheiro.</p> <p>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)</p>
<p>Verificar apenas os ficheiros novos e modificados</p>	<p>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.</p>
<p>Ignorar objetos verificados durante mais de N segundos</p>	<p>Limita a duração da verificação de um único objeto. Após o período especificado, o Kaspersky Endpoint Security interrompe a verificação de um ficheiro. Isto ajuda a reduzir a duração de uma verificação.</p>
<p>Verificar arquivos</p>	<p>A verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros formatos de arquivo.</p>
<p>Verificar pacotes de distribuição</p>	<p>A caixa de verificação ativa ou desativa a verificação de pacotes de distribuição.</p>
<p>Verificar ficheiros em formatos do Microsoft Office</p>	<p>Verifica ficheiros do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Ficheiros de formato do Office incluem objetos OLE também.</p>
<p>Verificar formatos de e-mail</p>	<p>Esta caixa de verificação ativa/desativa a opção de verificar ficheiros em formatos de e-mail e bases de dados de correio no Kaspersky Endpoint Security.</p>

	<p>A aplicação só verifica totalmente os formatos de ficheiro de correio do Microsoft Outlook, Windows Mail/Outlook Express e EML e apenas se o computador tiver o cliente de correio do Microsoft Outlook x86.</p> <p>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.</p> <p>Se esta caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security verifica o ficheiro de formato de e-mail como um ficheiro único.</p>
Verificar arquivos protegidos por password	<p>Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security verifica os arquivos protegidos por password. Para que seja possível verificar os ficheiros num arquivo ser-lhe-á pedido que introduza a password.</p> <p>Se a caixa de verificação estive desmarcada, o Kaspersky Endpoint Security ignora a verificação dos arquivos protegidos por password.</p>
Não descompactar ficheiros compostos extensos	<p>Se esta caixa de verificação estiver selecionada, o Kaspersky Endpoint Security não verifica ficheiros compostos se o tamanho destes exceder o valor especificado.</p> <p>Se esta caixa de verificação for desmarcada, o Kaspersky Endpoint Security verifica ficheiros compostos de todos os tamanhos.</p> <p>O Kaspersky Endpoint Security verifica ficheiros grandes que são extraídos dos arquivos, independentemente de a caixa de verificação estar marcada ou não.</p>
Aprendizagem automática e análise de assinaturas	<p>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.</p> <p>Com base nas recomendações dos especialistas da Kaspersky, a aprendizagem automática e a análise de assinaturas estão sempre ativadas.</p>
Análise heurística	<p>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.</p> <p>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.</p>
Tecnologia iSwift	<p>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 considera a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições da verificação. A tecnologia iSwift é um avanço da tecnologia iChecker para o sistema de ficheiros NTFS.</p>
Tecnologia iChecker	<p>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).</p>

Controlo da 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* destina-se a verificar ficheiros da aplicação. Execute a tarefa *Verificação de integridade* se o Kaspersky Endpoint Security detetar um objeto malicioso, mas não o neutralizou.

Pode criar a tarefa *Verificação de integridade* 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 Consola de Administração, dirija-se à pasta **Administration Server** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **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 (11.8.0)** → **Verificação de integridade**.

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

Sair do 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 de Web, seleccione **Devices** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **Add**.

O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

a. Na lista suspensa **Application**, seleccione **Kaspersky Endpoint Security for Windows (11.8.0)**.

b. Na lista pendente **Tipo de tarefa**, seleccione **Verificação de integridade**.

c. No campo **Task name**, introduza uma breve descrição, por exemplo, *Verificar a integridade da aplicação após infeção do computador*.

d. Na secção **Select devices to which the task will be assigned**, seleccione o âmbito de tarefa.

4. Seleccione os dispositivos de acordo com a opção do âmbito da tarefa seleccionada. Avance para o passo seguinte.

5. Sair do Assistente.

Será apresentada uma nova tarefa na lista de tarefas.

6. Seleccione 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; seleccione a tarefa *Verificação de integridade* e clique em **Executar verificação**.

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* 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 de verificações	Manualmente. Modo de execução, no qual pode iniciar a verificação manualmente quando for conveniente para si. Por agendamento. Neste modo de execução da tarefa, o Kaspersky Endpoint Security inicia a tarefa de verificação em conformidade com o agendamento criado pelo utilizador. Se este modo de execução da tarefa de verificação estiver seleccionado, pode também iniciar manualmente a tarefa de verificação.
Executar	Se a caixa de verificação estiver seleccionada, o Kaspersky Endpoint Security inicia a tarefa

tarefas ignoradas	de verificação ignorada logo que possível. A tarefa de verificação pode ser ignorada, por exemplo, se o computador estiver desligado no momento de início da tarefa de verificação agendada. Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security não executa tarefas de verificação ignoradas. Em alternativa, executa a tarefa de verificação seguinte, em conformidade com o agendamento atual.
Executar apenas quando o computador está inativo	Início adiado da tarefa de verificação 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.

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 das tarefas de *Verificação Completa* e *Verificação de Áreas Críticas*.

O Kaspersky Endpoint Security tem os seguintes objetos predefinidos como parte do âmbito de verificação:

- **O meu e-mail.**
Ficheiros relevantes para o cliente de e-mail do Outlook: ficheiros de dados (PST), ficheiros de dados offline (OST).
- **Memória do sistema.**
- **Objetos de inicialização.**
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.**

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 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 **Tarefas**.
4. Selecione a tarefa de verificação e clique duas vezes para abrir as propriedades da tarefa.
Se necessário, [crie uma tarefa de Verificação de vírus](#).
5. Na janela de propriedades da tarefa, selecione a secção **Definições**.
6. Na secção **Âmbito de verificação**, clique em **Definições**.
7. Na janela aberta, selecione os objetos que deseja adicionar ao âmbito de verificação ou excluir do mesmo.
8. Se pretender adicionar um novo objeto ao âmbito de verificação:
 - a. Clique no botão **Add**.
 - 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:\Pasta***.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas designadas `Pasta` e nas suas subpastas. 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 caracteres.

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 junto ao objeto.

9. Guarde as suas alterações.

[Como editar o âmbito de verificação na Consola Web e na Cloud Console](#) 

1. Na janela principal da Consola de Web, seleccione **Devices** → **Tasks**.

A lista de tarefas é aberta.

2. Clique na tarefa de verificação.

É apresentada a janela de propriedades da tarefa. Se necessário, [crie uma tarefa de Verificação de vírus](#).

3. Seleccione o separador **Application settings**.

4. Na secção **Scan scope**, seleccione 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 no botão **Add**.

b. No campo **Path**, 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:\Pasta***.txt** incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas designadas **Pasta** e nas suas subpastas. 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 caracteres.

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. Na lista de tarefas, selecione a tarefa de *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 das tarefas de *Verificação Completa* e *Verificação de Áreas Críticas*.

3. Na janela aberta, 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

Uma verificação completa do computador poderá demorar algum tempo e irá usar os recursos do computador. Deve escolher o momento ideal para executar uma verificação do computador para evitar afetar o desempenho de outro software. O Kaspersky Endpoint Security permite configurar um agendamento regular da verificação do computador. Tal é conveniente se a sua organização tiver um horário de trabalho. Pode configurar uma verificação do computador para que seja executada à noite ou aos fins de semana. Se, por algum motivo, não for possível executar a tarefa de verificação (por exemplo, o computador estava desligado naquela altura), pode configurar a tarefa ignorada para ser automaticamente executada assim que for possível.

Se for impossível configurar um agendamento ideal da verificação, o Kaspersky Endpoint Security permite-lhe executar uma verificação do computador quando as seguintes condições especiais forem cumpridas:

- 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 quando decorrido um determinado período de tempo após o início de 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.

- 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 usar 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 vírus* 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. Tal significa que a aplicação pode demorar vários dias até concluir uma verificação completa do computador.

Como configurar o agendamento de verificações 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 **Tarefas**.
4. Selecione a tarefa de verificação e clique duas vezes para abrir as propriedades da tarefa.
Se necessário, [crie uma tarefa de Verificação de vírus](#).
5. Na janela de propriedades da tarefa, selecione a secção **Agendar**.
6. Configure o agendamento da tarefa de verificação.
7. Dependendo da frequência selecionada, configure as definições avançadas que especificam o agendamento de execução da tarefa (consulte a tabela abaixo).
8. Guarde as suas alterações.

Como configurar o agendamento de verificações na Consola Web e na Cloud Console

1. Na janela principal da Consola de Web, selecione **Devices** → **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 **Agenda**.
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 *Virus scan* 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 no botão **Agendamento de verificações**.
4. Na janela aberta, 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 de verificações	Manualmente. Modo de execução, no qual pode iniciar a verificação manualmente quando for conveniente para si. Por agendamento. Neste modo de execução da tarefa, o Kaspersky Endpoint Security 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 de verificação ignorada logo que possível. A tarefa de verificação pode ser ignorada, por exemplo, se o computador estiver desligado no momento de início da tarefa de verificação agendada. Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security não executa tarefas de verificação ignoradas. Em alternativa, executa a tarefa de verificação seguinte, em conformidade com o agendamento atual.
Executar apenas quando o computador está inativo	Início adiado da tarefa de verificação 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.
Use automatically randomized delay for task starts	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.

<p><i>(disponível apenas na Consola do Kaspersky Security Center)</i></p>	<p>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.</p> <p>Se a caixa de verificação não estiver selecionada, a tarefa será executada exatamente na hora agendada.</p>
<p>Interromper tarefa se estiver em execução durante mais de N (min)</p> <p><i>(disponível apenas na Consola do Kaspersky Security Center)</i></p>	<p>Limitando o tempo de execução da tarefa, o Kaspersky Endpoint Security interrompe a tarefa após o período de tempo especificado. 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.</p> <p>Para reduzir o tempo de execução da tarefa, pode, por exemplo, configurar o âmbito de verificação ou otimizar a verificação.</p>
<p>Activate the device before the task is started through Wake-on-LAN (min)</p> <p><i>(disponível apenas na Consola do Kaspersky Security Center)</i></p>	<p>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.</p> <p>Selecione a caixa de verificação se desejar executar a tarefa em todos os computadores, incluindo computadores desligados.</p>

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 do Kaspersky Endpoint Security 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 **Tarefas**.
4. Selecione a tarefa de verificação e clique duas vezes para abrir as propriedades da tarefa.
5. Na janela de propriedades da tarefa, selecione a secção **Conta**.
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 de Web, selecione **Devices** → **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. Na secção **Account**, clique em **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 **Advanced settings** → **Run scan as**.
4. Na janela aberta, 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

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 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 **Tarefas**.
4. Selecione a tarefa de verificação e clique duas vezes para abrir as propriedades da tarefa.
Se necessário, [crie uma tarefa de Verificação de vírus](#).
5. Na janela de propriedades da tarefa, selecione a secção **Definições**.
6. No bloco **Nível de segurança**, clique no botão **Definições**.
Tal abre a janela de definições da tarefa de verificação.
7. No bloco **Otimização da verificação**, 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 segundos.** Esta opção define um tempo limite para verificar um único objecto. Após o período especificado, o Kaspersky Endpoint Security interrompe a verificação de um ficheiro. Isto ajuda a reduzir a duração de uma verificação.
8. Clique no botão **Adicional**.
Tal abre a janela de definições de verificação de ficheiros compostos.
9. Na secção **Limite de tamanho**, selecione a caixa de verificação **Não descompactar ficheiros compostos extensos**. Define um limite de tempo para verificar um único objeto. Após o período especificado, o Kaspersky Endpoint Security interrompe a verificação de um ficheiro. Isto ajuda a reduzir a duração de uma verificação.

O Kaspersky Endpoint Security verifica ficheiros extensos extraídos de arquivos, independentemente de a caixa de verificação **Não descompactar ficheiros compostos extensos** estar selecionada.

10. Clique em **OK**.
11. Selecione o separador **Adicional**.
12. 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 considera a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições da 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).

13. Guarde as suas alterações.

Como otimizar a verificação na Consola Web e na Cloud Console

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

A lista de tarefas é aberta.

2. Clique na tarefa de verificação.

É apresentada a janela de propriedades da tarefa. Se necessário, [crie uma tarefa de Verificação de vírus](#).

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

4. Na secção **Action on threat detection**, selecione a caixa de verificação **Scan only new and changed 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. Selecione a caixa de verificação **Não descompactar ficheiros compostos extensos**. Define um limite de tempo para verificar um único objeto. Após o período especificado, o Kaspersky Endpoint Security interrompe a verificação de um ficheiro. Isto ajuda a reduzir a duração de uma verificação.

O Kaspersky Endpoint Security verifica ficheiros extensos extraídos de arquivos, independentemente de a caixa de verificação **Não descompactar ficheiros compostos extensos** estar selecionada.

6. Na secção **Definições avançadas**, selecione a caixa de verificação **Ignorar ficheiros verificados durante mais de N segundos**. Define um limite de tempo para verificar um único objeto. Após o período especificado, o Kaspersky Endpoint Security interrompe a verificação de um ficheiro. Isto ajuda a reduzir a duração de uma verificação.

7. 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 no botão **Definições avançadas**.
4. No bloco **Otimização da verificação**, 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 objetos verificados durante mais de N segundos.** Define um limite de tempo para verificar um único objeto. Após o período especificado, o Kaspersky Endpoint Security interrompe a verificação de um ficheiro. Isto ajuda a reduzir a duração de uma verificação.
5. Na secção **Limite de tamanho**, selecione a caixa de verificação **Não descompactar ficheiros compostos extensos**. Define um limite de tempo para verificar um único objeto. Após o período especificado, o Kaspersky Endpoint Security interrompe a verificação de um ficheiro. Isto ajuda a reduzir a duração de uma verificação.

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 considera a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições da 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.

As atualizações regulares requerem uma licença válida. Se não existir uma licença atual, só poderá executar uma atualização uma vez.

A principal origem de atualização do Kaspersky Endpoint Security são os servidores de atualização da Kaspersky.

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.

Os ficheiros de ajuda de contexto podem ser atualizados juntamente com as atualizações dos módulos da aplicação.

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](#).

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.

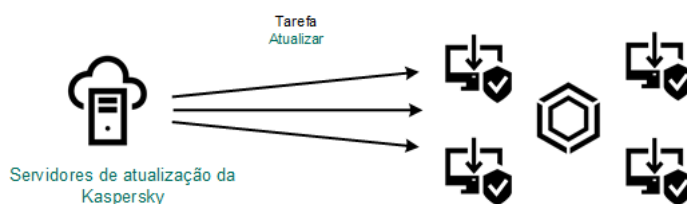
Os seguintes objetos são atualizados nos computadores dos utilizadores:

- 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 *Transferir atualizações para o armazenamento no Servidor de Administração*.

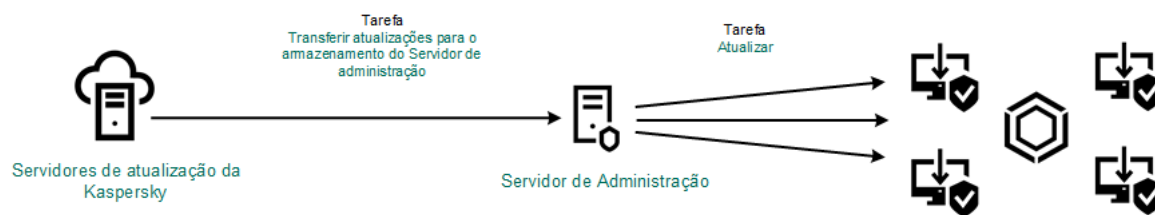
2. Transfira o pacote de atualização para uma pasta partilhada (opcional).

Pode transferir o pacote de atualização para uma pasta partilhada utilizando os seguintes métodos:

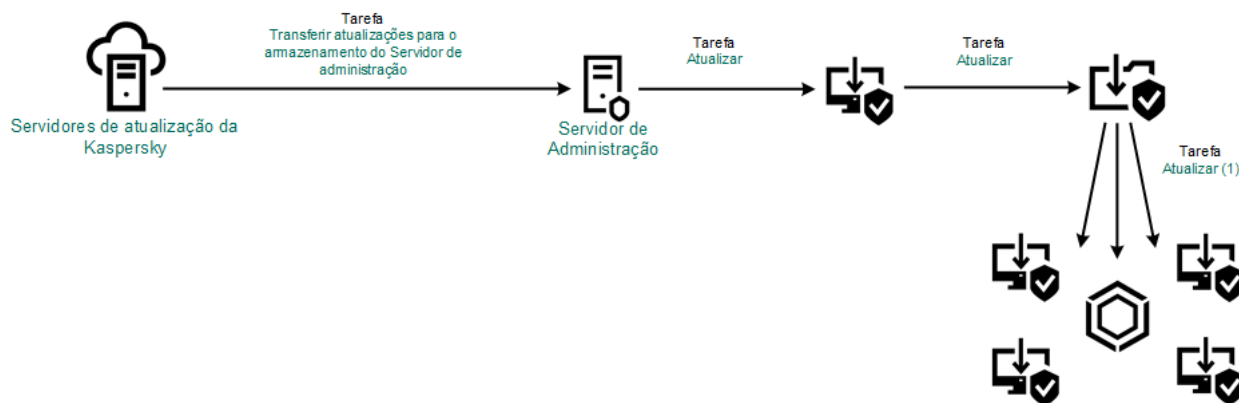
- Utilizando a tarefa *Atualizar* do Kaspersky Endpoint Security. A tarefa destina-se a um dos computadores na rede local da empresa.
- Utilizar o Utilitário Kaspersky Update. Para obter informações detalhadas sobre a utilização do Utilitário Kaspersky Update, consulte a [Base de Conhecimento da Kaspersky](#).

3. Distribuir o pacote de atualização para computadores cliente.

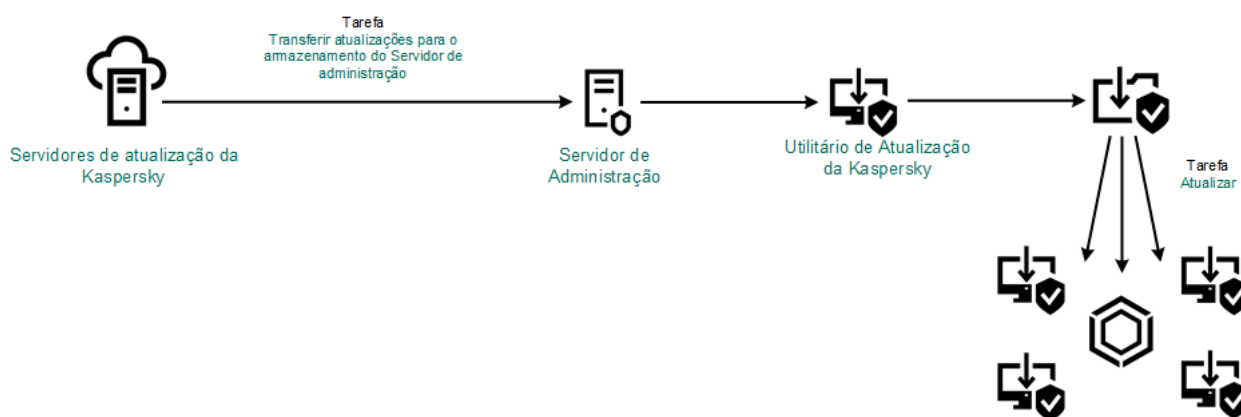
O pacote de atualização é distribuído aos computadores cliente pela tarefa *Atualizar* do Kaspersky Endpoint Security. Pode criar um número ilimitado de tarefas de atualização para cada grupo de administração.



Atualizar a partir do armazenamento de um servidor



Atualizar a partir de uma pasta partilhada



Atualizar utilizando o Utilitário Kaspersky Update

Para a Consola de Web, a lista predefinida de fontes 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 informações 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. Configurar a transferência de um pacote de atualização para o armazenamento no Servidor de administração (tarefa *Transferir atualizações para o armazenamento no Servidor de Administração*).
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 *Atualizar*).



Para configurar a transferência do pacote de atualização para o armazenamento de um servidor:

1. Na janela principal da Consola de Web, seleccione **Devices** → **Tasks**.

A lista de tarefas é aberta.

2. Seleccione a tarefa **Download updates to the Administration Server repository** do Administration Server.

É apresentada a janela de propriedades da tarefa.

A tarefa *Download updates to the Administration Server repository* do Administration Server é criada automaticamente pelo Quick Start Wizard da Consola Web do Kaspersky Security Center e esta tarefa apenas pode ter uma única instância.

3. Seleccione o separador **Application settings**.

4. Na secção **Other settings**, clique em **Configure**.

5. No campo **Folder for storing updates**, especifique o endereço do servidor FTP ou HTTP, pasta de rede ou pasta local onde o Kaspersky Security Center copia o pacote de atualização recebido dos servidores de atualização da Kaspersky.

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://dn1-01.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://<nome do utilizador>:<password>@<nó>:<porta>`.

- 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\AVP11\Update distribution\`.

6. Guarde as suas alterações.

Para configurar a atualização do Kaspersky Endpoint Security do armazenamento do servidor especificado:

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

A lista de tarefas é aberta.

2. Clique na tarefa **Update** para o Kaspersky Endpoint Security.

É apresentada a janela de propriedades da tarefa.

A tarefa *Update* é criada automaticamente pelo Quick Start Wizard do Kaspersky Security Center. Para criar a tarefa *Update*, instale o plug-in Web do Kaspersky Endpoint Security for Windows enquanto executa o Assistente.

3. Selecione o separador **Application settings** → **Local mode**.

4. Na lista de origens da atualização, clique no botão **Adicionar**.

5. No campo **Source**, 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 (consulte o *instruções acima*).

6. Na secção **Status**, selecione **Enabled**.

7. Clique em **OK**.

8. Configure as prioridades das origens da atualização utilizando os botões **Up** e **Down**.

9. Guarde as suas alterações.

Se não for possível executar uma atualização através da primeira origem de atualização, o Kaspersky Endpoint Security muda automaticamente para o servidor seguinte.

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.

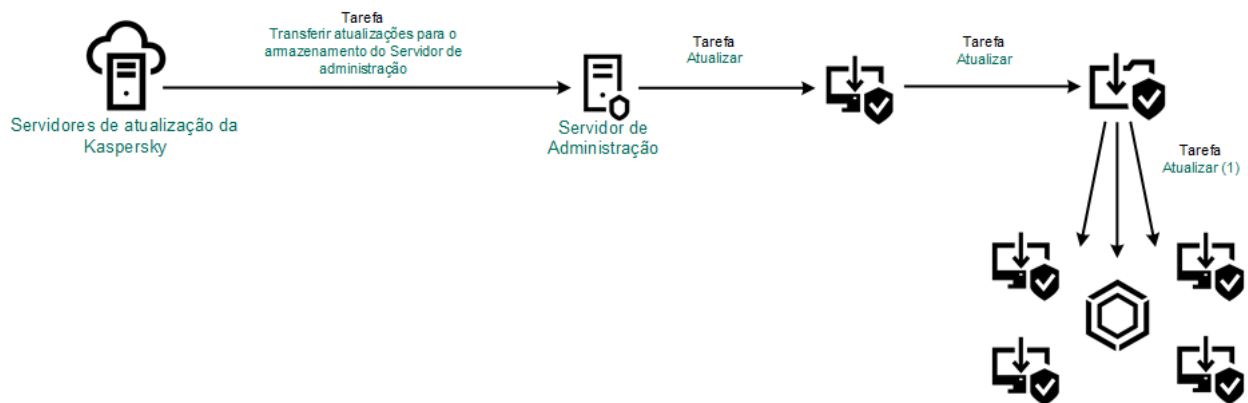
Configurar as atualizações da base de dados e dos módulos da aplicação a partir de uma pasta partilhada compõem-se dos seguintes passos:

1. [Configurar as atualizações da base de dados e dos módulos da aplicação a partir do armazenamento de um servidor](#).

2. Ative a cópia de um pacote de atualização para uma pasta partilhada num dos computadores da rede local da empresa (consulte as instruções abaixo).

3. Configure as atualizações da base de dados e do módulo da aplicação a partir da pasta partilhada especificada para os computadores restantes na rede local da empresa (consulte as instruções abaixo).

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.



Atualizar a partir de uma pasta partilhada

Para ativar a cópia do pacote de atualização para a pasta partilhada:

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

A lista de tarefas é aberta.

2. Clique na tarefa **Update** para o Kaspersky Endpoint Security.

É apresentada a janela de propriedades da tarefa.

A tarefa *Update* é criada automaticamente pelo Quick Start Wizard do Kaspersky Security Center. Para criar a tarefa *Update*, instale o plug-in Web do Kaspersky Endpoint Security for Windows 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 **Copiar atualizações para a pasta**.

6. No campo **Path**, introduza o caminho UNC para a pasta partilhada (por exemplo, \\Server\Share\Update distribution).

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\AVP11\Update distribution\.

7. Guarde as suas alterações.

A tarefa *Atualizar* deve ser atribuída a um computador que servirá de origem das atualizações.

Para configurar as atualizações a partir de uma pasta partilhada:

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

A lista de tarefas é aberta.

2. Clique no botão **Add**.

O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

a. Na lista suspensa **Application**, selecione **Kaspersky Endpoint Security for Windows (11.8.0)**.

b. Na lista pendente **Task type**, selecione **Update**.

c. No campo **Task name**, introduza uma breve descrição, por exemplo, *Updating from a shared folder*.

d. No bloco **Select 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. Sair do Assistente.

Será apresentada uma nova tarefa na tabela de tarefas.

6. Clique no recém criado *Update* tarefa.

É apresentada a janela de propriedades da tarefa.

7. Aceda à secção **Application settings**.

8. Selecione o separador **Local mode**.

9. No bloco **Origens da atualização**, clique em **Adicionar**.

10. No campo **Source**, 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*).

11. Clique em **OK**.

12. Configure as prioridades das origens da atualização utilizando os botões **Up** e **Down**.

13. Guarde as suas alterações.

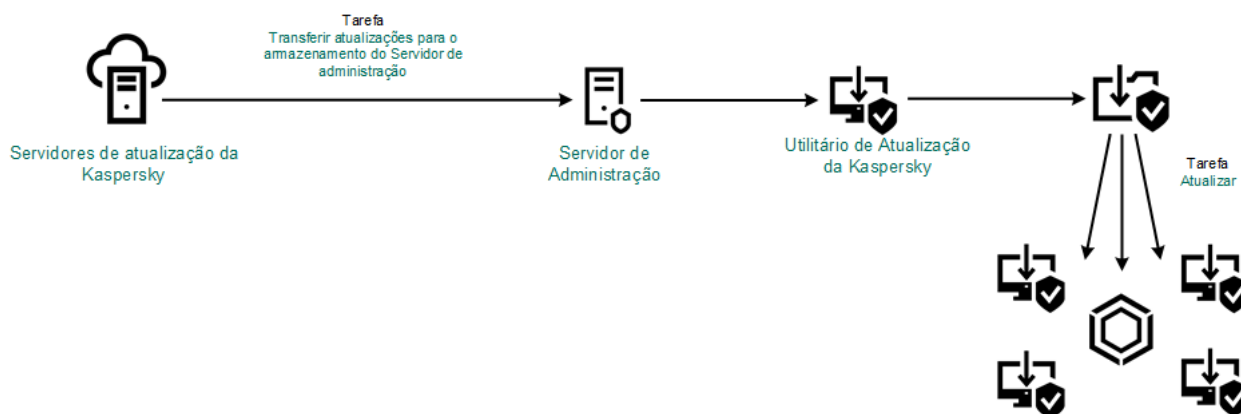
Atualizar utilizando o Utilitário Kaspersky Update

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.

Configurar as atualizações da base de dados e dos módulos da aplicação a partir de uma pasta partilhada compõem-se dos seguintes passos:

1. [Configurar as atualizações da base de dados e dos módulos 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.
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.

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.



Atualizar utilizando o 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, seleccione 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](#).

Para configurar as atualizações a partir de uma pasta partilhada:

1. Na janela principal da Consola de Web, seleccione **Devices** → **Tasks**.
A lista de tarefas é aberta.
2. Clique na tarefa **Update** para o Kaspersky Endpoint Security.
É apresentada a janela de propriedades da tarefa.

A tarefa *Update* é criada automaticamente pelo Quick Start Wizard do Kaspersky Security Center. Para criar a tarefa *Update*, instale o plug-in Web do Kaspersky Endpoint Security for Windows enquanto executa o Assistente.

3. Selecione o separador **Application settings** → **Local mode**.
4. Na lista de origens da atualização, clique no botão **Adicionar**.
5. No campo **Source**, introduza o caminho UNC para a pasta partilhada (por exemplo, \\Server\Share\Update distribution).

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 **Up** e **Down**.
8. Guarde as suas alterações.

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.

Para configurar as definições de atualização no modo móvel:

1. Na janela principal da Consola de Web, selecione **Devices** → **Tasks**.
A lista de tarefas é aberta.
2. Clique na tarefa **Update** para o Kaspersky Endpoint Security.
É apresentada a janela de propriedades da tarefa.
A tarefa *Update* é criada automaticamente pelo Quick Start Wizard do Kaspersky Security Center. Para criar a tarefa *Update*, instale o plug-in Web do Kaspersky Endpoint Security for Windows enquanto executa o Assistente.
Selecione o separador **Application settings** → **Mobile mode**.
3. 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.
4. 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 **Atualização** 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 do Kaspersky Endpoint Security, 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:

1. Na janela principal da aplicação, aceda à secção **Atualizar**.
2. Tal abre a lista de tarefas; selecione a tarefa de atualização e clique em .
3. Clique em **Executar atualizações da base de dados como**.
4. Esta opção abre uma janela; nesta janela, 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:

1. Na janela principal da aplicação, aceda à secção **Atualizar**.
2. Tal abre a lista de tarefas; selecione a tarefa de atualização e clique em .
3. Clique em **Agendamento da atualização das bases de dados**.
4. Na janela aberta, 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.

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.

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 tentará 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.

Para adicionar uma origem de atualização:

1. Na janela principal da aplicação, aceda à secção **Atualizar**.
2. Tal abre a lista de tarefas; selecione a tarefa de atualização e clique em .
3. Clique no botão **Selecionar origens de atualização**.
4. Na janela aberta, clique no botão **Adicionar**.
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://dn1-01.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://<nome do utilizador>:<password>@<nó>:<porta>`.
- 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\AVP11\Update distribution\`.

6. Clique no botão **Selecionar**.
7. Configure as prioridades das origens da atualização utilizando os botões **Up** e **Down**.
8. Guarde as suas alterações.


Configurar atualizações 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.


Configurar as atualizações da base de dados e dos módulos da aplicação a partir de uma pasta partilhada compõem-se dos seguintes passos:

1. Ative a cópia de um pacote de atualização para uma pasta partilhada em um dos computadores na rede local.
2. Configure as atualizações da base de dados e do módulo da aplicação da pasta partilhada especificada para os computadores restantes na LAN da organização.

Para ativar a cópia do pacote de atualização para a pasta partilhada:

1. Na janela principal da aplicação, aceda à secção **Atualizar**.
2. Tal abre a lista de tarefas; selecione a tarefa de atualização e clique em .
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\Share\Update distribution).
5. Guarde as suas alterações.

Para configurar as atualizações a partir de uma pasta partilhada:

1. Na janela principal da aplicação, aceda à secção **Atualizar**.
2. Tal abre a lista de tarefas; selecione a tarefa de atualização e clique em .
3. Clique no botão **Selecionar origens de atualização**.
4. Na janela que é aberta, 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 no botão **Selecionar**.
7. Configure as prioridades das origens da atualização utilizando os botões **Up** e **Down**.
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. Quando uma atualização estiver disponível, a aplicação mostrará uma das seguintes notificações na janela principal do Kaspersky Endpoint Security: atualização importante (🔔), ou atualização crítica (🔴). 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. Para obter detalhes sobre como controlar as atualizações do módulo da aplicação e confirmar uma atualização no Kaspersky Security Center, consulte a [Ajuda do Kaspersky Security Center](#).

Depois de instalar uma atualização da aplicação, poderá ser necessário reiniciar o computador.


Para configurar as atualizações de atualização dos módulos da aplicação:

1. Na janela principal da aplicação, aceda à secção **Atualizar**.
2. Tal abre a lista de tarefas; selecione a tarefa de atualização e clique em .
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 **Devices** → **Policies & Profiles**.
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 **Definições gerais** → **Definições da rede**.
5. Na secção **Definições do servidor de proxy**, selecione **Ignorar o servidor de proxy nos endereços locais**.
6. 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 de definições da aplicação, selecione **Definições gerais** → **Definições de rede**.
3. No bloco **Servidor de proxy**, clique na ligação **Definições do servidor de proxy**.
4. Na janela aberta, selecione uma das seguintes opções para determinar o endereço do servidor de proxy:
 - **Detetar automaticamente as definições do servidor de proxy.**
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. Se quiser ativar a autenticação no servidor de proxy, selecione a caixa de verificação **Usar autenticação do servidor de proxy** e forneça as credenciais da sua conta do utilizador.
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 o 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 palavra-passe.

Reverter última atualização

Depois de as bases de dados e os módulos da aplicação serem atualizados pela primeira vez, a função de reversão das bases de dados e 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 atualização mais recente é útil, por exemplo, quando a nova versão da base de dados contém uma assinatura inválida que leva o Kaspersky Endpoint Security a bloquear uma aplicação segura.

Para reverter a última atualização:

1. Na janela principal da aplicação, aceda à secção **Atualizar**.
2. No mosaico **Reversão das bases de dados para a sua versão anterior**, clique no botão **Reverter**.

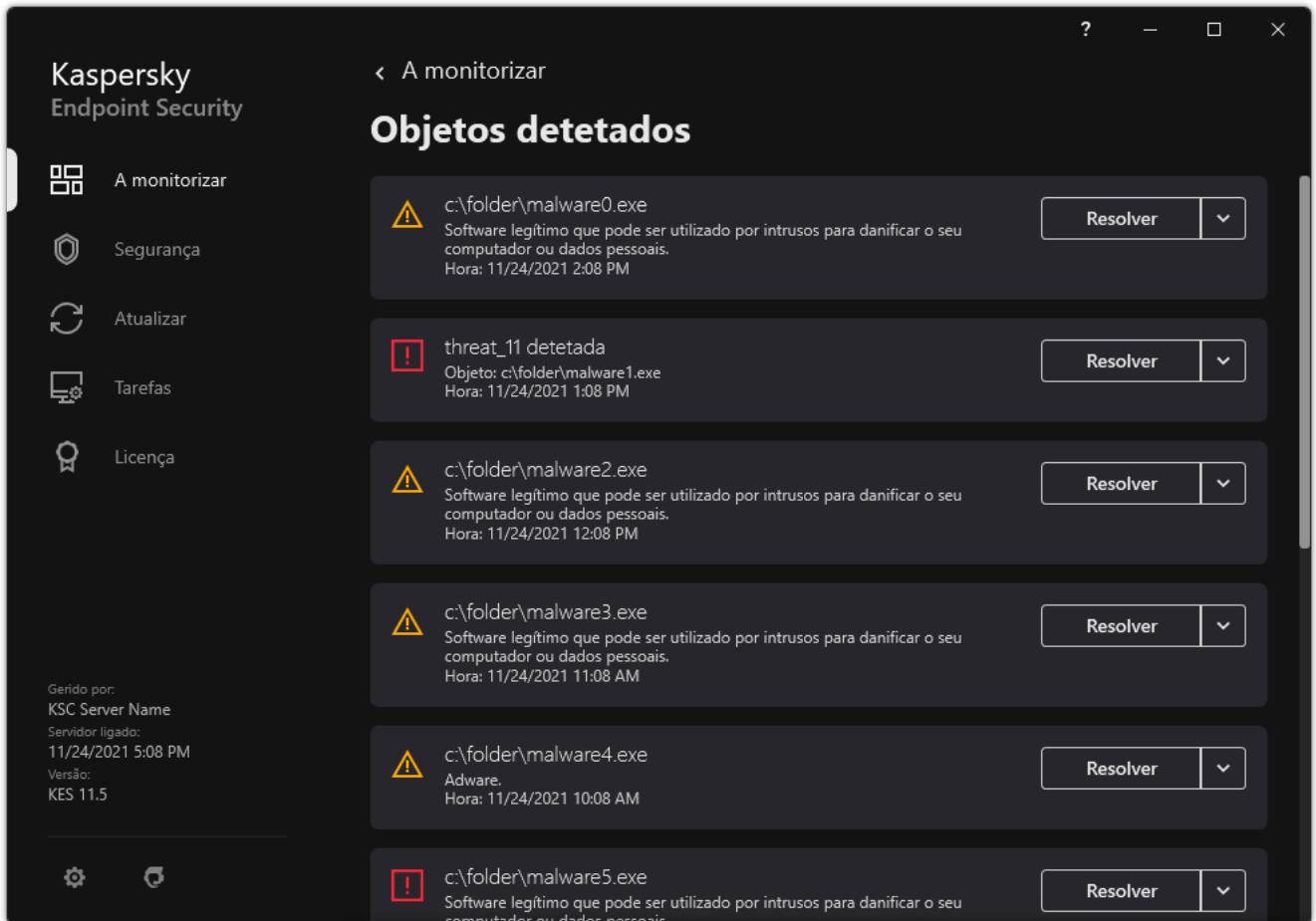
O Kaspersky Endpoint Security começará a reverter a última atualização da base de dados. A aplicação apresentará o progresso da reversão, o tamanho dos ficheiros transferidos e a origem da atualização. Pode parar a tarefa a qualquer momento clicando no botão **Parar atualização**.

Para iniciar ou parar uma tarefa de reversão 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 reversão que não esteja em execução para a iniciar.
 - Selecione uma tarefa de reversão que esteja em execução para a parar.
 - Selecione uma tarefa de reversão pausada para a retomar ou reiniciar.

Trabalhar com ameaças ativas

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). Para detetar ameaças ativas, o Kaspersky Endpoint Security usa a [tecnologia Desinfecção avançada](#). A Desinfecção avançada funciona de forma diferente para computadores e servidores. Pode configurar a desinfecção avançada nas definições de tarefa da [Verificação de vírus](#) e nas [definições da aplicação](#).

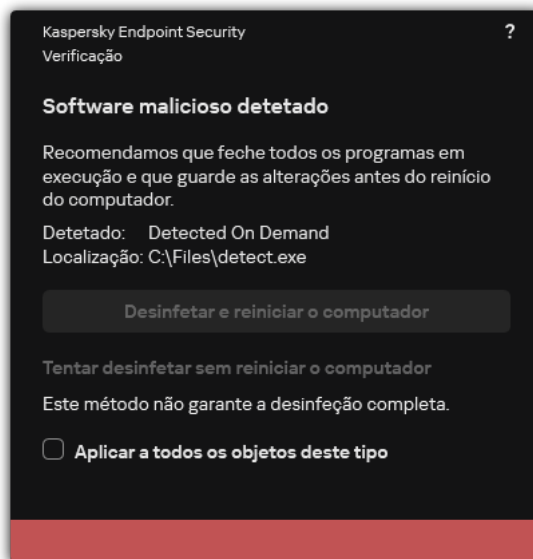


Uma lista de ameaças ativas

Desinfecção de ameaças ativas em computadores

Para detetar ameaças ativas em computadores, [ative a tecnologia Desinfecção avançada](#) nas definições da aplicação. De seguida, configure a experiência do utilizador nas propriedades da tarefa de [Verificação de vírus](#). Existe uma caixa de verificação **Executar a Desinfecção Avançada imediatamente** nas propriedades da tarefa. Se a opção estiver ativa, o Kaspersky Endpoint Security irá realizar a desinfecção 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 Desinfecção Avançada durante uma tarefa de verificação de vírus num computador só é executada se a [funcionalidade Desinfecção Avançada](#) for ativada nas propriedades da política aplicada a este computador.



Notificação sobre ameaça ativa

Desinfecção de ameaças ativas em servidores

Para detetar ameaças ativas nos servidores, tem de fazer o seguinte:

- [ativar a tecnologia Desinfecção avançada](#) nas definições da aplicação;
- [ativar a Desinfecção avançada imediata](#) nas propriedades da tarefa *Verificação de vírus*.

Se o Kaspersky Endpoint Security for instalado num computador com o Windows para servidores, o Kaspersky Endpoint Security não apresenta a notificação. Como tal, o utilizador não pode seleccionar uma ação para desinfetar uma ameaça ativa. Para desinfetar uma ameaça, tem de [Ativar Tecnologia de Desinfecção Avançada](#) nas definições da aplicação e [ativar a desinfecção avançada imediata](#) nas definições da *Verificação de vírus*. Depois, tem de iniciar uma tarefa *Verificação do vírus*.

Ativar ou desativar a Tecnologia de Desinfecção Avançada

Se o Kaspersky Endpoint Security não conseguir interromper a execução de malware, pode usar a tecnologia Desinfecção avançada. Por predefinição, a Desinfecção avançada está desativada por ser uma tecnologia que usa um volume significativo de recursos de computação. Como tal, pode ativar a Desinfecção avançada apenas quando [estiver em contacto com ameaças ativas](#).

A Desinfecção avançada funciona de forma diferente para computadores e servidores. Para usar a tecnologia em servidores, tem de [ativar a desinfecção avançada imediata](#) nas propriedades da tarefa *Verificação antivírus*. Este pré-requisito não é necessário para usar a tecnologia em computadores.


[Como ativar ou desativar a Tecnologia de Desinfecção Avançada 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela da política, selecione **Definições gerais** → **Definições da aplicação**.
6. Na secção **Operating mode**, use a caixa de verificação **Ativar Tecnologia de Desinfecção Avançada** para ativar ou desativar a Tecnologia de Desinfecção Avançada.
7. Guarde as suas alterações.

Como ativar ou desativar a Tecnologia de Desinfecção Avançada na Consola Web e na Cloud Console

1. Na janela principal da Consola Web, selecione **Devices** → **Policies & Profiles**.
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 **Definições gerais** → **Definições da aplicação**.
5. Na secção **Operating mode**, use a caixa de verificação **Ativar Tecnologia de Desinfecção Avançada** para ativar ou desativar a Tecnologia de Desinfecção Avançada.
6. Guarde as suas alterações.

Como ativar ou desativar a Tecnologia de Desinfecção Avançada na interface da aplicação

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Definições gerais** → **Definições da aplicação**.
3. Na secção **Modo operativo**, use a caixa de verificação **Utilizar a tecnologia de Desinfecção Avançada (requer recursos do computador consideráveis)** para ativar ou desativar a Tecnologia de Desinfecção Avançada.
4. Guarde as suas alterações.

O utilizador não irá conseguir usar a maioria das funcionalidades do sistema operativo enquanto a Desinfecção avançada estiver em progresso. Quando a desinfecção for concluída, o computador será reiniciado.

Processamento 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 vírus](#), a ação após deteção de ameaças é definida como **Notificar**. 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 *Crítico* - .

[Como processar uma ameaça na Consola de administração \(MMC\)](#)

1. Na Consola de administração, aceda à pasta **Servidor de Administração** → **Adicional** → **Repositórios** → **Ameaças ativas**.

Abre-se a lista de ameaças ativas.

2. Selecione o objeto que pretende processar.

3. Escolha de que forma pretende tratar da ameaça:

- **Desinfetar**. 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 apaga os ficheiros.
- **Eliminar**.

[Como processar uma ameaça na Consola Web e na Cloud Console](#)

1. Na janela principal da Consola Web, seleccione **Operações** → **Repositórios** → **Ameaças ativas**.

Abre-se a lista de ameaças ativas.

2. Seleccione o objeto que pretende processar.

3. Escolha de que forma pretende tratar da ameaça:

- **Desinfetar.** Se esta opção estiver seleccionada, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção falhar, o Kaspersky Endpoint Security apaga os ficheiros.
- **Eliminar.**


Como processar uma ameaça na interface da aplicação

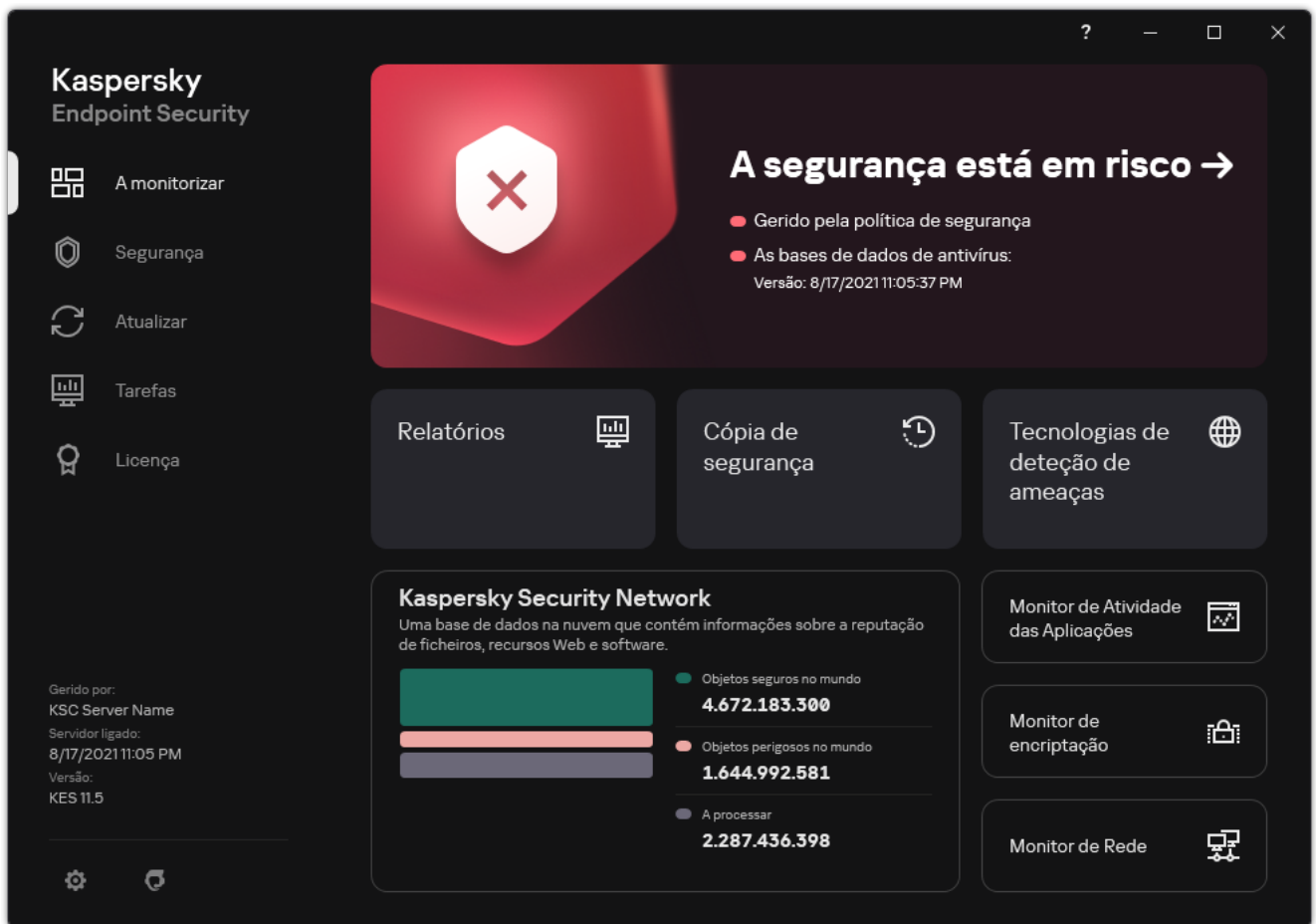
1. Na janela principal da aplicação, na secção **Monitorização**, clique no mosaico **Proteção está em risco**.

Abre-se a lista de ameaças ativas.

2. Seleccione o objeto que pretende processar.

3. Escolha de que forma pretende tratar da ameaça:

- **Resolver.** Se esta opção estiver seleccionada, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção falhar, o Kaspersky Endpoint Security apaga os ficheiros.
- **Adicionar às exclusões.** Se esta ação for seleccionada, 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 seleccionada, 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 seleccionada, 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 dentro do âmbito de proteção.
- **Aprender mais.** Se esta opção for seleccionada, o Kaspersky Endpoint Security abre o [site da Kaspersky Virus Encyclopedia](#) .



Janela principal da aplicação quando é detetada uma ameaça

Proteção do computador

Proteção contra ameaças de ficheiros

O componente Proteção contra ameaças de ficheiros permite prevenir a infeção do sistema de ficheiros do computador. Por predefinição, o componente Proteção contra ameaças de ficheiros reside permanentemente na RAM do computador. O componente verifica ficheiros em todas as unidades do computador, bem como nas unidades ligadas. 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 pelo utilizador ou a 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 na 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 que são armazenados na aplicação são designados *níveis de segurança*: **Alta**, **Recomendada**, **Baixa**. 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.

Para ativar ou desativar o componente Proteção contra ameaças de ficheiros:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de ficheiros**.
3. Utilize o botão de alternar **Proteção contra ameaças de ficheiros** para ativar ou desativar o componente.
4. Se ativou este componente, execute uma das seguintes ações na secção **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. Os valores das definições para o nível de segurança recomendado são fornecidos na tabela abaixo.

- **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 suas próprias definições do componente.
Pode restaurar os valores dos níveis de segurança predefinidos clicando no botão **Restaurar nível de segurança recomendado** na parte superior da janela.

5. 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, o Kaspersky Endpoint Security 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	Ativar	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.
Tecnologia iSwift	Ativar	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 considera a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições da verificação. A tecnologia iSwift é um avanço da tecnologia iChecker para o sistema de ficheiros NTFS.
Tecnologia iChecker	Ativar	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	Ativar	Verifica ficheiros do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Ficheiros de formato do Office incluem objetos OLE também.
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 desinfecção falhar	Se esta opção estiver selecionada, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfecção falhar, o Kaspersky Endpoint Security apaga os ficheiros.

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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de ficheiros**.
3. Clique no botão **Definições avançadas**.
4. No bloco **Pôr a proteção contra ameaças de ficheiros em pausa**, clique na ligação **Pôr a proteção contra ameaças de ficheiros em pausa**.
5. Na janela aberta, 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 de definições da aplicação, 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, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção falhar, o Kaspersky Endpoint Security apaga os ficheiros.
 - **Desinfetar; bloquear se a desinfeção falhar**. Se esta opção estiver selecionada, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção não for possível, o Kaspersky Endpoint Security adiciona a informação sobre os ficheiros infetados que são detetados à lista de ameaças ativas.
 - **Bloquear**. Se esta opção estiver selecionada, o componente Proteção contra ameaças de ficheiros bloqueia automaticamente todos os ficheiros infetados sem tentar desinfetá-los.

Antes de tentar desinfetar ou eliminar um ficheiro infetado, o Kaspersky Endpoint Security 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 outra 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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de ficheiros**.
3. Clique no botão **Definições avançadas**.
4. Na secção **File type**, 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, o Kaspersky Endpoint Security 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, o Kaspersky Endpoint Security verifica [apenas ficheiros infetáveis](#) . O formato do ficheiro é então determinado com base na extensão do ficheiro.
5. Clique na ligação **Editar âmbito de proteção**.
6. Na janela aberta, 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 no botão **Add**.

Abre-se a árvore de pastas.

- b. Selecione um objeto para adicionar ao âmbito de proteção.

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 junto ao 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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de ficheiros**.
3. Clique no botão **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 aprofundado**.
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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de ficheiros**.
3. Clique no botão **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:
 - **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 considera a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições da 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).


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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de ficheiros**.
3. Clique no botão **Definições avançadas**.
4. Na secção **Otimização da verificação**, 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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de ficheiros**.
3. Clique no botão **Definições avançadas**.
4. Na secção **Verificação de ficheiros compostos**, especifique os tipos de ficheiros compostos que pretende verificar: arquivos, pacotes de distribuição ou ficheiros em formatos 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.

O Kaspersky Endpoint Security apenas fornece acesso a ficheiros compostos que são menores do que o valor 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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de ficheiros**.
3. Clique no botão **Definições avançadas**.
4. Na secção **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.
 - **No momento de acesso e alteração**. Neste modo, a Proteção contra ameaças de ficheiros verifica os objetos sem que há uma tentativa para os abrir ou modificar.
 - **No momento de acesso**. Neste modo, a Proteção contra ameaças de ficheiros verifica os objetos apenas aquando de uma tentativa para os abrir.
 - **No momento de execução**. Neste modo, a Proteção contra ameaças de ficheiros verifica os objetos aquando de uma tentativa para os executar.
5. Guarde as suas alterações.

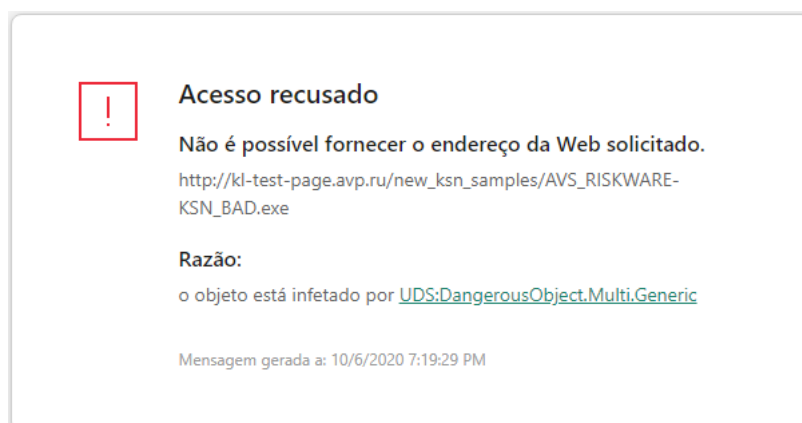
Proteção contra ameaças da Web

O componente Proteção contra Ameaças da Web impede a transferência de ficheiros maliciosos da Internet e também bloqueia 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. Pode [especificar as portas que o Kaspersky Endpoint Security irá monitorizar](#) ou selecionar todas as portas.

Para monitorização do tráfego HTTPS, precisa de [ativar a verificação de ligações encriptadas](#).



Quando um utilizador tenta abrir um website de phishing ou malicioso, o Kaspersky Endpoint Security bloqueia o acesso e apresenta um aviso (consulte a figura abaixo).



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, o Kaspersky Endpoint Security pode aplicar diferentes grupos de definições. Estes grupos de definições que são armazenados na aplicação são designados *níveis de segurança*: **Alta**, **Recomendada**, **Baixa**. 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 seleccionar 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.

Para ativar ou desativar o componente Proteção contra ameaças da Web:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças da Web**.
3. Use o botão de alternar **Proteção contra ameaças da Web** para ativar ou desativar o componente.
4. Se ativou este componente, execute uma das seguintes ações na secção **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 o computador recebe através dos protocolos 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 Kaspersky Endpoint Security 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 médio de verificação.
 - Se pretender configurar um nível de segurança personalizado, clique no botão **Definições Avançadas** e defina suas próprias definições do componente.

Pode restaurar os valores dos níveis de segurança predefinidos clicando no botão **Restaurar nível de segurança recomendado** na parte superior da janela.

5. 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	Ativar	A verificação das ligações para determinar se estão incluídas na base de dados de endereços Web maliciosos permite localizar sites que foram

da Internet na base de dados de endereços da Internet maliciosos		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 na base de dados de endereços da Internet de phishing	Ativar	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.
Utilizar 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.
Utilizar Análise heurística (Anti-Phishing)	Ativar	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 transferência	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.

Alterar a ação a executar em objetos maliciosos de tráfego de Internet

Por predefinição, após a deteção de um objeto infetado no tráfego de Internet, o componente Proteção contra ameaças da Web bloqueia o acesso ao objeto e apresenta uma notificação sobre a ação.

Para alterar a ação a executar em objetos maliciosos de tráfego de Internet:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças da Web**.
3. Na secção **Ação após deteção de ameaças**, selecione a ação executada pelo Kaspersky Endpoint Security em objetos maliciosos de tráfego de Internet:
 - **Bloquear transferência**. 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.

- **Notificar.** Se essa opção for selecionada e um objeto infectado for detectado no tráfego de Internet, o Kaspersky Endpoint Security permitirá que esse objeto seja descarregado para o computador, mas adiciona informações sobre o objeto infectado à lista de ameaças ativas.


4. Guarde as suas alterações.

Verificar URL por comparação com bases de dados de endereços Web de phishing e maliciosos

Verificar as ligações para determinar se estas estão incluídas na lista de endereços de Internet de phishing permite impedir os *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 mensagens do ICQ, 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.

Para configurar o componente Proteção contra ameaças da Web para verificar se as ligações constam das bases de dados de phishing e endereços de Internet maliciosos:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças da Web**.
3. Clique no botão **Definições avançadas**.
4. Execute as seguintes ações:
 - Se pretender que o componente de Proteção Contra Ameaças da Web verifique as ligações por comparação com as bases de dados de endereços de Internet maliciosos, na secção **Métodos de verificação**, selecione a caixa de verificação **Verificar o endereço da Internet contra a base de dados de endereços Web 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 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.

- 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 Web 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.


Também pode verificar as ligações através das bases de dados de reputação da [Kaspersky Security Network](#).

5. Guarde as suas alterações.

Utilizar a análise heurística no funcionamento do componente Proteção contra ameaças da Web

Para aumentar a eficácia da proteção, pode utilizar a 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.

Para configurar a utilização da análise heurística:


1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, seleccione **Proteção essencial contra ameaças** → **Proteção contra ameaças da Web**.
3. Clique no botão **Definições avançadas**.
4. No bloco **Métodos de verificação**, seleccione 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. Utilize então a barra de deslocamento para definir o nível da análise heurística: **Nível superficial**, **Nível médio** ou **Nível aprofundado**.
5. No bloco **Anti-phishing**, seleccione 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.
6. Guarde as suas alterações.

Criar a lista de URL fiáveis

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.

Para criar uma lista de endereços da Internet fiáveis:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças da Web**.
3. Clique no botão **Definições avançadas**.
4. Selecione a caixa de verificação **Não verificar o tráfego de Internet de URL fiáveis**.
Se a caixa de verificação 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.
6. Guarde as suas alterações.

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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela da política, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças da Web**.
6. No bloco **Nível de segurança**, clique no botão **Definições**.
7. Na janela aberta, selecione o separador **Endereços da Internet fiáveis**.
8. 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 ligação **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.
9. Para importar a lista de endereços fiáveis:
 - a. Clique na ligação **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.
10. 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, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Proteção essencial contra ameaças** → **Proteção contra ameaças da Internet**.
5. Para exportar a lista de exclusões no bloco **Endereços da Internet fiáveis**:
 - a. Seleccione os endereços de Internet fiáveis que pretende exportar.
 - b. Clique na ligação **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 seleccione 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.
6. Para importar a lista de exclusões no bloco **Endereços da Internet fiáveis**:
 - a. Clique na ligação **Importar**.
Na janela que se abre, seleccione 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.
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
- Microsoft Outlook Express
- Windows Mail

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 operações com o Outlook 2010, 2013, 2016 e 2019.


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 muda o nome do assunto da mensagem: [A mensagem necessita da sua participação no processamento] <assunto da mensagem> ou [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 a Proteção contra ameaças de correio, o Kaspersky Endpoint Security aplica diferentes grupos de definições. Estes grupos de definições que são armazenados na aplicação são designados *níveis de segurança*: **Alta**, **Recomendada**, **Baixa**. 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.

Para ativar ou desativar o componente Proteção contra ameaças de correio:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de correio**.
3. Use o botão de alternar **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 do Kaspersky Endpoint Security 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 suas próprias definições do componente.

Pode restaurar os valores dos níveis de segurança predefinidos clicando no botão **Restaurar nível de segurança recomendado** na parte superior da janela.

5. 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	<p>O <i>Âmbito de proteção</i> inclui objetos que o componente verifica quando está em execução: Mensagens de entrada e de saída ou Apenas mensagens de entrada.</p> <p>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.</p>
Ligar a extensão do Microsoft Outlook	Ativar	<p>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.</p> <p>Se o correio for verificado utilizando a extensão do Microsoft Outlook, recomenda-se a utilização do Modo Exchange em Cache. Para obter informações mais detalhadas sobre o Modo Exchange em Cache e recomendações sobre a sua utilização, consulte a Base de Conhecimentos da Microsoft.</p>
Verificar arquivos anexados	Ativar	A verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros formatos de arquivo.
Analisar ficheiros anexados com formatos do Microsoft Office	Ativar	Verifica ficheiros do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Ficheiros de formato do Office incluem objetos OLE também.
Filtro de anexos	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.
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, o Kaspersky Endpoint Security tenta desinfetar o objeto detetado. O utilizador poderá aceder à mensagem com um anexo seguro. Se não for possível desinfetar o objeto, o Kaspersky Endpoint Security elimina o objeto infetado. O Kaspersky Endpoint Security adiciona as informações sobre a ação executada ao assunto da mensagem: [A mensagem foi processada] <assunto da mensagem>.

Alterar a ação a executar em mensagens de e-mail 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 de definições da aplicação, 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, o Kaspersky Endpoint Security tenta desinfetar o objeto detetado. O utilizador poderá aceder à mensagem com um anexo seguro. Se não for possível desinfetar o objeto, o Kaspersky Endpoint Security elimina o objeto infetado. O Kaspersky Endpoint Security adiciona as informações sobre a ação executada ao assunto da mensagem: [A mensagem foi processada] <assunto da mensagem>.
 - **Desinfetar; bloquear se a desinfeção falhar.** Quando um objeto infetado é detetado numa mensagem de entrada, o Kaspersky Endpoint Security tenta desinfetar o objeto detetado. O utilizador poderá aceder à mensagem com um anexo seguro. Se não for possível desinfetar o objeto, o Kaspersky Endpoint Security adiciona um aviso ao assunto da mensagem: [A mensagem necessita da sua participação no processamento] <assunto da mensagem>. O utilizador poderá aceder à mensagem com o anexo original. Quando um objeto infetado é detetado numa mensagem de saída, o Kaspersky Endpoint Security tenta desinfetar o objeto detetado. Se não for possível desinfetar o objeto, o Kaspersky Endpoint Security 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, o Kaspersky Endpoint Security adiciona um aviso ao assunto da mensagem: [A mensagem necessita da sua participação no processamento] <assunto da mensagem>. O utilizador poderá aceder à mensagem com o anexo original. Se for detetado um objeto infetado numa mensagem de saída, o Kaspersky Endpoint Security 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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de correio**.
3. Clique no botão **Definições avançadas**.
4. No bloco **Âmbito de verificação**, 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. Na secção **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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de correio**.
3. Clique no botão **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.
 - **Verificar arquivos anexados**. A verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros formatos de arquivo.

Se, durante a análise, o Kaspersky Endpoint Security detetar uma password para um arquivo no texto da mensagem, esta password será usada para analisar o conteúdo do arquivo relativamente a aplicações maliciosas. A password não é guardada. O arquivo é descompactado antes da verificação. Se ocorrer um erro da aplicação durante o processo de descompactação, pode eliminar manualmente os ficheiros descompactados que são guardados no seguinte caminho: %systemroot%\temp. Os ficheiros têm o prefixo PR.

- **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.
- **Limitar o tempo da verificação de arquivos a N segundos.** 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 funcionalidade de filtro 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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de correio**.
3. Clique no botão **Definições avançadas**.
4. No bloco **Filtro de anexos**, 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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças de Correio**.
6. No bloco **Nível de segurança**, clique no botão **Definições**.
7. Na janela aberta, selecione o separador **Filtro de anexos**.
8. 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 ligação **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.
9. Para importar a lista de extensões:
 - a. Clique na ligação **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.
10. Guarde as suas alterações.

[Como exportar e importar uma lista de extensões de filtro de anexos na Consola Web e na Cloud Console](#)

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Proteção essencial contra ameaças** → **Proteção contra ameaças de correio**.
5. Para exportar a lista de extensões, no bloco **Filtro de anexos**:
 - a. Seleccione as extensões que pretende exportar.
 - b. Clique na ligação **Exportar**.
 - c. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de extensões e seleccione 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 **Filtro de anexos**:
 - a. Clique na ligação **Importar**.
 - b. Na janela que se abre, seleccione 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.

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). 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 da Proteção contra ameaças de correio para Outlook pode verificar mensagens recebidas e enviadas através dos protocolos POP3, SMTP, NNTP, IMAP e MAPI. O Kaspersky Endpoint Security suporta também o trabalho com outros clientes de e-mail (incluindo o Microsoft Outlook Express®, Windows Mail e Mozilla™ Thunderbird™).

A extensão Proteção contra ameaças de correio suporta operações com o Outlook 2010, 2013, 2016 e 2019.

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.

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.

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.

Se o correio for verificado utilizando a extensão da Proteção contra ameaças de correio para o Outlook, recomenda-se a utilização do Modo de intercâmbio em cache. Para obter informações mais detalhadas sobre o Modo Exchange em Cache e recomendações sobre a sua utilização, consulte a [Base de Conhecimentos da Microsoft](#).

Para configurar o modo operativo da extensão da Proteção contra ameaças de correio para Outlook utilizando o Kaspersky Security Center:

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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças de Correio**.
6. No bloco **Nível de segurança**, clique no botão **Definições**.
7. Na secção **Conetividade**, clique no botão **Definições**.
8. Na **Proteção de e-mail**:
 - 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. Guarde as suas alterações.


Proteção contra ameaças de Rede

O componente Proteção contra ameaças de Rede verifica o tráfego de rede de entrada quanto à existência de atividades típicas de ataques de rede. Quando o Kaspersky Endpoint Security deteta uma tentativa de ataque à rede no computador do utilizador, bloqueia a ligação da rede a o computador atacante. As bases de dados do Kaspersky Endpoint Security 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. Se necessário, pode desativar a Proteção contra ameaças de Rede.


Para ativar ou desativar a Proteção contra ameaças de Rede:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de rede**.
3. Use o botão de alternar **Proteção contra ameaças de rede** para ativar ou desativar o componente.
4. Guarde as suas alterações.

Como resultado, se a Proteção contra ameaças de rede estiver ativada, o Kaspersky Endpoint Security verifica o tráfego de entrada da rede em busca de atividades típicas de ataques de rede. Quando o Kaspersky Endpoint Security deteta uma tentativa de ataque à rede no computador do utilizador, bloqueia a ligação da rede a o computador atacante.

Bloquear um computador atacante

Para bloquear um computador atacante:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de rede**.
3. Selecione a caixa de verificação **Adicionar um computador de ataque à lista de computadores bloqueados durante N minutos**.

Se a caixa de verificação estiver selecionada, o componente Proteção contra ameaças de Rede adiciona o computador atacante 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 32 768 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.


1. Defina uma duração de bloqueio diferente para um computador atacante no campo à direita da caixa de verificação **Adicionar um computador de ataque à lista de computadores bloqueados durante N minutos**.
2. Guarde as suas alterações.

Como resultado, quando o Kaspersky Endpoint Security deteta uma tentativa de ataque à rede contra o computador do utilizador, bloqueia todas as ligações com o computador atacante.

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.

Para configurar moradas de exclusões de bloqueio:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de rede**.
3. Clique na ligação **Gerir exclusões**.
4. Na janela que é aberta, clique no botão **Adicionar**.
5. Introduza o endereço IP do computador para o qual não devem ser bloqueados os ataques de rede.
6. Guarde as suas alterações.

Como resultado, o Kaspersky Endpoint Security não rastreia a atividade dos dispositivos na lista de exclusões.

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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Proteção essencial contra ameaças** → **Proteção contra ameaças de Rede**.
6. No bloco de **Definições de Proteção contra ameaças de Rede**, clique no botão **Exclusões**.
7. 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. Clique na ligação **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.
8. Para importar a lista de exclusões:
 - a. Clique no 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.
9. 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 **Devices** → **Policies & Profiles**.
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 **Proteção essencial contra ameaças** → **Proteção contra ameaças de rede**.
5. No bloco **Definições de Proteção contra ameaças de Rede**, clique na ligação **Exclusões**.
Abre-se a lista de exclusões.
6. Para exportar a lista de regras:
 - a. Selecione as exclusões que pretende exportar.
 - b. Clique no botão **Export**.
 - c. Confirme que quer exportar apenas as exclusões selecionadas ou exportar toda a lista de exclusões.
 - d. 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.
 - e. Guardar o ficheiro.
O Kaspersky Endpoint Security exporta toda a lista de exclusões para o ficheiro XML.
7. Para importar a lista de exclusões:
 - a. Clique no 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.
8. Guarde as suas alterações.

Configurar a proteção contra ataques 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.

Para configurar a proteção contra ataques de rede por tipo:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção essencial contra ameaças** → **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.
4. Utilize o botão de alternar **Proteção contra ataques de MAC Spoofing**.
5. No bloco **Sobre a deteção de um ataque de MAC spoofing**, selecione uma das seguintes opções:
 - **Notificar apenas.**
 - **Notificar e bloquear.**
6. Guarde as suas alterações.

Firewall

A Firewall bloqueia ligações não autorizadas ao computador enquanto trabalha na Internet ou na 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 impõem 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 usando 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 fiáveis*: Fiável/Restrições baixas/Restrições altas/Não fiável.

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 de Intrusão do Host.

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 Alta Restrição 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 da seguinte maneira: uma regra de rede para aplicações inclui regras de acesso com base no estado da rede: *pública*, *local* ou *fiável*. Por exemplo, por predefinição, não é permitida nenhuma atividade de rede das aplicações no grupo *fiável* Alta Restrição 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.

Estados da ligação de rede

A Firewall permite controlar a atividade da rede, dependendo do estado da ligação de rede. O Kaspersky Endpoint Security recebe o estado da ligação de rede a partir do sistema operativo do computador. O estado da ligação de rede no sistema operacional é definido pelo utilizador ao configurar a ligação. Pode [alterar o estado da ligação de rede nas definições do Kaspersky Endpoint Security](#). A Firewall monitoriza a atividade da rede, dependendo do estado da rede nas definições do Kaspersky Endpoint Security, e não do sistema operativo.


A ligação de rede pode ter um dos seguintes tipos de estado:

- **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 estado *Rede pública* à Internet. Não é possível alterar o estado 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 o 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.

Ativar ou desativar a Firewall

Por predefinição, a Firewall está ativada e funciona no modo otimizado.

Para ativar ou desativar a Firewall:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Firewall**.
3. Use o botão de alternar **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 verifica o tráfego de rede de entrada quanto à existência de atividades típicas de ataques de 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 estado da ligação de rede

Por predefinição, a Firewall atribui o estado *Rede pública* à Internet. Não é possível alterar o estado da Internet.

Para alterar a situação da ligação de rede:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Firewall**.
3. Clique no botão **Redes disponíveis**.
4. Selecione a ligação de rede cujo estado pretende alterar.
5. Na coluna **Tipo de rede**, selecione o estado 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 o 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

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.

Ao criar regras de pacotes de rede, note que estas têm prioridade sobre as regras de rede para aplicações.

[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. Selecione o 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 **Ativado** 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 clicando 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 **Registrar eventos**.
8. Clique no botão **Save**.

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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Firewall**.
3. Clique no botão **Regras de pacotes**.
Esta ação abre a lista das regras de rede predefinidas definidas pela Firewall.
4. Clique no botão **Add**.
Esta ação abre as propriedades da regra de rede.
5. Defina o estado **Ativado** 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 clicando 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 no botão **Save**.
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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.
6. 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.
7. Selecione o separador **Regras de pacotes de rede**.
Esta ação abre a lista das regras de rede predefinidas definidas pela Firewall.
8. Clique no botão **Add**.
Abre-se as propriedades da regra de pacotes.
9. Introduza manualmente o nome do serviço de rede no campo **Nome**.
10. 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.
11. Se pretender que as ações da regra de rede se reflitam no [relatório](#), selecione a caixa de verificação **Registar eventos**.
12. Guardar a nova regra de rede.
13. Utilize os botões **Para cima/Para baixo** para definir a prioridade da regra de rede.
14. 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 junto ao objeto.

[Como criar uma regra de pacotes de rede na Consola Web e na Cloud Console](#) 

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Seleccione **Essential Threat protection** → **Firewall**.
5. No bloco **Definições da Firewall**, clique na ligação **Regras de pacotes de rede**.
Esta ação abre a lista das regras de rede predefinidas definidas pela Firewall.
6. Clique no botão **Add**.
Abre-se as propriedades da regra de pacotes.
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 seleccionar um modelo de regra predefinido ao clicar na ligação **Selecionar modelo**. 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](#), seleccione a caixa de verificação **Registar eventos**.
10. Guardar a regra de rede.
A nova regra de rede será adicionada à lista.
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. Utilize o botão de alternar na coluna **Estado** para ativar ou desativar a regra de pacotes.

Definições da regra de pacotes de rede

Parâmetro	Descrição
Ação	<p>Permitir.</p> <p>Bloquear.</p> <p>Segundo as regras da aplicação. Se esta opção estiver seleccionada, a Firewall aplica as regras de rede de aplicações à ligação de rede.</p>
Protocolo	<p>Controle a atividade de rede executada através do protocolo seleccionado: TCP, UDP, ICMP, ICMPv6, IGMP e GRE.</p> <p>Se ICMP ou ICMPv6 estiver seleccionado como protocolo, pode definir o código e o tipo de pacote ICMP.</p> <p>Se TCP ou UDP estiver seleccionado como o tipo de protocolo, pode especificar os números de porta separados por vírgulas dos computadores locais e remotos entre os quais a ligação deve ser monitorizada.</p>

Direção	<p>Entrada (pacote). A Firewall aplica a regra de rede a todos os pacotes de rede de entrada.</p> <p>Entrada. A Firewall aplica a regra de rede a todos os pacotes de rede enviados através de uma ligação iniciada por um computador remoto.</p> <p>Entrada/Saída. A Firewall aplica a regra de rede aos pacotes de rede de entrada e de saída, independentemente de a ligação ter sido iniciada pelo computador do utilizador ou por um computador remoto.</p> <p>Saída (pacote). A Firewall aplica a regra de rede a todos os pacotes de rede de saída.</p> <p>Saída. A Firewall aplica a regra de rede a todos os pacotes de rede enviados através de uma ligação iniciada pelo computador do utilizador.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>O protocolo TCP estabelece uma ligação. Para TCP, utilize as direções Entrada, Saída e Entrada/Saída. Todos os outros protocolos não estabelecem ligações, mas enviam pacotes. Para todos os outros protocolos, utilize as direções Entrada (pacote), Saída (pacote) e Entrada/Saída.</p> </div>
Adaptadores de rede	<p>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.</p>
Time to live (TTL)	<p>Restrinja o controlo dos pacotes de rede com base no seu tempo de vida (TTL).</p>
Endereço remoto	<p>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.</p>
Endereço local	<p>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. 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.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Por vezes, o endereço local não pode ser obtido para aplicações. Se for este o caso, este parâmetro é ignorado.</p> </div>

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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Firewall**.

3. Clique no botão **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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Firewall**.

3. Clique no botão **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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Firewall**.
3. Clique no botão **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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.
6. 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.
7. Selecione o separador **Regras de pacotes de rede**.
8. 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 ligação **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.
9. Para importar uma lista de regras de pacotes de rede:
 - a. Clique na ligação **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.
10. 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, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Seleccione **Essential Threat protection** → **Firewall**.
5. Clique na ligação **Regras de pacotes de rede**.
6. Para exportar a lista de regras de pacotes de rede:
 - a. Seleccione as regras que pretende exportar.
 - b. Clique no botão **Export**.
 - c. Confirme que deseja exportar apenas as regras seleccionadas 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 uma lista de regras de pacotes de rede:
 - a. Clique na ligação **Importar**.
Na janela que se abre, seleccione 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.

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. Selecione a **Atividade de rede** ou o separador **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 no botão **Add**.


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 seleccionar um modelo de regra predefinido clicando 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 no botão **Save**.

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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Firewall**.
3. Clique no botão **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 no botão **Add**.
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 clicando 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 no botão **Save**.
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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Proteção Essencial Contra Ameaças** → **Firewall**.
6. 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.
7. Selecione o separador **Regras de rede de aplicações**.
8. Clique no botão **Add**.
9. Na janela aberta, 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.
10. Clique no botão **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.
11. Selecione a aplicação necessária.
12. Na lista suspensa **Adicionar a aplicação selecionada ao grupo fiável**, selecione **Grupos predefinidos** e clique em **OK**.
A aplicação será adicionada ao grupo predefinido.
13. 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.
14. Selecione o separador **Regras de rede**.
Esta ação abre a lista das regras de rede predefinidas definidas pela Firewall.
15. Clique no botão **Add**.
Esta ação abre as propriedades da regra de rede.
16. Introduza manualmente o nome do serviço de rede no campo **Nome**.
17. Configure as definições da regra de rede (consulte a tabela abaixo).
Pode seleccionar 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.

18. Se pretender que as ações da regra de rede se reflitam no [relatório](#), selecione a caixa de verificação **Registrar eventos**.
19. Guardar a nova regra de rede.
20. Utilize os botões **Para cima/Para baixo** para definir a prioridade da regra de rede.
21. 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, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Seleccione **Essential Threat protection** → **Firewall**.
5. No bloco **Firewall settings**, clique na ligação **Application network rules**.
Esta ação abre a janela de configuração dos direitos de aplicações e a lista de recursos protegidos.
6. Seleccione o separador **Direitos de aplicações**.
Uma lista de grupos fiáveis será apresentada no lado esquerdo da janela e as respetivas propriedades serão apresentadas no lado direito.
7. Clique no botão **Add**.
É iniciado o Assistente para adicionar uma aplicação a um grupo fiável.
8. Seleccione o grupo fiável relevante para a aplicação.
9. Seleccione o tipo de **Aplicação**. Clique no botão **Next**.
Se pretender criar uma regra de rede para várias aplicações, seleccione o tipo de **Grupo** e defina um nome para o grupo de aplicações.
10. Na lista aberta de aplicações, seleccione 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. Clique em **OK** para terminar o Assistente.
A aplicação será adicionada ao grupo fiável.
12. Na parte esquerda da janela, seleccione a aplicação relevante.
13. Na parte direita da janela, seleccione **Regras de rede** na lista suspensa.
Esta ação abre a lista das regras de rede predefinidas definidas pela Firewall.
14. Clique no botão **Add**.
Esta ação abre as propriedades da regra de aplicações.
15. Introduza manualmente o nome do serviço de rede no campo **Nome**.
16. Configure as definições da regra de rede (consulte a tabela abaixo).
Pode seleccionar um modelo de regra predefinido ao clicar na ligação **Selecionar modelo**. 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](#), seleccione a caixa de verificação **Registar eventos**.
18. Guardar a regra de rede.

A nova regra de rede será adicionada à lista.

19. Utilize os botões **Para cima/Para baixo** 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 separados por vírgulas dos computadores locais e remotos entre os quais a ligação deve ser monitorizada.
Direção	Entrada. Entrada/Saída. Saída.
Endereço remoto	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.
Endereço local	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. 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. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">Por vezes, o endereço local não pode ser obtido para aplicações. Se for este o caso, este parâmetro é ignorado.</div>

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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Firewall**.

3. Clique no botão **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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Firewall**.
3. Clique no botão **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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Firewall**.
3. Clique no botão **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**.
 - **Negar**.
 - **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 de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Firewall**.
3. Clique no botão **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 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 ao 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.

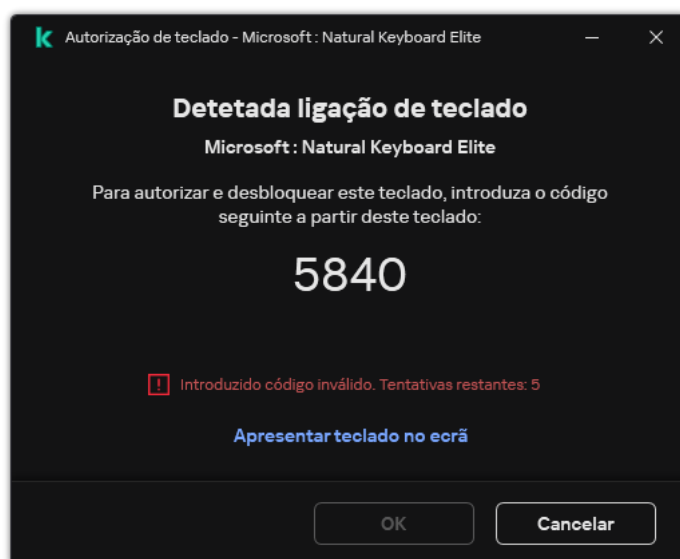
Se o código tiver sido introduzido corretamente, a aplicação guarda os parâmetros de identificação – VID/PID do teclado e o número da porta à qual foi ligado – na lista de teclados autorizados. A autorização de teclado não precisa de ser repetida quando o teclado voltar a ser ligado ou depois de o sistema operativo ser reiniciado.

Quando o teclado autorizado é ligado ao computador numa porta USB diferente, a aplicação volta a mostrar uma solicitação para 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.

Por predefinição, o componente Prevenção de ataques BadUSB não está instalado. Se precisar do componente Prevenção de ataques BadUSB, pode adicionar o componente nas propriedades do [pacote de instalação](#) antes de instalar a aplicação ou [alterar os componentes disponíveis da aplicação](#) depois da instalação da aplicação.




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.

Para ativar ou desativar a Prevenção de ataques BadUSB:


1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Prevenção de ataques BadUSB**.
3. Use o botão de alternar **Prevenção de Ataques BadUSB** para ativar ou desativar o componente.
4. Em **Autorização de teclado USB ao ligar**, ajuste as definições de segurança para a introdução do código de autorização:
 - **Número máximo de tentativas de autorização do dispositivo.** 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 5 tentativas de introdução do código de autorização, o dispositivo USB será bloqueado após a quinta tentativa falhada. O Kaspersky Endpoint Security apresenta a duração do bloqueio do dispositivo USB. Após decorrido este tempo, tem 5 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 falhadas de introdução do 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 usado para a autorização de dispositivos USB que não suportam a introdução de caracteres aleatórios (p. ex., leitores de códigos de barras). Não recomendamos a utilização do teclado no ecrã para a autorização de dispositivos USB desconhecidos.

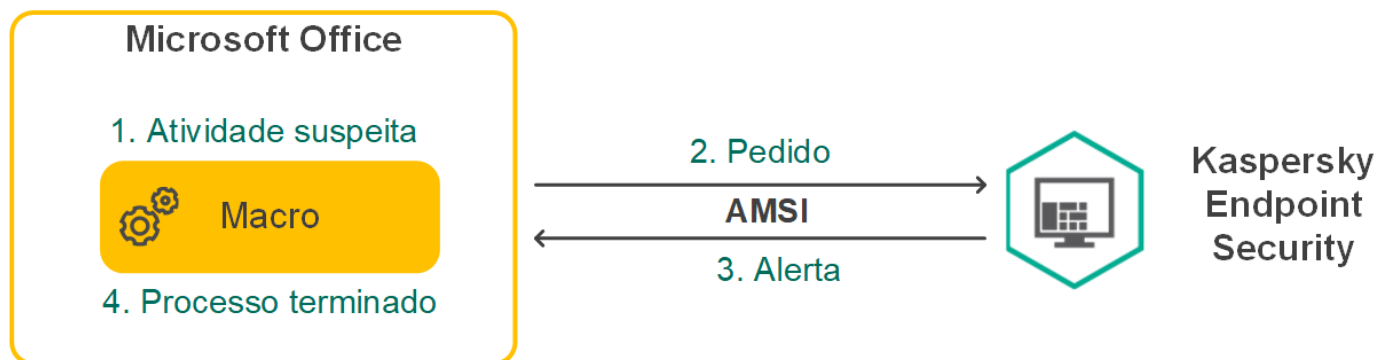
Para permitir ou proibir o uso do teclado no ecrã para autorização:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Prevenção de ataques BadUSB**.
3. 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.
4. Guarde as suas alterações.

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. A aplicação de terceiros depois de receber uma notificação de uma ameaça não permite a realização de ações maliciosas (por exemplo, terminação).



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;
- Windows 11;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

Ativar e desativar a Proteção AMSI

Por predefinição, a Proteção AMSI está ativada.


Para ativar ou desativar a Proteção AMSI:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção AMSI**.
3. Use o botão de alternar **Proteção AMSI** para ativar ou desativar o componente.
4. Guarde as suas alterações.

Utilizar a Proteção AMSI para verificar ficheiros compostos

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 os tipos de ficheiros compostos a verificar, aumentando assim a velocidade da verificação.

Para configurar verificações da Proteção AMSI de ficheiros compostos:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção essencial contra ameaças** → **Proteção AMSI**.
3. Na secção **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 no campo **Tamanho máximo dos ficheiros**. 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.

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.

Ativar e desativar a prevenção de explorações

Por predefinição, a prevenção de explorações está ativada e é executada no modo recomendado pelos especialistas da Kaspersky. Se necessário, pode desativar a prevenção de explorações.

Para ativar ou desativar a prevenção de explorações:

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


2. Na janela de definições da aplicação, selecione **Proteção avançada contra ameaças** → **Prevenção de explorações**.
3. Use o botão de alternar **Prevenção de explorações** para ativar ou desativar o componente.
4. Guarde as suas alterações.

Como resultado, se a Prevenção de explorações estiver ativada, o Kaspersky Endpoint Security monitorizará os ficheiros executáveis 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).

Selecionar uma ação a executar quando é detetada uma exploração

Por predefinição, ao detetar uma exploração, o Kaspersky Endpoint Security bloqueia as operações tentadas pela exploração.


Para escolher uma ação a executar quando é detetada uma exploração:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção avançada contra ameaças** → **Prevenção de explorações**.
3. Selecione a ação relevante no bloco **Ao detetar exploração**:
 - **Bloquear operação**. 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.
 - **Notificar**. 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](#).
4. Guarde as suas alterações.

Proteção da memória de processos do sistema

Por predefinição, a proteção da memória de processos do sistema está ativada.

Para ativar e desativar a proteção da memória de processos do sistema:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção avançada contra ameaças** → **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.

Como resultado, o Kaspersky Endpoint Security bloqueará os processos externos que tentam aceder aos processos do 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 com base em assinaturas de fluxos de comportamento proporciona defesa proativa ao computador.

Ativar e desativar a Deteção de comportamento

Por predefinição, a Deteção de comportamento está ativada e é executada no modo recomendado pelos especialistas da Kaspersky. Se necessário, pode desativar a Deteção de comportamento.

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.


Para ativar ou desativar a Deteção de comportamento:

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Deteção de Comportamento**.
3. Use o botão de alternar **Deteção de comportamento** para ativar ou desativar o componente.
4. 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.

Selecionar a ação a ser executada ao detetar atividade de software malicioso

Para selecionar o que fazer se uma aplicação se envolver em atividades maliciosas, execute os seguintes passos:

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Deteção de Comportamento**.
3. Selecione a ação relevante no bloco **Ao detetar atividade de software malicioso**:
 - **Delete file**. 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.

- **Terminar a aplicação.** Se este item estiver selecionado, ao detetar atividade maliciosa, o Kaspersky Endpoint Security encerra a aplicação em questão.
- **Notificar.** 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.

4. Guarde as suas alterações.

Proteção de pastas partilhadas contra encriptação externa

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.

A proteção de pastas partilhadas contra a encriptação externa fornece a análise da 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.


Por predefinição, a proteção de pastas partilhadas contra encriptação externa está desativada.

Após a instalação do Kaspersky Endpoint Security, a proteção de pastas partilhadas contra encriptação externa estará limitada até o computador ser reiniciado.

Ativar ou desativar a proteção de pastas partilhadas contra encriptação externa


Após a instalação do Kaspersky Endpoint Security, a proteção de pastas partilhadas contra encriptação externa estará limitada até o computador ser reiniciado.

Para ativar ou desativar a proteção de pastas partilhadas contra encriptação externa:

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Deteção de Comportamento**.
3. Use o botão de alternar **Ativar a proteção de pastas partilhadas contra encriptação externa** para ativar ou desativar a deteção de atividade típica da encriptação externa.
4. Guarde as suas alterações.

Selecionar a ação a executar ao detetar encriptação externa de pastas partilhadas

Para selecionar a ação a executar ao detetar encriptação externa de pastas partilhadas:

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Deteção de Comportamento**.
3. Selecione a ação relevante no bloco **Proteção de pastas partilhadas contra encriptação externa**:
 - **Bloquear ligação durante N min. (de 1 a 43800)**. Se esta opção estiver selecionada e 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 da interface da aplicação local](#).
 - Envia informações sobre a atividade maliciosa detetada ao Kaspersky Security Center.

De igual modo, se o componente Motor de remediação estiver ativado, o Kaspersky Endpoint Security restaura os ficheiros modificados a partir das cópias de segurança.

 - **Notificar**. Se esta opção estiver selecionada e o Kaspersky Endpoint Security detetar uma tentativa de modificação dos ficheiros nas pastas partilhadas, realiza as seguintes ações:
 - Adiciona uma entrada aos [relatórios da interface da aplicação local](#).
 - Adiciona uma entrada à lista de ameaças ativas.
 - Envia informações sobre a atividade maliciosa detetada ao Kaspersky Security Center.
4. Guarde as suas alterações.

Criar uma exclusão para proteção de pastas partilhadas contra encriptação externa

A exclusão de uma pasta 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.

[Como criar uma exclusão para proteção de pastas partilhadas 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 **Policies**.
4. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Definições gerais** → **Exclusions**.
6. No bloco **Analisar exclusões e aplicações fiáveis**, clique no botão **Definições**.
7. Na janela apresentada, selecione o separador **Exclusões de verificação**.
Abre-se uma janela que contém uma lista de exclusões.
8. 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.
9. Selecione a caixa de verificação **Allow use of local trusted applications** 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. Se tiver sido gerada uma lista local, depois de esta funcionalidade ser desativada, o Kaspersky Endpoint Security continua a excluir os ficheiros listados das verificações.
10. Clique em **Adicionar**.
11. No bloco **Propriedades**, selecione a caixa de verificação **Ficheiro ou pasta**.
12. Clique na ligação **selecionar 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**.
13. 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:\Pasta***.txt incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da Pasta, exceto a própria Pasta. 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 caracteres.

14. Se necessário, no campo **Comentário**, introduza um breve comentário na exclusão de verificação que está a criar.
15. Clique na ligação **qualquer** no bloco **Descrição da exclusão de verificação** (clique nos itens sublinhados **para editar os mesmos**) para ativar a ligação **selecionar componentes**.
16. Clique na ligação **selecionar componentes** para abrir a janela **Componentes de proteção**.
17. Selecione a caixa de verificação junto ao componente **Deteção de comportamento**.
18. Guarde as suas alterações.

[Como criar uma exclusão para proteção de pastas partilhadas utilizando a Consola Web e a Cloud Console](#) 


1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Definições gerais** → **Exclusions**.
5. No bloco **Scan exclusions and trusted applications**, clique na ligação **Scan exclusions**.
6. Seleccione 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. Seleccione a caixa de verificação **Allow use of local trusted applications** 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. Se tiver sido gerada uma lista local, depois de esta funcionalidade ser desativada, o Kaspersky Endpoint Security continua a excluir os ficheiros listados das verificações.
8. Clique no botão **Add**.
9. Seleccione como pretende adicionar a exclusão: **File or folder**.
10. Clique em **Procurar** e seleccione 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:\Pasta***.txt incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da Pasta, exceto a própria Pasta. 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 caracteres.
11. No bloco **Componentes de proteção**, seleccione o componente **Deteção de comportamento**.
12. Se necessário, no campo **Comentário**, introduza um breve comentário na exclusão de verificação que está a criar.

13. Selecione o estado **Ativo** para a exclusão.

Pode usar o botão de alternar para [parar uma exclusão](#) a qualquer momento.

14. Guarde as suas alterações.

[Como criar uma exclusão para proteção de pastas partilhadas na interface da aplicação](#)

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

2. Na janela Application settings, selecione **Definições gerais** → **Ameaças e exclusões**.

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:\Pasta***.txt incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas incorporadas dentro da Pasta, exceto a própria Pasta. 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 caracteres.

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.

Configurar endereços das exclusões da proteção de pastas partilhadas contra encriptação externa

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.

Para excluir computadores remotos que realizem a encriptação externa de pastas partilhadas:

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, seleccione **Proteção avançada contra ameaças** → **Deteção de Comportamento**.
3. No bloco **Exclusões**, clique na ligação **Configurar endereços das exclusões**.
4. Se pretender adicionar um endereço IP ou nome de computador à lista de exclusões, clique no botão **Adicionar**.
5. Introduza o endereço IP ou nome de computador a partir do qual as tentativas de encriptação externa não devem ser abordadas.
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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela da política, selecione **Proteção avançada contra ameaças** → **Deteção de comportamento**.
6. No bloco de **Definições de Proteção contra ameaças de Rede**, clique no botão **Exclusões**.
7. Para exportar a lista de regras:
 - a. Selecione as exclusões que pretende exportar. Para seleccionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.

Se não tiver seleccionado nenhuma exclusão, o Kaspersky Endpoint Security exportará todas as exclusões.
 - b. Clique na ligação **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.
8. Para importar a lista de exclusões:
 - a. Clique no 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.
9. 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, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Proteção avançada contra ameaças** → **Deteção de comportamento**.
5. Para exportar a lista de exclusões no bloco **Exclusões**:
 - a. Seleccione as exclusões que pretende exportar.
 - b. Clique no botão **Export**.
 - c. Confirme que quer exportar apenas as exclusões seleccionadas ou exportar toda a lista de exclusões.
 - d. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de exclusões e seleccione a pasta onde pretende guardar este ficheiro.
 - e. Guardar o ficheiro.
O Kaspersky Endpoint Security exporta toda a lista de exclusões para o ficheiro XML.
6. Para importar a lista de exclusões no bloco **Exclusões**:
 - a. Clique no botão **Importar**.
 - b. Na janela que se abre, seleccione 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.

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 (como ficheiros e aplicações)

A atividade de rede das aplicações é controlada pela [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 usando 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 fiáveis*: Fiável/Restrições baixas/Restrições altas/Não fiável.

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 de Intrusão do Host.

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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela da política, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
6. Utilize a caixa de verificação **Prevenção contra invasões** para ativar ou desativar o componente.
7. 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 **Devices** → **Policies & Profiles**.
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 **Advanced Threat Protection** → **Host Intrusion Prevention**.
5. Use o botão de alternar **Prevenção contra invasões** 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 de definições da aplicação, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
3. Use o botão de alternar **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 seleccionar o grupo fiável ao qual o Kaspersky Endpoint Security tem de [atribuir automaticamente todas as aplicações desconhecidas](#). As aplicações que foram iniciadas antes do Kaspersky Endpoint Security são automaticamente movidas para a janela do grupo fiável [especificado nas definições do componente 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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela da política, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
6. 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.
7. Selecione o separador **Direitos de aplicações**.
8. Clique no botão **Add**.
9. Na janela aberta, 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.
10. Clique no botão **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.
11. Selecione a aplicação necessária.
12. Na lista pendente **Adicionar a aplicação selecionada ao grupo fiável**, selecione o grupo fiável necessário para a aplicação.
13. Guarde as suas alterações.

[Como alterar o grupo fiável de uma aplicação na Consola Web e na Cloud Console](#) 

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Advanced 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. Seleccione o separador **Direitos de aplicações**.
Uma lista de grupos fiáveis será apresentada no lado esquerdo da janela e as respetivas propriedades serão apresentadas no lado direito.
7. Clique no botão **Add**.
É iniciado o Assistente para adicionar uma aplicação a um grupo fiável.
8. Seleccione o grupo fiável relevante para a aplicação.
9. Seleccione o tipo de **Aplicação**. Clique no botão **Next**.
Se pretender alterar o grupo fiável de várias aplicações, seleccione o tipo de **Group** e defina um nome para o grupo de aplicações.
10. Na lista de aplicações aberta, seleccione 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. Clique em **OK** para terminar 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 de definições da aplicação, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
3. Clique no botão **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 noutra 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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
 5. Na janela da política, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
 6. 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.
 7. Selecione o separador **Direitos de aplicações**.
 8. Selecione o grupo fiável necessário.
 9. Selecione **Direitos de grupos** no menu de contexto do grupo fiável.
Esta ação abre as propriedades do grupo fiável.
 10. 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 o separador **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 o separador **Direitos**.
- A atividade de rede das aplicações é controlada pela [Firewall](#) usando *regras de rede*.
11. 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** (⊗).
 12. 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.
 13. 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, seleccione **Devices** → **Policies & Profiles**.
 2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
 3. Seleccione o separador **Application settings**.
 4. Aceda a **Advanced 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. Seleccione o separador **Direitos de aplicações**.
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, seleccione 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, seleccione **Ficheiros e registo do sistema**.
 - Se pretender editar os direitos do grupo fiável que regulam o acesso aos processos e objetos do sistema operativo, seleccione **Direitos**.
- A atividade de rede das aplicações é controlada pela [Firewall](#) usando *regras de rede*.
9. Para o recurso relevante, na coluna da ação correspondente, seleccione a opção necessária: **Herdar**, **Permitir** (✔) ou **Proibir** (✘).
 10. Se pretender monitorizar a utilização de recursos do computador, seleccione **Registrar 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. 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 de definições da aplicação, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
3. Clique no botão **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 o separador **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 o separador **Direitos**.

A atividade de rede das aplicações é controlada pela [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 **Registrar 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 do utilizador*) 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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela da política, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
6. No bloco **Direitos de aplicações e recursos protegidos**, clique no botão **Editar**.
7. Para a definição **Grupo fiável para aplicações iniciadas antes do Kaspersky Endpoint Security for Windows começar a trabalhar**, selecione o [grupo fiável](#) adequado.
8. Guarde as suas alterações.

[Como seleccionar 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 **Devices** → **Policies & Profiles**.
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 **Advanced Threat Protection** → **Host Intrusion Prevention**.
5. Para a definição **Grupo fiável para aplicações iniciadas antes do Kaspersky Endpoint Security for Windows começar a trabalhar**, selecione o [grupo fiável](#) adequado.
6. Guarde as suas alterações.

[Como seleccionar 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 de definições da aplicação, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
3. Em **Grupo fiável para aplicações iniciadas antes do Kaspersky Endpoint Security for Windows começar a trabalhar**, 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. 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, seleccione o separador **Policies**.
4. Seleccione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela da política, seleccione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
6. No bloco **Regras de processamento da aplicação**, utilize a lista suspensa **Grupo fiável para aplicações que não foi possível adicionar a grupos existentes** para seleccionar 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.
7. Utilize a caixa de verificação **Atualizar direitos para as aplicações previamente desconhecidas das bases de dados da KSN** para configurar a atualização automática dos direitos de aplicações desconhecidas.
8. 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, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Advanced Threat Protection** → **Host Intrusion Prevention**.
5. No bloco **Regras de processamento da aplicação**, utilize a lista suspensa **Grupo fiável para aplicações que não foi possível adicionar a grupos existentes** para seleccionar 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 **Atualizar direitos para as aplicações previamente desconhecidas das bases de dados da KSN** para configurar a atualização automática dos direitos de aplicações desconhecidas.
7. Guarde as suas alterações.

[Como seleccionar um grupo fiável para aplicações desconhecidas na interface da aplicação](#)

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, seleccione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
3. Em **Regras de processamento da aplicação**, seleccione 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.
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 seleccionar um grupo fiável para aplicações assinadas digitalmente 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela da política, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
6. No bloco **Regras de processamento da aplicação**, utilize a caixa de verificação **Confiar nas aplicações assinadas digitalmente** 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](#).
7. 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 **Devices** → **Policies & Profiles**.
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 **Advanced Threat Protection** → **Host Intrusion Prevention**.
5. No bloco **Regras de processamento da aplicação**, utilize a caixa de verificação **Confiar nas aplicações assinadas digitalmente** 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 de definições da aplicação, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
3. No bloco **Regras de processamento da aplicação**, utilize a caixa de verificação **Confiar nas aplicações assinadas digitalmente** 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. Se uma aplicação for iniciada diretamente por outra aplicação mas não estiver subordinada à aplicação que a executa, as regras não serão herdadas.

[Como alterar os direitos de aplicações 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela da política, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
6. 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.
7. Selecione o separador **Direitos de aplicações**.
8. Clique no botão **Add**.
9. Na janela aberta, 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.
10. Clique no botão **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.
11. Selecione a aplicação necessária.
12. Na lista suspensa **Adicionar a aplicação selecionada ao grupo fiável**, selecione **Grupos predefinidos** e clique em **OK**.
A aplicação será adicionada ao grupo predefinido.
13. Selecione a aplicação relevante e, em seguida, selecione **Direitos de aplicações** no menu de contexto da aplicação.
Abrem-se as propriedades da aplicação.
14. 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 o separador **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 o separador **Direitos**.

A atividade de rede das aplicações é controlada pela [Firewall](#) usando *regras de rede*.

15. 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** (⊗).

16. 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.

17. Guarde as suas alterações.





[Como alterar os direitos de aplicações na Consola Web e na Cloud Console](#) 

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
 2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
 3. Seleccione o separador **Application settings**.
 4. Aceda a **Advanced 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. Seleccione o separador **Direitos de aplicações**.
Uma lista de grupos fiáveis será apresentada no lado esquerdo da janela e as respetivas propriedades serão apresentadas no lado direito.
 7. Clique no botão **Add**.
É iniciado o Assistente para adicionar uma aplicação a um grupo fiável.
 8. Seleccione o grupo fiável relevante para a aplicação.
 9. Seleccione o tipo de **Aplicação**. Clique no botão **Next**.
Se pretender alterar o grupo fiável de várias aplicações, seleccione o tipo de **Group** e defina um nome para o grupo de aplicações.
 10. Na lista aberta de aplicações, seleccione 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. Clique em **OK** para terminar o Assistente.
A aplicação será adicionada ao grupo fiável.
 12. Na parte esquerda da janela, seleccione 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, seleccione **Ficheiros e registo do sistema**.
 - Se pretender editar os direitos do grupo fiável que regulam o acesso aos processos e objetos do sistema operativo, seleccione **Direitos**.
- A atividade de rede das aplicações é controlada pela [Firewall](#) usando *regras de rede*.
14. Para o recurso relevante, na coluna da ação correspondente, seleccione a opção necessária: **Herdar**, **Permitir** (✓) ou **Proibir** (✗).
 15. Se pretender monitorizar a utilização de recursos do computador, seleccione **Registrar 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.

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 de definições da aplicação, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
3. Clique no botão **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 o separador **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 o separador **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 **Registrar 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	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. A atividade da aplicação é monitorizada pelos seguintes componentes: Deteção de comportamento , Prevenção de explorações , Prevenção contra invasões , Motor de remediação e Firewall .
Não herdar restrições do processo principal (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 de	O Kaspersky Endpoint Security não monitorizará a atividade de ficheiros ou de rede de aplicações iniciadas por esta aplicação.

subaplicação	
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 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.

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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela da política, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
6. 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.
7. Selecione o 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.
8. Selecione a categoria de recursos protegidos aos quais pretende adicionar um novo recurso protegido.
Se pretender adicionar uma subcategoria, clique em **Adicionar** → **Categoria**.
9. Clique no botão **Add**. Na lista suspensa, selecione o tipo de recurso que pretende adicionar: **Ficheiro ou pasta** ou **Chave de registo**.
10. Na janela aberta, 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.
11. Guarde as suas alterações.

[Como adicionar um recursos protegido na Consola Web e na Cloud Console](#) 

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Advanced 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. Seleccione o 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 no botão **Add**.
É iniciado o Assistente de Novo Recurso.
8. Clique na ligação **Group name** para seleccionar a categoria de recursos protegidos aos quais pretende adicionar um novo recurso protegido.
Se pretender adicionar uma subcategoria, seleccione a opção **Category of protected resources**.
9. Seleccione o tipo de recurso que pretende adicionar: **Ficheiro ou pasta** ou **Registry key**.
10. Seleccione um ficheiro, pasta ou chave de registo.
11. Clique em **OK** para terminar o Assistente.
Pode ver os direitos das aplicações para aceder aos recursos adicionados. Para tal, seleccione 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 de definições da aplicação, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
3. Clique no botão **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. Clique no botão **Add**. Na lista suspensa, selecione o tipo de recurso que pretende adicionar: **Ficheiro ou pasta** ou **Chave de registo**.
6. Na janela aberta, 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  **Desativar 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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela da política, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.
6. No bloco **Regras de processamento da aplicação**, execute uma das seguintes ações:
 - Se pretende configurar a eliminação automática, selecione a caixa de verificação **Eliminar regras para as aplicações que não são iniciadas há mais de N dias** e especifique 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 pretende desativar a eliminação automática, desmarque a caixa de verificação **Eliminar regras para as aplicações que não são iniciadas há mais de N dias**.

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.
7. 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, seleccione **Devices** → **Policies & Profiles**.

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

É apresentada a janela de propriedades da política.

3. Seleccione o separador **Application settings**.

4. Aceda a **Advanced Threat Protection** → **Host Intrusion Prevention**.

5. No bloco **Regras de processamento da aplicação**, execute uma das seguintes ações:

- Se pretende configurar a eliminação automática, seleccione a caixa de verificação **Eliminar regras para as aplicações que não são iniciadas há mais de N dias** e especifique 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 pretende desativar a eliminação automática, desmarque a caixa de verificação **Eliminar regras para as aplicações que não são iniciadas há mais de N dias**.

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 de definições da aplicação, selecione **Proteção avançada contra ameaças** → **Prevenção contra invasões**.

3. No bloco **Regras de processamento da aplicação**, execute uma das seguintes ações:

- Se pretende configurar a eliminação automática, selecione a caixa de verificação **Eliminar regras para as aplicações que não são iniciadas há mais de N dias** e especifique 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 pretende desativar a eliminação automática, desmarque a caixa de verificação **Eliminar regras para as aplicações que não são iniciadas há mais de N dias**.

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

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 predefinição, o Kaspersky Endpoint Security controla o acesso das aplicações ao fluxo de áudio e de vídeo do seguinte modo:

- As aplicações fiáveis e com restrições baixas têm, por predefinição, permissão para receber o fluxo de áudio e de vídeo de dispositivos.
- As aplicações com Restrições altas e Não fiáveis não têm, por predefinição, permissão para receber o fluxo de áudio e de 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 fiável ou para o grupo Restrições altas depois de a 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.

Motor de remediação

O 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 um [scan de vírus](#).

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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela da política, selecione **Proteção avançada contra ameaças** → **Motor de remediação**.
6. Utilize a caixa de verificação **Motor de remediação** para ativar ou desativar o componente.
7. 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, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Proteção avançada contra ameaças** → **Motor de remediação**.
5. Use o botão de alternar **Motor de remediação** 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 de definições da aplicação, seleccione **Proteção avançada contra ameaças** → **Motor de remediação**.
3. Use o botão de alternar **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 *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 categoria e reputação dos ficheiros verificados bem como informações sobre a reputação dos endereços da Web verificados.

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.

Para reduzir a sobrecarga nos servidores da KSN, os peritos da Kaspersky podem laçar atualizações da aplicação que desativam temporariamente ou restringem em parte os pedidos à Kaspersky Security Network. Neste caso, o estado da ligação à KSN na interface local da aplicação é *Ativado com restrições*.

Infraestrutura da KSN

O Kaspersky Endpoint Security suporta as seguintes soluções infraestruturais da KSN:

- *KSN Global* é a solução usada pela maioria das aplicações da Kaspersky. Os participantes na KSN recebem informações da Kaspersky Security Network 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.
- *Private KSN* 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 KSN Privado 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.

Por predefinição, o Kaspersky Security Center usa a KSN Global. Pode configurar a utilização do KSN Privado na Consola de Administração (MMC), na Consola Web do Kaspersky Security Center e na [Command line](#). Não é possível configurar a utilização da KSN Privada na Consola de Nuvem do Kaspersky Security Center.

Para obter mais informações detalhadas sobre o KSN Privado, consulte a *documentação sobre a Kaspersky Private Security Network*.

Ativar e desativar a utilização da Kaspersky Security Network

Para ativar ou desativar a utilização da Kaspersky Security Network:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, 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.
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.
4. Se necessário, desligue o botão de alternar **Ativar o modo KSN alargado**.
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 KSN privado

A KSN privada (doravante também referida como KPSN) 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 fiável» na base de dados de reputação local, mas tiver uma reputação de «fiável» na KSN/KPSN, o Kaspersky Endpoint Security detetará o ficheiro como «não fiável» 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](#).

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.

Para ativar ou desativar o modo de nuvem para componentes de proteção:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Proteção avançada contra ameaças** → **Kaspersky Security Network**.
3. Use o botão de alternar **Ativar o cloud mode** 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 através do serviço KSN Proxy.

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 informações sobre a configuração do KSN Proxy, 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 janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Proteção avançada contra ameaças** → **Kaspersky Security Network**.
3. No bloco **Definições do KSN Proxy**, utilize a caixa de verificação **Utilizar Proxy da KSN** para ativar ou desativar a proteção de ficheiros.
4. Se necessário, selecione a caixa de verificação **Utilizar os servidores da KSN quando o proxy da KSN não está disponível**.
Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security utiliza os servidores da KSN quando o serviço de proxy da KSN estiver indisponível. Os servidores da KSN podem estar localizados quer na Kaspersky (quando a KSN Global é utilizada) quer em terceiros (quando a KSN Privada é utilizada).
5. Guarde as suas alterações.

Como ativar ou desativar o KSN Proxy na Consola Web

1. Na janela principal da Consola Web, selecione **Devices** → **Policies & Profiles**.
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 **Advanced Threat Protection** → **Kaspersky Security Network**.
5. Use a caixa de verificação **Use KSN Proxy** para ativar ou desativar o KSN Proxy.
6. Se necessário, selecione a caixa de verificação **Use KSN servers when KSN Proxy is not available**.
Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security utiliza os servidores da KSN quando o serviço de proxy da KSN estiver indisponível. Os servidores da KSN podem estar localizados quer na Kaspersky (quando a KSN Global é utilizada) quer em terceiros (quando a KSN Privada é utilizada).
7. 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. Na Consola de Administração, dirija-se à pasta **Administration Server** → **Additional** → **Remote installation** → **Installation packages**.
2. No menu de contexto dos **Pacotes de instalação**, selecione **Propriedades**.
3. No separador **Geral** na janela aberta, especifique o novo endereço do servidor do KSN proxy.
4. Guarde as suas alterações.

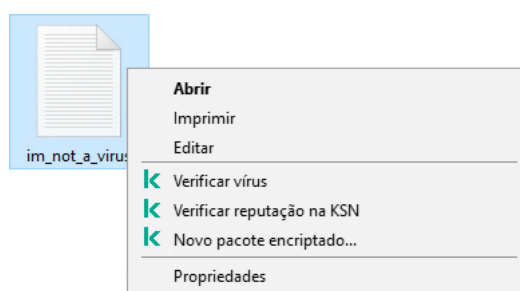
Verificar a reputação de um ficheiro na Kaspersky Security Network

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 seleccione 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 maioria dos utilizadores da Kaspersky Security Network confirmou que o ficheiro é fiável.

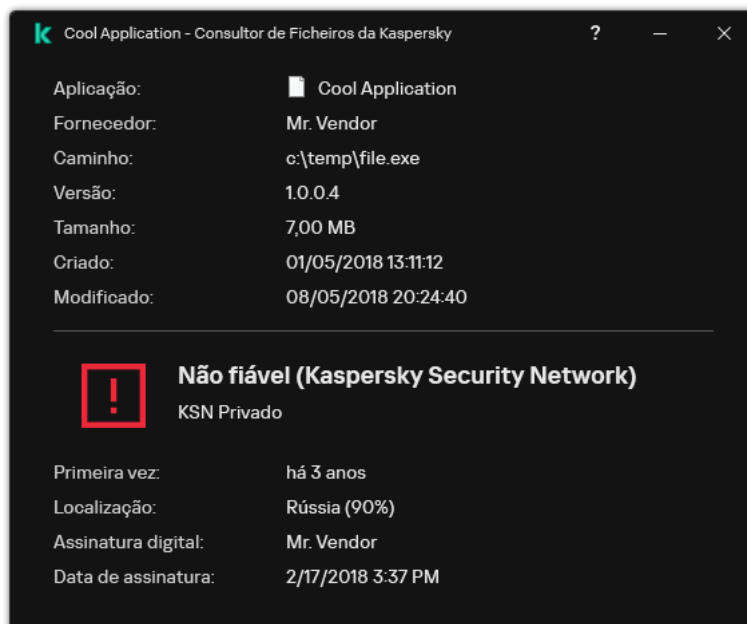
 **Software legítimo que pode ser utilizado por intrusos para danificar o seu computador ou dados pessoais**. Embora não tenham funções maliciosas, estas aplicações podem ser exploradas por intrusos. Para mais informações sobre software legal que pode ser utilizado por criminosos para danificar o computador 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](#).

 **Desconhecida (Kaspersky Security Network)**. A Kaspersky Security Network não possui nenhuma informação acerca do ficheiro. Pode verificar um ficheiro utilizando bases de dados de antivírus (a opção **Verificar a presença de vírus** no menu de contexto).

O Kaspersky Endpoint Security exibe a solução KSN usada para determinar a reputação do arquivo: *KSN Global* ou *KSN Privada*.

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 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](#) podem descriptar 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.

Configurar as definições da verificação de ligações encriptadas

Para configurar as definições da verificação de ligações encriptadas:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Definições gerais** → **Definições de rede**.
3. No bloco **Verificar as 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 de Ficheiros, 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).
6. Guarde as suas alterações.

Definições de verificação das ligações encriptadas

Parâmetro	Descrição
Ao visitar um domínio com um certificado não fiável	<ul style="list-style-type: none">• Permitir. Se esta opção estiver selecionada, 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. 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.• Bloquear ligação. Se este item estiver selecionado, 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.
Ao ocorrerem erros de verificação de ligação encriptada	<ul style="list-style-type: none">• Bloquear ligação. Se este item estiver selecionado, quando ocorre um erro de verificação das ligações encriptadas, o Kaspersky Endpoint Security bloqueia a ligação de rede.• Adicionar domínio às exclusões. Se este item estiver selecionado, quando ocorre 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 ligação.
Bloquear ligações SSL 2.0 (recomendado)	Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security bloqueia as ligações de rede estabelecidas através do protocolo SSL 2.0.

	Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security não bloqueia as ligações de rede estabelecidas através do protocolo SSL 2.0 e não monitoriza o tráfego de rede transmitido através destas ligações.
Descriptar uma ligação encriptada com um site que utilize certificado EV	<p>Certificados EV (Extended Validation Certificates) 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 endereços a verde.</p> <p>Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security descripta e monitoriza as ligações encriptadas com sites que utilizem um certificado EV.</p> <p>Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security 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, <code>https://google.com</code>.</p> <p>Se estiver a abrir um site com um certificado EV pela primeira vez, a ligação encriptada será descriptada, independentemente de a caixa de verificação estar selecionada ou não.</p>

Verificar ligações encriptadas no Firefox e no Thunderbird


Após a instalação, o Kaspersky Endpoint Security adiciona um certificado da Kaspersky ao armazenamento do sistema para certificados fiáveis (loja de certificados Windows). Por predefinição, o Firefox e o Thunderbird utilizam o seu próprio armazenamento de certificados Mozilla proprietário em vez do armazenamento de certificados do 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 no Firefox e no Thunderbird 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 pelas aplicações Mozilla. Se tiver selecionado o armazenamento de certificados Mozilla, adicione manualmente um certificado da Kaspersky ao mesmo. 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, o Kaspersky Endpoint Security não verifica o tráfego no navegador Mozilla Firefox e no cliente de e-mail Thunderbird.

Antes de adicionar um certificado ao armazenamento Mozilla, exporte o certificado da Kaspersky do Painel de Controlo do Windows (propriedades do navegador). Para obter detalhes sobre a exportação do certificado da Kaspersky, consulte a [Base de Conhecimento do Suporte Técnico](#). Para obter detalhes sobre como adicionar um certificado ao armazenamento, visite o [site de suporte técnico do Mozilla](#).

Pode escolher o armazenamento de certificados apenas na interface local da aplicação.

Para escolher um armazenamento de certificados para verificar ligações encriptadas no Firefox e no Thunderbird:


1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Definições gerais** → **Definições de rede**.

3. Na secção **Mozilla Firefox and Thunderbird**, selecione a caixa de verificação **Utilize o armazenamento de certificados selecionado para verificar as ligações encriptadas em aplicações do Mozilla**.
4. Selecionar um armazenamento de certificados:
 - **Utilizar o armazenamento de certificados do Windows (recomendado)**. O certificado raiz da Kaspersky é adicionado a este armazenamento durante a instalação do Kaspersky Endpoint Security.
 - **Utilizar o armazenamento de certificados do Mozilla**. 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.
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*. 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.

Para excluir um domínio das verificações da ligação encriptada:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Definições gerais** → **Definições de rede**.
3. No bloco **Verificar as ligações encriptadas**, clique no botão **Endereços fiáveis**.
4. Clique no botão **Add**.
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 máscaras para endereços IP. Pode introduzir um intervalo de endereços IP na interface local da aplicação (por exemplo, 198.51.100.0/24). Não é possível introduzir um intervalo de endereços IP na Consola do Kaspersky Security Center.

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 `dominio.com`.

- `*.domain.com` - o registo inclui os seguintes endereços: `https://movies.domain.com`, `https://images.domain.com/page123`. O registo não inclui o domínio `dominio.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 de definições da aplicação, selecione **Definições gerais** → **Definições de rede**.
3. No bloco **Verificar as 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 de definições da aplicação, selecione **Definições gerais** → **Definições de rede**.
3. No bloco **Verificar as 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.

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 de Web, seleccione **Devices** → **Tasks**.
A lista de tarefas é aberta.
2. Clique no botão **Add**.
O Assistente de Tarefas é iniciado.
3. Configurar as definições de tarefa:
 - a. Na lista suspensa **Application**, seleccione **Kaspersky Endpoint Security for Windows (11.8.0)**.
 - b. Na lista pendente **Tipo de tarefa**, seleccione **Eliminar dados**.
 - c. No campo **Task name**, introduza uma breve descrição, por exemplo, *Eliminar dados (Antirroubo)*.
 - d. Na secção **Select devices to which the task will be assigned**, seleccione o âmbito de tarefa.
4. Seleccione os dispositivos de acordo com a opção do âmbito da tarefa seleccionada. 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. Sair do Assistente.

Será apresentada uma nova tarefa na lista de tarefas.

6. Clique na tarefa **Eliminar dados** 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:

- **Eliminar através do sistema operativo.** O Kaspersky Endpoint Security usa os recursos do sistema operativo para eliminar ficheiros sem os enviar para a reciclagem.
- **Eliminar completamente, impossível recuperar.** 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 dias**. 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 eliminação de dados adiada, lembre-se de que os funcionários podem desligar o computador antes de sair de férias. Neste caso, o período de ausência de ligação pode ser excedido e os dados serão eliminados. 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 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 caracteres ";" ou "," para especificar várias extensões.
- **Âmbito predefinido.** O Kaspersky Endpoint Security eliminará os ficheiros das seguintes áreas:
 - **Documentos.** 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).
 - **Ambiente de Trabalho.** Ficheiros na pasta *Ambiente de trabalho* padrão do sistema operativo e respetivas subpastas.

- **Ficheiros temporários do Internet Explorer.** Ficheiros temporários relacionados com o funcionamento do Internet Explorer, por exemplo, cópias de páginas Web, imagens e ficheiros multimédia.
- **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).
- **Perfil do utilizador.** 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 no botão **Run**.

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 dos utilizadores 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).

O Kaspersky Endpoint Security monitoriza apenas os tráfegos HTTP e HTTPS.

Para monitorização do tráfego HTTPS, precisa de [ativar a verificação de ligações encriptadas](#).

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 dos utilizadores aos dados num site e ocultar imagens gráficas, 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 "Ficheiros 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 do Office» apenas para a categoria do site «Correio eletrónico baseado na Internet».

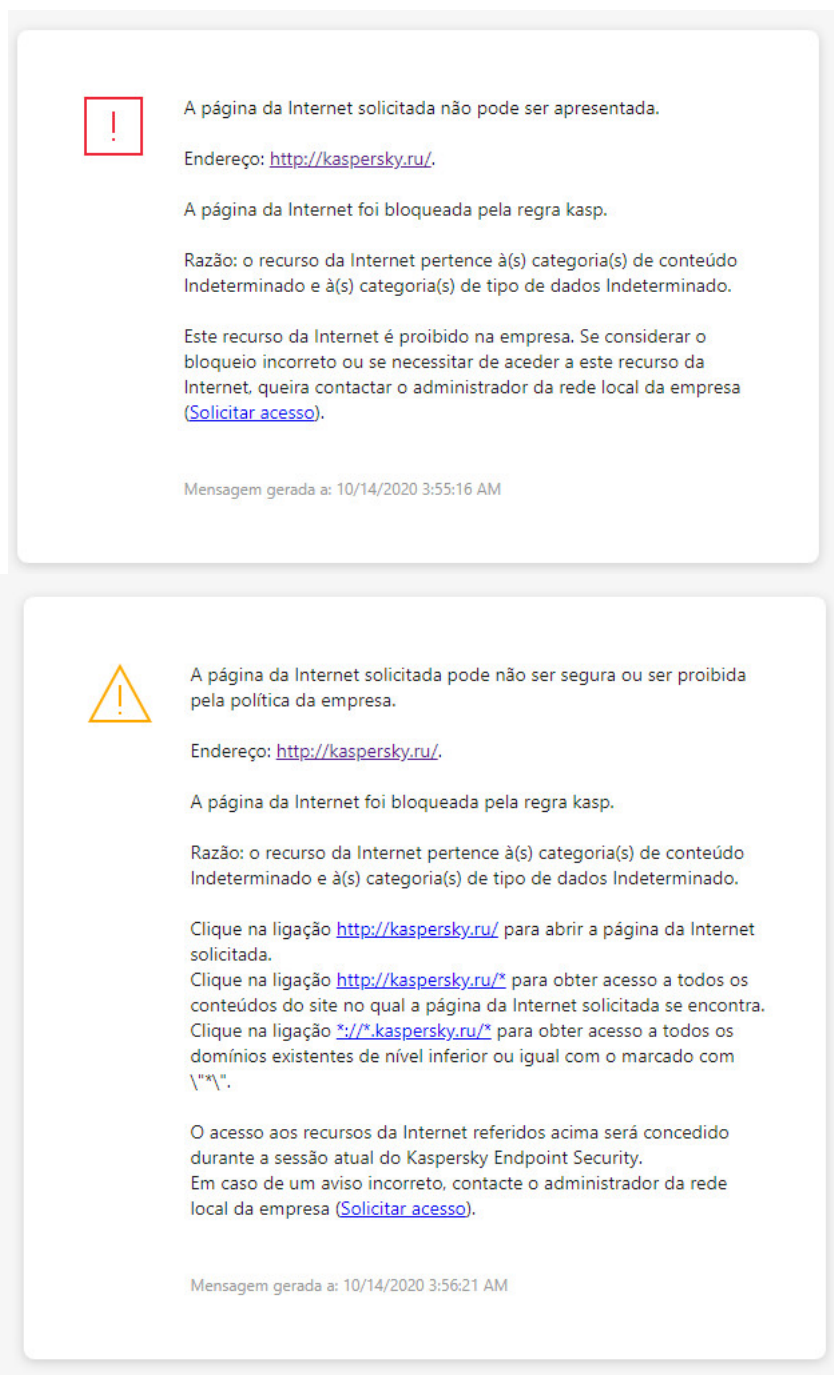
Regras de acesso a sites


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.



 A página da Internet solicitada não pode ser apresentada.


Endereço: <http://kaspersky.ru/>.

A página da Internet foi bloqueada pela regra kasp.

Razão: o recurso da Internet pertence à(s) categoria(s) de conteúdo Indeterminado e à(s) categoria(s) de tipo de dados Indeterminado.

Este recurso da Internet é proibido na empresa. Se considerar o bloqueio incorreto ou se necessitar de aceder a este recurso da Internet, queira contactar o administrador da rede local da empresa ([Solicitar acesso](#)).

Mensagem gerada a: 10/14/2020 3:55:16 AM

 A página da Internet solicitada pode não ser segura ou ser proibida pela política da empresa.

Endereço: <http://kaspersky.ru/>.

A página da Internet foi bloqueada pela regra kasp.

Razão: o recurso da Internet pertence à(s) categoria(s) de conteúdo Indeterminado e à(s) categoria(s) de tipo de dados Indeterminado.

Clique na ligação <http://kaspersky.ru/> para abrir a página da Internet solicitada.

Clique na ligação http://kaspersky.ru/* para obter acesso a todos os conteúdos do site no qual a página da Internet solicitada se encontra.

Clique na ligação */*.kaspersky.ru/* para obter acesso a todos os domínios existentes de nível inferior ou igual com o marcado com \".

O acesso aos recursos da Internet referidos acima será concedido durante a sessão atual do Kaspersky Endpoint Security.

Em caso de um aviso incorreto, contacte o administrador da rede local da empresa ([Solicitar acesso](#)).


Mensagem gerada a: 10/14/2020 3:56:21 AM

Mensagens do Controlo de Internet

Ativar e desativar o Controlo de Internet

Por predefinição, o Controlo de Internet está ativado.

Para ativar ou desativar o Controlo de Internet:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, seleccione **Controlos de segurança** → **Controlo de Internet**.
3. Use o botão de alternar **Controlo de Internet** para ativar ou desativar o componente.
4. Guarde as suas alterações.

Ações com regras de acesso a recursos da Internet

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 seleccionada, 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 seleccionadas, o Kaspersky Endpoint Security não controla o acesso a todos os recursos da Internet nas categorias de conteúdo e/ou tipo de dados seleccionadas. 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 em branco. Existem duas regras predefinidas:

- A regra Scripts e Folhas de Estilo que concede a todos os utilizadores acesso em qualquer altura a todos os recursos da Internet cujos endereços contenham os nomes de ficheiros com extensões CSS, JS ou VBS. Por exemplo: <http://www.example.com/style.css>, <http://www.example.com/style.css?mode=normal>.

- Regra 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.

Adicionar uma regra de acesso a recursos da Internet

Para adicionar ou editar uma regra de acesso a recursos da Internet:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, seleccione **Controlos de segurança** → **Controlo de Internet**.
3. No bloco **Definições**, clique no botão **Regras de acesso a recursos web**.
4. Na janela que é aberta, clique no botão **Adicionar**.
É apresentada a janela **Regra de acesso a recursos da Internet**.
5. No campo **Nome da regra**, introduza o nome da regra.
6. Seleccione o estado **Ativado** 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**, seleccione a opção relevante:
 - **Permitir**. Se este valor for seleccionado, o Kaspersky Endpoint Security permite o acesso a recursos da Internet que correspondem aos parâmetros da regra.
 - **Bloquear**. Se este valor for seleccionado, o Kaspersky Endpoint Security impede o acesso a recursos da Internet que correspondem aos parâmetros da regra.
 - **Aviso**. Se este valor estiver seleccionado, o Kaspersky Endpoint Security apresenta um aviso de que um recurso da Internet não é desejado quando o utilizador tenta aceder a recursos da Internet que correspondem à regra. Utilizando as ligações da mensagem de aviso, o utilizador pode obter acesso ao recurso da Internet solicitado.
8. No bloco **Conteúdo do filtro**, seleccione 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 a recursos da Internet com base no tipo específico dos dados publicados (por exemplo, *Imagens gráficas*).

Para configurar o filtro de conteúdos:

- a. Clique na ligação **Definições**.
- b. Seleccione as caixas de verificação junto dos nomes das categorias de conteúdo e/ou tipos de dados pretendidas.
Seleccionar 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 seleccionadas e/ou categorias de tipos de dados.
- c. Regresse à janela para configurar a regra de acesso a recursos da Internet.

9. No bloco **Endereços**, selecione o filtro de endereços de recursos da Internet relevante:

- **Para todos os endereços.** O Controlo de Internet não filtra recursos da Internet por endereço.
- **Para endereços individuais.** O Controlo de Internet filtra apenas os endereços de recursos da Internet da lista. Para criar uma lista de endereços de recursos da Internet:
 - a. Clique no botão **Adicionar endereço** ou **Adicionar um grupo de endereços**.
 - b. Na janela aberta, crie 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](#).
 - c. Regresse à janela para configurar a regra de acesso a recursos da Internet.

Se a [Verificação de ligações encriptadas estiver desativada](#), para o protocolo HTTPS só pode filtrar por nome do servidor.

10. 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.
- **Para utilizadores individuais e/ou grupos.** O Controlo de Internet filtra recursos da Internet apenas para utilizadores específicos. Para criar uma lista de utilizadores aos quais pretende aplicar a regra:
 - a. Clique no botão **Add**.
 - b. Na janela aberta, selecione os utilizadores ou o grupo 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.

11. 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 no botão **Editar ou adicionar novo**.
- b. Na janela que é aberta, clique no botão **Adicionar**.
- c. Na janela aberta, 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.

12. Guarde as suas alterações.

Atribuir prioridades a regras de acesso a recursos da Internet


Pode atribuir prioridades a cada regra a partir da lista de regras, ordenando as regras por uma determinada ordem.

Para atribuir uma prioridade a uma regra de acesso de recursos da Internet:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Controlos de segurança** → **Controlo de Internet**.
3. No bloco **Definições**, clique no botão **Regras de acesso a recursos web**.
4. Na janela aberta, selecione a regra cuja prioridade pretende alterar.
5. Utilize os botões **Para cima** e **Para baixo** para mover a regra para a posição relevante na lista de regras de acesso a recursos da Internet.
6. Guarde as suas alterações.

Ativar e desativar uma regra de acesso a recursos da Internet

Para ativar ou desativar uma regra de acesso a recursos da Internet:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Controlos de segurança** → **Controlo de Internet**.
3. No bloco **Definições**, clique no botão **Regras de acesso a recursos web**.
4. Na janela aberta, selecione a regra que pretende ativar ou desativar.
5. Na coluna **Estado**, execute a seguinte ação:
 - Se pretender ativar a utilização da regra, selecione o valor **On**.
 - Se pretender desativar a utilização da regra, selecione o valor **Off**.
6. Guarde as suas alterações.

Exportar e importar a lista de endereços Web fiáveis

Pode exportar a lista de regras de Controlo de Internet para um ficheiro XML. 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. 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, seleccione o separador **Policies**.
4. Seleccione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, seleccione **Controlos de Segurança** → **Controlo de Internet**.
6. Para exportar a lista de regras de Controlo de Internet:
 - a. Seleccione as regras que pretende exportar. Para seleccionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.
Se não tiver seleccionado nenhuma regra, o Kaspersky Endpoint Security exportará todas as regras.
 - b. Clique na ligação **Exportar**.
 - c. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de regras e seleccione 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 a lista de regras de Controlo de Internet:
 - a. Clique na ligação **Importar**.
Na janela que se abre, seleccione 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 Controlo de Internet na Consola Web e na Cloud Console](#) 

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Controlos de segurança** → **Controlo de Internet**.
5. Para exportar a lista de regras, no bloco **Rule List**:
 - a. Seleccione as regras que pretende exportar.
 - b. Clique no botão **Export**.
 - c. Confirme que deseja exportar apenas as regras seleccionadas 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.
6. Para importar a lista de regras, no bloco **Rule List**:
 - a. Clique na ligação **Importar**.
Na janela que se abre, seleccione 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.
7. Guarde as suas alterações.

Testar regras de acesso a recursos da Internet

Para verificar a consistência das regras de Controlo de Internet, pode testar as mesmas. Para este fim, o componente Controlo de Internet inclui uma função de Diagnósticos de regras.

Para testar as regras de acesso do recurso da Internet:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, seleccione **Controlos de segurança** → **Controlo de Internet**.
3. No bloco **Definições**, clique na ligação **Diagnósticos de regras**.
É aberta 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, seleccione a caixa de verificação **Especifique o endereço**. Introduza o endereço do recurso da Internet 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 no botão **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 a lista de endereços de recursos da 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 .txt. 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.

Para importar ou exportar uma lista de endereços de recursos da Internet para um ficheiro:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Controlos de segurança** → **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 no botão **Export**.
 - c. Na janela aberta, 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.
6. Para importar a lista de recursos da Internet, faça o seguinte no bloco **Endereços**:

a. Clique no botão **Importar**.

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.

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.


O Kaspersky Endpoint Security cria os seguintes eventos de atividade da Internet do utilizador:

- Bloquear o site (estado *Critical events* .
- Visita a um site não recomendado (*Avisos* estado .
- Visita a um site permitido (estado *Informational messages* .

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](#).

Para injetar um script de interação de página de Internet no tráfego de Internet:

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Definições gerais** → **Definições de rede**.
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](#).

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 **Definições de notificação**.

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>, and <http://www.example.com/gallery>, o Kaspersky Endpoint Security só enviará um evento com o objeto <http://www.example.com>.

Para ativar o registo de eventos para visitar sites permitidos:

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

2. Na janela Application settings, selecione **Controlos de segurança** → **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**.

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 **Aviso** 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, 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.

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. Pode modificar o conteúdo das mensagens.

Para alterar o modelo das mensagens de Controlo de Internet:

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Controlos de segurança** → **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.
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 `imagens`.
- `http://user.pictures.example.com`. A máscara de domínio `*.` representa `imagens` e `utilizador`.
- `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.

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.

Migrar as regras de acesso de recursos da Internet de versões anteriores da aplicação

Quando o Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou uma versão anterior da aplicação é atualizada para o Kaspersky Endpoint Security for Windows 11.8.0, as regras de acesso a recursos da Internet baseadas em categorias de conteúdo do recurso da Internet são migradas segundo os seguintes princípios:

- As regras de acesso a recursos da Internet baseadas numa ou várias categorias de conteúdo de recursos da Internet das listas «Conversas e fóruns», «Correio eletrónico baseado na Internet» e «Redes sociais» migram para a categoria de conteúdo de recursos da Internet «Comunicações de rede».
- As regras de acesso a recursos da Internet baseadas numa ou várias categorias de conteúdo de recursos da Internet das listas «Lojas online» e «Sistemas de pagamento» migram para a categoria de conteúdo de recursos da Internet «Lojas online, bancos, sistemas de pagamento».
- As regras de acesso a recursos da Internet baseadas na categoria de conteúdo de recursos da Internet «Jogos de apostas» migram para a categoria de conteúdo «Jogo, lotarias, apostas».
- As regras de acesso a recursos da Internet baseadas na categoria de conteúdo de recursos da Internet «Jogos de navegador» migram para a categoria de conteúdo «Jogos de computador».
- As regras de acesso a recursos da Internet baseadas em categorias de conteúdo que não estão enumeradas na lista acima são migradas sem alterações.

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.

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 – ⓧ.
- Depende do barramento de ligação (exceto para 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). Como tal, o utilizador pode restringir a ligação de todos os dispositivos, por exemplo, a 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 (ID do hardware ou HWID). Pode ver a ID nas propriedades de dispositivo utilizando ferramentas do sistema operativo. Exemplo de 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 ID do fornecedor (VID) e um ID do produto (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 carácter `*` substitui qualquer conjunto de caracteres. O Kaspersky Endpoint Security não suporta o carácter `?` 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 carácter `*` substitui qualquer conjunto de caracteres. O Kaspersky Endpoint Security não suporta o carácter `?` 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).



O acesso a <dispositivo> está bloqueado

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](#).

Ativar e desativar o Controlo de Dispositivos

Por predefinição, o Controlo de Dispositivos está ativado.

Para ativar e desativar o Controlo de Dispositivos:

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

2. Na janela de definições da aplicação, selecione **Controlos de segurança** → **Controlo de Dispositivos**.

3. Use o botão de alternar **Controlo de Dispositivos** para ativar ou desativar o componente.

4. Guarde as suas alterações.

Como resultado, 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** → **Storage** → **Hardware**.

Sobre as regras de acesso

As *regras de acesso* são um grupo de definições que determinam que utilizadores podem aceder aos dispositivos que são instalados ou ligados ao computador. 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	✓	✓	✓	✓	✓
Impressoras	✓	–	–	–	–
Disquetes	✓	✓	✓	✓	✓
Unidades de CD/DVD	✓	✓	✓	✓	✓
Modems	✓	–	–	–	–
Dispositivos de fita	✓	–	–	–	–
Dispositivos multifuncionais	✓	–	–	–	–
Leitores de smart card	✓	–	–	–	–
Dispositivos Windows CE USB ActiveSync	✓	–	–	–	–
Adaptadores de rede externos	✓	–	–	–	–
Dispositivos portáteis (MTP)	✓	✓	✓	✓	✓


Bluetooth	✓	–	–	–	–
Câmeras e scanners	✓	–	–	–	–

Regras de acesso para dispositivos móveis




Os dispositivos móveis com Android ou iOS são classificados como 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.

Tenha em atenção as seguintes considerações especiais sobre o acesso a dispositivos ADB ou iTunes:



- Não é possível configurar o horário de acesso a um dispositivo. Se o acesso aos dispositivos for restrito por regras (têm o estado ) , os dispositivos ADB e iTunes estão sempre acessíveis.
- Não é possível configurar o acesso ao dispositivo para utilizadores individuais, ou configurar permissões de acesso (leitura/gravação). Se o acesso aos dispositivos for restrito por regras (têm o estado ) , os dispositivos ADB e iTunes são acessíveis a todos os utilizadores com todas as permissões.
- Não é possível configurar o acesso a dispositivos ADB ou iTunes fiáveis para utilizadores individuais. Se o dispositivo for fiável, os dispositivos ADB e iTunes estarão acessíveis a todos os utilizadores.
- Se instalou as aplicações ADB ou iTunes após ligar um dispositivo ao computador, o ID exclusivo do dispositivo poderá ser repostado. 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.

Por defeito, estas regras de acesso concedem a todos os utilizadores acesso total aos dispositivos, em qualquer altura, caso o acesso aos barramentos de ligação para os tipos correspondentes de dispositivos seja permitido (o estado ) .

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

As regras de acesso a barramentos de ligação determinam se a ligação de dispositivos é permitida (o estado ) ou proibida (o estado ) . 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.

Editar uma regra de acesso a dispositivos

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.

Para editar uma regra de acesso a dispositivos:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, 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 dispositivos de armazenamento**, selecione a regra de acesso que pretende editar. O bloco contém dispositivos que possuem um sistema de ficheiros para o qual pode configurar definições de acesso adicionais. Por predefinição, uma regra de acesso a dispositivos atribui a todos os utilizadores acesso total ao tipo especificado de dispositivos em qualquer altura.

a. Na coluna **Acesso**, selecione a opção de acesso a dispositivos apropriada:

- **Permitir.**
- **Bloquear.**
- **Depende do barramento de ligação.**

Para bloquear ou permitir o acesso a um dispositivo, [configure o acesso ao barramento de ligação](#).

- **Restringir pelas regras.**

Esta opção permite configurar os direitos do utilizador, as permissões e um agendamento para o acesso a dispositivos.

b. No bloco **Direitos dos utilizadores**, clique no botão **Adicionar**.

Abre-se uma janela para adicionar uma nova regra de acesso a dispositivos.

c. Atribua uma prioridade à *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.

d. Selecione o estado **Ativado** para a regra de acesso a dispositivos.


e. Configure as permissões de acesso a dispositivos dos utilizadores: leitura e/ou gravação.

f. Selecione os utilizadores ou o grupo de utilizadores aos quais pretende aplicar a regra de acesso a dispositivos.

- g. Configure um agendamento de acesso a dispositivos para os utilizadores.
 - h. Clique no botão **Add**.
5. No bloco **Acesso a dispositivos externos**, selecione a regra e configure o acesso: **Permitir**, **Bloquear** ou **Depende do barramento de ligação**. Se necessário, [configure o acesso ao barramento de ligação](#).
 6. No bloco **Acesso a redes Wi-Fi**, clique na ligação **Wi-Fi** e configure o acesso: **Permitir**, **Bloquear** ou **Bloquear com exceções**. Se necessário, [adicione redes Wi-Fi à lista fiável](#).
 7. Guarde as suas alterações.

Editar uma regra de acesso a barramentos de ligação


Para editar uma regra de acesso a barramentos de ligação:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, 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**.
6. Guarde as suas alterações.

Adicionar uma rede Wi-Fi à lista fiável

Pode permitir que os utilizadores se liguem às redes Wi-Fi que considera seguras como, por exemplo, uma rede Wi-Fi empresarial. Para tal, tem de adicionar a rede à lista de redes Wi-Fi fiáveis. O Controlo de dispositivos irá bloquear o acesso a todas as redes Wi-Fi exceto às especificadas na lista fiável.

Para adicionar uma rede Wi-Fi à lista fiável:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, 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.

5. No bloco **Acesso**, selecione **Bloquear com exceções**.
6. No bloco **Redes Wi-Fi fiáveis**, clique no botão **Adicionar**.
7. Na janela aberta, execute uma das seguintes ações:
 - a. No campo de **Nome de rede**, especifique o nome da rede Wi-Fi que pretende adicionar à lista fiável.
 - b. Na lista pendente **Tipo de autenticação**, selecione o tipo da autenticação utilizado ao estabelecer ligação à rede Wi-Fi fiável.
 - c. Na lista pendente **Tipo de encriptação**, selecione o tipo da encriptação utilizado para assegurar o tráfego da rede Wi-Fi fiável.
 - d. No campo **Comentário**, pode especificar qualquer informação sobre a rede Wi-Fi adicionada.

Uma rede Wi-Fi considera-se fiável se as suas definições corresponderem a todas as definições especificadas na regra.

8. Guarde as suas alterações.


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 de *Informational messages*.

Para ativar o monitorização do uso de uma unidade amovível:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, 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 dispositivos de armazenamento**, selecione **Unidades amovíveis**.
5. Na janela aberta, selecione o separador **Registo**.
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 formatos 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 notificações](#) 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
- Veredicto de 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\environment]
- Para sistemas operativos de 32 bits:
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\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 1000 dispositivos de confiança, 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 de *Evento informativo*.

O Kaspersky Endpoint Security tem as seguintes limitações ao trabalhar com dispositivos fiáveis:


- O plug-in de administração do Kaspersky Endpoint Security das versões 11.0.0–11.2.0 não funciona com uma lista de dispositivos fiáveis que foi criada no Kaspersky Endpoint Security da versão 11.3.0 e 11.4.0. Para trabalhar com uma lista de dispositivos fiáveis dessas versões, o plug-in de administração tem de ser atualizado para as versão 11.3.0 e 11.4.0, respetivamente.
- O plug-in de administração do Kaspersky Endpoint Security da versão 11.3.0 e 11.4.0 não pode funcionar com uma lista de dispositivos fiáveis criada no Kaspersky Endpoint Security da versão 11.2.0 ou anterior. Para que essas versões funcionem com uma lista de dispositivos fiáveis, a aplicação tem de ser atualizada para a versão 11.3.0 e 11.4.0, respetivamente. Também pode enviar um pedido contendo uma descrição da sua situação para o Suporte Técnico através da [Kaspersky CompanyAccount](#).

- Para migrar uma lista de dispositivos fiáveis do Kaspersky Endpoint Security da versão 11.2.0 para a versão 11.3.0, envie um pedido contendo uma descrição da sua situação para o Suporte Técnico através da [Kaspersky CompanyAccount](#).

Adicionar um dispositivo à lista fiável a partir da interface da aplicação

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).

Para adicionar um dispositivo à lista fiável a partir da interface da aplicação:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, 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 no botão **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.
6. No campo **Comentário**, pode fornecer quaisquer informações relevantes sobre o dispositivo fiável.
7. Selecione os utilizadores ou o grupo de utilizadores para os quais pretende permitir o acesso a dispositivos fiáveis.
8. Guarde as suas alterações.

Adicionar um dispositivo à lista fiável do Kaspersky Security Center

O Kaspersky Security Center recebe informações sobre os dispositivos se o Kaspersky Endpoint Security estiver instalado nos computadores e o [Controlo de Dispositivos estiver ativado](#). Só é possível adicionar um dispositivo à lista fiável se as informações sobre esse dispositivo estiverem disponíveis no Kaspersky Security Center.

Pode adicionar um dispositivo à lista fiável de acordo com os seguintes dados:

- **Dispositivos por ID.** Cada dispositivo possui um identificador exclusivo (ID do hardware ou HWID). Pode ver a ID nas propriedades de dispositivo utilizando ferramentas do sistema operativo. Exemplo de 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 ID do fornecedor (VID) e um ID do produto (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 carácter `*` substitui qualquer conjunto de caracteres. O Kaspersky Endpoint Security não suporta o carácter `?` 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 carácter `*` substitui qualquer conjunto de caracteres. O Kaspersky Endpoint Security não suporta o carácter `?` ao introduzir uma máscara. Por exemplo, `VID_05AC & PID_*`.

Para adicionar dispositivos à lista de dispositivos fiáveis:

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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Controlos de Segurança** → **Controlo de Dispositivos**.
6. Na parte direita da janela, selecione o separador **Dispositivos fiáveis**.
7. 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.
8. Clique no botão **Adicionar** e selecione um método para adicionar um dispositivo à lista fiável.
9. Para filtrar dispositivos, selecione um tipo de dispositivo na lista pendente **Tipo de Dispositivo** (por exemplo, **Unidades amovíveis**).
10. 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 **Atualizar**. Para apresentar a lista de dispositivos corretamente, pode adicionar dispositivos por máscara de ID do dispositivo.

11. Para filtrar dispositivos, no campo **Nome do computador**, insira o nome do computador ou de uma máscara para o nome do computador ao qual o dispositivo está conectado.
O carácter `*` substitui qualquer conjunto de caracteres. O carácter `?` substitui qualquer carácter individual.
12. Clique no botão **Atualizar**.

A tabela apresenta uma lista de dispositivos que cumprem os critérios de filtragem definidos.

13. Selecione as caixas de verificação junto aos nomes dos dispositivos que pretende adicionar à lista fiável.
14. No campo **Comentário**, insira uma descrição do motivo da adição de dispositivos à lista fiável.
15. Clique no botão **Selecionar** à direita do campo **Permitir a utilizadores e / ou grupos de utilizadores**.
16. Selecione um utilizador ou um grupo no Active Directory e confirme a sua seleção.
Por predefinição, o acesso a dispositivos fiáveis é permitido para o grupo Todos.
17. 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 de definições da aplicação, 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 no botão **Export**.

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.

Se o computador já tiver uma lista de dispositivos fiáveis, o Kaspersky Endpoint Security irá solicitar a eliminação da lista existente ou a adição de novas entradas a tal lista a partir do ficheiro XML.

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.

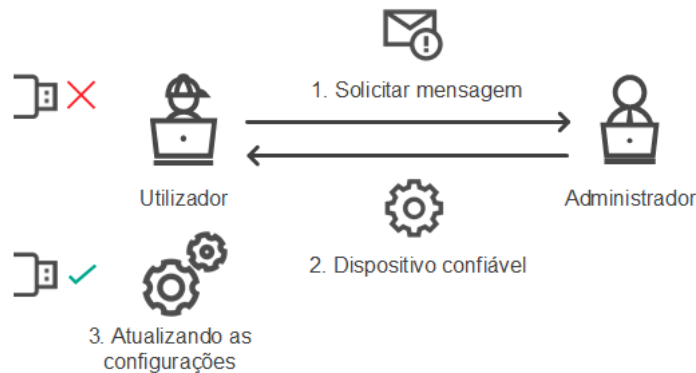
A concessão de acesso no modo online consiste nos seguintes passos:

1. O utilizador envia ao administrador uma mensagem com um pedido de acesso.

2. O administrador 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.

3. O administrador atualiza as definições do Kaspersky Endpoint Security no computador do utilizador.



Esquema para conceder acesso a um dispositivo no modo online

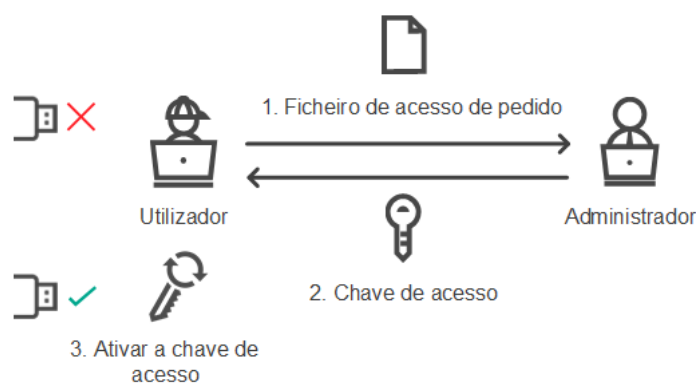
Modo offline para conceder acesso

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 pedido de acesso temporário** deve ser seleccionada.

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.

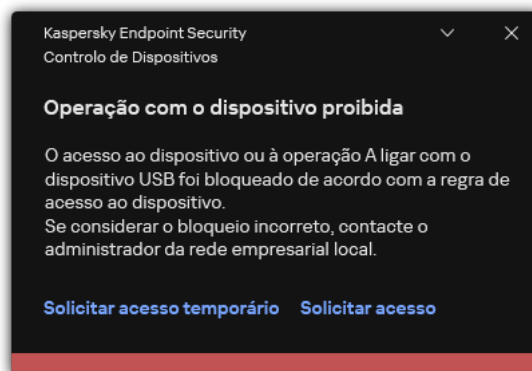
O Kaspersky Endpoint Security irá apresentar uma notificação a indicar que o acesso ao dispositivo está bloqueado (ver a figura abaixo).

2. Clique na ligação **Solicitar acesso**.

Esta ação abre uma janela com uma mensagem para o administrador. Esta mensagem contém informações sobre o dispositivo bloqueado.

3. Clique no botão **Enviar**.

O administrador irá receber uma mensagem contendo um pedido para fornecer acesso, por exemplo, por email. Para obter mais informações detalhadas sobre como processar os pedidos dos utilizadores, consulte a [Ajuda do Kaspersky Security Center](#). O utilizador receberá acesso ao dispositivo depois de [adicionar o dispositivo à lista fiável](#) e atualizar as configurações do Kaspersky Endpoint Security no computador.



Notificação de Controlo de Dispositivos

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 pedido de acesso temporário** deve ser selecionada.

Um utilizador solicita acesso a um dispositivo bloqueado da seguinte maneira:

1. Ligue o dispositivo ao computador.

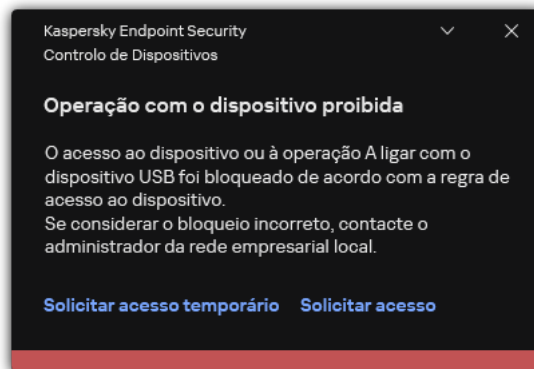
O Kaspersky Endpoint Security irá apresentar uma notificação a indicar que o acesso ao dispositivo está bloqueado (ver a figura abaixo).

2. Clique na hiperligação **Solicitar acesso temporário**.

Abre-se uma janela que contém uma lista dos dispositivos ligados.

3. Na lista de dispositivos ligados, seleccione 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. Na janela que abre, 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, seleccione **Devices** → **Managed devices**.
2. Na lista de computadores clientes, seleccione 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, seleccione a secção **Device Control**.
5. Clique no botão **Browse** 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, seleccione **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, seleccione 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. 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.

Estão disponíveis modelos para mensagens sobre acesso bloqueado a dispositivos ou operações proibidas com conteúdos do dispositivo, e para a mensagem enviada ao administrador. Pode modificar os modelos de mensagem.

Editar os modelos para mensagens de Controlo de Dispositivos:

1. Na janela principal da aplicação, clique no botão .
2. Na janela Application settings, selecione **Controlos de segurança** → **Controlo de Dispositivos**.
3. No bloco **Modelos de mensagem**, configure os modelos para mensagens de Controlo de Dispositivos:
 - **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.
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 de definições da aplicação, 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 de definições da aplicação, 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 de definições da aplicação, 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 apenas para o Kaspersky Endpoint Security for Business Advanced e para o Kaspersky Total Security for Business. Para obter mais informações sobre o Kaspersky Endpoint Security for Business, visite o [site da Kaspersky](#).

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 do *Início do Microsoft PowerShell a partir de uma aplicação do escritório*). 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 de regras](#) e no repositório do **Triggering of rules in Smart Training state**.

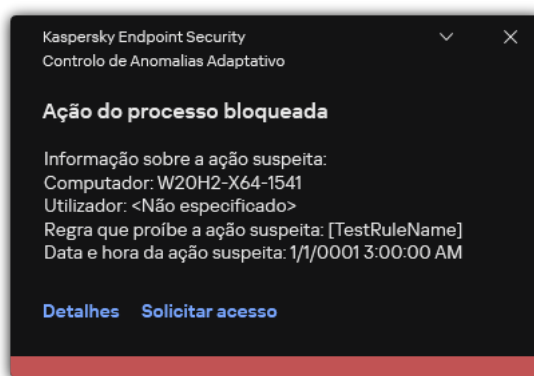
2. A analisar o relatório de acionamento de regras.

O administrador analisa o [relatório de acionamento de regras](#) ou o conteúdo do repositório do **Triggering of rules 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. O Controlo de Anomalias Adaptativo é configurado 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 **Triggering of rules in Smart Training state**.
Recomenda-se a verificação do relatório de acionamento de regras e o conteúdo do repositório de **Triggering of rules in Smart Training state**.

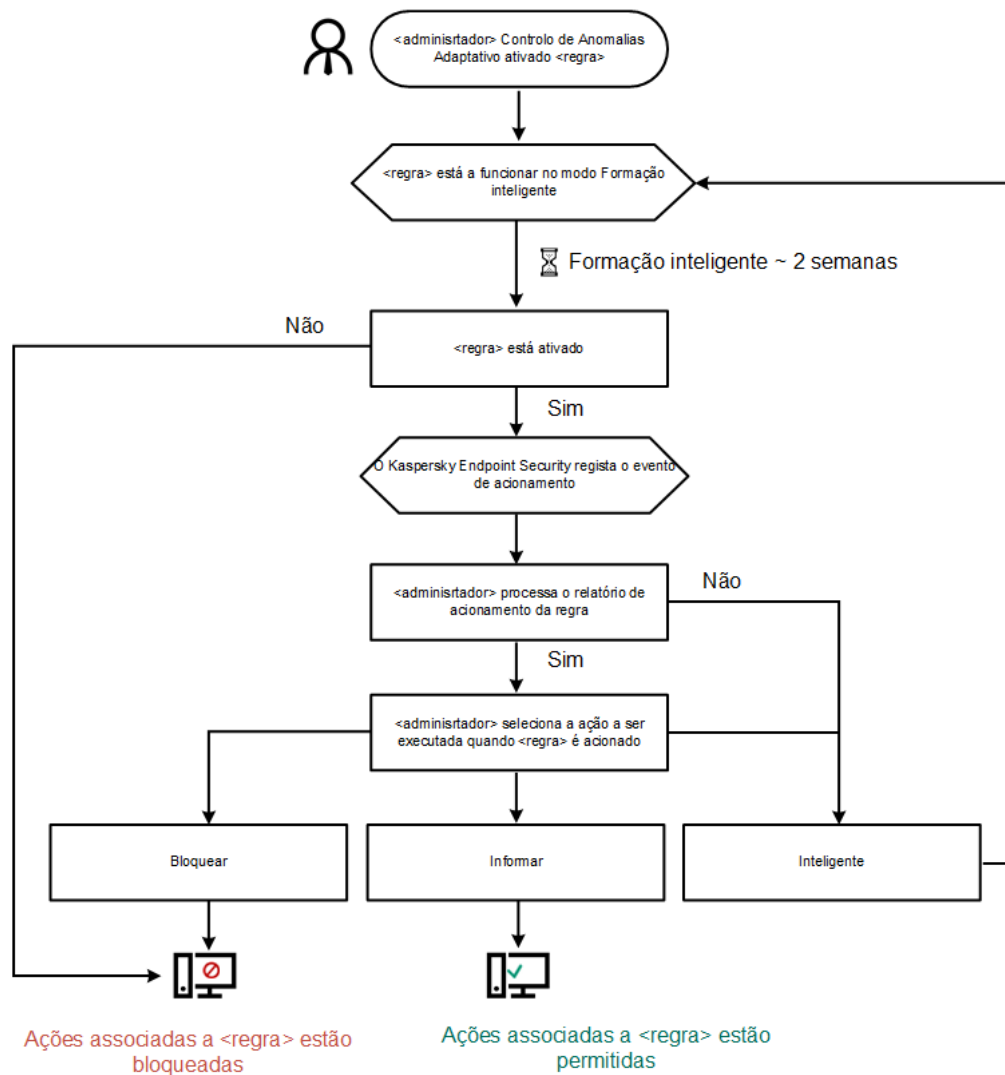
Quando uma aplicação maliciosa tentar realizar uma ação, o Kaspersky Endpoint Security irá bloquear a ação e exibir uma notificação (ver figura abaixo).



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

Ativar e desativar o Controlo de Anomalias Adaptativo

O Controlo de Anomalias Adaptativo está ativado como predefinição.

Para ativar ou desativar o Controlo das 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. Use o botão de alternar da **Controlo de Anomalias Adaptativo** para ativar ou desativar o componente.
4. Guarde as suas alterações.

Como resultado, o Controlo de Anomalias Adaptativo irá mudar para o modo de formação. Durante a formação, o Controlo de Anomalias Adaptativo monitoriza o acionamento de regras. Terminada a formação, o Controlo de Anomalias Adaptativo começa a bloquear as ações que são atípicas dos computadores na rede de uma empresa.

Se a sua organização começou a usar algumas ferramentas novas e o Controlo de Anomalias Adaptativo bloqueia as ações destas ferramentas, pode redefinir os resultados do modo de formação e repetir a mesma. Para o fazer, precisa de [alterar a ação que é executada quando a regra é acionada](#) (por exemplo, defina-a como **Notificar**). Depois precisa de reativar o modo de formação (defina o valor **Inteligente**).


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 de definições da aplicação, 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 de aplicações de escritório*) e expanda o conjunto.
5. Selecione uma regra (por exemplo, *Iniciar o Windows PowerShell de aplicações de escritório*).
6. Use o botão de alternar na coluna **Estado** 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 de definições da aplicação, 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 no botão **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 **Triggering of rules 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.
- **Notificar.** 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 de definições da aplicação, seleccione **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. Seleccione uma regra na tabela.
5. Clique no botão **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. Seleccione o utilizador para o qual pretende configurar uma exclusão.

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. Defina 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.** Código de hash 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.** Código de hash 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.** Código de hash do ficheiro.
- **Objeto de destino.** O comando para iniciar o processo alvo. Especifique o comando usando o seguinte padrão object://<comando>, 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.** Código de hash 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 de definições da aplicação, 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 no botão **Export**.

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 regras:

a. Clique no 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.

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 de definições da aplicação, 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 é aberta, 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.

Encontram-se disponíveis modelos especiais para a mensagem sobre o bloqueio de mensagens potencialmente perigosas e para a mensagem ser enviada ao administrador. Pode modificar os modelos de mensagem.

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.
4. Guarde as suas alterações.

Visualizar relatórios de Controlo Adaptativo de Anomalia

Para ver os relatórios do Controlo de Anomalias Adaptativo:

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

5. Na janela de política, selecione **Controlos de Segurança** → **Controlo de Anomalias Adaptativo**.

As definições do componente de Controlo de Anomalias Adaptativo são apresentadas na parte direita da janela.

6. Execute uma das ações seguintes:

- Se quiser visualizar um relatório sobre as definições das regras de Controlo de Anomalia Adaptativo, clique em **Reportar o estado das regras do Controlo de anomalias adaptativo**.
- Se quiser visualizar um relatório sobre a ativação das regras do Controlo de Anomalia Adaptativo, clique no botão **Reportar as regras acionadas do Controlo de anomalias adaptativo**.

7. O processo de criação do relatório é iniciado.

O relatório é apresentado numa nova janela.

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.

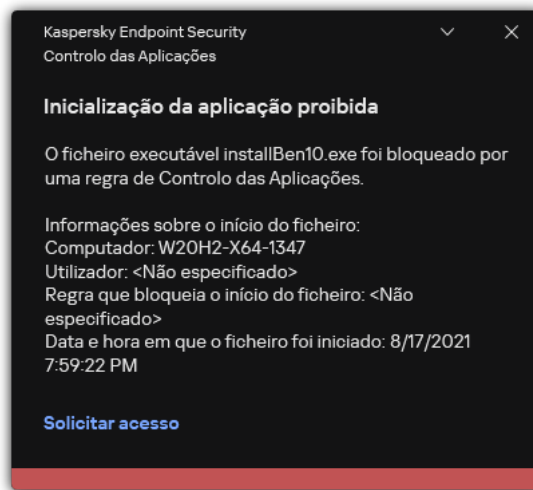
3. [Selecionar o modo de Controlo das Aplicações](#).

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.

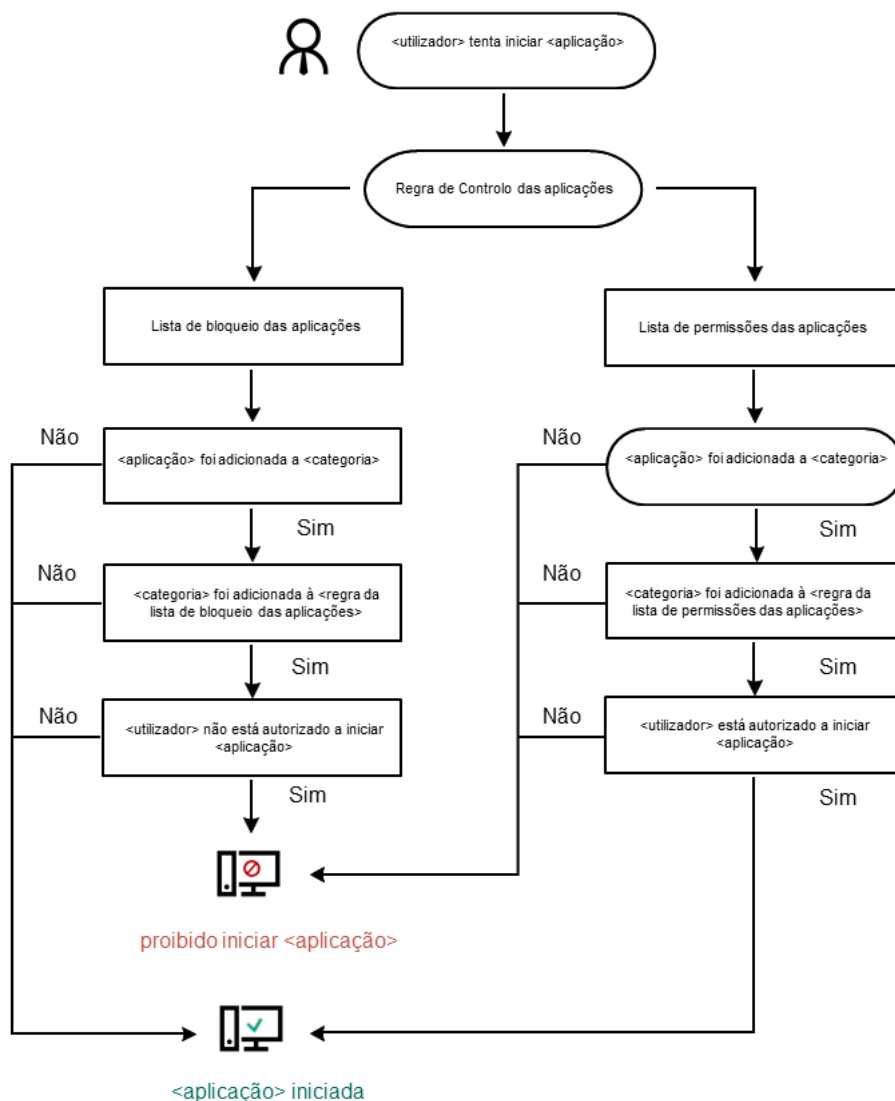
Contudo, o Kaspersky Security Center fornece ferramentas que não estão disponíveis na interface local do Kaspersky Endpoint Security, como por exemplo, as ferramentas necessárias para as tarefas seguintes:

- [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.
- Quando a versão da aplicação é atualizada, a importação das definições do componente Controlo das Aplicações só é suportada se o Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou posterior for atualizado para Kaspersky Endpoint Security 11.8.0 for Windows.

Quando forem atualizadas outras versões que não o Kaspersky Endpoint Security 10 Service Pack 2 for Windows, as definições do Controlo das Aplicações têm de ser novamente configuradas para restaurar o estado operacional deste componente.

- 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 **Other applications**\Aplicações fiáveis de acordo com a reputação na 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.

Ativar e desativar o Controlo das Aplicações

Por predefinição, o Controlo das Aplicações está ativado.

Para ativar ou desativar o Controlo das Aplicações:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Controlos de segurança** → **Controlo das Aplicações**.
3. Use o botão de alternar **Controlo das Aplicações** para ativar ou desativar o componente.
4. Guarde as suas alterações.

Como resultado, se o Controlo das Aplicações estiver ativado, a aplicação encaminha informações sobre a execução de ficheiros executáveis para o Kaspersky Security Center. Pode ver a lista de ficheiros executáveis em execução no Kaspersky Security Center na pasta **Ficheiros executáveis**. Para receber informações sobre todos os ficheiros executáveis em vez de apenas sobre os ficheiros executáveis em execução, execute a tarefa [Inventário](#).

Selecionar o modo de Controlo das Aplicações

Para selecionar o modo de Controlo das Aplicações:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Controlos de segurança** → **Controlo das Aplicações**.

3. No bloco **Modo de controlo do arranque da aplicação**, selecione uma das seguintes 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.

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 à Categoria 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.

Todas as regras criadas durante o modo selecionado são guardadas depois de o modo ser alterado para que as regras possam ser usadas novamente. Para voltar a usar essas regras, tudo que precisa de fazer é selecionar o modo necessário.

4. Na secção **Ação no arranque das aplicações bloqueadas**, selecione a ação a executar pelo componente quando um utilizador tenta iniciar uma aplicação bloqueada pelas Regras de Controlo das Aplicações.

5. Selecione a caixa de verificação **Controlar a carga dos módulos DLL** se pretender que o Kaspersky Endpoint Security monitorize o carregamento de módulos DLL quando as aplicações são iniciadas pelos utilizadores.

A informação sobre o módulo e a aplicação que carregou o módulo será guardada num relatório.

O Kaspersky Endpoint Security só monitoriza os módulos DLL e os controladores carregados desde a seleção da caixa de verificação. Reinicie o computador após selecionar a caixa de verificação se quiser que o Kaspersky Endpoint Security monitorize todos os módulos DLL e controladores, incluindo os que foram carregados antes de o Kaspersky Endpoint Security ser iniciado.

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 "Certificados fiáveis", 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.

É recomendada a ativação da [proteção por password](#) para configurar as definições da aplicação, para que seja possível desativar os módulos DLL críticos e controladores desde o início, sem modificar as definições da política do Kaspersky Security Center.

6. Guarde as suas alterações.

Trabalhar com regras de controlo das aplicações na interface da aplicação

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 componente 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:

- **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 o arranque das aplicações às quais são aplicáveis as regras, mas regista informações sobre o arranque de tais aplicações no relatório.

Adicionar uma Regra de Controlo das Aplicações

Para adicionar uma Regra de Controlo das Aplicações:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, seleccione **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 no botão **Add**.
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. Compile ou edite uma lista de utilizadores e/ou grupos de utilizadores que tenham ou não permissão para iniciar aplicações que cumpram as condições de ativação de regras. Para tal, clique no botão **Adicionar** na tabela **Sujeitos e os seus direitos**.

Por predefinição, o valor **Todos** é adicionado à lista de utilizadores. A regra é aplicável a todos os utilizadores.

Se não existir utilizador especificado na tabela, a regra não pode ser guardada.


- d. Na tabela **Sujeitos 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 programas que satisfaçam as condições de ativação de regras para todos os utilizadores que não estejam listados na tabela **Sujeitos e os seus direitos** e não sejam membros de grupos de utilizadores listados na tabela **Sujeitos 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 **Sujeitos e os seus direitos** e que não pertencem aos grupos de utilizadores especificados na tabela **Sujeitos e os seus direitos**.

- f. Se pretender que o Kaspersky Endpoint Security considere as aplicações correspondentes às condições de ativação de regras enquanto atualizadores fiáveis com permissão para criar outros ficheiros executáveis que terão permissão para serem subsequentemente executados, selecione a caixa de verificação **Atualizadores fiáveis**.
6. No separador **Condições**, [crie](#) ou edite a lista de condições de inclusão para ativar a regra.
7. No separador **Exclusões**, 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.

Adicionar uma condição de ativação para uma Regra de Controlo das aplicações

Para adicionar uma nova condição de ativação para uma Regra de Controlo das aplicações:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, 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** ou **Exclusões** 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 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 **Assunto** 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**.

Alterar o estado de uma Regra de Controlo das aplicações

Para alterar o estado de uma Regra de Controlo das aplicações:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, 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:
 - **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 esta regra, mas regista informações sobre o arranque de tais aplicações no relatório.
5. Guarde as suas alterações.

Gerir Regras de Controlo das Aplicações no Kaspersky Security Center

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 componente 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:

- **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 o arranque das aplicações às quais são aplicáveis as regras, mas regista informações sobre o arranque de tais aplicações no relatório.

Receber informações sobre as aplicações instaladas nos computadores dos utilizadores

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.

As informações sobre as aplicações utilizadas nos computadores da rede local empresarial estão disponíveis na pasta **Applications registry** e na pasta **Ficheiros executáveis**. A pasta **Aplicações do registo** e a pasta **Ficheiros executáveis** estão localizadas na pasta **Gestão da aplicação** na árvore da Consola de Administração do Kaspersky Security Center.

A pasta **Aplicações do registo** contém a lista de aplicações detetadas pelo [Agente de Rede](#) instalado no computador cliente.

A pasta **Ficheiros executáveis** contém uma lista de todos os ficheiros executáveis que já foram iniciados em computadores cliente ou detetados durante a tarefa de inventário do Kaspersky Endpoint Security.

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 **Registo das aplicações** ou na pasta **Ficheiros executáveis**.

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, seleccione **Additional** → **Application management** → **Applications registry**.
3. Seleccione uma aplicação.
4. No menu de contexto da aplicação, seleccione **Properties**.

Para abrir a janela de propriedades de um ficheiro executável na pasta Ficheiros executáveis:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da Consola de Administração, seleccione a pasta **Additional** → **Application management** → **Executable files**.
3. Seleccione um ficheiro executável.
4. No menu de contexto do ficheiro executável, seleccione **Properties**.

Criar categorias de 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:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da Consola de Administração, seleccione a pasta **Adicional** → **Gestão de aplicações** → **Categorias da aplicação**.
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 categorias de utilizador.

Passo 1. Selecionar o tipo de categoria

Neste passo, seleccione um dos seguintes tipos de categorias da aplicação:

- **Category with content added manually.** Se tiver selecionado este tipo de categoria, no passo “Configurar as condições para a inclusão de aplicações numa categoria” e no passo “Configurar as condições para a exclusão de aplicações de uma categoria” poderá definir as categorias onde os ficheiros executáveis serão incluídos na categoria criada.
- **Categoria que inclui ficheiros executáveis de dispositivos selecionados.** Se tiver selecionado este tipo de categoria, no passo “Definições” poderá especificar um computador cujos ficheiros executáveis serão automaticamente incluídos na categoria.
- **Category that includes executable files from a specific folder.** Se tiver selecionado este tipo de categoria, no passo “Pasta de repositórios”, 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

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 thumbprint** 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 “aplicações do Office” inclui as aplicações do conjunto de programas do Microsoft Office, Adobe Acrobat e outros.
Pode seleccionar categorias KL para gerar uma lista ampliada de aplicações fiáveis.
- **Specify path to application.** 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 thumbprint** especificado.

- **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 seleccionado 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 “aplicações do Office” inclui as aplicações do conjunto de programas do Microsoft Office, Adobe Acrobat e outros.
Pode seleccionar categorias KL para gerar uma lista ampliada de aplicações fiáveis.
- **Specify path to application.** 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 seleccionado o tipo de **Categoria que inclui ficheiros executáveis de dispositivos seleccionados**.

Neste passo, clique no botão **Adicionar** 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 **Ficheiros executáveis** serão adicionados à categoria da aplicação pelo Kaspersky Security Center.

Neste passo, também pode configurar as seguintes definições:

- Algoritmo para o cálculo da função de hash por parte do Kaspersky Security Center. Para seleccionar um algoritmo, tem de seleccionar, pelo menos, uma das seguintes caixas de verificação:
 - **Calculate SHA-256 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).**
- 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 **Ficheiros executáveis**.

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.

- Campo **Scan period (h).** Neste campo, pode especificar o período de tempo (em horas) após o qual o Kaspersky Security Center limpa a categoria de aplicações e lhe adiciona ficheiros executáveis dos

computadores especificados apresentados na pasta **Ficheiros executáveis**.

O campo fica disponível se a caixa de verificação **Synchronize data with Administration Server repository** for selecionada.

Passo 6. Pasta do repositório

Esta passo fica disponível se tiver selecionado o tipo de **Category that includes executable files from a specific folder**.

Neste passo, clique no botão **Procurar** e 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:

- 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.

- 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 o cálculo da função de hash por parte do Kaspersky Security Center. Para selecionar um algoritmo, tem de selecionar, pelo menos, uma das seguintes caixas de verificação:
 - **Calculate SHA-256 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)**.
- 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.
- Campo **Scan period (h)**. 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.

Este campo fica disponível se a caixa de verificação **Force folder scan for changes** for selecionada.

Passo 7. Criar uma categoria personalizada

Sair do Assistente.

Adicionar ficheiros executáveis da pasta de Ficheiros executáveis à categoria de aplicações

Na pasta **Ficheiros executáveis** 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 de Ficheiros executáveis à categoria de aplicações:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da Consola de Administração, seleccione a pasta **Additional** → **Application management** → **Executable files**.
3. Na área de trabalho, seleccione 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 seleccione **Add to category**.
5. Na janela aberta, execute uma das seguintes ações:
 - 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 seleccionar uma categoria de aplicações existente e adicionar-lhe ficheiros executáveis.
 - No bloco **Rule type**, seleccione uma das seguintes opções:
 - **Rules for adding to inclusions**. Seleccione esta opção se quiser criar uma condição que adiciona ficheiros executáveis à categoria de aplicações.
 - **Rules for adding to exclusions**. Seleccione esta opção se quiser criar uma condição que exclui ficheiros executáveis da categoria de aplicações.
 - No bloco **Parameter used as a condition**, seleccione 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)**.
 - **Apenas MD5 (modo descontinuado, apenas para Kaspersky Endpoint Security 10 Service Pack 1)**.
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, seleccione 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. Clique no botão **Run selection**.
5. Seleccione 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 seleccionados e seleccione **Add to category**.
7. Na janela aberta, 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 seleccionar uma categoria de aplicações existente e adicionar-lhe ficheiros executáveis.
 - No bloco **Rule type**, seleccione uma das seguintes opções:
 - **Rules for adding to inclusions**. Seleccione esta opção se quiser criar uma condição que adiciona ficheiros executáveis à categoria de aplicações.
 - **Rules for adding to exclusions**. Seleccione esta opção se quiser criar uma condição que exclui ficheiros executáveis da categoria de aplicações.
 - No bloco **Parameter used as a condition**, seleccione 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)**.
 - **Apenas MD5 (modo descontinuado, apenas para Kaspersky Endpoint Security 10 Service Pack 1)**.
8. Guarde as suas alterações.

Adicionar e modificar uma Regra de Controlo das aplicações utilizando o Kaspersky Security Center

Para adicionar ou modificar uma regra de Controlo das Aplicações utilizando o Kaspersky Security Center:

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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. 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.
6. Execute uma das ações seguintes:

- Para adicionar uma regra, clique no botão **Adicionar**.
- Se quiser editar uma regra existente, selecione-a na lista de regras e clique no botão **Editar**.

A janela **Regra de Controlo das Aplicações** é apresentada.

7. Execute uma das ações seguintes:
 - Se pretende criar uma nova categoria:
 - a. Clique no botão **Criar categoria**.
O assistente de criação de categorias de utilizador é iniciado.
 - b. Siga as instruções apresentadas no assistente de criação de categorias de utilizador.
 - 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 no botão **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.
8. Na tabela **Sujeitos e os seus direitos**, clique no botão **Adicionar**.
9. Na janela aberta, especifique a lista de utilizadores e/ou grupos de utilizadores para a qual pretende configurar a permissão para iniciar aplicações a partir da categoria selecionada.
10. Na tabela **Sujeitos 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 **Deny** nas linhas relevantes.

11. Selecione a caixa de verificação **Recusar para outros utilizadores** se pretender que todos os utilizadores que não são apresentados na coluna **Subject** e que não façam parte do grupo de utilizadores especificado na coluna **Subject** sejam impedidos de iniciar aplicações que pertençam à categoria selecionada.
12. 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.

13. 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:

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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. 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.

6. 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 Controlo de Aplicações está em funcionamento.
- **Desativado**. Este estado significa que a regra será ignorada quando o Controlo de Aplicações está em funcionamento.
- **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.

7. 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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Controlos de segurança** → **Controlo das Aplicações**.
6. Para exportar a lista de regras de Controlo das Aplicações:
 - a. Selecione as regras que pretende exportar. Para seleccionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.

Se não tiver seleccionado nenhuma regra, o Kaspersky Endpoint Security exportará todas as regras.
 - b. Clique na ligação **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 exportar uma lista das regras de Controlo das Aplicações:
 - a. Clique na ligação **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 Controlo das Aplicações na Consola Web e na Cloud Console](#)

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Controlos de segurança** → **Controlo das Aplicações**.
5. Clique na ligação **Rules Lists Settings**.
6. Seleccione uma lista de regras: lista de bloqueio ou de permissão de aplicações.
7. Para exportar a lista de regras de Controlo das Aplicações:
 - a. Seleccione as regras que pretende exportar.
 - b. Clique no botão **Export**.
 - c. Confirme que deseja exportar apenas as regras seleccionadas 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.
8. Para exportar uma lista das regras de Controlo das Aplicações:
 - a. Clique na ligação **Importar**.
Na janela que se abre, seleccione 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.
9. Guarde as suas alterações.

Testar Regras de Controlo das Aplicações utilizando o Kaspersky Security Center

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.

Para ativar ou desativar os testes das Regras de Controlo das Aplicações no Kaspersky Security Center:

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, seleccione o separador **Policies**.
4. Seleccione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, seleccione **Controlos de segurança** → **Controlo das Aplicações**.
Na parte direita da janela, são apresentadas as definições do componente Controlo das Aplicações.
6. Na lista pendente **Modo de Controlo**, seleccione um dos seguintes itens:
 - **Lista de bloqueio**. Se esta opção estiver seleccionada, 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 seleccionada, 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.
7. Execute uma das ações seguintes:
 - Para ativar os testes das Regras de Controlo das Aplicações, seleccione 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, seleccione **Aplicar regras**.
8. Guarde as suas alterações.

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, seleccione o separador **Events**.
3. Clique no botão **Create a selection**.
4. Na janela que surgir, aceda à secção **Eventos**.
5. Clique no botão **Clear all**.

6. Na tabela **Eventos**, 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. Clique no botão **Run selection**.

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 no botão **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 **Outro** → **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 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. Clique no botão **Create a selection**.
4. Na janela que surgir, aceda à secção **Eventos**.
5. Clique no botão **Clear all**.
6. Na tabela **Eventos**, 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. Clique no 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 no botão **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 **Outro** → **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.

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.

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 de definições da aplicação, 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 **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.

Monitor de atividade das aplicações

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 no mosaico **Monitor de atividade das aplicações**.

Abre-se a janela **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 para 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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Definições gerais** → **Interface**.
6. Utilize a caixa de verificação **Secção Ocultar Monitor de Atividade das Aplicações** para conceder ou revogar o acesso à ferramenta.
7. 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 **Devices** → **Policies & Profiles**.
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 **Definições gerais** → **Interface**.
5. Utilize a caixa de verificação **Secção Ocultar Monitor de Atividade das Aplicações** 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 caracteres comuns.

Pode utilizar os seguintes caracteres 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 caracteres.

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. 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.

Estão disponíveis modelos especiais para a mensagem que é apresentada quando o arranque de uma aplicação é bloqueado e para a mensagem enviada ao administrador. Pode modificar os modelos de mensagem.

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 das Aplicações**.
3. No bloco **Modelos**, 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.
 - **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.
4. Guarde as suas alterações.

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 seleccionar 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 pasta Aplicação 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 pasta Aplicação 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 seleccionados.** 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 [Ficheiros executáveis](#).

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 à Categoria 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 **Assunto** 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 "Pasta da aplicação" e especifique o caminho para a pasta. Em seguida, crie uma regra de permissão e selecione esta categoria.

A utilização da pasta Aplicação 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 pasta Aplicação 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 o funcionamento do Kaspersky Endpoint Security, os componentes [Controlo de Internet](#), [Proteção contra ameaças de correio](#) e [Proteção contra ameaças da Web](#) 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.


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 de definições da aplicação, selecione **Definições gerais** → **Definições de rede**.
3. Na secção **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 de definições da aplicação, selecione **Definições gerais** → **Definições de rede**.
3. Na secção **Portas monitorizadas**, selecione **Monitorizar apenas as portas seleccionadas**.
4. Clique no botão **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 no botão **Add**.
 - b. Na janela que se abre, introduza o número da porta de rede e uma breve descrição.
 - c. Defina o estado **Ativado** ou **Inativado** 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 de definições da aplicação, selecione **Definições gerais** → **Definições de rede**.
3. Na secção **Portas monitorizadas**, selecione **Monitorizar apenas as portas seleccionadas**.
4. Selecione a caixa de verificação **Monitorizar todas as portas para as aplicações da lista recomendada pela Kaspersky**.

Se a caixa de verificação estiver seleccionada, o Kaspersky Endpoint Security monitoriza todas as portas para as seguintes aplicações:

- Adobe 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 no botão **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 no botão **Add**.
 - b. Na janela que se abre, introduza o caminho para o ficheiro executável da aplicação e uma breve descrição.

c. Defina o estado **Ativado** ou **Inativado** 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. 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, seleccione o separador **Policies**.
4. Seleccione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, seleccione **Definições gerais** → **Definições de rede**.
6. Na secção **Portas monitorizadas**, seleccione **Monitorizar apenas as portas seleccionadas**.
7. Clique no botão **Definições**.

É aberta 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.

8. Para exportar a lista de portas de rede:
 - a. Na lista de portas de rede, seleccione as portas que pretende exportar. Para seleccionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.

Se não tiver seleccionado nenhuma porta, o Kaspersky Endpoint Security exportará todas as portas.
 - b. Clique no botão **Export**.
 - c. Na janela aberta, introduza o nome do ficheiro XML para o qual pretende exportar a lista de portas de rede e seleccione a pasta onde pretende guardar este ficheiro.
 - d. Guardar o ficheiro.

O Kaspersky Endpoint Security exporta toda a lista de portas de rede para o ficheiro XML.
9. Para exportar a lista de aplicações cujas portas são monitorizadas pelo Kaspersky Endpoint Security:
 - a. Seleccione a caixa de verificação **Monitorizar todas as portas das aplicações especificadas**.
 - b. Na lista de aplicações, seleccione as aplicações que pretende exportar. Para seleccionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.

Se não tiver seleccionado nenhuma aplicação, o Kaspersky Endpoint Security exportará todas as aplicações.
 - c. Clique no botão **Export**.
 - d. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de aplicações e seleccione 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.
10. 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.

11. 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 aberta, 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.

12. Guarde as suas alterações.

[Como exportar/importar listas de portas monitorizadas na Consola Web e na Cloud Console](#) 

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Definições gerais** → **Definições da rede**.
5. Para exportar a lista de portas de rede:
 - a. Na secção **Portas monitorizadas**, seleccione **Monitorizar apenas as portas seleccionadas**.
 - b. Clique no link das **portas N seleccionadas**.
É aberta 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.
 - c. Na lista de portas de rede, seleccione as portas que pretende exportar.
 - d. Clique no botão **Export**.
 - e. Na janela aberta, introduza o nome do ficheiro XML para o qual pretende exportar a lista de portas de rede e seleccione a pasta onde pretende guardar este ficheiro.
 - 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. Na secção **Portas monitorizadas**, seleccione a caixa de verificação **Monitorizar todas as portas das aplicações especificadas**.
 - b. Clique no link das **aplicações N seleccionadas**.
 - c. Na lista de aplicações, seleccione as aplicações que pretende exportar.
 - d. Clique no botão **Export**.
 - e. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de aplicações e seleccione 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 **Importar**.
Na janela que se abre, seleccione 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 **Importar**.

Na janela aberta, 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.

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 usar a conta KLAdmin.

- 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.

Quando um utilizador tenta executar uma ação protegida por password, o Kaspersky Endpoint Security solicita ao utilizador o nome de utilizador e a password ou 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.

Kaspersky X

Tem a certeza de que pretende alterar as definições?

Nome de utilizador:

Valor predeterminado do nome de utilizador: KLAdmin.

Introduzir password:

Não pedir confirmação nos próximos:

Para trocar o idioma de entrada, carregue nas teclas ALT+SHIF **ENU**

Pedido de password de acesso do Kaspersky Endpoint Security

Utilizador e password

Para aceder ao Kaspersky Endpoint Security, deve inserir as suas credenciais de conta de domínio. A proteção por password suporta as seguintes contas:

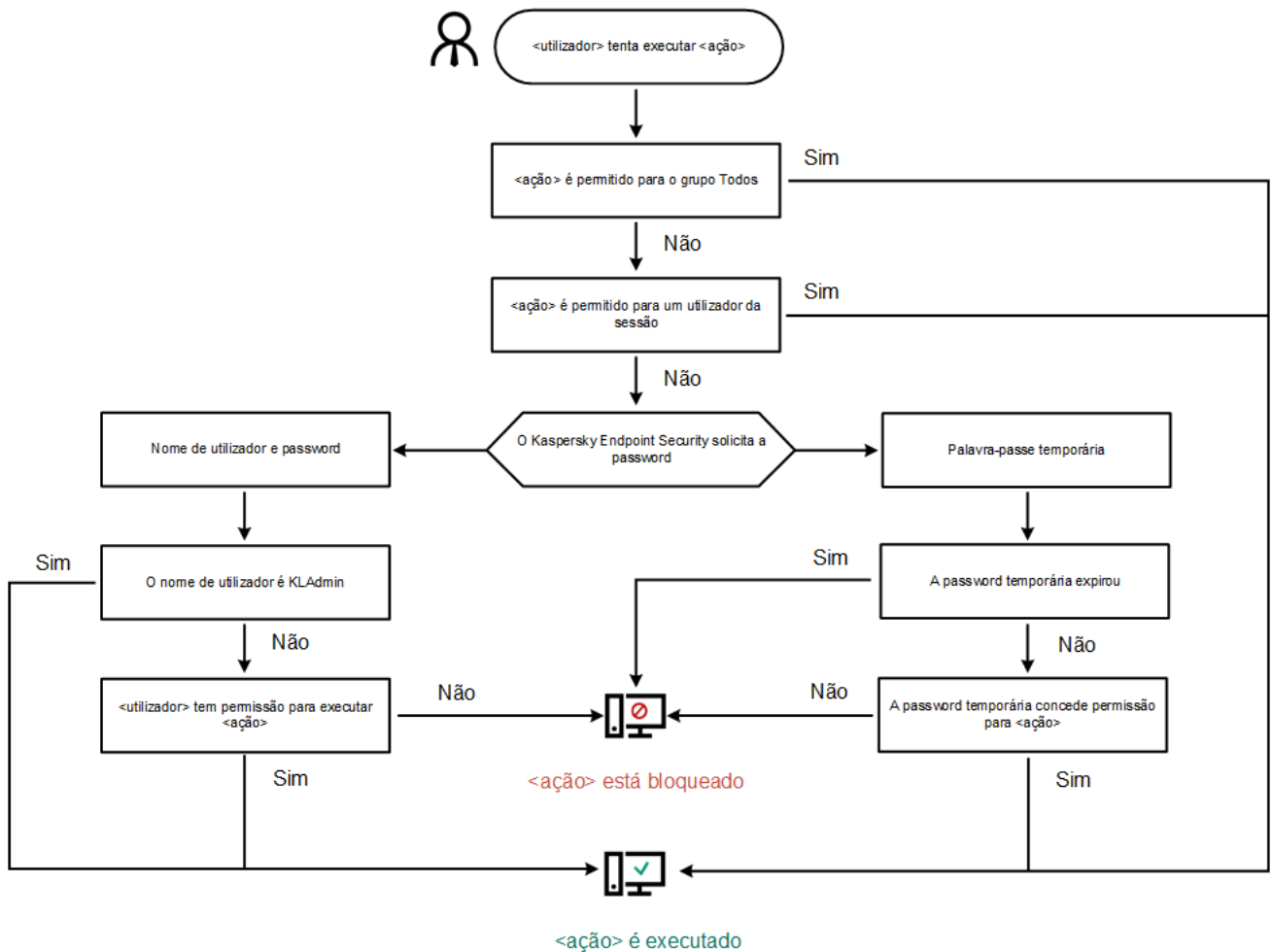
- **KLAdmin.** Uma conta de administrador com acesso sem restrições ao Kaspersky Endpoint Security. A conta KLAdmin tem o direito de executar qualquer ação protegida por password. As permissões para a conta KLAdmin não podem ser revogadas. Quando ativa a proteção por password, o Kaspersky Endpoint Security solicita que defina uma password para a conta do KLAdmin.
- **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.

Palavra-passe 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.

Algoritmo operacional de proteção por password

O Kaspersky Endpoint Security decide se permite ou bloqueia uma ação protegida por password com base no seguinte algoritmo (veja a figura abaixo).




Algoritmo operacional de proteção por password

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).

Para ativar a proteção por password:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Definições gerais** → **Interface**.
3. Use o botão de alternar **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 [aspectos 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

Pode conceder acesso ao Kaspersky Endpoint Security a utilizadores ou grupos individuais. 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](#).

Para conceder permissões a utilizadores ou grupos individuais:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Definições gerais** → **Interface**.
3. Na tabela de contas, clique em **Adicionar**.
4. Na janela que é aberta, clique no botão **Selecionar utilizador ou grupo**.
A caixa de diálogo padrão Selecionar utilizadores ou grupos é aberta.
5. Selecione um utilizador ou um grupo no Active Directory e confirme a sua seleção.

6. 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 palavra-passe.

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 [aspectos a considerar](#). Certifique-se de que todas as condições para aceder ao Kaspersky Endpoint Security são cumpridas.

7. 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

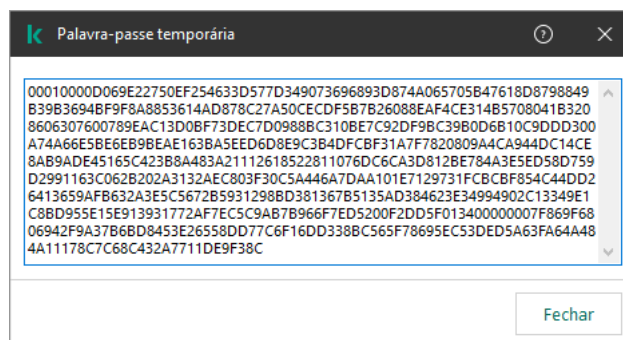
Uma password temporária pode ser usada para conceder acesso temporário ao Kaspersky Endpoint Security para um computador individual fora da rede corporativa. Isso é necessário para permitir que o utilizador execute uma ação bloqueada sem obter as credenciais da conta do KLAdmin. Para usar uma password 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 **Aplicações**.
6. Na lista de aplicações da Kaspersky instaladas no computador, selecione **Kaspersky Endpoint Security for Windows** e clique duas vezes para abrir as propriedades da aplicação.
Na janela de definições da aplicação, selecione **Definições gerais** → **Interface**.
7. No bloco **Proteção de password**, clique no botão **Definições**.
8. No bloco **Password temporária**, clique no botão **Definições**.
9. A janela **Criar password temporária** abre-se.
10. No campo **Expiration date**, especifique a data de expiração em que a password temporária expirará.
11. 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.
12. Clique em **Gerar**.
Abre-se uma janela contendo a password temporária (veja a figura abaixo).
13. 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 **Devices** → **Managed devices**.
2. Clique no nome do computador no qual pretende permitir que um utilizador execute uma ação bloqueada.
3. Selecione o separador **Aplicações**.
4. Clique em **Kaspersky Endpoint Security for Windows**.
As definições da aplicação locais são apresentadas.
5. Selecione o separador **Application settings**.
6. Na janela de definições da aplicação, selecione **Definições gerais** → **Interface**.
7. No bloco **Proteção de password**, clique no botão **Password temporária**.
8. No campo **Expiration date**, 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.




Palavra-passe temporária

Aspetos especiais de permissões de proteção por password

As permissões de proteção por password têm alguns aspetos e limitações importantes a ter em consideração.


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 KAdmin 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 KAdmin 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 KAdmin 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 permitido 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 a dados em unidades encriptadas

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.

Visualizar relatórios

Não há considerações ou limitações especiais.

Restaurar da cópia de segurança

Não há considerações ou limitações especiais.

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.

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. Embora não tenham funções maliciosas, estas aplicações podem ser exploradas por intrusos. Para mais informações sobre software legal que pode ser utilizado por criminosos para danificar o computador ou os dados pessoais dos utilizadores, visite o [website da Kaspersky IT Encyclopedia](#).

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](#).
- [Tarefas de verificação](#).

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 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Definições gerais** → **Exclusões**.
6. Na secção **Analisar exclusões e aplicações fiáveis**, clique no botão **Configuração**.
7. Na janela aberta, selecione o separador **Exclusões de verificação**.
Abre-se uma janela que contém uma lista de exclusões.
8. 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.
9. Selecione a caixa de verificação **Permitir a utilização de aplicações fiáveis 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. Se tiver sido gerada uma lista local, depois de esta funcionalidade ser desativada, o Kaspersky Endpoint Security continua a excluir os ficheiros listados das verificações.
10. Clique no botão **Add**.
11. Para excluir um ficheiro ou pasta da verificação:
 - a. Na secção **Propriedades**, selecione a caixa de verificação **Ficheiro ou pasta**.
 - b. Clique na ligação **Selecionar ficheiro ou pasta** na secção **Descrição da exclusão de verificação (clique nos itens sublinhados para editá-los)** para abrir a janela **Nome do ficheiro ou pasta**.
 - c. 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:\Pasta***.txt** incluirá todos os caminhos para ficheiros com a extensão TXT encontrados

nas pastas designadas **Pasta** e nas suas subpastas. 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 caracteres.

d. Guarde as suas alterações.

12. Para excluir objetos com um nome específico da verificação:

a. Na secção **Propriedades**, selecione a caixa de verificação **Nome do objeto**.

b. Clique na ligação **introduza o nome do objeto** na secção **Descrição da exclusão de verificação (clique nos itens sublinhados para editá-los)** para abrir a janela **Nome do objeto**.

c. 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 carácter **?** (substitui qualquer carácter único) e o carácter ***** (substitui qualquer número de caracteres). Por exemplo, se a máscara do **Cliente*** for especificada, o Kaspersky Endpoint Security exclui os objetos **Client-IRC**, **Client-P2P** e **Client-SMTP** das verificações.

d. Guarde as suas alterações.

13. Se quiser eliminar um ficheiro individual das verificações:

a. Na secção **Propriedades**, selecione a caixa de verificação **Hash do objeto**.

b. Clique na ligação de entrada do hash do objeto para abrir a janela **Hash do objeto**.

c. 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.

d. Guarde as suas alterações.

14. Se necessário, no campo **Comentário**, introduza um breve comentário na exclusão de verificação que está a criar.

15. Especifique os componentes do Kaspersky Endpoint Security que devem utilizar a exclusão de verificação:

a. Clique na ligação **qualquer** na secção **Descrição da exclusão de verificação (clique nos itens sublinhados para editá-los)** para ativar a ligação **selecionar componentes**.

b. Clique na ligação **selecionar componentes** para abrir a janela **Componentes de proteção**.

c. Selecione as caixas de verificação à frente dos componentes aos quais a exclusão de verificação deve ser aplicada.

d. Guarde as suas alterações.

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.

16. Pode usar a caixa de verificação para [parar uma exclusão](#) a qualquer momento.
17. Guarde as suas alterações.

[Como criar uma exclusão de verificação na Consola Web e na Cloud Console](#) 

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Definições gerais** → **Exclusões**.
5. No bloco **Analisar exclusões e aplicações fiáveis**, clique na ligação **Exclusões de verificação**.
6. Seleccione 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. Seleccione a caixa de verificação **Permitir a utilização de aplicações fiáveis 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. Se tiver sido gerada uma lista local, depois de esta funcionalidade ser desativada, o Kaspersky Endpoint Security continua a excluir os ficheiros listados das verificações.
8. Clique no botão **Add**.
9. Seleccione como pretende adicionar a exclusão: **Ficheiro ou pasta**, **Nome do objeto** ou **Hash do objeto**.
10. Se quiser excluir um ficheiro ou uma pasta das verificações, seleccione o ficheiro ou a pasta clicando no botão **Procurar**.

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:\Pasta***.txt incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas designadas Pasta e nas suas subpastas. 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 caracteres.

11. Se quiser excluir um tipo específico de objeto das verificações, no campo **Objeto**, 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 carácter `?` (substitui qualquer carácter único) e o carácter `*` (substitui qualquer número de caracteres). Por exemplo, se a máscara do `Cliente*` 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 **Hash do ficheiro**.

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 **Componentes de proteção**, selecione os componentes aos quais pretende que a exclusão de verificação se aplique.

14. Se necessário, no campo **Comentário**, introduza um breve comentário na exclusão de verificação que está a criar.

15. Pode usar o botão de alternar para [parar uma exclusão](#) a qualquer momento.

16. 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 de definições da aplicação, selecione **Definições gerais** → **Ameaças e Exclusões**.
3. No bloco **Exclusões**, clique na ligação **Gerir exclusões**.
4. Clique no botão **Add**.
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 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:\Pasta***.txt incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas designadas Pasta e nas suas subpastas. 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 caracteres.
6. Se quiser excluir um tipo específico de objeto das verificações, no campo **Objeto**, 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 carácter ? (substitui qualquer carácter único) e o carácter * (substitui qualquer número de caracteres). Por exemplo, se a máscara do **Cliente*** 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 ficheiro**.
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 **Ativado** para a exclusão.
Pode usar o botão de alternar para [parar uma exclusão](#) a qualquer momento.
11. Guarde as suas alterações.

Exemplos de máscara de caminho:

Caminhos para ficheiros localizados em qualquer pasta:

- A máscara `*.exe` inclui todos os caminhos para ficheiros com a extensão exe.
- O exemplo `*.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\, mas não nas subpastas de C:\dir\.
- 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*.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\teste` inclui todos os caminhos para ficheiros denominados "teste" localizados na pasta C:\dir\, mas não nas subpastas de C:\dir\.
- A máscara `C:\dir*\teste` inclui todos os caminhos em ficheiros denominados "teste" localizados na pasta C:\dir\ e nas subpastas de C:\dir\.

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\teste` inclui todos os caminhos para ficheiros denominados "teste" nas pastas denominadas "dir", mas não nas subpastas dessas pastas.

Ativar e desativar a exclusão de verificação


Para ativar ou desativar uma exclusão de verificação:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Definições gerais** → **Ameaças e Exclusões**.
3. No bloco **Exclusões**, clique na ligação **Gerir exclusões**.

4. Selecione a exclusão necessária na lista de exclusões de verificação.
5. Utilize o botão de alternar junto de um objeto para o incluir ou excluir no âmbito de verificação.
6. Guarde as suas alterações.

Selecionar tipos de objetos detetáveis

Para seleccionar tipos de objetos detetáveis:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Definições gerais** → **Ameaças e Exclusões**.
3. Na secção **Tipos de objetos detetados**, selecione as caixas de verificação em frente aos tipos de objetos que pretende que o Kaspersky Endpoint Security detete:

- [Vírus e worms](#) 

Subcategoria: vírus e worms (Viruses_and_Worms)

Nível de ameaça: alto

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 de *substituição* 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 *parasitas* modificam ficheiros, deixando-os total ou parcialmente funcionais. Os *vírus de companhia* 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: *vírus de ligação*, *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	Nome	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 salas de conversação (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 contêm 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: <ul style="list-style-type: none"> • 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 contêm 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 \(incluindo ransomware\)](#),^[2]

Subcategoria: Trojans

Nível de ameaça: alto

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	Nome	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: <ul style="list-style-type: none">• 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-	Trojans de	Estes acedem à página da Internet a partir do computador do

Clicker	comandos	<p>utilizador, enviando comandos para um navegador ou alterando os endereços da Internet especificados nos ficheiros do sistema operativo.</p> <p>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).</p>
Trojan-Downloader	Trojans de transferências	<p>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.</p>
Trojan-Dropper	Trojans instaladores	<p>Estes contêm outros Trojans que instalam no disco rígido.</p> <p>Os intrusos podem utilizar programas do tipo Trojan Dropper com os objetivos seguintes:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>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.</p>
Trojan-Proxy	Trojans proxies	<p>Permitem ao intruso aceder a páginas de Internet de forma anónima, utilizando o computador do utilizador e são muitas vezes utilizados para enviar spam.</p>
Trojan-PSW	Software de roubo de passwords	<p>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.</p> <p>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).</p>
Trojan-Spy	Trojans espiões	<p>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,</p>

		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.
Processo oculto (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: meio

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	Nome	Descrição
Constructor	Construtores	Permitem criar novos vírus, worms e Trojans. Alguns construtores apresentam uma interface padrão baseada em janelas, na qual o utilizador pode seleccionar 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).
Exploração de vulnerabilidades	Exploração de vulnerabilidades	<p>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".</p> <p>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.</p> <p>Os worms de rede (Net-Worms) disseminam-se nas redes através da exploração de vulnerabilidades. <i>O exploit Nuker</i> é constituído por pacotes de rede que desativam os computadores.</p>
FileCryptor	Encriptadores	Estes encriptam outras aplicações maliciosas, para os ocultarem das aplicações antivírus.
Flooder	Programas para "contaminar"	Estes enviam um elevado número de mensagens através de canais de rede. Este tipo de ferramentas inclui, por

	redes	<p>exemplo, programas que contaminam canais de salas de conversação (IRC).</p> <p>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).</p>
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 intercepção de passwords. Os programas farejadores são programas que permitem visualizar o tráfego de rede.
Programas de engodo (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.
Spoofers	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 ameaça: 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 criminosos para danificar o computador ou os dados pessoais do utilizador.

Nível de perigo: meio

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	Nome	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.
Dialer	Auto-dialers	Estes conseguem estabelecer ligações telefónicas através de um modem, de forma oculta.
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	<p>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.</p> <p>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.</p>
Server-FTP	Servidores 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 de 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 de 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 de 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 rede	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	Clientes de rede peer-to-peer (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 ferramentas para 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.

- [Detetar outro software que pode ser utilizado por intrusos para danificar o seu computador ou dados pessoais](#) 

Subcategoria: software legal que pode ser utilizado por criminosos para danificar o computador ou os dados pessoais do utilizador.

Nível de perigo: meio

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	Nome	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.
Dialer	Auto-dialers	Estes conseguem estabelecer ligações telefónicas através de um modem, de forma oculta.
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	<p>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.</p> <p>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.</p>
Server-FTP	Servidores 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 de 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 de 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 de 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 rede	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	Clientes de rede peer-to-peer (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 ferramentas para 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 desinfectam qualquer ameaça.

- **Objetos comprimidos, cuja compactação pode ser utilizada para proteger um código malicioso** 

O Kaspersky Endpoint Security verifica objetos comprimidos e o módulo de descompressão com arquivos SFX (extração automática).

Para ocultar programas perigosos das aplicações antivírus, os intrusos arquivam os mesmos utilizando Ficheiros comprimidos especiais ou criando ficheiros multi-comprimidos.

Os analistas de vírus da Kaspersky identificaram os Ficheiros comprimidos mais populares entre os hackers.

Se o Kaspersky Endpoint Security detetar algum desses utilitários de compressão num ficheiro, o mais provável é que esse ficheiro contenha uma aplicação maliciosa ou um aplicação que pode ser utilizado por criminosos para danificar o computador ou os dados pessoais do utilizador.

O Kaspersky Endpoint Security isola os tipos de programas seguintes:

- *Ficheiros comprimidos que podem provocar danos* – utilizados para comprimir software malicioso, como vírus, worms, e Trojans.
- *Ficheiros multi-comprimidos* (nível de ameaça médio) – o objeto foi comprimido três vezes, por um ou mais ficheiros de compressão.

- **Objetos multicomprimidos** 

O Kaspersky Endpoint Security verifica objetos comprimidos e o módulo de descompressão com arquivos SFX (extração automática).

Para ocultar programas perigosos das aplicações antivírus, os intrusos arquivam os mesmos utilizando Ficheiros comprimidos especiais ou criando ficheiros multi-comprimidos.

Os analistas de vírus da Kaspersky identificaram os Ficheiros comprimidos mais populares entre os hackers.

Se o Kaspersky Endpoint Security detetar algum desses utilitários de compressão num ficheiro, o mais provável é que esse ficheiro contenha uma aplicação maliciosa ou um aplicação que pode ser utilizado por criminosos para danificar o computador ou os dados pessoais do utilizador.

O Kaspersky Endpoint Security isola os tipos de programas seguintes:

- *Ficheiros comprimidos que podem provocar danos* – utilizados para comprimir software malicioso, como vírus, worms, e Trojans.
- *Ficheiros multi-comprimidos* (nível de ameaça médio) – o objeto foi comprimido três vezes, por um ou mais ficheiros de compressão.

4. Guarde as suas alterações.

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 verifica 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. Contudo, uma aplicação que tenha sido adicionada à lista de aplicações fiáveis fica excluída das verificações pelo Kaspersky Endpoint Security.

Por exemplo, se considerar como seguros, sem verificação, 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. Deste modo, a verificação ignora objetos utilizados por esta aplicação.

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.

A exclusão de aplicações fiáveis da verificação permite evitar conflitos de compatibilidade entre o Kaspersky Endpoint Security e outros programas (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), bem como aumentar o desempenho do computador, o que é fundamental ao utilizar aplicações de servidor.

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 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
 5. Na janela de política, selecione **Definições gerais** → **Exclusões**.
 6. Na secção **Analisar exclusões e aplicações fiáveis**, clique no botão **Configuração**.
 7. Na janela aberta, selecione o separador **Aplicações fiáveis**.
Abre-se uma janela que contém a lista das aplicações fiáveis.
 8. 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.
 9. 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. Se tiver sido gerada uma lista local, depois de esta funcionalidade ser desativada, o Kaspersky Endpoint Security continua a excluir as aplicações fiáveis listadas das verificações.
 10. Clique no botão **Add**.
 11. Na janela aberta, introduza 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 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.
12. Configure as definições avançadas para a aplicação fiável (consulte a tabela abaixo).
 13. Pode usar a caixa de verificação para [excluir uma aplicação da zona fiável](#) a qualquer momento.
 14. Guarde as suas alterações.


1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Definições gerais** → **Exclusões**.
5. No bloco **Analisar exclusões e aplicações fiáveis**, clique na ligação **Aplicações fiáveis**.
Abre-se uma janela que contém a lista das aplicações fiáveis.
6. Seleccione 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. Seleccione 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. Se tiver sido gerada uma lista local, depois de esta funcionalidade ser desativada, o Kaspersky Endpoint Security continua a excluir as aplicações fiáveis listadas das verificações.
8. Clique no botão **Add**.
9. Na janela aberta, introduza 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 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. Pode usar a caixa de verificação para [excluir uma aplicação da zona fiável](#) a qualquer momento.
12. 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 de definições da aplicação, selecione **Definições gerais** → **Ameaças e Exclusões**.
3. No bloco **Exclusões**, clique na ligação **Especificar aplicações fiáveis**.
4. Na janela que é aberta, clique no botão **Adicionar**.
5. Selecione o ficheiro executável da aplicação fiável.

Também pode introduzir o caminho manualmente. O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres `*` e `?` ao inserir uma máscara.

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 fiável, configure as definições avançadas (consulte a tabela abaixo).
7. Pode usar o botão de alternar para [excluir uma aplicação da zona fiável](#) a qualquer momento.
8. Guarde as suas alterações.


Definições da aplicação fiável

Parâmetro	Descrição
Não verificar ficheiros antes de abrir	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. A atividade da aplicação é monitorizada pelos seguintes componentes: Deteção de comportamento , Prevenção de explorações , Prevenção contra invasões , Motor de remediação e Firewall .
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 de subaplicação	O Kaspersky Endpoint Security não monitorizará a atividade de ficheiros ou de rede de aplicações iniciadas por esta aplicação.
Permitir	A Autodefesa do Kaspersky Endpoint Security bloqueia todas as tentativas de gerir

interação com a interface da aplicação	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.
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: <ul style="list-style-type: none"> • O estado Ativado significa que a aplicação está na zona fiável. • O estado Inativado significa que a aplicação foi excluída da zona fiável.

Ativar e desativar as regras da zona fiável para uma aplicação da lista de aplicações fiáveis

Ativar ou desativar a ação de regras da zona fiável para uma aplicação da lista de aplicações fiáveis:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Definições gerais** → **Ameaças e Exclusões**.
3. No bloco **Exclusões**, clique na ligação **Especificar aplicações fiáveis**.
4. Na lista de aplicações fiáveis, selecione a aplicação fiável pretendida.
5. Use o botão de alternar na coluna **Estado** para incluir ou excluir uma aplicação fiável do âmbito de verificação.
6. Guarde as suas alterações.

Utilizar o armazenamento de certificados de sistema 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*.

Para começar a utilizar o armazenamento de certificados de sistema fiáveis:

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

2. Na janela de definições da aplicação, selecione **Definições gerais** → **Ameaças e Exclusões**.
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.

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 desinfectado 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\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 desinfectado, 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, seleccione **Definições gerais** → **Relatórios e Armazenamento**.
3. Se quiser limitar o período de armazenamento para cópias de ficheiros em Cópia de Segurança, seleccione a caixa de verificação **Armazenar objetos no máximo durante 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, selecione **Definições gerais** → **Relatórios e Armazenamento**.
3. Se quiser limitar o tamanho da Cópia de Segurança, selecione a caixa de verificação **Limitar o tamanho da Cópia de Segurança a N MB** no bloco **Cópia de Segurança**. Especifique o tamanho máximo da Cópia de Segurança.
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 *Infetado*, coloca uma cópia em Cópia de segurança e tenta desinfetá-lo. Se a desinfecção 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 desinfetado quando o computador for reiniciado* não podem ser restaurados. Reinicie o computador e o estado do ficheiro muda para *Desinfetado* 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 Microsoft Windows 8 (consulte os *ficheiros de ajuda do Microsoft Windows 8* 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.

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, seleccione os ficheiros que deseja eliminar da Cópia de Segurança e clique em **Eliminar**.

O Kaspersky Endpoint Security elimina as cópias de segurança seleccionadas dos ficheiros da 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 de definições da aplicação, selecione **Definições gerais** → **Interface**.
3. No bloco **Notificações**, clique no botão **Definições de notificação**.

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 seleccionadas 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** seleccionada são apresentados em Registos do Windows no canal Aplicação.
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 de definições da aplicação, selecione **Definições gerais** → **Interface**.
3. No bloco **Notificações**, clique no botão **Definições de notificação**.

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 o componente ou tarefa seleccionados.

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 seleccionados 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 seleccionados 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 no botão **Definições de 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 de definições da aplicação, selecione **Definições gerais** → **Interface**.
3. Na secção **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\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 da **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:


 **Informational messages**. 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.


 **Critical events**. 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**.

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 apresentada uma secção 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, selecione **Definições gerais** → **Relatórios e Armazenamento**.


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, selecione **Definições gerais** → **Relatórios e Armazenamento**.
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**.
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, selecione **Definições gerais** → **Relatórios e Armazenamento**.
3. No bloco **Relatórios**, clique no botão **Limpar**.
4. Se a [Proteção por palavra-passe 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).


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: <ul style="list-style-type: none">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 ² . 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 aplicações de administração remota (por exemplo, TeamViewer ou RemotelyAnywhere) obtenham acesso ao Kaspersky Endpoint Security.	✓	– (exceto para o Windows 7)

Ativar e desativar a Autodefesa

O mecanismo de Autodefesa do Kaspersky Endpoint Security está ativado por predefinição.

Para ativar ou desativar a Autodefesa:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Definições gerais** → **Definições da aplicação**.
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.

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.

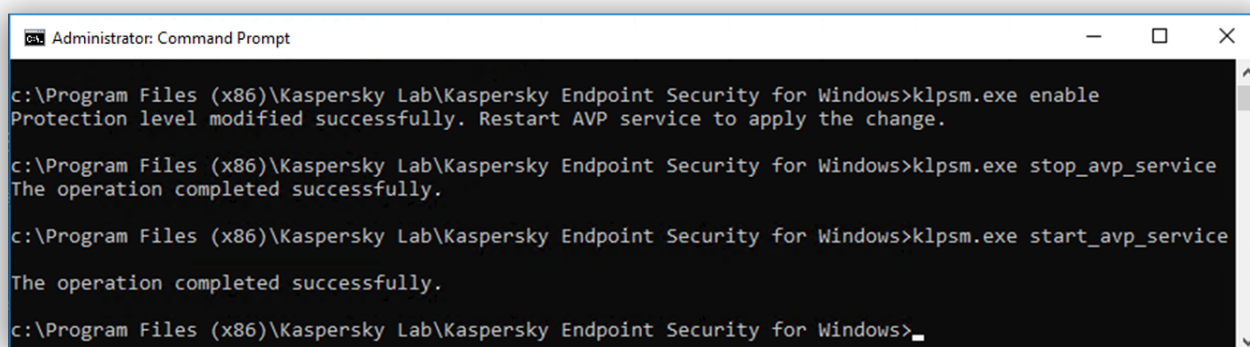
3. Vá para a pasta onde o ficheiro executável do Kaspersky Endpoint Security está localizado.

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.](#)



```
Administrator: Command Prompt
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe enable
Protection level modified successfully. Restart AVP service to apply the change.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe stop_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe start_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>
```

Ativar suporte da tecnologia AM-PPL


Ativar e desativar a defesa de gestão externa

A defesa de gestão externa impede que aplicações de administração remota (por exemplo, TeamViewer ou RemotelyAnywhere) obtenham acesso ao Kaspersky Endpoint Security. Esta tecnologia inclui as seguintes funcionalidades de defesa de gestão externa:

- Proteção contra modificação das definições do Kaspersky Endpoint Security.
- Proteção de serviços do Kaspersky Endpoint Security (como o serviço AVP).
- Proteção dos processos da aplicação.

A proteção contra gestão externa está disponível apenas em computadores que executem um sistema operativo de 32 bits, exceto para o Windows 7. Para o Windows 7, a tecnologia está disponível para sistemas operativos de 32 e 64 bits.

Para ativar ou desativar a proteção contra a gestão externa:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Definições gerais** → **Definições da aplicação**.
3. Use a caixa de verificação **Permitir gestão das definições do Kaspersky Endpoint Security através de aplicações de controlo remoto** para ativar ou desativar a defesa de gestão externa.
Se a caixa de verificação estiver selecionada, pode usar aplicações de administração remota para configurar o Kaspersky Endpoint Security e gerir os seus serviços e processos.
Se a caixa de verificação não estiver selecionada, a defesa de gestão externa impede que aplicações de administração remota obtenham acesso ao Kaspersky Endpoint Security. Pode permitir a configuração do Kaspersky Endpoint Security utilizando aplicações específicas de administração remota. Para tal, deve [adicionar a aplicação de administração remota à lista fiável](#). Neste caso, a defesa de administração remota ainda assim impedirá que a aplicação de administração remota obtenha acesso aos serviços e processos do Kaspersky Endpoint Security.
4. Utilize a caixa de verificação **Ativar controlo externo de serviços** para ativar ou desativar a proteção dos serviços do Kaspersky Endpoint Security contra gestão externa.

Para sair da aplicação a partir da command line, desative a proteção dos serviços do Kaspersky Endpoint Security contra gestão externa.


5. Guarde as suas alterações.

Como resultado, quando a defesa de gestão externa está ativada, o Kaspersky Endpoint Security evita que o ponteiro do rato entre na janela da aplicação. Quando um utilizador remoto tenta encerrar um serviço de aplicação, aparece uma janela do sistema com uma mensagem de erro.

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 de definições da aplicação, selecione **Definições gerais** → **Ameaças e Exclusões**.
3. No bloco **Exclusões**, clique na ligação **Especificar aplicações fiáveis**.
4. Na janela que é aberta, 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 **Não monitorizar a atividade da aplicação**.
7. Guarde as suas alterações.

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 consumo 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 atualização;
- 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

A utilização de recursos do computador pelo Kaspersky Endpoint Security pode afetar o desempenho de outras aplicações. 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 pausar as tarefas agendadas e conceder recursos para outras aplicações.

Contudo, várias aplicações são iniciadas imediatamente quando os recursos da CPU ficam disponíveis, continuando a funcionar em segundo plano. Para que a verificação não dependa do desempenho de outras aplicações, não deverá conceder recursos do sistema operativo a outras aplicações.

Pode iniciar essas tarefas manualmente, se necessário.

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 reinício 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 Ativa. Para desinfetar uma infeção ativa de um servidor de ficheiros, ative a tecnologia de Desinfeção Ativa para servidores e inicie uma tarefa de grupo de *Verificação de vírus* numa altura conveniente para os utilizadores do servidor.

Ativar ou desativar o modo de poupança de energia

Para ativar ou desativar o modo de poupança de energia:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Definições gerais** → **Definições da aplicação**.
3. Na secção **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.


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:

- Tarefa de atualização;
- Tarefa de Verificação Completa;
- Tarefa de Verificação de Áreas Críticas;
- Tarefa de Verificação Personalizada;
- Tarefa de Verificação de Integridade;

4. Guarde as suas alterações.

Ativar ou desativar a concessão de recursos para outras aplicações

Para ativar ou desativar a concessão de recursos para outras aplicações:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, selecione **Definições gerais** → **Definições da aplicação**.
3. Na secção **Desempenho**, use a caixa de verificação **Conceder recursos para outras aplicações** para ativar ou desativar a concessão de recursos para outras aplicações.

Quando configurado para conceder recursos para outras aplicações, o Kaspersky Endpoint Security adia as tarefas agendadas que conduzem ao funcionamento lento de outras aplicações:

- Tarefa de atualização;
- Tarefa de Verificação Completa;
- Tarefa de Verificação de Áreas Críticas;
- Tarefa de Verificação Personalizada;
- Tarefa de Verificação de Integridade;

Por predefinição, a aplicação está configurada para conceder 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.

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 vírus nas estações de trabalho

Ativar [Verificação em segundo plano](#) é recomendado para Verificação de vírus em estações de trabalho. A *Verificação de fundo* 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 vírus 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 vírus* de acordo com as seguintes recomendações:

1. [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 os seus computadores no final do dia, pode configurar a tarefa de verificação da seguinte maneira:

- Ative o Wake-on-LAN. A funcionalidade Wake-on-LAN permite ligar o computador remotamente mediante o envio de um sinal especial pela rede local. Para usar esta funcionalidade, deve ativar a Wake-on-LAN nas definições do BIOS. Pode também desligar o computador automaticamente após a conclusão da verificação.
- Desative a funcionalidade "Executar tarefas ignoradas". O Kaspersky Endpoint Security ignorará as tarefas ignoradas quando o utilizador ligar o computador. A execução de tarefas depois de ligar o computador pode ser inconveniente para o utilizador, pois a verificação exige um grande compromisso de recursos.

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.

2. [Definir um âmbito de verificação.](#)

Selecione os seguintes objetos para verificar:

- Memória Kernel;
- Executar processos e objetos de arranque;
- Setores de arranque;
- Unidade do sistema (%systemdrive%).

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 considera a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições da 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](#).

Verificação de vírus em servidores

Configure a tarefa de *Verificação de vírus* de acordo com as seguintes recomendações:

1. [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.

2. [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 considera a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições da 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.

3. [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](#).

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 categoria e reputação dos ficheiros verificados bem como informações sobre a reputação dos endereços da Web 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. Configure o KSN Privado.

Private KSN 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.

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 AES (Padrão de Encriptação Avançado).

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 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 seleccionar 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 palavra-passe do token ou smart card ligado ao computador ou o nome de utilizador e a palavra-passe da conta do Agente de Autenticação criada pelo administrador da rede local, utilizando a tarefa [Gestão de contas do 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 de autenticação única \(SSO\)](#), 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.

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 Express Cache.
- 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 Think Center 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 palavra-passe 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 100
- 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

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)
- Castelhana (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 Restauo 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

Encriptação de disco completa utilizando a tecnologia de 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.

Para executar a encriptação de disco completa utilizando a tecnologia de encriptação de disco Kaspersky:

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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Encriptação de Dados** → **Encriptação de disco completa**.
6. Na lista pendente da **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.

7. Na lista pendente **Modo de Encriptação**, selecione a opção **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](#).

8. Configure as regras para adicionar contas do Agente de Autenticação durante a encriptação de disco. O Agente permite a um utilizador concluir a autenticação para aceder a unidades encriptadas e para iniciar o sistema operativo. Para adicionar automaticamente contas do Agente de Autenticação, configure as seguintes definições:

- **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 palavra-passe e alteração da palavra-passe na primeira autenticação. Como tal, não é necessário [adicionar manualmente contas do Agente de Autenticação](#) através da tarefa *Gestão de contas do Agente de Autenticação* para computadores com unidades já encriptadas.

Se desativou a criação automática de contas do Agente de Autenticação, pode [adicionar manualmente contas do Agente de Autenticação](#) através da tarefa *Gestão de contas*. Pode também utilizar esta tarefa para alterar as definições das contas do Agente de Autenticação que foram criadas automaticamente.

9. Para conveniência do utilizador, pode guardar o nome de utilizador na memória do Agente de Autenticação para que apenas seja necessário introduzir a palavra-passe na próxima vez que iniciar sessão no sistema. Para tal, selecione a caixa de verificação **Guardar o nome de utilizador introduzir no Agente de Autenticação**.
10. Selecione um dos seguintes métodos de encriptação:
 - Se pretender aplicar a encriptação apenas aos setores das unidades de disco rígido que estão ocupadas por ficheiros, selecione a caixa de verificação **Encriptar apenas espaço utilizado do disco (reduz tempo de encriptação)**.

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 pretender aplicar a encriptação à totalidade da unidade de disco rígido, desmarque a caixa de verificação **Encriptar apenas espaço utilizado do disco (reduz tempo de encriptação)**.

Se um dispositivo tiver sido encriptado anteriormente utilizando a opção **Encriptar apenas espaço utilizado do disco (reduz tempo de encriptação)**, depois de aplicar uma política no modo **Encriptar todas as unidades de discos rígido**, os seus setores que não estejam ocupados por ficheiros permanecem desencriptados.

11. Se ocorrer um problema de incompatibilidade de hardware durante a encriptação do computador, pode seleccionar a caixa de verificação **Utilizar Legacy USB Support (não recomendado)**.

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). Legacy USB Support não afeta o suporte para dispositivos USB após iniciar o sistema operativo.

Quando a função Suporte de USB de Legado 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.

12. 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](#).

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.

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

5. Na janela de política, selecione **Encriptação de Dados** → **Encriptação de disco completa**.

6. Na lista pendente da **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.

7. Para adicionar unidades de disco rígido à lista de unidades de disco rígido excluídas da encriptação:

a. Clique no botão **Add**.

b. Esta ação irá abrir uma janela; nessa janela, edite as definições **Nome do dispositivo**, **Nome do computador**, **Tipo de disco**, **Encriptação de Disco Kaspersky**.

c. Clique no botão **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**.

8. 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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Encriptação de Dados** → **Encriptação de disco completa**.
6. Na lista pendente da **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**.
7. 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. Clique na ligação **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.
8. Para importar a lista de regras:
 - a. Clique no 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.
9. 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, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Dirija-se a **Data Encryption** → **Full Disk Encryption**.
5. Seleccione a tecnologia **Encriptação de disco Kaspersky** e siga a ligação para configurar as definições.
As definições de encriptação surgem.
6. Clique na ligação **Exclusões**.
7. Para exportar a lista de regras:
 - a. Seleccione as exclusões que pretende exportar.
 - b. Clique no botão **Export**.
 - c. Confirme que quer exportar apenas as exclusões seleccionadas ou exportar toda a lista de exclusões.
 - d. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de exclusões e seleccione a pasta onde pretende guardar este ficheiro.
 - e. Guardar o ficheiro.
O Kaspersky Endpoint Security exporta toda a lista de exclusões para o ficheiro XML.
8. Para importar a lista de regras:
 - a. Clique no botão **Importar**.
 - b. Na janela que se abre, seleccione 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.
9. Guarde as suas alterações.

Ativação da tecnologia de autenticação única (SSO)

A tecnologia de autenticação única (SSO) permite que efetue o início de sessão automaticamente no sistema operativo usando as credenciais 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.

A tecnologia de autenticação única não é compatível com o fornecimento de credenciais de conta por parte de terceiros.

Como ativar a utilização da tecnologia de autenticação única 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Encriptação de dados** → **Definições de encriptação comuns**.
6. No bloco **Definições de password**, clique no botão **Definições**.
7. Na janela que surgir, no separador **Agente de Autenticação**, selecione a caixa de verificação **Utilizar a tecnologia SSO (Single Sign-On)**.
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.

Como ativar a utilização da tecnologia de autenticação única na Consola da Web

1. Na janela principal da Consola Web, selecione **Devices** → **Policies & Profiles**.
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. Dirija-se a **Data Encryption** → **Full Disk Encryption**.
5. Selecione a tecnologia **Encriptação de disco Kaspersky** e siga a ligação para configurar as definições.
As definições de encriptação surgem.
6. Na secção **Definições de password**, selecione a caixa de verificação **Utilizar a tecnologia SSO (Single Sign-On)**.
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.

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. Depois disso, o Kaspersky Endpoint Security substitui a password da conta do Agente de Autenticação pela password da conta 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 *Gerir contas do Agente de Autenticação* 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 *Gerir contas do Agente de Autenticação*. 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 Consola de Administração, dirija-se à pasta **Administration Server** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **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 (11.8.0)** → **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

Sair do 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.

1. Na janela principal da Consola de Web, seleccione **Devices** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **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 suspensa **Application**, seleccione **Kaspersky Endpoint Security for Windows (11.8.0)**.

2. Na lista pendente **Task type**, seleccione **Manage Authentication Agent accounts**.

3. No campo **Task name**, introduza uma breve descrição, por exemplo, *Administrator accounts*.

4. Na secção **Select devices to which the task will be assigned**, seleccione 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

Sair do Assistente. Será apresentada uma nova tarefa na lista de tarefas.

Para executar uma tarefa, seleccione a caixa de selecção 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 *Gerir contas do Agente de Autenticação*. É conveniente usar uma tarefa de grupo, por exemplo, para adicionar uma conta de administrador a todos os computadores.

O Kaspersky Endpoint Security permite 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 *Manage Authentication Agent accounts*.
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 *Gerir contas do 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. Sob **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.

1. Na janela principal da Consola de Web, seleccione **Devices** → **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. Seleccione o separador **Application settings**.

4. Na lista de contas do Agente de Autenticação, clique no botão **Add**.

Isto inicia o Assistente de Gestão de Contas do Agente de Autenticação.

5. Seleccione o tipo de comando **Add**.

6. Seleccione uma conta de utilizador. Pode seleccionar 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 (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.

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.** Seleccione 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. Seleccione 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 palavra-passe 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 *Manage Authentication Agent accounts*.
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 *Gerir contas do 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 de Web, selecione **Devices** → **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**.

Isto inicia o Assistente de Gestão de Contas do Agente de Autenticação.

5. Selecione o tipo de comando **Change**.

6. Selecione uma conta de utilizador. Pode seleccionar 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 (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.

7. Selecione as caixas de verificação junto às definições que pretende editar.

8. 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.

9. Guarde as suas alterações.

10. 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 *Gerir contas do Agente de Autenticação*. 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 *Manage Authentication Agent accounts*.
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 *Gerir contas do 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 de Web, selecione **Devices** → **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**.
Isto inicia o Assistente de Gestão de Contas do Agente de Autenticação.
5. Selecione o tipo de comando **Delete**.
6. Selecione uma conta de utilizador. Pode seleccionar uma conta na lista de contas de domínio ou inserir manualmente o nome da conta.
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, 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 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 **Tarefas**.
A lista de tarefas locais é aberta.
6. Selecione a tarefa **Gestão das contas de Agente de Autenticação**.
7. 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.

Como consultar uma lista de contas do Agente de Autenticação através da Consola da Web

1. Na janela principal da Consola Web, selecione **Devices** → **Managed 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. Na janela de propriedades do computador, selecione a secção **Tarefas**.
A lista de tarefas locais é aberta.
4. Selecione a tarefa **Gestão das contas de Agente de Autenticação**.
5. Na janela de propriedades da tarefa, selecione a secção **Definições da Aplicação**.

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 *Gerir contas do 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](#).

Descriptação de unidade de disco ríido

Pode descriptar unidades de disco ríido mesmo que não exista nenhuma licença ativa que permita a encriptação de dados.

Para descriptar unidades de disco ríido:

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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Encriptação de Dados** → **Encriptação de disco completa**.
6. Na lista pendente **Tecnologia de Encriptação**, selecione a tecnologia com a qual foram encriptados os discos ríidos.
7. Execute uma das ações seguintes:
 - Na lista pendente **Modo de encriptação**, selecione a opção **Descriptar todas as unidades de discos ríido** se pretender descriptar todas as unidades de disco ríido encriptadas.
 - Adicione as unidades de disco ríido que pretende descriptar à tabela **Não encriptar as unidades de disco ríido seguintes**.

Esta opção está disponível apenas para a tecnologia de Encriptação de disco Kaspersky.

8. Guarde as suas alterações.

Pode utilizar a ferramenta Monitor de Encriptação para controlar o processo de encriptação ou descriptação de disco no computador de um utilizador. Pode executar a ferramenta Monitor de Encriptação na [janela principal da aplicação](#).

Se o utilizador encerra ou reinicia o computador durante a descriptação de unidades de disco ríido 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 descriptação da unidade de disco ríido 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 descriptação de unidades de disco ríido 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 descriptação da unidade de disco ríido após a autenticação com êxito no agente de autenticação e arranque do sistema operativo. Após a descriptação da unidade de disco ríido, o modo de hibernação está indisponível até o primeiro reinício do sistema operativo.

Se o sistema operativo entrar em modo de descanso durante a descriptação da unidade de disco rígido, o Kaspersky Endpoint Security retoma a descriptação da unidade de disco rígido quando o sistema operativo sair do modo de descanso sem carregar o Agente de Autenticação.

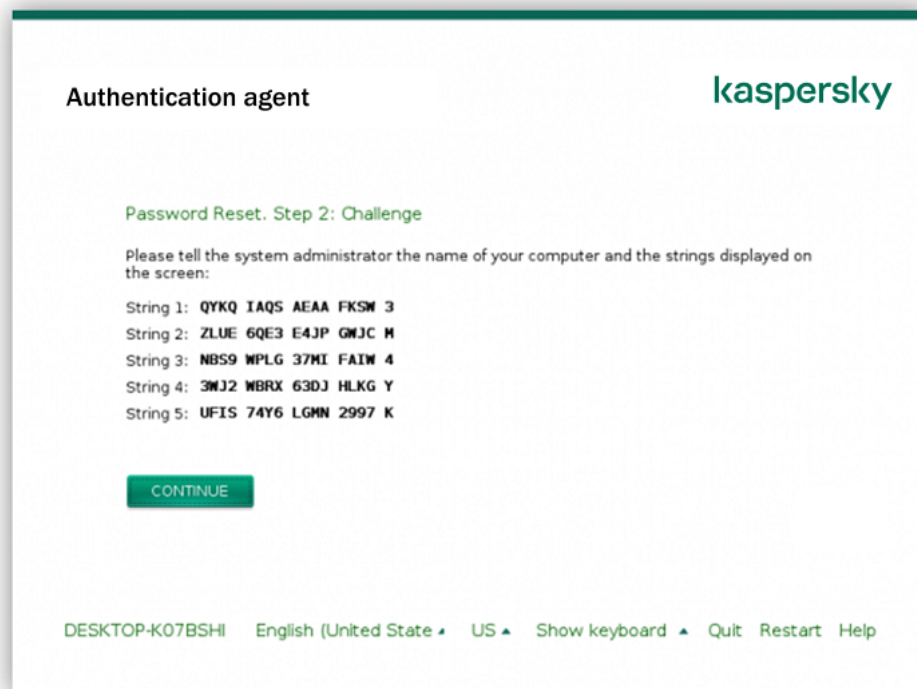
Restaurar acesso a uma unidade protegida pela tecnologia Encriptação de disco Kaspersky

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).

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 \(MMC\)](#) ²

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. 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.
5. No menu de contexto, selecione **Conceder acesso em modo offline**.
6. Na janela que é aberta, selecione o separador **Agente de Autenticação**.
7. Na secção **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: *Encriptação forte (AES256)* ou *Encriptação leve (AES56)*. A biblioteca de encriptação AES é instalada juntamente com a aplicação.
8. Na lista pendente **Conta**, selecione o nome da conta do Agente de Autenticação do utilizador que solicitou a recuperação do acesso a uma unidade.
9. Na lista pendente **Disco rígido**, selecione a unidade de disco rígido encriptada para a qual necessita de recuperar o acesso.
10. Na secção **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.

[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 **Devices** → **Managed devices**.
2. Selecione a caixa de verificação ao lado do nome do computador a cuja unidade pretende restaurar o acesso.
3. Clique no botão **Grant access to the device in offline mode**.
4. Na janela apresentada, selecione a secção **Agente de Autenticação**.
5. Na lista pendente **Conta**, 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 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. 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.
5. No menu de contexto, selecione **Conceder acesso em modo offline**.
6. Na janela que é aberta, selecione o separador **Encriptação de dados**.
7. No separador **Encriptação de dados**, clique no botão **Procurar**.
8. Na janela para seleccionar 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.

[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, seleccione **Devices** → **Managed devices**.
2. Seleccione a caixa de verificação ao lado do nome do computador a cujos dados pretende restaurar o acesso.
3. Clique no botão **Grant access to the device in offline mode**.
4. Seleccione a secção **Data Encryption**.
5. Clique no botão **Select file** e seleccione 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 seleccione 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.

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.

Para obter detalhes sobre como atualizar o sistema operativo em segurança, consulte a [Base de Conhecimento do Suporte Técnico](#).

A atualização automática do sistema operativo está disponível nas seguintes condições:

1. O sistema operativo é atualizado através dos WSUS (Serviços de Atualização do Windows Server).
2. O Windows 10 versão 1607 (RS1) ou posterior está instalado no computador.
3. O Kaspersky Endpoint Security, versão 11.2.0 ou posterior, está instalado no computador.

Se todas as condições forem cumpridas, pode atualizar o sistema operativo do modo habitual.

Se estiver a utilizar a tecnologia de Encriptação de Disco Kaspersky (FDE) e o Kaspersky Endpoint Security for Windows versão 11.1.0 ou 11.1.1 estiver instalado no computador, não será necessário desencriptar os discos rígidos para atualizar o Windows 10.

Para atualizar o sistema operativo, precisa de fazer o seguinte:

1. Antes de atualizar o sistema, copie os controladores denominados cm_km.inf, cm_km.sys, klfde.cat, klfde.inf, klfde.sys, klfdefsf.cat, klfdefsf.inf e klfdefsf.sys para uma pasta local. Por exemplo, C:\fde_drivers.
2. Execute a instalação da atualização do sistema com a opção `/ReflectDrivers` e especifique a pasta que contém os controladores guardados:
`setup.exe/ReflectDrivers C:\fde_drivers`

Se estiver a utilizar a tecnologia de Encriptação de Unidade BitLocker, não é necessário descriptar 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 11.8.0.

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](#).

Selecionar o nível de rastreio do 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 selecionar o nível de rastreio do Agente de autenticação:

1. 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.
2. Selecione o nível de rastreio na janela de definições do Agente de autenticação:

- **Disable debug logging (default).** Se esta opção estiver selecionada, a aplicação não regista a informação sobre eventos do Agente de Autenticação no ficheiro de rastreio.
- **Enable debug logging.** 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.
- **Enable verbose logging.** 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 com esta opção é superior quando comparado com o nível da opção **Enable debug logging**. Um elevado nível de detalhe das entradas pode tornar mais lento o arranque do Agente de Autenticação e do sistema operativo.

- **Enable debug logging and select serial port.** 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.

- **Enable verbose debug logging and select serial port.** 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 **Enable debug logging and select serial port**. Um elevado nível de detalhe das entradas pode tornar mais lento o arranque do Agente de Autenticação e do sistema operativo.

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.

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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Encriptação de dados** → **Definições de encriptação comuns**.
6. No bloco **Modelos**, clique no botão **Ajuda**.
7. Na janela aberta, execute uma das seguintes ações:
 - 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.
8. 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 caracteres.

9. 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 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 o Kaspersky Security Center. O BitLocker encripta volumes lógicos. Não pode utilizar o BitLocker para encriptação de unidades removíveis. Para obter mais informações sobre o BitLocker, consulte a [documentação da Microsoft](#).

O BitLocker fornece armazenamento seguro de chaves de acesso utilizando um módulo de plataforma fiável. Um *Módulo de plataforma fiável (TPM)* 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 uma unidade, o BitLocker cria uma chave mestra. O Kaspersky Endpoint Security envia a chave mestra 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 [informações sobre a encriptação do disco ao Kaspersky Security Center](#). No entanto, o Kaspersky Endpoint Security não enviará a chave mestra ao Kaspersky Security Center, por isso será impossível restaurar o acesso ao disco utilizando o Kaspersky Security Center. Para que o BitLocker funcione corretamente com o Kaspersky Security Center, [desencripte a unidade](#) e [volte a encriptar a unidade](#) utilizando uma política. Pode desencriptar uma unidade localmente ou utilizando uma política.

Depois de encriptar o disco rígido do sistema, o utilizador precisa passar pela autenticação do BitLocker para inicializar o sistema operativo. Depois do procedimento de autenticação, o BitLocker permitirá aos utilizadores iniciarem sessão. O BitLocker não oferece suporte à tecnologia de início de sessão único (SSO).

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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Encriptação de Dados** → **Encriptação de disco completa**.
6. Na lista pendente **Tecnologia de Encriptação**, selecione a opção **Encriptação de Unidade BitLocker**.
7. Na lista pendente **Modo de Encriptação**, selecione a opção **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.

8. Configure as opções avançadas da Encriptação de Unidade BitLocker (consulte a tabela abaixo).
9. Guarde as suas alterações.

[Como executar a Encriptação de Unidade BitLocker através da Consola Web e da Cloud Console ?](#)

1. Na janela principal da Consola Web, selecione **Devices** → **Policies & Profiles**.
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. Dirija-se a **Data Encryption** → **Full Disk Encryption**.
5. No bloco **Gerir encriptação**, selecione **Encriptação de Unidade BitLocker**.
6. Clique na hiperligação **Encriptação de Unidade BitLocker**.
Abre a janela de definições Encriptação de Unidade BitLocker.
7. Na lista pendente **Modo de Encriptação**, selecione a opção **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.

8. Configure as opções avançadas da Encriptação de Unidade BitLocker (consulte a tabela abaixo).
9. 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](#).

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	<p>Esta caixa de verificação ativa / desativa a utilização da autenticação com 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).</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>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.</p> </div> <p>Se a caixa de verificação estiver selecionada, é permitida a utilização da autenticação com entrada de pré-arranque. Recomenda-se 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.</p> <p>Se a caixa de verificação estiver desmarcada, não é possível executar a Encriptação de Unidade BitLocker em tablets.</p>
Utilizar a encriptação de hardware (Windows 8 e	<p>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.</p>

<p>versões mais recentes)</p>	<p>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.</p> <div data-bbox="416 288 1493 483" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Ativar ou desativar a funcionalidade Encriptar apenas espaço utilizado do disco (Windows 8 e versões mais recentes) após o início da encriptação não altera esta definição até que os discos rígidos sejam descriptados. Tem de seleccionar ou desmarcar a caixa de verificação antes de iniciar a encriptação.</p> </div> <p>Se a caixa de verificação estiver seleccionada, são encriptadas apenas as partes do disco rígido que estiverem ocupadas por ficheiros. O Kaspersky Endpoint Security encripta automaticamente dados novos quando são adicionados.</p> <p>Se a caixa de verificação estiver seleccionada, é encriptado o disco rígido completo, incluindo os fragmentos residuais de ficheiros anteriormente eliminados e modificados.</p> <div data-bbox="416 752 1493 978" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>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.</p> </div> <p>Esta caixa de verificação está desmarcada por predefinição.</p>
<p>Definições de autenticação</p>	<p>Utilizar password (Windows 8 e versões mais recentes)</p> <p>Se esta opção estiver seleccionada, o Kaspersky Endpoint Security pede uma password ao utilizador quando este tenta aceder a unidade encriptada.</p> <p>Esta opção pode ser seleccionada quando um Trusted Platform Module (TPM) não está a ser utilizado.</p> <p>Utilizar Trusted Platform Module (TPM)</p> <p>Se esta opção estiver seleccionada, o BitLocker utiliza um Trusted Platform Module (TPM).</p> <p>Um <i>Módulo de plataforma fiável (TPM)</i> 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.</p> <div data-bbox="416 1637 1493 1832" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>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.</p> </div> <p>Um dispositivo equipado com um Trusted Platform Module pode criar chaves de encriptação que apenas podem ser descriptadas 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.</p> <p>Esta ação está seleccionada por predefinição.</p>

Pode definir uma camada adicional de proteção para o acesso à chave de encriptação, e encriptar a chave com uma password ou um PIN:

- **Use PIN for 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.
Pode permitir que o utilizador utilize o PIN avançado. O *PIN avançado* permite a utilização de outros caracteres além dos caracteres numéricos: letras latinas maiúsculas e minúsculas, caracteres especiais e espaços.
- **Utilizar Trusted Platform Module (TPM); se não estiver disponível - utilizar password.** Se a caixa de verificação 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.

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. 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, seleccione o separador **Policies**.
4. Seleccione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, seleccione **Encriptação de Dados** → **Encriptação de disco completa**.
6. Na lista pendente **Tecnologia de Encriptação**, seleccione a opção **Encriptação de Unidade BitLocker**.
7. Na lista pendente **Modo de Encriptação**, seleccione **Desencriptar todas as unidades de discos rígido**.
8. 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, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Dirija-se a **Data Encryption** → **Full Disk Encryption**.
5. Seleccione a tecnologia **Encriptação de Unidade BitLocker** e siga a ligação para configurar as definições.
As definições de encriptação surgem.
6. Na lista pendente **Modo de Encriptação**, seleccione **Desencriptar todas as unidades de discos rígido**.
7. Clique em **OK**.

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](#).

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.


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 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. 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.
5. No menu de contexto, selecione **Conceder acesso em modo offline**.
6. Na janela apresentada, selecione o separador **Acesso à unidade do sistema protegido pelo BitLocker**.
7. 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.

[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 **Devices** → **Managed devices**.
2. Selecione a caixa de verificação ao lado do nome do computador a cuja unidade pretende restaurar o acesso.
3. Clique no botão **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 no botão **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 palavra-passe ou o código PIN. Depois de definir uma nova palavra-passe ou um novo código PIN, o BitLocker criará uma nova chave mestra 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, seleccione a pasta **Additional** → **Data encryption and protection** → **Encrypted drives**.
3. Na área de trabalho, seleccione o dispositivo encriptado para o qual pretende criar um ficheiro-chave de acesso e, no menu de contexto do dispositivo, seleccione **Obter acesso ao dispositivo no Kaspersky Endpoint Security for Windows**.
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 seleccionado corresponde ao nome do computador do utilizador.

5. Envie ao utilizador a chave que está indicada no campo **Chave de recuperação**.

[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 da Web, seleccione **Operations** → **Data encryption and protection** → **Encrypted Drives**.

2. Seleccione a caixa de verificação ao lado do nome do computador a cuja unidade pretende restaurar o acesso.

3. Clique no botão **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. Seleccione 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 seleccionado corresponde ao nome do computador do utilizador.

c. Clique no botão **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 Consola de Administração, dirija-se à pasta **Administration Server** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **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 (11.8.0)** → **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

Sair do 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 de Web, seleccione **Devices** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **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 suspensa **Application**, seleccione **Kaspersky Endpoint Security for Windows (11.8.0)**.

2. Na lista pendente **Task type**, seleccione **BitLocker Protection Management**.

3. No campo **Task name**, introduza uma breve descrição, por exemplo, *Updating to Windows 10*.

4. Na secção **Select devices to which the task will be assigned**, seleccione o âmbito de tarefa.

Passo 2. Gestão de segurança BitLocker

Configure a autenticação do BitLocker. Para pausar a proteção por BitLocker, seleccione **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. Completar a criação da tarefa

Sair do Assistente. Será apresentada uma nova tarefa na lista de tarefas.

Para executar uma tarefa, seleccione a caixa de selecção 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. Também pode descobrir o número de reinícios restantes nas propriedades do computador na Consola do Kaspersky Security Center.

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

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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Encriptação de Dados** → **Encriptação ao nível dos ficheiros**.

6. Na lista pendente **Modo de encriptação**, selecione **De acordo com as regras**.

7. 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.
- **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. Pode usar o conjunto `\..\` (p. ex. C:\Users\..\UserFolder\). O conjunto `\..\` indica a transição para a pasta principal.
- Não use os caracteres `*` e `?`.
- Não use caminhos UNC.
- Use `;` ou `,` como um carácter 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.

8. 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

Para formar regras de acesso a ficheiros encriptados para aplicações:

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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Encriptação de Dados** → **Encriptação ao nível dos ficheiros**.
6. 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.

7. Na parte direita da janela, selecione o separador **Regras de Aplicações**.
8. Se quiser seleccionar 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 da secção **Grupo**.
 - b. Clique no botão **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 **Regras 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**.

9. 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 **Regras 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**.

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

5. Na janela de política, selecione **Encriptação de Dados** → **Encriptação ao nível dos ficheiros**.

6. 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.

7. Na parte direita da janela, selecione o separador **Regras de Aplicações**.

8. Se quiser seleccionar 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 da secção **Grupo**.

b. Clique no botão **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 **Regras de aplicações**, selecione **Encriptar todos os ficheiros criados**.

e. Na lista pendente **Ações para as aplicações seleccionadas 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 seleccionadas é apresentada na tabela no separador **Regras de aplicações**.

9. Se pretender seleccionar 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 **Regras de aplicações**, selecione **Encriptar todos os ficheiros criados**.

A informação sobre a regra de encriptação para ficheiros criados ou alterados pelas aplicações seleccionadas é apresentada na tabela no separador **Regras de aplicações**.

10. Guarde as suas alterações.

Criar uma regra de desencriptação

Para criar uma regra de descriptação:

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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Encriptação de Dados** → **Encriptação ao nível dos ficheiros**.
6. Na lista pendente **Modo de encriptação**, selecione **De acordo com as regras**.
7. 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 descriptação.
 - b. Selecione o item **Pasta predefinida** para adicionar um caminho de pasta introduzido manualmente para uma regra de descriptação.
 - c. Selecione o item **Ficheiros por extensão** para adicionar extensões de ficheiro individuais a uma regra de descriptação. 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 descriptação (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.
8. Guarde as suas alterações.

Se o mesmo ficheiro tiver sido adicionado à regra de encriptação e à regra de descriptação, 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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Encriptação de Dados** → **Encriptação ao nível dos ficheiros**.

6. Na parte direita da janela, selecione o separador **Encriptação**.

7. 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 **Remove**.

Os ficheiros e as pastas removidos da lista de encriptação são automaticamente adicionados à lista de desencriptação.

8. [Formar uma lista de desencriptação de ficheiros](#).

9. 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 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 palavra-passe ao criar arquivos encriptados 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Encriptação de dados** → **Definições de encriptação comuns**.
6. No bloco **Definições de password**, clique no botão **Definições**.
7. Na janela apresentada, selecione o separador **Pacotes encriptados**.
8. Configure as definições de complexidade da password ao criar pacotes encriptados.

Como ativar a verificação dos requisitos de segurança da palavra-passe ao criar arquivos encriptados na Consola Web


1. Na janela principal da Consola Web, selecione **Devices** → **Policies & Profiles**.
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 **Definições da password do pacote encriptado**, configure os critérios de segurança da password necessários para a criação de pacotes encriptados.

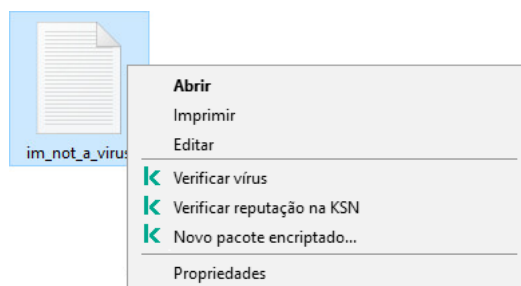
Pode criar pacotes encriptados em computadores com o Kaspersky Endpoint Security instalado com a Encriptação ao nível dos ficheiros disponível.

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).
3. Na janela que surgir, selecione uma localização numa unidade amovível para guardar o pacote encriptado → especifique o nome do pacote e clique no botão **Guardar**.
4. Na janela surgir, especifique a password e confirme-a.
A password deve cumprir aos critérios de complexidade especificados na política.
5. Clique no botão **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.



Criar um pacote encriptado

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.

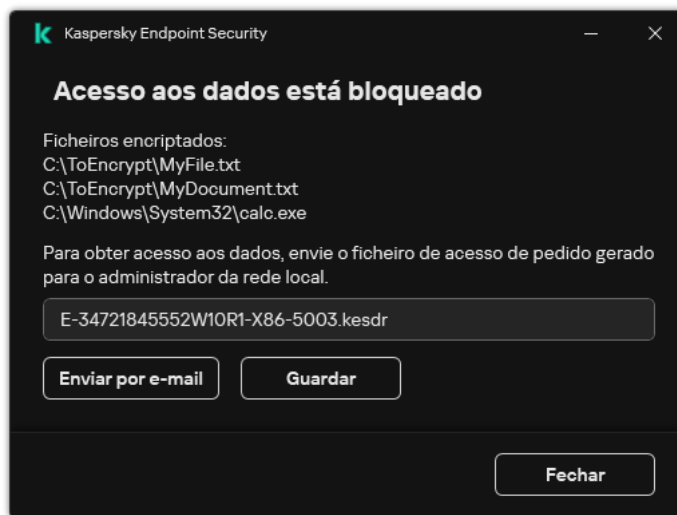
O utilizador pode trabalhar com ficheiros encriptados nas seguintes circunstâncias:

- 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 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, seleccione o separador **Devices**.
4. No separador **Devices**, seleccione o computador do utilizador que solicitou acesso a dados encriptados, e clique com o botão direito do rato para abrir o menu de contexto.
5. No menu de contexto, seleccione **Conceder acesso em modo offline**.
6. Na janela que é aberta, seleccione o separador **Encriptação de dados**.
7. No separador **Encriptação de dados**, clique no botão **Procurar**.
8. Na janela para seleccionar 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.

[Como obter um ficheiro da chave de acesso a dados encriptados na Consola da Web [?]](#)

1. Na janela principal da Consola Web, seleccione **Devices** → **Managed devices**.
2. Seleccione a caixa de verificação ao lado do nome do computador a cujos dados pretende restaurar o acesso.
3. Clique no botão **Grant access to the device in offline mode**.
4. Seleccione a secção **Data Encryption**.
5. Clique no botão **Select file** e seleccione 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 seleccione 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. 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, seleccione o separador **Policies**.
4. Seleccione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, seleccione **Encriptação de dados** → **Definições de encriptação comuns**.
6. No bloco **Modelos**, clique no botão **Modelos**.
7. Na janela aberta, execute uma das seguintes ações:
 - Se pretender editar o modelo de mensagem de utilizador, seleccione o separador **Mensagem do utilizador**. A janela **Acesso aos dados está bloqueado** é aberta quando o utilizador tenta aceder a um ficheiro encriptado sem uma chave disponível no computador para aceder aos ficheiros encriptados. Ao clicar no botão **Enviar por e-mail** na janela **Acesso aos dados está bloqueado**, 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, seleccione o separador **Mensagem do administrador**. Esta mensagem é criada automaticamente quando clica no botão **Enviar por e-mail** na janela **Solicitar acesso aos ficheiros encriptados** e é enviada ao utilizador depois de acesso a ficheiros encriptados ter sido concedido ao utilizador.
8. Editar os modelos da mensagem.
9. Guarde as suas alterações.

Encriptação de unidades amovíveis

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:

- Encriptação Completa do Disco (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).

- Encriptação ao Nível dos Ficheiros (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 descriptar 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 descriptação de dados em unidades amovíveis depende do computador ao qual a unidade amovível está ligada.

O Kaspersky Endpoint Security suporta a encriptação nos sistemas de ficheiros FAT32 e NTFS. Se uma unidade amovível com um sistema de ficheiros não suportado for ligada ao computador, a encriptação da unidade amovível termina com um erro e o Kaspersky Endpoint Security atribui o estado apenas de leitura à unidade amovível.

Para encriptar unidades amovíveis:

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, seleccione o separador **Policies**.
4. Seleccione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, seleccione **Encriptação de Dados** → **Encriptação de unidades amovíveis**.
6. Na lista pendente **Modo de encriptação**, seleccione 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.

7. Se quiser [usar o modo portátil](#) para a encriptação de unidades amovíveis, seleccione 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.

8. 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.

9. Se quiser configurar a encriptação para unidades amovíveis individuais, [defina regras de encriptação](#).

10. 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.

11. Guarde as suas alterações.

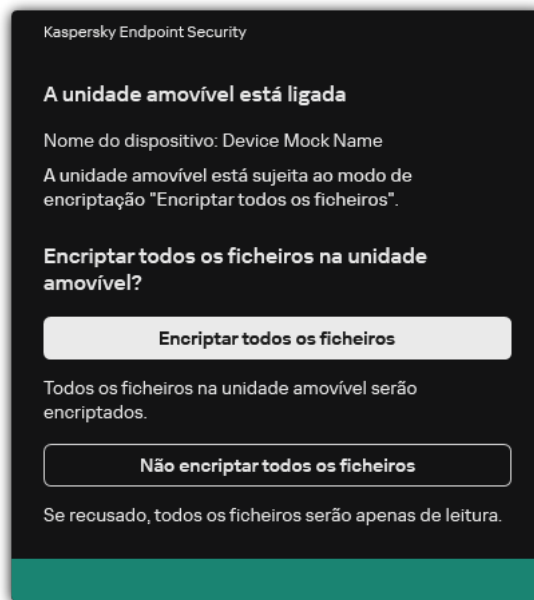
Após a aplicação da política, quando o utilizador liga uma unidade amovível ou se uma unidade amovível já estiver ligada, o Kaspersky Endpoint Security solicita ao utilizador uma confirmação para executar a operação de encriptação (ver a figura abaixo).

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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Encriptação de Dados** → **Encriptação de unidades amovíveis**.
6. 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**.
7. 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.
8. 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](#).

9. 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.

10. 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**.

11. 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. 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, seleccione o separador **Policies**.
4. Seleccione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, seleccione **Encriptação de Dados** → **Encriptação de unidades amovíveis**.
6. Para exportar a lista de regras de encriptação de unidades amovíveis:
 - a. Seleccione as regras que pretende exportar. Para seleccionar várias portas, utilize as teclas **CTRL** ou **SHIFT**.
Se não tiver seleccionado nenhuma regra, o Kaspersky Endpoint Security exportará todas as regras.
 - b. Clique na ligação **Exportar**.
 - c. Na janela que se abre, especifique o nome do ficheiro XML para o qual pretende exportar a lista de regras e seleccione 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 encriptação de unidades amovíveis:
 - a. Clique na ligação **Importar**.
Na janela que se abre, seleccione 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 encriptação da unidade amovível na Consola Web](#) 

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Dirija-se a **Encriptação de Dados** → **Encriptação de unidades amovíveis**.
5. No bloco **Regras de encriptação para dispositivos seleccionados**, clique na ligação **Regras de encriptação**.
Abre-se uma lista de regras de encriptação para unidades amovíveis.
6. Para exportar a lista de regras de encriptação de unidades amovíveis:
 - a. Seleccione as regras que pretende exportar.
 - b. Clique no botão **Export**.
 - c. Confirme que deseja exportar apenas as regras seleccionadas 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 ligação **Importar**.
Na janela que se abre, seleccione 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.

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:

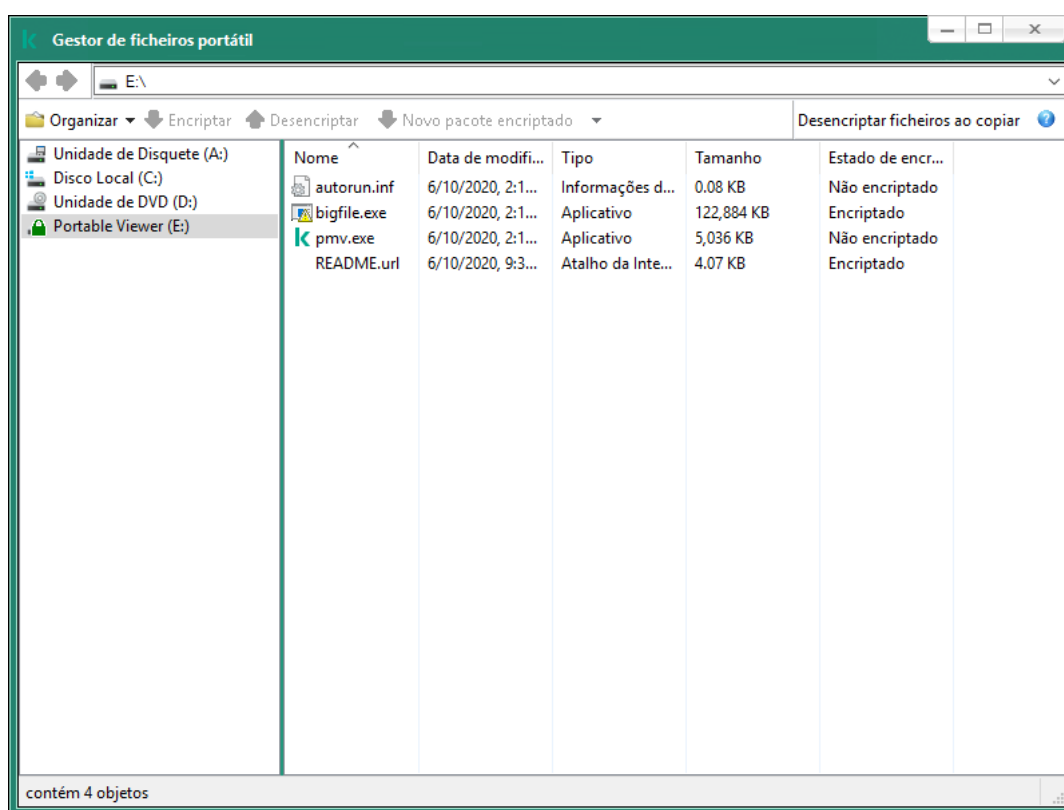
- Não há ligação entre o computador e o Servidor de Administração do Kaspersky Security Center.
- A infraestrutura mudou com a alteração do Servidor de Administração do Kaspersky Security Center.
- O Kaspersky Endpoint Security não está instalado no computador.

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. 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, selecione **Encriptação de Dados** → **Encriptação de unidades amovíveis**.
6. 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).

7. Selecione a caixa de verificação **Modo portátil**.
8. Se necessário, [adicione regras de encriptação para unidades amovíveis individuais](#).
9. Guarde as suas alterações.
10. Após aplicar a política, ligue a unidade amovível ao computador.
11. Confirme a operação de encriptação da unidade amovível.
Isto abre uma janela na qual pode criar uma password para o Gestor de ficheiros portátil.
12. Especifique uma password que cumpra os requisitos de força e confirme-a.
13. 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.

[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, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Dirija-se a **Encriptação de Dados** → **Encriptação de unidades amovíveis**.
5. Em **Gerir encriptação**, seleccione **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).

6. Seleccione a caixa de verificação **Modo portátil**.
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.
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.

- 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.

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 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, seleccione o separador **Devices**.
4. No separador **Devices**, seleccione o computador do utilizador que solicitou acesso a dados encriptados, e clique com o botão direito do rato para abrir o menu de contexto.
5. No menu de contexto, seleccione **Conceder acesso em modo offline**.
6. Na janela que é aberta, seleccione o separador **Encriptação de dados**.
7. No separador **Encriptação de dados**, clique no botão **Procurar**.
8. Na janela para seleccionar 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.

[Como obter um ficheiro de acesso a dados encriptados na consola da Web](#)

1. Na janela principal da Consola Web, seleccione **Devices** → **Managed devices**.
2. Seleccione a caixa de verificação ao lado do nome do computador a cujos dados pretende restaurar o acesso.
3. Clique no botão **Grant access to the device in offline mode**.
4. Seleccione a secção **Data Encryption**.
5. Clique no botão **Select file** e seleccione 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 seleccione 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 descriptar 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 descriptação de dados em unidades amovíveis depende do computador ao qual a unidade amovível está ligada.

Para descriptar unidades amovíveis:

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, seleccione o separador **Policies**.
4. Seleccione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela de política, seleccione **Encriptação de Dados** → **Encriptação de unidades amovíveis**.
6. Se pretende descriptar todos os ficheiros encriptados que estão armazenados em unidades amovíveis, na lista pendente **Modo de encriptação** seleccione **Descriptar unidade amovível completa**.
7. Para descriptar dados armazenados em unidades amovíveis individuais, edite as regras de encriptação para unidades amovíveis cujos dados pretende descriptar. Para tal:
 - a. Na lista de unidades amovíveis para as quais as regras de encriptação foram configuradas, seleccione 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 seleccionada.
 - c. No menu de contexto do botão **Definir uma regra**, clique em **Descriptar unidade amovível completa**.
8. Guarde as suas alterações.

Como resultado, se um utilizador ligar uma unidade amovível ou se esta já estiver ligada, o Kaspersky Endpoint Security descripta a unidade amovível. A aplicação avisa o utilizador de que o processo de descriptação pode demorar algum tempo. Se o utilizador inicia a remoção segura de uma unidade amovível durante a descriptação de dados, o Kaspersky Endpoint Security interrompe o processo de descriptação de dados e permite a remoção da unidade amovível antes da conclusão da operação de descriptação. A descriptação de dados continuará na próxima vez que a unidade removível for conectada a este computador.

Se a descriptação 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 descriptação decorrem, o Kaspersky Endpoint Security transmite informação sobre o estado dos parâmetros de encriptação aplicados a computadores cliente para o Kaspersky Security Center.

Os seguintes valores de estado de encriptação são possíveis:

- *Política de encriptação não definida.* Não foi definida uma política de encriptação do Kaspersky Security Center para o computador.
- *Aplicar política.* A encriptação e/ou desencriptação de dados está a decorrer no computador.
- *Erro.* Ocorreu um erro durante a encriptação e/ou desencriptação de dados no computador.
- *Reinicialização necessária.* O sistema operativo tem de ser reinicializado para iniciar ou concluir a encriptação ou desencriptação de dados no computador.
- *Em conformidade com a política.* A encriptação de dados no computador foi concluída utilizando as definições de encriptação especificadas na política do Kaspersky Security Center aplicada ao computador.
- *Cancelado pelo utilizador.* O utilizador recusou confirmar a operação de encriptação do ficheiro na unidade amovível.

Visualizar o estado de encriptação

Para ver o estado de encriptação dos dados do computador:

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. No separador **Dispositivos** da área de trabalho, faça deslizar a barra de deslocamento totalmente para a direita.
5. Se a coluna **Estado de encriptação** não for exibida:
 - a. Clique com o botão direito do rato para abrir o menu de contexto do cabeçalho da tabela.
 - b. No menu de contexto, na lista pendente **Ver**, selecione **Add/Remove columns**.
 - c. Na janela apresentada, selecione a caixa de verificação **Encryption status**.
 - d. Clique em **OK**.

A coluna **Estado de encriptação** 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.

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 **Estatísticas**.

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 aberta, clique no botão **Adicionar**.
- c. Esta ação abre uma janela; nessa janela, na secção **Geral**, introduza o nome da página.
- d. Na secção **Information panels**, clique no botão **Adicionar**.
- e. Na janela aberta 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, seleccionando o item **Encriptação de unidades amovíveis** 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. Clique no botão **Close**.

5. No separador **Estatísticas**, 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 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. Selecione o nome do computador na lista e clique com o botão direito do rato para abrir o menu de contexto.
5. No menu de contexto do computador, selecione o item **Propriedades**. Na janela que surgir, selecione a secção **Proteção**.
6. Clique na ligação **Ver erros de encriptação de dados** para abrir a janela **Erros de encriptação de dados**.

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

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, seleccione o separador **Reports**.
3. Clique no 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**, seleccione um dos seguintes itens:
 - **Report on encryption status of managed devices.**
 - **Report on encryption status of mass storage devices.**
 - **Report on file encryption errors.**
 - **Report on blockage of access to encrypted files.**

Depois de concluir o Novo Assistente de Modelos de Relatório, o novo modelo de relatório é apresentado na tabela no separador **Reports**.

5. Seleccione o modelo de relatório que foi criado nos passos prévios das instruções.
6. No menu de contexto do modelo, seleccione **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 Restauo de Dispositivo Encriptado](#) (doravante designada Ferramenta de Restauo) 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 Restauo estão na memória do computador do utilizador na forma descriptada 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 Restauo 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 Restauo. Se os metadados da conta do Agente de Autenticação tiverem sido corrompidos, o utilizador deve concluir o procedimento de restauo ao utilizar um ficheiro de acesso de pedido.

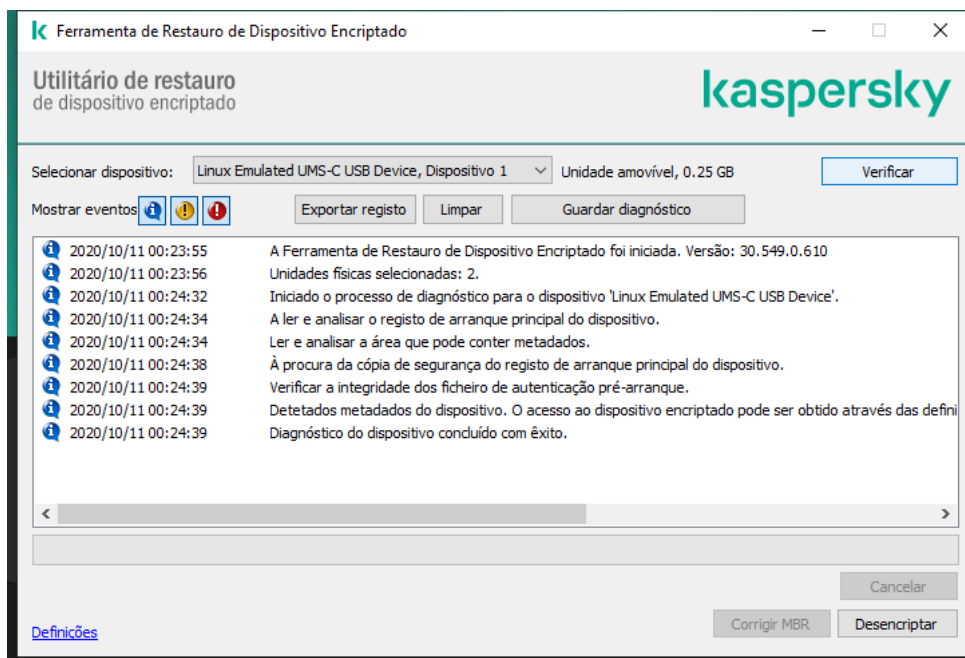
Antes de restaurar dados em dispositivos encriptados, recomenda-se que cancele a política do Kaspersky Security Center ou desative a encriptação nas definições da política do Kaspersky Security Center no computador onde o procedimento será executado. Este procedimento impede que o dispositivo seja encriptado novamente.

Recuperar dados utilizando Utilitário de Restauo 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 descriptar 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 surgir, 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 Restauo:

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 Restauo, selecione o dispositivo encriptado para o qual pretende restaurar o acesso.
3. Clique no botão **Verificação** 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 Restauo 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 Restauo 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 descriptar o dispositivo completo, selecione a opção **Descriptar todo o dispositivo**.
- Se quiser descriptar uma porção dos dados num dispositivo, selecione a opção **Descriptar áreas individuais do dispositivo** e especificar os limites da área de descriptação.
- Selecione o local de escrita dos dados descriptados:
 - Se pretender que os dados no dispositivo original sejam reescritos com os dados descriptados, desmarque a caixa de verificação **Descriptar para ficheiro de imagem de disco**.
 - Se pretender guardar os dados descriptados separadamente dos dados encriptados originais, selecione a caixa de verificação **Descriptar 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/descriptação 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 **Additional** → **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 **Obter acesso ao dispositivo no Kaspersky Endpoint Security for Windows**.

Se não tiver a certeza para o qual computador o ficheiro de pedido de acesso foi gerado, na árvore da Consola de Administração selecione a pasta **Adicional** → **Encriptação e proteção de dados** e, na área de trabalho, clique em **Obter a chave de encriptação do dispositivo no Kaspersky Endpoint Security for Windows**.

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: *Encriptação forte (AES256)* ou *Encriptação leve (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 no botão **Abrir**.

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 da Web, seleccione **Operations** → **Data encryption and protection** → **Encrypted Drives**.

2. Seleccione a caixa de verificação ao lado do nome do computador no qual pretende recuperar dados.

3. Clique no botão **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. Seleccione o plug-in **Kaspersky Endpoint Security for Windows**.

b. Seleccione 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: *Encriptação forte (AES256)* ou *Encriptação leve (AES56)*. A biblioteca de encriptação AES é instalada juntamente com a aplicação.

c. Clique no botão **Select file** e seleccione o ficheiro de pedido de acesso recebido do utilizador (um ficheiro com a extensão FDERTC).

d. Clique no botão **Save key** e seleccione uma pasta onde guardar o ficheiro da chave para aceder a 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](#) ²⁴).

Soluções Detection and Response

O Kaspersky Endpoint Security suporta soluções Detection and Response utilizando um agente integrado. Para utilizar o Detection and Response, tem de ativar a integração com estas soluções ao instalar a aplicação. 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 Sandbox 2.0.

O Kaspersky Endpoint Security também inclui o kit de distribuição do Kaspersky Endpoint Agent. O Kaspersky Endpoint Agent é compatível com o Kaspersky Anti Targeted Attack Platform (componente do Endpoint Detection and Response Expert (KATA EDR)). Para instalar o Kaspersky Endpoint Agent, tem de seleccionar o componente Endpoint Agent ao instalar a aplicação.

Não pode seleccionar o agente integrado e o Kaspersky Endpoint Agent em simultâneo ao instalar a aplicação. Se precisar de instalar o agente integrado e o Kaspersky Endpoint Agent, instale o Kaspersky Endpoint Agent em separado.

Pode utilizar a solução Kaspersky Endpoint Security com Detection and Response em diferentes configurações, por exemplo, [MDR+EDR Optimum 2.0+Kaspersky Sandbox 2.0].

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 for Windows 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 Kaspersky Endpoint Agent está incluído no [kit de distribuição do Kaspersky Endpoint Security](#). Pode instalar o Kaspersky Endpoint Agent durante a instalação do Kaspersky Endpoint Security. Para o fazer, tem de seleccionar o componente Endpoint Agent durante a instalação da aplicação (por exemplo, no [pacote de instalação](#)). Após a instalação da aplicação com o Agente Endpoint, o Kaspersky Endpoint Security e o Kaspersky Endpoint Agent serão adicionados à lista de aplicações instaladas. Após a desinstalação do Kaspersky Endpoint Security, o Kaspersky Endpoint Agent também será desinstalado automaticamente.

O kit de distribuição do Kaspersky Endpoint Agent está incluído no kit de distribuição do Kaspersky Endpoint Security for Windows.

Correspondência das versões KES e KEA

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

Migração de Política e Tarefa para o Kaspersky Endpoint Agent

O Kaspersky Endpoint Security 11.7.0 tem agora um assistente para a migração 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 (EDR);
- Kaspersky Managed Detection and Response (MDR).

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 o Kaspersky Endpoint Security com o 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

Sair do Assistente. Como resultado, o assistente:

- 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 um estado *Inativo*. Para continuar, altere os estatutos das políticas do Kaspersky Endpoint Agent e Kaspersky Endpoint Security para *Inativo* 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 para o Kaspersky Endpoint Detection and Response e o Kaspersky Sandbox. Simultaneamente, o Assistente deixa as tarefas do Kaspersky Endpoint Agent inalteradas.

Migrar a configuração [KES+KEA] para a configuração [KES+agente incorporado]

O Kaspersky Endpoint Security 11.7.0 tem agora agentes integrados para as soluções Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum) e Kaspersky Sandbox 2.0. Já não precisa de uma aplicação Kaspersky Endpoint Agent em separado para trabalhar com estas soluções. Quando atualiza o Kaspersky Endpoint Security para a versão 11.7.0, as soluções EDR Optimum e Kaspersky Sandbox continuam a trabalhar com o Kaspersky Endpoint Security. Além disso, o Kaspersky Endpoint Agent é removido do computador.

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, incluindo o Agente de Administração 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. Para gerir os componentes EDR Optimum e Kaspersky Sandbox, tem de utilizar a Consola Web.

3 Migração da política e das tarefas

Utilize a [Política do Kaspersky Endpoint Agent e o Assistente de Migração de Políticas](#) 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 um estado *Inativo*. Para aplicar a política, abra as propriedades da política, aceite a Declaração da Kaspersky Security Network e defina o estado para *Ativo*.

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 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 [Adicionar chave](#).

Não é necessário ativar a funcionalidade do Kaspersky Sandbox. A funcionalidade do Kaspersky Sandbox estará disponível imediatamente após a atualização e ativação do Kaspersky Endpoint Security for Windows.

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:

- Seleccione os componentes Endpoint Detection and Response Optimum ou Kaspersky Sandbox nas definições do pacote de instalação.
- Exclua o componente Kaspersky Endpoint Agent nas definições do pacote de instalação.

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.

Neste caso, tem de verificar a configuração do Kaspersky Endpoint Agent que está instalado no computador. Se o Kaspersky Endpoint Agent instalado incluir o componente Endpoint Detection and Response Expert (KATA EDR), remova o componente antes de atualizar a aplicação. Se não conseguir remover o componente Endpoint Detection and Response Expert (KATA EDR), o Kaspersky Endpoint Security irá ignorar os componentes EDR Optimum e Kaspersky Sandbox quando atualizar a aplicação. Pode instalar componentes usando a tarefa [Alterar componentes da aplicação](#) depois de atualizar a aplicação.

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 ativas 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 (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 ativas das soluções da Kaspersky. Neste caso, o Kaspersky Endpoint Security seleciona automaticamente os componentes com base na configuração do Kaspersky Endpoint Agent da seguinte forma:

- Se o componente Endpoint Detection and Response Expert (KATA EDR) estiver instalado, o Kaspersky Endpoint Security seleciona o componente Endpoint Agent. O Kaspersky Endpoint Security seleciona apenas o componente Endpoint Agent, mesmo que o Kaspersky Endpoint Agent tenha outros componentes instalados, por exemplo a configuração [KATA EDR+KSB].
- Se o componente Kaspersky Sandbox, EDR Optimum ou a configuração [Kaspersky Sandbox+EDR Optimum] estiver instalada, o Kaspersky Endpoint Security seleciona os componentes relevantes. Isto faz com que o Kaspersky Endpoint Security troque 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 *Crítico* na consola do Kaspersky Security Center:

- Certifique-se de que o computador tem o Agente de Administração 13.2 instalado.
- Verifique o estado de funcionamento dos componentes EDR Optimum e Kaspersky Sandbox, ao consultar o *Relatório de estado dos componentes da aplicação*. Se um componente tiver o estado *Não instalado*, instale os componentes usando a tarefa [Alterar componentes da aplicação](#).
- 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 *Relatório de estado dos componentes da aplicação*. 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](#).

Atualização da aplicação como parte do KATA EDR

Se tiver instalado o Kaspersky Endpoint Agent para integração com a Kaspersky Anti Targeted Attack Platform (o componente Endpoint Detection and Response Expert (KATA EDR)), pode atualizar o Kaspersky Endpoint Security for Windows de qualquer uma das seguintes formas:

- Usando uma tarefa de instalação remota.

Para tal, tem de editar as definições seguintes:

- Exclua os componentes Endpoint Detection and Response Optimum e Kaspersky Sandbox nas definições do pacote de instalação.
- Selecione o componente Kaspersky Endpoint Agent nas definições do pacote de instalação. Se o computador já tiver o Kaspersky Endpoint Agent instalado, a aplicação é atualizada para a versão 3.11.
- Utilizando o serviço de atualização da Kaspersky (SMU).

Para fazer isto, deve confirmar a atualização da aplicação. O Kaspersky Endpoint Security exclui o Endpoint Detection and Response Optimum e o Kaspersky Sandbox da instalação. A atualização do Kaspersky Endpoint Agent não é suportada. Pode atualizar o Kaspersky Endpoint Agent manualmente.

- Localmente, usando o Assistente de Configuração.

O Kaspersky Endpoint Security exclui o Endpoint Detection and Response Optimum e o Kaspersky Sandbox da instalação. Se o computador já tiver o Kaspersky Endpoint Agent instalado, a aplicação é atualizada para a versão 3.11.

Managed Detection and Response



O Kaspersky Endpoint Security 11.6.0 implementa o agente integrado para 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](#).

Integração com o MDR

Para configurar a integração com o Kaspersky Managed Detection and Response, deve ativar o componente Endpoint Detection and Response e configurar o Kaspersky Managed Security.

O componente Managed Detection and Response não é compatível com o componente Endpoint Detection and Response Expert.

Deve ativar os componentes seguintes para que a Managed Detection and Response funcione:

- [Kaspersky Security Network \(modo ampliado\)](#).
- [Deteção de comportamento](#).

Ativar estes componentes não é opcional. Caso contrário, o Kaspersky Managed Detection and Response não pode funcionar, porque não recebe os dados de telemetria necessários.

Além disso, o Kaspersky Managed Detection and Response utiliza dados recebidos de outros componentes da aplicação. Ativar este componentes é opcional. Os componentes que fornecem dados adicionais incluem:

- [Proteção contra ameaças da Web](#).
- [Proteção contra ameaças de correio](#).
- [Firewall](#).

Para o Kaspersky Managed Detection and Response funcionar com o Administration Server através do Consola Web do Kaspersky Security Center, deve igualmente 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. Para informações sobre a integração do Kaspersky Security Center com outras soluções da Kaspersky, consulte a Ajuda do [Kaspersky Security Center](#).

A integração com o Kaspersky Managed Detection and Response consiste nos seguintes passos:

1 Configurar a Kaspersky Security Network privada

Ignore este passo se estiver a utilizar o Kaspersky Security Center Cloud Console. O Kaspersky Security Center Cloud Console configura automaticamente o Kaspersky Security Network Local ao instalar o plug-in MDR.

A KSN privada suporta a troca de dados entre os computadores e servidores dedicados da Kaspersky Security Network, mas não da KSN Global.

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 Security Network privada, veja 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 Security Network Privada 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 KSN /private <nome do ficheiro>
```

quando <nome do ficheiro> é o nome do ficheiro de configuração que contém as definições da KSN Privada (formato de ficheiro PKCS7 ou PEM).

Exemplo:

```
avp.com KSN /private C:\kpsn_config.pkcs7
```

Deste modo, o Kaspersky Endpoint Security utilizará o KSN Privado para determinar a reputação dos ficheiros, das aplicações e dos sites. As definições de políticas na secção **Kaspersky Security Network** serão apresentadas no estado de funcionamento: *Rede da KSN: KSN Privado*.

Deve [ativar o modo KSN alargado](#) para que a Managed Detection and Response funcione.

2 Ative o 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](#).

[Como ativar o Managed Detection and Response 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. Selecione a política necessária e clique duas vezes para abrir as propriedades da política.
5. Na janela da política, selecione **Detection and Response** → **Managed Detection and Response**.
6. Selecione a caixa de verificação **Managed Detection and Response**.
7. No bloco **Definições**, clique em **Importar** e selecione o ficheiro BLOB recebido na Consola do Kaspersky Managed Detection and Response. O ficheiro possui a extensão P7.
8. Guarde as suas alterações.

[Como ativar o Managed Detection and Response na Consola Web e na Consola de Nuvem](#)

1. Na janela principal da Consola Web, selecione **Devices** → **Policies & Profiles**.
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 **Detection and Response** → **Managed Detection and Response**.
5. Ative o botão de alternar **Managed Detection and Response**.
6. Clique em **Importar** e selecione o ficheiro BLOB que foi obtido na Consola do Kaspersky Managed Detection and Response. O ficheiro possui a extensão P7.
7. Guarde as suas alterações.

[Como ativar o 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 <nome do ficheiro> /login=<nome de utilizador>  
/password=<palavra-passe>
```

Para executar este comando, [a proteção por password deve estar ativada](#). O utilizador deve ter a permissão **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 carregará 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 *Relatório de estado dos componentes da aplicação*. 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.

Migração do Kaspersky Endpoint Agent

O Kaspersky Endpoint Security versão 11 e posteriores suporta a solução MDR. O Kaspersky Endpoint Security versões 11–11.5.0 envia dados de telemetria para o Kaspersky Managed Detection and Response apenas para ativar a deteção de ameaças. O Kaspersky Endpoint Security versão 11.6.0 tem todas as funcionalidades do agente integrado (Kaspersky Endpoint Agent).

Se estiver a utilizar o Kaspersky Endpoint Security versões 11–11.5.0, tem de atualizar as bases de dados para a versão mais recente, para funcionar com a solução MDR. Também tem de instalar o Kaspersky Endpoint Agent.

Se estiver a utilizar o Kaspersky Endpoint Security versão 11.6.0 ou posterior, para funcionar com a solução MDR, tem de selecionar o componente Managed Detection and Response ao instalar a aplicação. Neste caso, não tem de instalar o Kaspersky Endpoint Agent.

Para migrar o Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows:

1. Configure a integração com o Kaspersky Managed Detection and Response na política do Kaspersky Endpoint Security.
2. Desative o componente Managed Detection and Response na política do Kaspersky Endpoint Agent.

Se a política do Kaspersky Endpoint Security também se aplicar aos computadores que não têm o Kaspersky Endpoint Security versões 11–11.5.0 instalado, primeiro tem de criar uma política separada do Kaspersky Endpoint Agent para esses computadores. Na nova política, configure a integração com o Kaspersky Managed Detection and Response.

Endpoint Detection and Response



O Kaspersky Endpoint Security 11.7.0 agora tem um agente integrado para a solução Kaspersky Endpoint Detection and Response Optimum (doravante também referida como "EDR Optimum"). O Kaspersky Endpoint Security 11.8.0 agora 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. 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](#).

O Kaspersky Endpoint Detection and Response utiliza as seguintes ferramentas de Informações sobre Ameaças:

- 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. O Kaspersky Endpoint Detection and Response utiliza a solução Kaspersky Private Security Network (KPSN), que envia dados para servidores regionais sem enviar dados de dispositivos para a KSN.
- 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](#).

Integração com o Kaspersky Endpoint Detection and Response

Para integrar com o Kaspersky Endpoint Detection and Response, tem de adicionar o componente Endpoint Detection and Response Optimum (EDR Optimum) ou o componente Endpoint Detection and Response Expert (EDR Expert), e configurar o Kaspersky Endpoint Security.

Os componentes EDR Optimum e EDR Expert não são compatíveis. Além disso, o componente EDR Expert não é compatível com o componente Managed Detection and Response.

Para o Endpoint Detection and Response funcionar, tem de cumprir as seguintes condições:

- Kaspersky Security Center 13.2. Nas versões anteriores do Kaspersky Security Center, é impossível ativar a funcionalidade Endpoint Detection and Response.
- 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](#).
 - [Detecção 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 seleccionar o componente EDR Optimum ou EDR Expert durante a [instalação](#) ou [atualização](#), bem como através da tarefa [Change application components](#). Tem de reiniciar o computador para terminar a atualização da aplicação com os novos componentes.

Depois da execução da tarefa *Alterar componentes da aplicação*, o estado da tarefa é apresentado incorretamente. Em vez de *Concluído com êxito*, a tarefa tem o estado *Agendada*. No entanto, a tarefa ainda pode ser concluída com êxito. Certifique-se de que o novo componente está instalado nas propriedades do computador da consola do Kaspersky Security Center (**Aplicações** → **Kaspersky Endpoint Security for Windows** → **Componentes**) ou na interface da aplicação local.

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 estará imediatamente disponível após a [ativação do Kaspersky Endpoint Security for Windows](#).

- Extensão da licença para utilização do EDR Optimum ou do 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 instaladas 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](#).

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 Consola Web e na Cloud Console](#)



1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Detection and Response** → **Endpoint Detection and Response**.
5. Ative o botão de alternar **Endpoint Detection and Response**.
6. Guarde as suas alterações.

O componente Kaspersky Endpoint Detection and Response está ativado. Verifique o estado de funcionamento do componente, ao consultar o *Relatório de estado dos componentes da aplicação*. 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** 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 e da Cloud Console. Por exemplo, pode descarregar um ficheiro da quarentena para análise na Consola Web e na Cloud Console.

- Dados de cadeia de desenvolvimento de ameaças.

Os dados são necessários para obter informações sobre ameaças detetadas num computador na Consola Web e na Cloud Console. Pode ver detalhes de deteção e tomar medidas de resposta na Consola Web e na Cloud Console.

[Como ativar a transferência de dados para o Servidor de Administração na Consola Web e na Cloud Console](#)

1. Na janela principal da Consola Web, selecione **Devices** → **Policies & Profiles**.
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 **Definições gerais** → **Relatórios e Armazenamento**.
5. Selecione as caixas seguintes no bloco **Transferência de dados para o Servidor de administração**:
 - **Sobre os Ficheiros da Quarentena**.
 - **Sobre a cadeia de desenvolvimento de ameaças**.
6. Guarde as suas alterações.

Migração do Kaspersky Endpoint Agent

Se estiver a utilizar o Kaspersky Endpoint Security 11.7.0 ou uma versão mais recente com o componente EDR Optimum (agente incorporado) instalado, o suporte de integração com o Kaspersky Endpoint Detection and Response Optimum está imediatamente disponível após a instalação. O componente EDR Optimum não é compatível com o Kaspersky Endpoint Agent. Se o Kaspersky Endpoint Agent estiver instalado no computador, quando o Kaspersky Endpoint Security for atualizado para a versão 11.7.0, o Kaspersky Endpoint Detection and Response Optimum continuará a funcionar com o Kaspersky Endpoint Security. ([migrar a configuração \[KES+KEA\] para \[KES+agente incorporado\]](#)). Além disso, o Kaspersky Endpoint Agent será removido do computador. Para concluir a migração do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows, tem de transferir as definições de tarefas e políticas através do [Assistente de migração](#).

Se estiver a utilizar o Kaspersky Endpoint Security 11.4.0–11.6.0 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.

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).

O componente EDR 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.

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 *Verificação IOC* 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 de Verificação IOC

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](#)

Criar uma tarefa de Verificação IOC

Pode criar tarefas *Verificação IOC* manualmente:

- Nos detalhes do alerta.

As *informações da deteção* é uma ferramenta para visualizar todas as informações recolhidas sobre uma ameaça detetada e gerir ações de resposta. 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.

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 Verificação IOC:

1. Na janela principal da Consola de Web, seleccione **Devices** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **Add**.

O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

a. Na lista suspensa **Application**, seleccione **Kaspersky Endpoint Security for Windows (11.8.0)**.

b. Na lista pendente **Tipo de tarefa**, seleccione **Verificação IOC**.

- c. No campo **Task name**, introduza uma breve descrição.
- d. No bloco **Select 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 *Verificação IOC* 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 seleccionar manualmente a conta de utilizador que tem acesso a esta unidade nas propriedades da tarefa.

6. Sair do 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 **Definições da verificação IOC**.
10. Carregue os IOC files para procurar indicadores de comprometimento.
Depois de carregar os ficheiros de IOC, é possível visualizar a lista de indicadores dos IOC files.

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. Configure ações na deteção de IOC:
- **Isolate computer 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](#).
 - **Mova a cópia para a Quarentena, elimine o objeto.** 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.
 - **Executar verificação de áreas críticas.** Se esta opção for selecionada, o Kaspersky Endpoint Security executa a tarefa [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.

12. Aceda à secção **Avançadas**.

13. 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 *Verificação IOC* 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 logs - EventLogItem.** Introduza o período de tempo no qual os eventos foram registados. Também pode seleccionar os registos de eventos do Windows que devem ser utilizados para a verificação IOC. Por defeito, são seleccionados os seguintes registos de eventos: registo de eventos da aplicação, registo de eventos do sistema e registo de eventos de segurança.

Para o tipo de dados **Windows registry - RegistryItem**, o Kaspersky Endpoint Security verifica [um conjunto de chaves de registo](#).

14. Guarde as suas alterações.

15. Selecione a caixa de verificação junto à tarefa.

16. Clique no botão **Run**.

Deste modo, o Kaspersky Endpoint Security procura indicadores de comprometimento do computador. Pode visualizar os resultados da tarefa nas propriedades da tarefa na secção **Resultados**. 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.

Mover ficheiro para Quarentena

Ao reagir a ameaças, o Kaspersky Endpoint Detection and Response Optimum pode criar tarefas *Move file to Quarantine*. A *Quarentena* é um armazenamento local especial no computador para onde os ficheiros infetados por vírus ou não desinfetáveis são movidos. Os ficheiros na quarentena são armazenados num estado encriptado e não põem em risco a segurança do dispositivo. O Kaspersky Endpoint Security apenas utiliza a Quarentena ao trabalhar com as soluções Kaspersky Sandbox e Kaspersky Endpoint 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](#).

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.

O tamanho do ficheiro não deve exceder 100 MB.

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 Move file to Quarantine:

1. Na janela principal da Consola de Web, seleccione **Devices** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **Add**.

O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

- a. Na lista suspensa **Application**, seleccione **Kaspersky Endpoint Security for Windows (11.8.0)**.

- b. Na lista pendente **Tipo de tarefa**, seleccione **Move file to Quarantine**.

- c. No campo **Task name**, introduza uma breve descrição.

- d. No bloco **Select devices to which the task will be assigned**, seleccione o âmbito de tarefa.

4. Seleccione os dispositivos de acordo com a opção do âmbito da tarefa seleccionada. Clique no botão **Next**.

5. Introduza as credenciais da conta do utilizador cujos direitos deseja usar para executar a tarefa. Clique no botão **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 **Concluir**.

Será apresentada uma nova tarefa na lista de tarefas.

7. Clique em nova tarefa.

É apresentada a janela de propriedades da tarefa.

8. Seleccione o separador **Application settings**.

9. Na lista de ficheiros, clique em **Adicionar**.

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 *File not found*.

11. Clique no botão **Save**.
12. Selecione a caixa de verificação junto à tarefa.
13. Clique no botão **Run**.

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 *Concluída*, 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.

A tarefa *Move file to Quarantine* pode terminar apresentando o erro *Acesso negado* 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 falhar com o erro *Espaço insuficiente no armazenamento da Quarentena* se estiver a tentar mover um ficheiro demasiado grande para a Quarentena. 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. Para obter o ficheiro, deve criar uma tarefa dedicada. Como resultado da execução da tarefa, o ficheiro é guardado na Quarentena. Pode transferir este ficheiro da Quarentena para o seu computador utilizando a Consola Web. No computador do utilizador, o ficheiro permanece na sua pasta original.

O tamanho do ficheiro não deve exceder 100 MB.

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 de Web, selecione **Devices** → **Tasks**.
A lista de tarefas é aberta.
2. Clique no botão **Add**.

O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

a. Na lista suspensa **Application**, selecione **Kaspersky Endpoint Security for Windows (11.8.0)**.

b. Na lista pendente **Tipo de tarefa**, selecione **Obter ficheiro**.

c. No campo **Task name**, introduza uma breve descrição.

d. No bloco **Select 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 no botão **Next**.

5. Introduza as credenciais da conta do utilizador cujos direitos deseja usar para executar a tarefa. Clique no botão **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 **Concluir**.

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 **Adicionar**.

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 *File not found*.

11. Clique no botão **Save**.

12. Selecione a caixa de verificação junto à tarefa.

13. Clique no botão **Run**.

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.

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 de Web, seleccione **Devices** → **Tasks**.

A lista de tarefas é aberta.

2. Clique no botão **Add**.

O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

a. Na lista suspensa **Application**, seleccione **Kaspersky Endpoint Security for Windows (11.8.0)**.

b. Na lista pendente **Tipo de tarefa**, seleccione **Delete file**.

c. No campo **Task name**, introduza uma breve descrição.

d. No bloco **Select devices to which the task will be assigned**, seleccione o âmbito de tarefa.

4. Seleccione os dispositivos de acordo com a opção do âmbito da tarefa seleccionada. Clique no botão **Next**.

5. Introduza as credenciais da conta do utilizador cujos direitos deseja usar para executar a tarefa. Clique no botão **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 **Concluir**.

Será apresentada uma nova tarefa na lista de tarefas.

7. Clique em nova tarefa.

É apresentada a janela de propriedades da tarefa.

8. Seleccione o separador **Application settings**.

9. Na lista de ficheiros, clique em **Adicionar**.

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 *File not found*.

11. Clique no botão **Save**.

12. Seleccione a caixa de verificação junto à tarefa.

13. Clique no botão **Run**.

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 *Concluída*, 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 *Acesso negado* 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.

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 Início do processo:

1. Na janela principal da Consola de Web, seleccione **Devices** → **Tasks**.
A lista de tarefas é aberta.
2. Clique no botão **Add**.
O Assistente de Tarefas é iniciado.
3. Configurar as definições de tarefa:
 - a. Na lista suspensa **Application**, seleccione **Kaspersky Endpoint Security for Windows (11.8.0)**.
 - b. Na lista pendente **Task type**, seleccione **Process start**.
 - c. No campo **Task name**, introduza uma breve descrição.
 - d. No bloco **Select devices to which the task will be assigned**, seleccione o âmbito de tarefa.
4. Seleccione os dispositivos de acordo com a opção do âmbito da tarefa seleccionada. Clique no botão **Next**.
5. Introduza as credenciais da conta do utilizador cujos direitos deseja usar para executar a tarefa. Clique no botão **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 **Concluir**.
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.

Por exemplo, se desejar executar um utilitário (`utility.exe`) que guarda as informações sobre a configuração do computador num ficheiro chamado `conf.txt`, deve introduzir os seguintes valores:

- **Executable command** – `utility.exe`
- **Command-line arguments** – `/R conf.txt`
- **Path to the working folder** – `C:\Users\admin\Diagnostic\`

Em alternativa, no campo **Executable command** campo, pode introduzir `C:\Users\admin\Diagnostic\utility.exe /R conf.txt`. Neste caso, não precisa de introduzir as restantes configurações.

11. Clique no botão **Save**.

12. Selecione a caixa de verificação junto à tarefa.

13. Clique no botão **Run**.

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 **Resultados**.

Terminação de Processo

Pode terminar processos remotamente utilizando a tarefa *Terminação de processo*. Por exemplo, pode terminar remotamente um utilitário de teste de velocidade da Internet que foi iniciado utilizando a [tarefa Início do 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 *Terminar processo* tem as seguintes limitações:

- Os processos de Objetos críticos do sistema (SCO) não podem ser terminados. SCO são ficheiros que o sistema operativo e a aplicação Kaspersky Endpoint Security for Windows requerem para serem executados.
- 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 Terminação de processo:

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

A lista de tarefas é aberta.

2. Clique no botão **Add**.

O Assistente de Tarefas é iniciado.

3. Configurar as definições de tarefa:

- a. Na lista suspensa **Application**, selecione **Kaspersky Endpoint Security for Windows (11.8.0)**.

- b. Na lista pendente **Tipo de tarefa**, selecione **Terminação de processos**.
 - c. No campo **Task name**, introduza uma breve descrição.
 - d. No bloco **Select 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 no botão **Next**.
 5. Introduza as credenciais da conta do utilizador cujos direitos deseja usar para executar a tarefa. Clique no botão **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 **Concluir**.
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 concluir o processo, tem de seleccionar o ficheiro que deseja terminar. Pode seleccionar 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 *File not found*.

10. Na janela de propriedades da tarefa, selecione a secção **Agendar**.
11. 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.

12. Clique no botão **Save**.
13. Selecione a caixa de verificação junto à tarefa.
14. Clique no botão **Run**.

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 **Resultados**.

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. 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. As *Regras de bloqueio de execução* são um conjunto de critérios que são tidos em consideração para o bloqueio. 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 hash (SHA256 ou MD5) ou caminho do ficheiro, ou o caminho do ficheiro e o hash do ficheiro.

Também pode gerir a prevenção da execução localmente utilizando a [command line](#).

Não é recomendado criar mais de 5000 regras de prevenção de execução, uma vez que tal pode provocar instabilidade do sistema.

As regras de prevenção não abrangem os ficheiros em CD ou imagens ISO. A aplicação não bloqueia a execução ou abertura de tais ficheiros.

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. Este modo está selecionado por predefinição.

- **Ativado.**

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

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 prevenção da execução:

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Detection and Response** → **Endpoint Detection and Response**.
5. Use o botão de alternar **Prevenção da execução** para ativar ou desativar o componente.
6. No bloco **Action on execution or opening of forbidden object**, seleccione o modo de operação do componente:
 - **Block and write to report**. 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.
 - **Log events only**. 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. Este modo está seleccionado por predefinição.
7. Crie uma lista de regras de bloqueio de execução:
 - a. Clique no botão **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 **Tipo**, seleccione o objeto que pretende bloquear: **Executable file, Script, Microsoft Office document**.
Se seleccionar 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.

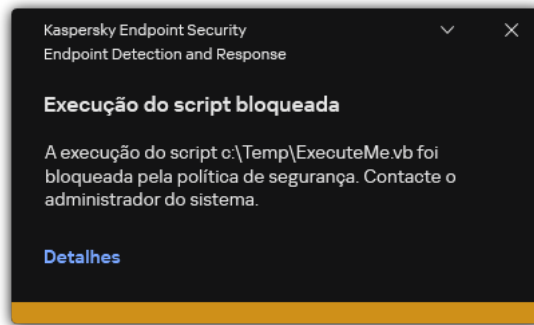
Se o ficheiro estiver localizado numa unidade de rede, introduza o caminho do ficheiro a partir dos caracteres `\\` e não da letra da unidade. Por exemplo, `\\server\shared_folder\file.exe`. Se o caminho do ficheiro contiver uma letra da unidade de rede, o Kaspersky Endpoint Security não bloqueia o ficheiro ou script.

A prevenção da execução suporta [um conjunto de extensões de ficheiros Office](#) e [um conjunto de interpretadores de script](#).

e. Clique em **OK**.

8. 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).

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 agente de Administração do Kaspersky Security Center.

Gerir o isolamento da rede

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.

Pode configurar a ativação automática do isolamento da rede em resposta a uma deteção de IOC. Também pode ativar e desativar manualmente o isolamento da rede.

Pode ativar o isolamento da rede:

- Nos detalhes do alerta (apenas para EDR Optimum).

As *informações da detecção* é uma ferramenta para visualizar todas as informações recolhidas sobre uma ameaça detetada. As informações da detecção incluem, por exemplo, o histórico dos ficheiros que aparecem no computador. Para conhecer os detalhes sobre a gestão de detecção, 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.

Como configurar a ativação automática do isolamento da rede em resposta a uma detecção de IOC

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

A lista de tarefas é aberta.

2. Clique na tarefa **Verificação IOC** do Kaspersky Endpoint Security.

É apresentada a janela de propriedades da tarefa.

Se necessário, crie a tarefa [Verificação IOC](#).

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

4. No bloco **Action on IOC detection**, selecione as caixas de verificação **Take response actions after an IOC is found** e **Isolate computer from the network**.

5. 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.

Como ativar manualmente o isolamento da rede de um computador

1. Na janela principal da Consola Web, selecione **Devices** → **Managed devices**.

2. Selecione um computador para o qual quer configurar definições da aplicação locais.

As propriedades do computador são apresentadas.

3. Selecione o separador **Aplicações**.

4. Clique em **Kaspersky Endpoint Security for Windows**.

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 **Isolamento da rede**, selecione **Isolate computer from the network**.

Pode configurar a desativação automática do isolamento da rede depois de decorrido 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. Após desativar o isolamento da rede, o computador pode utilizar a rede sem restrições.

Como configurar o atraso da desativação automática do isolamento da rede de um computador

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Detection and Response** → **Endpoint Detection and Response**.
5. No bloco **Isolamento da rede**, clique em **Configure computer unlock settings**.
6. Esta ação abre uma janela; nesta janela, seleccione a caixa de verificação **Automatically unlock isolated computer in N hours** e introduza o atraso para a desativação automática do 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, seleccione **Devices** → **Managed devices**.
2. Seleccione um computador para o qual quer configurar definições da aplicação locais.
As propriedades do computador são apresentadas.
3. Seleccione o separador **Aplicações**.
4. Clique em **Kaspersky Endpoint Security for Windows**.
As definições da aplicação locais são apresentadas.
5. Seleccione o separador **Application settings**.
6. Aceda a **Detection and Response** → **Endpoint Detection and Response**.
7. No bloco **Isolamento da rede**, seleccione **Unblock computer isolated from the network**.

Também pode desativar localmente o isolamento da rede utilizando a [Command line](#).

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](#)

1. Na janela principal da Consola Web, selecione **Devices** → **Policies & Profiles**.
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 **Detection and Response** → **Endpoint Detection and Response**.
5. No bloco **Exclusões de isolamento da rede**, clique em **Exclusões**.
6. 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.
7. Se necessário, pode adicionar uma exclusão de isolamento da rede manualmente. Para tal, na janela da lista de exclusões, clique em **Adicionar** e edite manualmente as definições da ligação de rede.
8. 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.

Anexo 1. 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	Extensão 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 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 2. Interpretadores de script suportados

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
- msixexec.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 3. Âmbito de verificação IOC no registo (RegistryItem)

Quando adiciona o tipo de dados RegistryItem ao âmbito de verificação IOC, o Kaspersky Endpoint Security verifica as seguintes chaves de registo:

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 4. 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.
- Se durante a criação da Tarefa de verificação IOC na linha de comandos tiver carregado ficheiros IOC (alguns dos quais não são suportados), a aplicação utiliza apenas os ficheiros IOC suportados ao executar a tarefa. Se durante a criação da Tarefa de verificação IOC na linha de comandos, todos os ficheiros IOC 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. Dito isto, o tamanho total de todos os ficheiros adicionados à coleção IOC pode exceder os 2 MB.
- É recomendado criar um IOC file por ameaça. Tal facilita a análise dos resultados da tarefa Verificação 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](#)

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 (as an exception from the set)
----------------------	--

	<p>contains containsnot (as an exception from the set) OpenIOC 1.1:</p> <p>is contains starts-with ends-with matches greater-than less-than</p>
Atributos da condição suportados	<p>OpenIOC 1.1:</p> <p>preserve-case negate</p>
Operadores suportados	<p>AND OR</p>
Tipos de dados suportados	<p>"date": data (condições aplicáveis: is, greater-than, less-than)</p> <p>"int": número inteiro (condições aplicáveis: is, greater-than, less-than)</p> <p>"string": cadeia (condições aplicáveis: is, contains, matches, starts-with, ends-with)</p> <p>"duration": duração em segundos (condições aplicáveis: is, greater-than, less-than)</p>
Funcionalidades da interpretação de tipos de dados	<p>Os tipos de dados "boolean string", "restricted string", "md5", "IP", "sha256" e "base64Binary" são interpretados como uma cadeia.</p> <p>A aplicação suporta a interpretação do campo Conteúdo para os tipos de dados int e date sempre que seja apresentado na forma de intervalos:</p> <p>OpenIOC 1.0: Utilizar o operador TO no campo Conteúdo: <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></p> <p>OpenIOC 1.1: Utilizar as condições greater-than e greater-than Utilizar o operador TO no campo Conteúdo 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.</p>

Kaspersky Sandbox



O Kaspersky Endpoint Security 11.7.0 possui agora um agente integrado para integração com a solução Kaspersky Sandbox. A *solução Kaspersky Sandbox* deteta e bloqueia automaticamente ameaças avançadas em computadores. O Kaspersky Sandbox analisa o comportamento do objeto para detetar atividades maliciosas e atividades características de ataques direcionados à infraestrutura de TI da organização. O Kaspersky Sandbox analisa e verifica objetos em servidores

especiais com imagens virtuais implementadas de sistemas operativos Microsoft Windows (servidores do Kaspersky Sandbox). Para obter mais informações sobre a solução, consulte a [Ajuda do Kaspersky Sandbox](#).

As seguintes configurações são possíveis para a solução Kaspersky Sandbox:

Kaspersky Sandbox 2.0

O Kaspersky Sandbox 2.0 suporta a configuração [KES+agente integrado].

Requisitos mínimos:

- Kaspersky Endpoint Security 11.7.0 for Windows ou posterior.
- O Kaspersky Endpoint Agent não é obrigatório.
- Kaspersky Security Center 13.2.

Kaspersky Sandbox 1.0

O Kaspersky Sandbox 1.0 suporta a configuração [KES+KEA].

Requisitos mínimos:

- Kaspersky Endpoint Security 11.2.0 – 11.6.0 for Windows.
- Kaspersky Endpoint Agent 3.8.
Pode instalar o Kaspersky Endpoint Agent a partir do kit de distribuição do Kaspersky Endpoint Security for Windows.
- Kaspersky Security Center 11.

Integração com o Kaspersky Sandbox

Adicionar o componente Kaspersky Sandbox é necessário para integração com o componente Kaspersky Sandbox. Pode seleccionar o componente Kaspersky Sandbox durante a [instalação](#) ou [atualização](#), bem como através da [tarefa *Alterar componentes da aplicação*](#).

Depois da execução da tarefa *Alterar componentes da aplicação*, o estado da tarefa é apresentado incorretamente. Em vez de *Concluído com êxito*, a tarefa tem o estado *Agendada*. No entanto, a tarefa ainda pode ser concluída com êxito. Certifique-se de que o novo componente está instalado nas propriedades do computador da consola do Kaspersky Security Center (**Aplicações** → **Kaspersky Endpoint Security for Windows** → **Componentes**) ou na interface da aplicação local.

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 **Devices** → **Policies & Profiles**.
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 **Definições gerais** → **Relatórios e Armazenamento**.
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 **Console settings** → **Integration**.
2. Aceda à secção **Cross-service integration**.
3. Ative o botão de alternar **Establish a background connection for cross-service integration**.
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.

- O componente Kaspersky Sandbox está ativado.

Pode ativar ou desativar a integração com o Kaspersky Sandbox na Consola Web ou localmente usando a [linha de comandos](#).

Para ativar ou desativar a integração com o Kaspersky Sandbox:

1. Na janela principal da Consola Web, selecione **Devices** → **Policies & Profiles**.
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 **Detection and Response** → **Kaspersky Sandbox**.
5. Use o botão de alternar **Integration with Kaspersky Sandbox** para ativar ou desativar o componente.
6. Guarde as suas alterações.

Deste modo, o componente Kaspersky Sandbox está ativado. Verifique o estado de funcionamento do componente, ao consultar o *Relatório de estado dos componentes da aplicação*. Pode também ver o estado de funcionamento de um componente em [relatórios](#) na interface local do Kaspersky Endpoint Security. O componente **Kaspersky Sandbox** será adicionado à lista de componentes do Kaspersky Endpoint Security.

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 Código de erro: XXX formato (por exemplo, 0xa67b01f4), contacte o [Suporte técnico](#).

Migração do Kaspersky Endpoint Agent

Se estiver a utilizar o Kaspersky Endpoint Security 11.7.0 ou uma versão mais recente com o componente Kaspersky Sandbox (agente incorporado) instalado, a interoperabilidade com a solução Kaspersky Sandbox estará disponível imediatamente após a instalação. O componente Kaspersky Sandbox não é compatível com o Kaspersky Endpoint Agent. Se o Kaspersky Endpoint Agent estiver instalado no computador, quando o Kaspersky Endpoint Security for atualizado para a versão 11.7.0, o Kaspersky Sandbox continuará a funcionar com o Kaspersky Endpoint Security ([migrando a configuração \[KES+KEA\], para \[KES+agente incorporado\]](#)). Além disso, o Kaspersky Endpoint Agent será removido do computador. Para concluir a migração do Kaspersky Endpoint Agent para o Kaspersky Endpoint Security for Windows, tem de transferir as definições de tarefas e políticas através do [Assistente de migração](#).

Se estiver a utilizar o Kaspersky Endpoint Security 11.4.0–11.6.0 para interoperabilidade com o Kaspersky Sandbox, a aplicação inclui o Kaspersky Endpoint Agent. Pode instalar o Kaspersky Endpoint Agent lado a lado com o Kaspersky Endpoint Security.

O componente Kaspersky Sandbox que faz parte do Kaspersky Endpoint Security suporta a interoperabilidade com a solução Kaspersky Sandbox 2.0. A solução Kaspersky Sandbox 1.0 não é compatível.

Adição de um certificado TLS

Para configurar uma ligação fiável com os servidores do Kaspersky Sandbox, deve preparar um certificado TLS. Em seguida, deve adicionar o certificado aos servidores do Kaspersky Sandbox e à política do Kaspersky Endpoint Security. Para obter mais informações sobre como preparar o certificado e adicionar o certificado aos servidores, consulte a [Ajuda do Kaspersky Sandbox](#).

Pode adicionar um Certificado TLS na Consola Web ou localmente utilizando a [Linha de comandos](#).

Para adicionar um Certificado TLS na Consola Web:

1. Na janela principal da Consola Web, selecione **Devices** → **Policies & Profiles**.

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 **Detection and Response** → **Kaspersky Sandbox**.

5. Clique na ligação **Server connection settings**.

Tal abre a janela de definições de ligação do servidor do Kaspersky Sandbox.

6. Em **Server TLS certificate**, clique em **Adicionar** e selecione o ficheiro de certificado TLS.

O Kaspersky Endpoint Security só pode ter um certificado TLS para um servidor do Kaspersky Sandbox. Se tiver previamente adicionado um certificado TLS, o certificado em causa será revogado. Apenas o último certificado adicionado é utilizado.

7. Estabeleça as definições avançadas de ligações para servidores do Kaspersky Sandbox:

- **Tempo limite.** Tempo limite de ligação para o servidor Kaspersky 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 Kaspersky Sandbox se a velocidade da sua ligação for baixa ou instável. O tempo limite recomendado do pedido é de 0,5 segundos ou menos.
- **Kaspersky Sandbox request queue.** Tamanho da pasta da fila de pedidos. Quando um objeto é acedido no computador (ficheiro executável iniciado ou documento aberto, por exemplo, em formato DOCX ou PDF), o Kaspersky Endpoint Security também pode enviar o objeto para ser verificado pelo Kaspersky Sandbox. Se houver vários pedidos, 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 Kaspersky 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.

8. 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.

Adicionar servidores do Kaspersky Sandbox

Para ligar computadores aos servidores do Kaspersky Sandbox com imagens virtuais de sistemas operativos, deve introduzir uma porta e um endereço de servidor. Para obter mais informações sobre como implementar imagens virtuais e configurar servidores do Kaspersky Sandbox, consulte a Ajuda do [Kaspersky Sandbox](#).

Para adicionar servidores Kaspersky Sandbox à Consola Web:

1. Na janela principal da Consola Web, selecione **Devices** → **Policies & Profiles**.

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. Acesse a **Detection and Response** → **Kaspersky Sandbox**.
5. Em **Servidores do Kaspersky Sandbox**, selecione **Adicionar**.
6. Esta ação abre uma janela; na janela, introduza a porta e o endereço do servidor do Kaspersky Sandbox (IPv4, IPv6, DNS).
7. Guarde as suas alterações.

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 *Verificação IOC* 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 de Verificação IOC

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 da tarefa de Verificação IOC

O Kaspersky Sandbox pode criar tarefas de *Verificação IOC* 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 Verificação IOC:

1. Na janela principal da Consola de Web, selecione **Devices** → **Tasks**.
A lista de tarefas é aberta.
2. Clique na tarefa **Verificação IOC** do Kaspersky Endpoint Security.

É apresentada a janela de propriedades da tarefa.

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

4. Aceda à secção **Definições da verificação IOC**.

5. Configure ações na deteção de IOC:

- **Mova a cópia para a Quarentena, elimine o objeto.** 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.
- **Executar verificação de áreas críticas.** Se esta opção for selecionada, o Kaspersky Endpoint Security executa a tarefa [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.

6. Configure o modo de execução da tarefa de Verificação IOC utilizando a caixa de verificação **Executar apenas quando o computador está inativo**. Esta caixa de verificação ativa/desativa a função que suspende a tarefa de *Verificação IOC* quando os recursos do computador são limitados. O Kaspersky Endpoint Security pausa a tarefa de *Verificação IOC* se a proteção de ecrã estiver desativada e o computador estiver desbloqueado.

Esta opção de agendamento permite-lhe conservar os recursos do computador quando o computador está a ser utilizado.

7. Guarde as suas alterações.

Pode visualizar os resultados da tarefa nas propriedades da tarefa na secção **Resultados**. 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.

Gerir a Quarentena

A *Quarentena* é um armazenamento local especial no computador para onde os ficheiros infetados por vírus ou não desinfetáveis são movidos. Os ficheiros na quarentena são armazenados num estado encriptado e não põem em risco a segurança do dispositivo. O Kaspersky Endpoint Security apenas utiliza a Quarentena ao trabalhar com as soluções Kaspersky Sandbox e Kaspersky Endpoint 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](#).

O Kaspersky Endpoint Security utiliza a conta de sistema (SYSTEM) para colocar os ficheiros na quarentena.

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). 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 200 MB. Quando o tamanho máximo é atingido, o Kaspersky Endpoint Security elimina automaticamente os ficheiros mais antigos da Quarentena.

Para configurar o tamanho máximo da Quarentena:

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Definições gerais** → **Relatórios e Armazenamento**.
5. No bloco **Quarentena** configure o tamanho da Quarentena:
 - **Limitar o tamanho da Quarentena a N MB.** Tamanho máximo da quarentena em MB. Por exemplo, pode definir o tamanho máximo da quarentena como 200 MB. Quando a Quarentena atinge o tamanho máximo, o Kaspersky Endpoint Security envia o evento correspondente ao 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.
 - **Notificar quando o armazenamento da Quarentena alcançar N por cento.** 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.

Para ativar a transferência de dados de ficheiros em quarentena para o Kaspersky Security Center:

1. Na janela principal da Consola Web, seleccione **Devices** → **Policies & Profiles**.
2. Clique no nome da política do Kaspersky Endpoint Security.
É apresentada a janela de propriedades da política.
3. Seleccione o separador **Application settings**.
4. Aceda a **Definições gerais** → **Relatórios e Armazenamento**.

5. Na secção **Data transfer to Administration Server**, selecione a caixa de verificação **About Quarantine files**.

6. Guarde as suas alterações.

Deste modo, na Consola Web, pode ver a lista de ficheiros em quarentena num computador (**Operações** → **Armazenamentos** → **Quarentena**) Pode utilizar a Consola Web para gerir objetos na quarentena (restaurar, eliminar, adicionar, etc).

Kaspersky Security for Windows Server



O Kaspersky Endpoint Security 11.8.0 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 informações detalhadas sobre como a solução funciona, consulte a [Ajuda do Kaspersky Security for Windows Server](#). A partir do Kaspersky Endpoint Security 11.8.0, pode migrar do KSWs para o Kaspersky Endpoint Security for Windows e usar a mesma solução para proteger estações de trabalho e servidores.

Instalar o KES sobre o KSWs

O Kaspersky Endpoint Security (KES) oferece suporte à funcionalidade básica da aplicação Kaspersky Security for Windows Server (KSWs). A partir do Kaspersky Endpoint Security versão 11.8.0, pode usar o KES em vez do KSWs.

Antes de instalar o KES, terá de desinstalar o KSWs. Pode desinstalar a aplicação remotamente através da tarefa [Desinstalar aplicação remotamente](#) ou [localmente no servidor](#). Depois de desinstalar o KSWs, poderá ser necessário reiniciar o servidor. Se quiser instalar o Kaspersky Endpoint Security sem reiniciar o computador, deverá assegurar-se de que o Kaspersky Security for Windows Server foi desinstalado completamente. Consulte abaixo a lista de ficheiros e serviços a verificar. Se a aplicação não for desinstalada completamente, poderão ocorrer falhas do servidor após a instalação do Kaspersky Endpoint Security. Recomendamos também que verifique se a aplicação foi desinstalada completamente se tiver usado o utilitário kavremove. [O utilitário Kavremove](#) não suporta o KSWs.

Depois de desinstalar o KSWs, [instale o Kaspersky Endpoint Security for Windows](#) através de qualquer métodos disponível.

Verificar a remoção do Kaspersky Security for Windows Server

Certifique-se de que o Kaspersky Security for Windows Server foi desinstalada completamente:

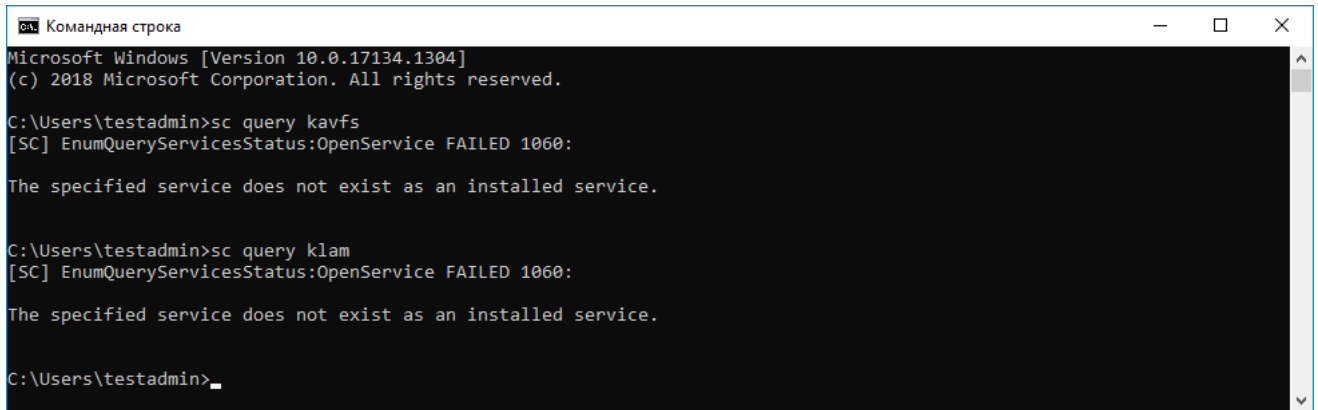
- A pasta %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\ não existe.
- Os seguintes serviços não estão em execução:
 - Kaspersky Security Service (KAVFS)
 - Kaspersky Security Management Service (KAVFSGT)
 - Kaspersky Security Exploit Prevention Service (KAVFSSLP)
 - Kaspersky Security Script Checker Service (KAVFSSCS)

Pode verificar os serviços em execução no Gestor de Tarefas ou através do comando `sc query` (consulte a imagem abaixo).

- Os seguintes controladores não estão instalados:
 - klam.sys
 - klflt.sys

- klrmdisk.sys
- klelaml.sys
- klfltdev.sys
- klips.sys
- klids.sys
- klwtpee

Pode verificar os controladores instalados na pasta C:\Windows\System32\controladores ou através do comando `sc query`. Se o serviço ou controlador estiverem em falta, receberá a seguinte resposta:



Verificar a remoção de serviços e controladores do Kaspersky Security for Windows Server

Se alguns ficheiros ou controladores da aplicação permanecerem no servidor, elimine-os manualmente. Se alguns serviços do Kaspersky Security for Windows Server permanecerem em execução, pare (`sc stop`) e elimine (`sc eliminar`) os mesmos 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).

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 .

<p>A chave do KSWs é adicionada localmente na interface da aplicação.</p>	<p>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.</p>
<p>A chave do KSWs é adicionada ao pacote de instalação.</p>	<p>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.</p>

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 `HELP`. Para ler sobre a sintaxe de um comando específico, digite `HELP <comando>`.

Os caracteres 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 carácter `%`, introduza `%%`.

Instalar a aplicação

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. 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.

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] [/pALLOWREBOOT=1]
[/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<nome do utilizador>
/pKLPASSWD=<password> /pKLPASSWDAREA=<âmbito da password>] [/pENABLETRACES=1|0
/pTRACESLEVEL=<nível de rastreio>] [/s]
```

ou

```
msiexec /i <nome do kit de distribuição> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]
[ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<nome do utilizador> KLPASSWD=<password>
KLPASSWDAREA=<âmbito da password>] [ENABLETRACES=1|0 TRACESLEVEL=<nível de rastreio>]
[/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](#).

EULA=1	<p>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.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>É necessário aceitar os termos do Contrato de Licença do Utilizador Final para instalar a aplicação ou para atualizar a versão da aplicação.</p> </div>
PRIVACYPOLICY=1	<p>Aceitação da Política de Privacidade. O texto da Privacy Policy encontra-se incluído no kit de distribuição do Kaspersky Endpoint Security.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Para instalar a aplicação ou atualizar a versão da aplicação, tem de aceitar a Privacy Policy.</p> </div>
KSN	<p>Aceitar ou recusar participar na Kaspersky Security Network. 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:</p> <ul style="list-style-type: none"> • 1 - acordo para participar na KSN. • 0 – Recusar participar na KSN (valor predefinido). <p>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.</p>
ALLOWREBOOT=1	<p>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.</p> <p>Reinício não é necessário ao instalar o Kaspersky Endpoint Security. O reinício é necessário apenas se precisar de remover aplicações incompatíveis antes da instalação. Reinício pode também ser necessário ao atualizar a versão da aplicação.</p>
SKIPPRODUCTCHECK=1	<p>Desativar a verificação de software incompatível. A lista de softwares incompatíveis 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 incompatível, a instalação do Kaspersky Endpoint Security será cancelada.</p>
SKIPPRODUCTUNINSTALL=1	<p>Desativar a remoção automática do software incompatível detetado. Se nenhum valor for definido para este parâmetro, o Kaspersky Endpoint Security tentará remover o software incompatível.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>A remoção automática de software incompatível não pode ser ativada ao instalar o Kaspersky Endpoint Security utilizando o instalador msisexec. Utilize o setup_kes.exe para ativar a remoção automática de software incompatível.</p> </div>

KLLOGIN	<p>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.</p>
KLPASSWD	<p>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).</p> <p>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.</p>
KLPASSWDAREA	<p>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 carácter ";" para especificar vários valores. Valores disponíveis:</p> <ul style="list-style-type: none"> • 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.
ENABLETRACES	<p>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\Traces. Valores disponíveis:</p> <ul style="list-style-type: none"> • 1 – os rastreios estão ativados. • 0 – os rastreios estão desativados (valor padrão).
TRACESLEVEL	<p>Nível de detalhe do rastreio. Valores disponíveis:</p> <ul style="list-style-type: none"> • 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).

	<ul style="list-style-type: none"> • 600 (baixo). Todas as mensagens.
AMPPL	<p>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.</p> <p>A tecnologia AM-PPL está disponível para os sistemas operacionais Windows 10 versão 1703 (RS2) ou posterior e Windows Server 2019.</p> <p>Valores disponíveis:</p> <ul style="list-style-type: none"> • 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.
RESTAPI	<p>Gestão da aplicação com API REST. Para gerir a aplicação com API REST, deve especificar o nome do utilizador (parâmetro RESTAPI_User).</p> <p>Valores disponíveis:</p> <ul style="list-style-type: none"> • 1 - a gestão com API REST é permitida. • 0 - a gestão com API REST é bloqueada (valor predefinido). <p>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.</p>
RESTAPI_User	<p>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 seleccionar um utilizador para trabalhar com API REST.</p> <p>Adicionar um nome de utilizador é um pré-requisito para gerir a aplicação com API REST.</p>
RESTAPI_Port	<p>Porta usada para gerir a aplicação com API REST. A porta 6782 é usada por defeito.</p>
RESTAPI_Certificate	<p>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.</p>
ADMINKITCONNECTOR	<p>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.</p> <p>Valores disponíveis:</p> <ul style="list-style-type: none"> • 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.

Exemplo:

```
setup_ks.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=SAIR; DISPOL.; DESINSTALAR /qn  
  
setup_ks.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](#) - definições gerais para instalação de aplicações
- [install.cfg](#) - definições da operação do Kaspersky Endpoint Security
- 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 configurações dos ficheiros setup.ini, install.cfg e setup.reg, coloque esses ficheiros 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 =<caminho para o ficheiro setup.reg>.

Ativar a aplicação

Para ativar a aplicação a partir da command line,

digite a seguinte cadeia na command line:

```
avp.com license /add <código de ativação ou ficheiro da chave> [/login=<nome do  
utilizador> /password=<password>]
```

Precisa de introduzir as credenciais da conta do utilizador (`/login=<nome do utilizador> /password=<password>`) se a [Proteção por password estiver ativada](#).

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 não assistido, o seu envolvimento no processo de remoção deixa de ser necessário. 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_ks.exe /s /x`
ou
`msiexec.exe /x <GUID> /qn`
<GUID> é a ID única da aplicação. Para ver o GUID da aplicação, utilize o seguinte comando:
`wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber.`
- Se o processo de remoção estiver [protegido por password](#):
`setup_ks.exe /pKLLLOGIN=<nome do utilizador> /pKLPASSWD=<password> /s /x`
ou
`msiexec.exe /x <GUID> KLLLOGIN=<nome de utilizador> KLPASSWD=<password> /qn`

Exemplo:

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLLOGIN=KLAdmin  
KLPASSWD=!Password1 /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.
3. Para executar um comando, escreva:

```
avp.com <comando> [opções]
```

Como resultado, o Kaspersky Endpoint Security executará o comando (ver figura abaixo).

```
Administrator: Command Prompt
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>avp.com SCAN MEMORY
2019-03-04 15:55:04 Scan_Objects$8959 starting 1%
```

Gerir a aplicação a partir da command line

SCAN. Scan de vírus

Execute a tarefa de verificação de vírus.

Sintaxe de comando

```
SCAN [<âmbito da verificação>] [<ação após a deteção da ameaça>] [<tipos de
ficheiro>] [<exclusões da verificação>] [/R[A]:<ficheiro de relatório>] [<tecnologias
de verificação>] [/C:<ficheiro com definições de verificação de vírus>]
```

Âmbito de verificação	
<ficheiros a verificar>	<p>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:</p> <ul style="list-style-type: none"> "C:\Program Files (x86)\Pasta de exemplo" – caminho longo. C:\PROGRA~2\EXAMPL~1 – caminho curto.
/ALL	<p>Execute a tarefa <i>Verificação Completa</i>. O Kaspersky Endpoint Security verifica os seguintes objetos:</p> <ul style="list-style-type: none"> 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
/MEMORY	Verifica a memória do Kernel
/STARTUP	Verifica os objetos que são carregados no arranque do sistema operativo
/MAIL	Verifica a caixa de correio do Outlook
/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.
/@: <ficheiro 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: <ul style="list-style-type: none"> • "C:\Program Files (x86)\Pasta de exemplo" – 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; bloquear se a desinfeção falhar. Se esta opção estiver selecionada, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção não for possível, 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, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção falhar, o Kaspersky Endpoint Security apaga os ficheiros. Esta ação está selecionada por predefinição.
/i3	Desinfete os arquivos infetados que são detetados. Elimine os ficheiros se a desinfeção falhar. Elimine também ficheiros compostos (por exemplo, arquivos) se o ficheiro infetado não puder ser desinfetado ou eliminado.
/i4	Elimine arquivos infetados. Elimine também ficheiros compostos (por exemplo, arquivos) se o ficheiro infetado não puder ser eliminado.
/i8	Solicitar uma ação por parte do utilizador logo que é detetada uma ameaça.
/i9	Solicitar uma ação por parte do utilizador após a conclusão da verificação.

Tipos de ficheiros	
/fe	Ficheiros verificados por extensão. Se esta configuração estiver ativada, o Kaspersky Endpoint Security 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, o Kaspersky Endpoint Security 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, o Kaspersky Endpoint Security 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:b	Bases de dados de correio, e-mails recebidos e enviados são excluídos do âmbito de verificação.
-e:<file mask>	Ficheiros que correspondem à máscara do ficheiro são excluídos do âmbito de verificação. Por exemplo: <ul style="list-style-type: none"> • A máscara *.exe inclui todos os caminhos para ficheiros com a extensão exe. • O exemplo* de máscara incluirá todos os caminhos para ficheiros com o nome EXAMPLE.
-e:<segundos>	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.

Guardar eventos num modo de ficheiro de relatório	
/R:<ficheiro do relatório>	Guarde apenas Critical events no ficheiro de relatório.
/RA:<ficheiro do relatório>	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 considera a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições da verificação. A tecnologia iSwift é um avanço da tecnologia iChecker para o sistema de ficheiros NTFS.

Definições avançadas	
/C:<ficheiro com definições de verificação de vírus>	Ficheiro com definições da tarefa de verificação de vírus. O ficheiro deve ser criado manualmente e guardado no formato TXT. O ficheiro pode ter o seguinte conteúdo: [<âmbito da verificação>] [<ação após de deteção da ameaça>] [<tipos de ficheiro>] [<exclusões da verificação>] [/R[A]:<ficheiro do relatório>] [<tecnologias de verificação>].

Exemplo:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Atualização de bases de dados e módulos de software de aplicação

Execute a tarefa de *Atualização*.

Sintaxe de comando

```
UPDATE [local] ["<origem da atualização>"] [/R[A]:<ficheiro do relatório>][/C:<ficheiro com definições das atualizações>]
```

Atualizar definições de tarefa	
local	<p>Início da tarefa de <i>Atualização</i> que foi criada automaticamente após a instalação da aplicação. Pode alterar as definições da tarefa de <i>Atualização</i> 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 <i>Atualização</i> com as definições predefinidas ou com as definições especificadas no comando. Pode configurar as definições da tarefa <i>Atualização</i> do seguinte modo:</p> <ul style="list-style-type: none">• A opção ATUALIZAR inicia a tarefa de <i>Atualização</i> 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 ATUALIZAÇÃO local inicia a tarefa de <i>Atualização</i> que foi criada automaticamente após a instalação (tarefa predefinida).• A opção ATUALIZAÇÃO <definições das atualizações> inicia a tarefa de <i>Atualização</i> com as definições definidas manualmente (ver abaixo).

Origem da atualização	
«<origem da atualização>»	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.

Guardar eventos num modo de ficheiro de relatório	
/R:<ficheiro do relatório>	Guarde apenas Critical events no ficheiro de relatório.
/RA:<ficheiro do relatório>	Guarde todos os eventos num ficheiro de relatório.

Definições avançadas	
----------------------	--

/C:<ficheiro com definições de atualização>

Ficheiro com as definições da tarefa de *Atualização*. O ficheiro deve ser criado manualmente e guardado no formato TXT. O ficheiro pode ter o seguinte conteúdo: ["<origem da atualização>"] [/R[A]:<ficheiro do relatório>].

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.

Sintaxe de comando

```
ROLLBACK [/R[A]:<ficheiro do relatório>]
```

Guardar eventos num modo de ficheiro de relatório

/R:<ficheiro do relatório>

Guarde apenas Critical events no ficheiro de relatório.

/RA:<ficheiro do relatório>

Guarde todos os eventos num ficheiro de relatório.

Exemplo:

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Rastreo

Ativar / desativar o rastreo. Os [ficheiros de rastreo](#) são armazenados no computador desde que a aplicação esteja a ser utilizada, sendo permanentemente eliminados quando a aplicação é removida. Os ficheiros de rastreo, exceto os ficheiros de rastreo do Agente de Autenticação, são armazenados na pasta %ProgramData%\Kaspersky Lab\KES\Traces. Por predefinição, o rastreo está desativado.

Sintaxe de comando

```
TRACES on|off [<nível de rastreo>] [<definições avançadas>]
```

Tracing level

<nível de rastreo>

Nível de detalhe do rastreo. 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 <code>dbg</code> , <code>ficheiro</code> e parâmetros <code>mem</code> .
dbg	Use a função <code>OutputDebugString</code> e guarde o ficheiro de rastreio. A função <code>OutputDebugString</code> envia uma cadeia de caracteres para o depurador da aplicação para fins de apresentação no ecrã. Para obter informações detalhadas, visite o website MSDN .
ficheiro	Guarde um ficheiro de rastreio (sem limite de tamanho).
rot	Guarde os rastreios num número limitado de ficheiros de tamanho limitado e substitua os ficheiros mais antigos quando o tamanho máximo for alcançado.
mem	Guardar rastreios para descarregar ficheiros.

Exemplos:

- `avp.com TRACES on 500`
- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`
- `avp.com TRACES on 500 dbg mem`
- `avp.com TRACES off file`

START. Iniciar o perfil

Inicie o perfil (por exemplo, para atualizar as bases de dados ou ativar um componente de proteção).

Sintaxe de comando

```
START <perfil> [/R[A]:<ficheiro do relatório>]
```

Perfil	
<perfil>	Nome do perfil. Um <i>Perfil</i> é um componente, tarefa ou funcionalidade do Kaspersky Endpoint Security. Pode ver a lista de perfis disponíveis executando o comando <code>HELP START</code> .

Guardar eventos num modo de ficheiro de

relatório	
/R:<ficheiro do relatório>	Guarde apenas Critical events no ficheiro de relatório.
/RA:<ficheiro do relatório>	Guarde todos os eventos num ficheiro de relatório.

Exemplo:

avp.com START Scan_Objects

STOP. Interromper um perfil

Interrompa o perfil em execução (por exemplo, interrompa a verificação, interrompa a verificação de unidades amovíveis ou desative 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**.

Sintaxe de comando

```
STOP <perfil> /login=<nome do utilizador> /password=<password>
```

Perfil	
<perfil>	Nome do perfil. Um <i>Perfil</i> é um componente, tarefa ou funcionalidade do Kaspersky Endpoint Security. Pode ver a lista de perfis disponíveis executando o comando <code>HELP STOP</code> .

Autenticação	
/login=<nome do utilizador> /password=<password>	Credenciais da conta do utilizador com as permissões de Proteção por palavra-passe necessárias.

STATUS. Estado do perfil

Apresentar informações do estado para [perfis da aplicação](#) (por exemplo, em `execução` ou `completado`). 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.

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

Ver informações estatísticas sobre 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`.

Sintaxe de comando

```
STATISTICS <perfil>
```

RESTORE. Restaurar ficheiros a partir da Cópia de segurança

Pode restaurar um ficheiro da cópia de segurança para a respetiva pasta original. Se já existir um ficheiro com o mesmo nome no caminho especificado, o sufixo "-copy" será anexado ao nome do 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 **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 desinfectado 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\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.

Sintaxe de comando

```
RESTORE [/REPLACE] <nome do ficheiro> /login=<nome do utilizador> /password=  
<password>
```

Definições avançadas	
/REPLACE	Substitui um ficheiro existente.
<nome do ficheiro>	O nome do ficheiro a restaurar.

Autenticação	
/login=<nome do utilizador> /password=<password>	Credenciais da conta do utilizador com as permissões de Proteção por palavra-passe necessárias.

Exemplo:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

EXPORT. Exportar definições da aplicação

Exportar as definições do Kaspersky Endpoint Security para um ficheiro. O ficheiro estará localizado na pasta C:\Windows\SysWOW64.

Sintaxe de comando

```
EXPORT <perfil> <nome do ficheiro>
```

Perfil	
<perfil>	Nome do perfil. Um <i>Perfil</i> é um componente, tarefa ou funcionalidade do Kaspersky Endpoint Security. Pode ver a lista de perfis disponíveis executando o comando <code>HELP EXPORT</code> .

Ficheiro para exportar	
<nome do ficheiro>	O nome do ficheiro para o qual as definições da aplicação serão exportadas. 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.

Exemplos:

- avp.com EXPORT ids ids_config.dat
- avp.com EXPORT fm fm_config.txt

IMPORT. Importar definições da aplicação

Importa as definições do Kaspersky Endpoint Security de um ficheiro criado com o comando `EXPORTAR`.

Para executar este comando, [a proteção por password deve estar ativada](#). O utilizador deve ter a permissão **Configurar as definições da aplicação**.

Sintaxe de comando

```
IMPORT <nome do ficheiro> /login=<nome do utilizador> /password=<password>
```

Ficheiro para importar	
<nome do	O nome do ficheiro do qual as definições da aplicação serão importadas. Pode importar as

ficheiro>	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=<nome do utilizador> /password=<password>	Credenciais da conta do utilizador com as permissões de Proteção por palavra-passe necessárias.

Exemplo:
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1

ADDKEY. Aplicar um ficheiro de chave

Aplice o ficheiro da chave para ativar o Kaspersky Endpoint Security. Se a aplicação já estiver ativada, a chave será adicionada como chave de reserva.

Sintaxe de comando
ADDKEY <nome do ficheiro> /login = <nome do utilizador> /password=<password>

Key file	
<nome do ficheiro>	Nome do key file.

Autenticação	
/login=<nome do utilizador> /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

Execute ações com as chaves de licença do Kaspersky Endpoint Security.

Para executar este comando e remover uma chave de licença, [a proteção por password deve estar ativada](#). O utilizador deve ter a permissão **Remover chave**.

Sintaxe de comando
LICENSE <operação> [/login=<nome do utilizador> /password=<password>]

Operação	

/ADD <nome do ficheiro>	Aplique o ficheiro da chave para ativar o Kaspersky Endpoint Security. Se a aplicação já estiver ativada, a chave será adicionada como chave de reserva.
/ADD <código de ativação>	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 <nome do ficheiro>	Renove sua licença com um ficheiro de chave. Como resultado, é adicionada uma chave de reserva. Esta fica ativa até à licença expirar. Não é possível adicionar uma chave ativa executando este comando.
/REFRESH <código de ativação>	Renove a sua licença com um código de ativação. Como resultado, é adicionada uma chave de reserva. Esta fica ativa até à licença expirar. Não é possível adicionar uma chave ativa executando este comando.
/DEL /login=<nome do utilizador> /password= <password>	Remova uma chave de licença. A chave de reserva também será removida.

Autenticação	
/login=<nome do utilizador> /password=<password>	Credenciais da conta do utilizador com as permissões de Proteção por palavra-passe necessárias.

Exemplo:

- avp.com LICENSE /ADD file.key
- avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
- avp.com LICENSE /DEL /login=KLAdmin /password=!Password1

RENEW. Comprar uma licença

Abra o website da Kaspersky para comprar ou renovar a sua licença.

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.

EXIT. Sair da aplicação

Sai 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**.

Sintaxe de comando

```
EXIT /login=<nome do utilizador> /password=<password>
```

EXITPOLICY. Desativar política

Desativa 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**.

Sintaxe de comando

```
EXITPOLICY /login=<nome do utilizador> /password=<password>
```

STARTPOLICY. Ativar a política

Ativa uma política do Kaspersky Security Center no computador. As definições da aplicação serão configuradas de acordo com a política.

DISABLE. Desativar a proteção

Desativa 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.

SPYWARE. Deteção de spyware

Ativar / desativar a deteção de spyware. Por predefinição, a deteção de spyware está ativada.

Sintaxe de comando

KSN. Transição do KSN Privado/Global

Selecionar uma solução do Kaspersky Security Network para determinar a reputação de ficheiros ou sites. O Kaspersky Endpoint Security suporta as seguintes soluções infraestruturais da KSN:

- *KSN Global* é a solução usada pela maioria das aplicações da Kaspersky. Os participantes na KSN recebem informações da Kaspersky Security Network 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.
- *Private KSN* 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 KSN Privado 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.

Sintaxe de comando

```
KSN /global | /private <nome do ficheiro>
```

Ficheiro de configuração do KSN Privado	
<nome do ficheiro>	Nome do ficheiro de configuração que contém as definições do servidor de proxy do KSN. Este ficheiro possui a extensão PKCS7 ou PEM.

Exemplo:

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

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 verificações de vírus e atualizações de bases de dados.

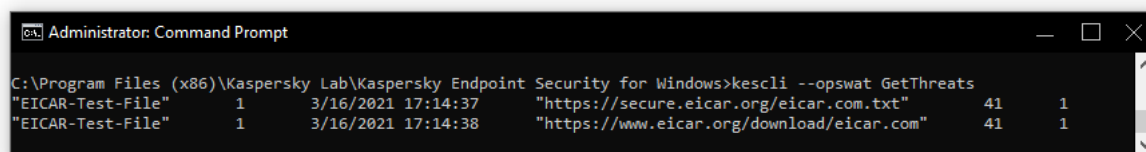
Pode ver a lista dos comandos KESCLI através do comando `--help` ou do comando abreviado `-h`.

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.
3. Para executar um comando, escreva:

```
kescli <comando> [opções]
```

Como resultado, o Kaspersky Endpoint Security executará o comando (ver figura abaixo).



```
Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File" 1 3/16/2021 17:14:37 "https://secure.eicar.org/eicar.com.txt" 41 1
"EICAR-Test-File" 1 3/16/2021 17:14:38 "https://www.eicar.org/download/eicar.com" 41 1
```

Gerir a aplicação a partir da command line

Scan. Scan de vírus

Execute a tarefa de verificação de vírus.

Sintaxe de comando

```
kescli --opswat Scan "<âmbito da verificação>" <ação após deteção de ameaças>
```

Pode verificar o estado da conclusão da tarefa de *Verificação Completa* 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	
<ficheiros a verificar>	;-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	Desinfectar; eliminar se a desinfeção falhar. Se esta opção estiver selecionada, o Kaspersky Endpoint Security tenta automaticamente desinfectar todos os ficheiros infetados detetados. Se a desinfeção falhar, o Kaspersky Endpoint Security apaga os ficheiros. 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

Receba informações sobre o estado da conclusão da tarefa *Verificação Completa*:

- 1 – a verificação está em curso.
- 0 – a verificação não está em execução.

Sintaxe de comando

```
--opswat GetScanState
```

Exemplo:

```
kescli --opswat GetScanState
```

GetLastScanTime. Determinar a hora de conclusão da verificação

Receba informações sobre a data e a hora da conclusão da última tarefa de *Verificação Completa*.

Sintaxe de comando

```
--opswat GetLastScanTime
```

Exemplo:

```
kescli --opswat GetLastScanTime
```

GetThreats. Obter dados sobre ameaças detetadas

Receba uma lista das ameaças detetadas (*Relatório de ameaças*). Este relatório contém informações sobre ameaças e atividades de vírus nos últimos 30 dias antes de criar o relatório.

Sintaxe de comando

```
--opswat GetThreats
```

Quando o comando for executado, o Kaspersky Endpoint Security irá enviar uma resposta no seguinte formato:

```
<nome do objeto detetado> <tipo de objeto> <data e hora da deteção> <caminho para o  
ficheiro> <ação após deteção de ameaças> <nível de perigo da ameaça>
```

```

Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File" 1 3/16/2021 17:14:37 "https://secure.eicar.org/eicar.com.txt" 41 1
"EICAR-Test-File" 1 3/16/2021 17:14:38 "https://www.eicar.org/download/eicar.com" 41 1

```

Gerir a aplicação a partir da command line

Object type	
0	Não conhecido (Desconhecido).
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 (Comprimido).
20	Objetos desconhecidos (Xfiles).
21	Aplicações conhecidas (Software).
22	Ficheiros ocultos (Oculto).
23	Aplicação que necessita de atenção (Pupware).
24	Comportamento anómalo (Anomalia).
30	Não determinado (Não detetado).
40	Faixas de publicidade (Banner).
50	Ataque de rede (Ataque).
51	Acesso ao registo (Registo).
52	Atividade suspeita (Suspeita).
60	Vulnerabilidades (Vulnerabilidade).
70	Phishing.
80	Anexos de mensagens de e-mail (Anexo).
90	Malware detetado pelo Kaspersky Security Network (Urgente).
100	Ligação desconhecida (URL suspeito).
110	Outro malware (Comportamental).

Ação após deteção de ameaças	
0	Não conhecido (desconhecido).

1	A ameaça foi remediada (ok).
2	O objeto estava infetado e não foi desinfetado (infetado).
5	O objeto está num arquivo e não foi desinfetado (arquivo).
9	O objeto foi desinfetado (desinfetado).
10	O objeto não foi desinfetado (não desinfetado).
11	O objeto foi eliminado (eliminado).
13	Foi criada uma cópia de segurança do objeto (com cópia de segurança).
15	O objeto foi movido para a Cópia de segurança (em quarentena).
23	O objeto foi eliminado ao reiniciar o computador (eliminar ao reiniciar).
25	O objeto foi desinfetado ao reiniciar o computador (desinfetar ao reiniciar).
29	O objeto foi movido para a Cópia de segurança por um utilizador (adicionado pelo utilizador).
30	O objeto foi adicionado às exclusões (adicionado à exclusão).
31	O objeto foi movido para a Cópia de segurança ao reiniciar o computador (colocar em quarentena ao reiniciar).
36	Falso positivo (falso alarme).
38	O processo foi terminado (terminado).
40	O objeto não foi detetado (não encontrado).
41	Não é possível resolver a ameaça (intratável).
42	O objeto foi restaurado (revertido).
43	O objeto foi criado como um resultado da atividade de ameaça (produzido pela ameaça).
44	O objeto foi restaurado ao reiniciar o computador (revertido ao reiniciar).
0xffffffff	O objeto não foi processado (descartado).

Nível de perigo da ameaça	
0	Desconhecido
1	Alto
2	Nível médio
4	Baixo
8	Informações (inferior a <i>Baixo</i>)

UpdateDefinitions. Atualização de bases de dados e módulos de software de aplicação

Execute a tarefa de *Atualização*. O Kaspersky Endpoint Security utiliza a origem predefinida: Servidores de atualização da Kaspersky.

Sintaxe de comando

```
--opswat UpdateDefinitions
```

Pode ver a data e a hora da última tarefa de *Atualização* concluída através do comando [GetDefinitionsetState](#).

Exemplo:

```
kescli --opswat UpdateDefinitions
```

GetDefinitionState. Determinar a hora de conclusão atualizada

Receba informações sobre a data e a hora da conclusão da última tarefa de *Atualização*.

Sintaxe de comando

```
--opswat GetDefinitionState
```

Exemplo:

```
kescli --opswat GetDefinitionState
```

EnableRTP. Ativar proteção

Ative 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.

Sintaxe de comando

```
--opswat EnableRTP
```

Pode verificar o estado de funcionamento da Proteção contra ameaças de ficheiros através do comando [GetRealTimeProtectionState](#).

Exemplo:

```
kescli --opswat EnableRTP
```

GetRealTimeProtectionState. Estado da Proteção contra ameaças de ficheiros

Receba informações sobre o estado de funcionamento do componente Proteção contra ameaças de ficheiros:

- 1 – o componente está ativado.
- 0 – o componente está desativado.

Sintaxe de comando

```
--opswat GetRealTimeProtectionState
```

Exemplo:

```
kescli --opswat GetRealTimeProtectionState
```

Versão. Identificar a versão da aplicação

Identificar a versão do Kaspersky Endpoint Security for Windows.

Sintaxe de comando

```
--Versão
```

Também pode utilizar o comando abreviado `-v`.

Exemplo:

```
kescli -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 <comando>`.

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. Para executar um comando, escreva:

```
avp.com <comando> [opções]
```

Como resultado, o Kaspersky Endpoint Security executará o comando (ver figura abaixo).

SANDBOX. Gerir o Kaspersky Sandbox

Comandos para gerir o componente Kaspersky Sandbox:

- Ativar ou desativar o componente Kaspersky Sandbox.

O componente Kaspersky Sandbox permite a interoperabilidade com a solução Kaspersky Sandbox.

- Configurar o componente Kaspersky Sandbox:

- Ligue o computador aos servidores do Kaspersky 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 como implementar imagens virtuais e configurar servidores do Kaspersky Sandbox, consulte a [Ajuda do Kaspersky Sandbox](#).

- Configure o tempo limite de ligação para o servidor do Kaspersky Sandbox.

Tempo limite para receber uma resposta de um pedido de verificação de objeto do servidor do Kaspersky Sandbox. Depois de decorrido o tempo limite, o Kaspersky Sandbox redireciona o pedido para o próximo servidor. O valor do tempo limite depende da velocidade e estabilidade da ligação. O valor predefinido é 5 segundos.

- Configure uma ligação fiável entre o computador e os servidores do Kaspersky Sandbox.

Para configurar uma ligação fiável com os servidores do Kaspersky Sandbox, deve preparar um certificado TLS. Em seguida, deve adicionar o certificado aos servidores do Kaspersky Sandbox e à política do Kaspersky Endpoint Security. Para obter mais informações sobre como preparar o certificado e adicionar o certificado aos servidores, consulte a [Ajuda do Kaspersky Sandbox](#).

- Apresentar as definições atuais do componente.

Sintaxe de comando

```
stop sandbox [/login=<user name> /password=<password>]
start sandbox
sandbox /set [--tls=yes|no] [--servers=<server address>:<port>] [--timeout=<Kaspersky
Sandbox server connection timeout (ms)>] [--pinned-certificate=<path to the TLS
certificate>][/login=<user name> /password=<password>]
sandbox /show
```

Operação	
stop	Desativação do componente Kaspersky Sandbox.
start	Ativação do componente Kaspersky Sandbox.
set	Configuração do componente Kaspersky Sandbox. Pode alterar as seguintes definições: <ul style="list-style-type: none"> • Utilizar uma ligação fiável (--tls); • Adicionar um certificado TLS (--pinned-certificate); • Definir o tempo limite de ligação ao servidor do Kaspersky Sandbox (--timeout); • Adicionar servidores do Kaspersky Sandbox (--servers).
show	Apresentar as definições atuais do componente. Obterá a seguinte resposta: <pre>sandbox.timeout=<Kaspersky Sandbox server connection timeout (ms)> sandbox.tls=<trusted connection status> sandbox.servers=<list of Kaspersky Sandbox servers></pre>

Autenticação	
/login=<nome do utilizador> /password=<password>	Credenciais da conta do utilizador com as permissões de Proteção por palavra-passe necessárias.

Exemplo:

```
avp.com start sandbox
avp.com sandbox /set --tls=yes --pinned-certificate="C:\Users\Admin\certificate.pem"
avp.com sandbox /set --servers=10.10.111.0:147
```

PREVENÇÃO. Gestão de prevenção de execução

Desative a Prevenção de Execução ou mostre as definições atuais dos componentes, incluindo a lista de regras de prevenção da execução.

Sintaxe de comando

```
prevention disable
prevention /show
```

Depois de executar o comando `prevenção/mostrar`, 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 é compatível com a versão do Kaspersky Endpoint Security instalada no dispositivo.
- 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).

ISOLAMENTO. Gerir o isolamento da rede

Desative o Isolamento da rede do computador ou mostre as definições atuais do componente. As definições dos componentes também incluem uma lista de ligações de rede adicionadas às exclusões.

Sintaxe de comando:

```
Isolation /OFF /login=<nome do utilizador> /password=<password>  
isolation /STAT
```

Como resultado da execução do comando `stat`, receberá a seguinte resposta: `Network isolation on|off`.

RESTORE. Restaurar ficheiros a partir da Quarentena

Pode restaurar um ficheiro da Quarentena para a respetiva pasta original. Se a pasta de destino tiver sido eliminada, a aplicação coloca o ficheiro numa pasta especial no computador. Depois tem de mover manualmente o ficheiro para a pasta de destino. A *Quarentena* é um armazenamento local especial no computador para onde os ficheiros infetados por vírus ou não desinfetáveis são movidos. Os ficheiros na quarentena são armazenados num estado encriptado e não põem em risco a segurança do dispositivo. O Kaspersky Endpoint Security apenas utiliza a Quarentena ao trabalhar com as soluções Kaspersky Sandbox e Kaspersky Endpoint 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](#).

Para executar este comando, [a proteção por password deve estar ativada](#). O utilizador deve ter a permissão **Restaurar da cópia de segurança**.

O objeto é colocado em quarentena na conta do sistema (SYSTEM).

Sintaxe de comando

```
RESTORE [/REPLACE] <nome do ficheiro> /login=<nome do utilizador> /password=  
<password>
```

Definições avançadas	
/REPLACE	Substitui um ficheiro existente.
<nome do ficheiro>	O nome do ficheiro a restaurar.

Autenticação	
/login=<nome do utilizador> /password=<password>	Credenciais da conta do utilizador com as permissões de Proteção por palavra-passe necessárias.

Exemplo:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

Valores de retorno do comando:

- -1 significa que o comando não é compatível com a versão do Kaspersky Endpoint Security instalada no dispositivo.
- 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)

Execute a tarefa Verificar indicadores de comprometimento (IOC). 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 *Verificação IOC* permite localizar indicadores de comprometimento no computador e adotar medidas de resposta a ameaças.

Sintaxe de comando

```
IOCSCAN <caminho completo para o ficheiro IOC>[/path=<caminho para a pasta dos
ficheiros IOC> [/process=on|off] [/hint=<caminho completo para ficheiro executável de
um processo|caminho completo do ficheiro>] [/registry=on|off] [/dnsentry=on|off]
[/arpreentry=on|off] [/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off]
[/volumes=on|off] [/eventlog=on|off] [/datetime=<data de publicação do evento>]
[/channels=<lista de canais>] [/files=on|off] [/drives=
<todos|sistema|crítico|personalizado>] [/excludes=<lista de exclusões>][scope=<lista
de pastas a verificar>]
```

IOC files	
<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=<caminho para a pasta com ficheiros IOC>	Caminho para a pasta com os IOC files que deseja utilizar para a verificação. Os <i>IOC files</i> 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).

	<p>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.</p>
<p>/Hint=<caminho completo para o ficheiro executável do processo caminho completo para o ficheiro></p>	<p>Analise os dados do ficheiro ao executar a verificação IOC (termos ProcessItem e FileItem).</p> <p>Pode seleccionar um ficheiro através de uma das seguintes formas:</p> <ul style="list-style-type: none"> • <caminho completo para o ficheiro executável do processo> – ProcessItem; • <caminho completo para o ficheiro> – FileItem.
<p>/registry=on off</p>	<p>Analise os dados de registo do Windows ao executar uma verificação IOC (termo RegistryItem).</p> <p>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).</p> <p>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.</p> <p>Para o tipo de dados RegistryItem, o Kaspersky Endpoint Security verifica um conjunto de chaves de registo.</p>
<p>/dnsentry=on off</p>	<p>Analise os dados sobre os registos na cache DNS local ao executar a verificação IOC (termo DnsEntryItem).</p> <p>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).</p> <p>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.</p>
<p>/arpentry=on off</p>	<p>Analise os dados sobre os registos na tabela ARP ao realizar a verificação IOC (termo ArpEntryItem).</p> <p>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).</p> <p>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.</p>
<p>/ports=on off</p>	<p>Analise os dados sobre as portas de escuta abertas ao executar a verificação IOC (termo PortItem).</p> <p>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).</p>

	<p>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.</p>
<code>/services=on off</code>	<p>Analise os dados sobre os serviços instalados no dispositivo ao executar a verificação IOC (termo ServiceItem).</p> <p>Se o valor do argumento for <code>off</code> (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).</p> <p>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.</p>
<code>/system=on off</code>	<p>Analise os dados de ambiente ao executar a verificação IOC (termo SystemInfoItem).</p> <p>Se o valor do argumento for <code>off</code> (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).</p> <p>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.</p>
<code>/users=on off</code>	<p>Analise os dados sobre os utilizadores ao executar a verificação IOC (termo UserItem).</p> <p>Se o valor do argumento for <code>off</code> (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).</p> <p>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.</p>
<code>/volumes=on off</code>	<p>Analise os dados do volume ao executar a verificação IOC (termo VolumeItem).</p> <p>Se o valor do argumento for <code>off</code> (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).</p> <p>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.</p>
<code>/eventlog=on off</code>	<p>Analise os dados sobre os registos no registo de eventos do Windows ao executar a verificação IOC (termo EventLogItem).</p> <p>Se o valor do argumento for <code>off</code> (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).</p>

	<p>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.</p>
<p>/datetime=<data de publicação do evento></p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>A definição só é utilizada se o documento EventLogItem IOC for descrito no ficheiro IOC fornecido para a verificação.</p>
<p>/Channel=<lista de canais></p>	<p>Lista de nomes de canais (registo) nos quais deseja executar uma verificação IOC.</p> <p>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.</p> <p>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.</p> <p>Se o argumento não for especificado, o Kaspersky Endpoint Security verifica os registos dos canais Aplicação, Sistema, Segurança.</p>
<p>/files=on off</p>	<p>Analise os dados do ficheiro ao executar a verificação IOC (termo FileItem).</p> <p>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).</p> <p>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.</p>
<p>/drives=<all system critical custom></p>	<p>Defina o âmbito de verificação IOC ao analisar dados para o documento FileItem IOC.</p> <p>Pode definir os seguintes valores para o âmbito de verificação:</p> <ul style="list-style-type: none"> • <all> para todos os âmbitos de ficheiro disponíveis. • <system> para ficheiros em pastas nas quais o sistema operativo está instalado.

	<ul style="list-style-type: none"> • <critical> para ficheiros temporários nas pastas do utilizador e do sistema. • <personalizado> para ficheiros em âmbitos definidos pelo utilizador (--scope=<lista de pastas a verificar>). <p>Se o argumento não for especificado, a verificação será executada em áreas críticas.</p>
/excludes=<lista de exclusões>	Defina o âmbito de exclusão ao analisar dados para o documento Fileitem IOC. Pode especificar vários caminhos separados por espaços.
/scope=<lista de pastas a verificar>	Âmbito de verificação IOC definido pelo utilizador ao analisar dados para o documento Fileitem IOC (/drives=custom). Pode especificar vários caminhos separados por espaços.

Valores de retorno do comando:

- -1 significa que o comando não é compatível com a versão do Kaspersky Endpoint Agent instalada no dispositivo.
- 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="">)
Nome	Descrição do ficheiro IOC do cabeçalho da estrutura do ficheiro IOC (a etiqueta <description></description>)
Itens indicadores correspondentes	Lista de ID de todos os indicadores correspondentes.
Objetos correspondentes	Dados de cada documento IOC para o qual houve uma correspondência.

MDRLICENSE. Ativação MDR

Execute operações com 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 (🔑).

Sintaxe de comando

```
MDRLICENSE <operação> [/login=<nome de utilizador> /password=<palavra-passe>]
```

Operação	
/ADD <nome do ficheiro>	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=<nome do utilizador> /password=<password>	Credenciais da conta do utilizador com as permissões de Proteção por palavra-passe necessárias.

Exemplo:

- avp.com MDRLICENSE /ADD file.key
- avp.com MDRLICENSE /DEL /login=KLAdmin /password=!Password1

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, `Erro: Não é possível iniciar a tarefa 'EntAppControl'`. O Kaspersky Endpoint Security também pode apresentar informações adicionais sob a forma de um código, por exemplo, `erro = 8947906D` (consulte a tabela abaixo).

Códigos de erro

Código de erro	Descrição
09479001	A chave de licença do Kaspersky Endpoint Security já está a ser utilizada neste computador.
0947901D	A licença expirou. A atualização da base de dados não está disponível.
89479002	Chave não encontrada.
89479003	Assinatura digital em falta ou corrompida.
89479004	Dados corrompidos.
89479005	Ficheiro de chave corrompido.
89479006	Licença expirada ou chave de licença expirada.
89479007	Ficheiro de chave não especificado.
89479008	Não é possível aplicar o ficheiro de chave.

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 de chave inválido para adicionar uma chave de reserva.
89479012	Erro de sistema.
89479013	Lista de bloqueio de chaves corrompida.
89479014	A assinatura digital do ficheiro não corresponde à assinatura digital da Kaspersky.
89479015	Não é possível utilizar uma chave para uma licença não comercial como chave para uma licença comercial.
89479016	É necessária a licença beta para utilizar a versão beta da aplicação.
89479017	Ficheiro de chave não compatível com esta aplicação.
89479018	Chave bloqueada pela Kaspersky.
89479019	A aplicação já foi utilizada com uma licença de avaliação. Não é possível adicionar a chave de teste novamente.
8947901A	Ficheiro de chave corrompido.
8947901B	Assinatura digital 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 de 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	Erro nos dados do serviço da chave de licença.
89479023	Não é possível utilizar um ficheiro de chave inválido para adicionar uma chave de reserva.
89479025	Erro ao enviar pedido ao servidor de ativação. Motivos possíveis: erro de ligação à Internet ou problemas temporários no servidor de ativação. Tente ativar a aplicação mais tarde com o código de ativação. Se o erro persistir, contacte o fornecedor de Internet.
89479026	Erro na resposta do servidor de ativação.
89479027	Não é possível obter o estado da resposta.
89479028	Ocorreu um erro ao guardar o ficheiro temporário.
89479029	O código de ativação foi inserido incorretamente ou a data do sistema está incorreta. Verifique a data do sistema do computador.
8947902A	Ficheiro de chave não compatível com esta aplicação ou a licença expirou. Não pode ativar o Kaspersky Endpoint Security utilizando um ficheiro de chave para uma outra aplicação.

8947902B	Falha ao receber o ficheiro de chave. Foi introduzido um código de ativação incorreto.
8947902C	O servidor de ativação devolveu o erro 400.
8947902D	O servidor de ativação devolveu o erro 401.
8947902E	O servidor de ativação devolveu o erro 403.
8947902F	O servidor de ativação devolveu o erro 404.
89479030	O servidor de ativação devolveu o erro 405.
89479031	O servidor de ativação devolveu o erro 406.
89479032	É necessária autenticação no servidor de proxy. Verifique as opções de rede.
89479033	O tempo limite do pedido expirou.
89479034	O servidor de ativação devolveu o erro 409.
89479035	O servidor de ativação devolveu o erro 410.
89479036	O servidor de ativação devolveu o erro 411.
89479037	O servidor de ativação devolveu o erro 412.
89479038	O servidor de ativação devolveu o erro 413.
89479039	O servidor de ativação devolveu o erro 414.
8947903A	O servidor de ativação devolveu o erro 415.
8947903C	Erro interno do servidor.
8947903D	Funcionalidade não suportada.
8947903E	Resposta inválida da porta de ligação. Verifique as opções de rede.
8947903F	Serviço indisponível (erro HTTP 503).
89479040	Excedido o tempo limite de resposta da porta de ligação. Verifique as opções de rede.
89479041	O protocolo não é suportado pelo servidor.
89479043	Erro de HTTP desconhecido.
89479044	ID de recurso inválido.
89479046	URL inválido.
89479047	Pasta de destino inválida.
89479048	Erro na distribuição da memória.
89479049	Erro ao converter os parâmetros para a sequência ANSI (URL, pasta, agente).
8947904A	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 de chave não encontrado no servidor de ativação.
8947904E	A chave está bloqueada.
8947904F	Erro interno do servidor de ativação.
89479050	Não existem dados suficientes no pedido de ativação.
89479053	Chave de licença expirada.

89479054	Data do sistema incorreta no computador.
89479055	A licença de avaliação expirou.
89479056	A licença expirou.
89479057	O limite de ativações da aplicação foi excedido para o código especificado.
89479058	O procedimento de ativação terminou com um erro do sistema.
89479059	Não é possível utilizar uma chave para uma licença não comercial como chave para uma 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 data de distribuição da base de dados da aplicação excede a data de validade da licença.
89479066	Não é possível substituir a chave ativa por uma chave expirada.
89479067	Não é possível adicionar uma chave de reserva se a mesma expirar antes da licença atual.
89479068	Chave de subscrição atualizada em falta.
8947906A	Código de ativação incorreto (a soma de verificação não corresponde).
8947906B	A chave já está 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 chave de subscrição como uma chave de reserva.
89479213	Erro geral de camada de transporte.
89479214	Falhou a ligação ao servidor de ativação.
89479215	Formato de URL 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	Falhou a ligação ao servidor de ativação ou servidor de proxy.
89479219	Acesso remoto recusado.
8947921A	Esgotado o tempo limite de resposta.
8947921B	Erro ao enviar pedido HTTP.
8947921C	Erro de ligação SSL.
8947921D	Operação interrompida por chamada de retorno.
8947921E	Demasiadas tentativas de reencaminhamento.
8947921F	Falha na verificação do destinatário.
89479220	Resposta vazia do servidor de ativação.
89479221	Erro ao enviar dados.
89479222	Erro ao receber dados.

89479223	Erro de certificado SSL local.
89479224	Erro de encriptação SSL.
89479225	Erro de certificado SSL do servidor.
89479226	Conteúdos do pacote de rede inválidos.
89479227	Acesso de utilizador recusado.
89479228	Ficheiro de certificado SSL inválido.
89479229	Falha ao estabelecer a ligação SSL.
8947922A	Falha ao enviar ou receber pacote de rede. Tente novamente mais tarde.
8947922B	Ficheiro inválido com certificados revogados.
8947922C	Erro de pedido de certificado SSL.
89479401	Erro de servidor desconhecido.
89479402	Erro interno do servidor.
89479403	Nenhuma chave de licença disponível para o código de ativação introduzido.
89479404	Chave ativa bloqueada.
89479405	Os parâmetros necessários do pedido de ativação da aplicação estão em falta.
89479406	Nome de utilizador ou password incorretos.
89479407	Código de ativação incorreto enviado para o servidor.
89479408	O código de ativação é inválido para o Kaspersky Endpoint Security. Não pode ativar o Kaspersky Endpoint Security utilizando um ficheiro de chave para uma aplicação desconhecida.
89479409	Falta um código de ativação na solicitação.
8947940B	Licença expirada (de acordo com os dados do servidor de ativação).
8947940C	O número de ativações com este código foi excedido.
8947940D	Formato não válido do ID de pedido.
8947940E	O código de ativação é inválido para o Kaspersky Endpoint Security. O código de ativação é para uma outra aplicação da Kaspersky.
8947940F	Não é possível atualizar a chave de licença.
89479410	O código de ativação é inválido para esta região.
89479411	O código de ativação é inválido para a versão do idioma do Kaspersky Endpoint Security.
89479412	É necessário acesso adicional ao servidor de ativação.
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	Formato do código de ativação não suportado pelo servidor de ativação.
89479418	Formato de código de ativação inválido.
89479419	Hora do sistema incorreta no computador.

8947941A	O código de ativação é inválido para a versão do Kaspersky Endpoint Security.
8947941B	A assinatura expirou.
8947941C	Número de ativações excedido para esta chave de licença.
8947941D	Assinatura digital inválida da chave de licença.
8947941E	São necessários dados adicionais.
8947941F	Falha na verificação dos dados do utilizador.
89479420	Subscrição inativa.
89479421	Servidor de ativação em manutenção.
89479501	Erro desconhecido do Kaspersky Endpoint Security.
89479502	Parâmetro inválido transferido (por exemplo, uma lista vazia de endereços de servidores de ativação).
89479503	Código de ativação incorreto.
89479504	Nome de utilizador inválido.
89479505	Password de utilizador inválida.
89479506	Resposta inválida do servidor de ativação.
89479507	Pedido de ativação interrompido.
89479509	O servidor de ativação retornou uma lista de encaminhamento 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 **INICIAR**, **STOP**, **ESTADO**, **ESTATÍSTICAS**, **EXPORTAR** e **IMPORTAR**. Utilizando os perfis, pode configurar as definições da aplicação (por exemplo, **STOP DeviceControl**) ou executar tarefas (por exemplo, **INICIAR Scan_My_Computer**).

Estão disponíveis as seguintes perfis:

- **AdaptiveAnomaliesControl** – Controlo de Anomalias Adaptativo.
- **AMSI** – Proteção AMSI.
- **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.
- Mail_Monitoring ou EM – Proteção contra ameaças de correio.
- Rollback – reversão da atualização.
- 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.
- 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 discrecionário – 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 seleccionar um utilizador para trabalhar com API REST.

- RESTAPI_Port=<Port>

Porta usada para troca de dados. Parâmetro opcional. A porta 6782 é a porta predefinida.

- 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\Rest

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 palavra-passe](#). Por exemplo, não é possível impedir que um utilizador desative a proteção com API REST. Pode configurar a Proteção por Palavra-passe 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 seleccionar 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

A página do Kaspersky Endpoint Security no site Kaspersky

Na [Página do Kaspersky Endpoint Security](#), pode ver informações gerais sobre a aplicação e as suas funções e recursos.

A página do Kaspersky Endpoint Security contém uma ligação para a loja online. Aqui pode adquirir ou renovar a aplicação.

A página do Kaspersky Endpoint Security na Base de Conhecimento

A *Base de Conhecimentos* é uma secção no website do Suporte Técnico.

Na [Página do Kaspersky Endpoint Security na Base de Conhecimentos](#), pode ler artigos que fornecem informações úteis, recomendações e respostas a perguntas frequentes sobre como comprar, instalar e usar a aplicação.

Os artigos da Base de Conhecimentos podem responder a perguntas relacionadas não apenas ao Kaspersky Endpoint Security, mas também a outras aplicações da Kaspersky. Os artigos da Base de Conhecimentos também podem conter notícias do Suporte Técnico.

Discussão das aplicações da Kaspersky na comunidade de utilizadores

Se a sua pergunta não exigir uma resposta urgente, poderá discuti-la com os especialistas da Kaspersky e outros utilizadores na nossa [Comunidade](#).

Na Comunidade, pode visualizar os tópicos existentes, deixar os seus comentários e criar novos tópicos de debate.

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 execução de comandos da aplicação, passo-a-passo, e determinar a fase do funcionamento da aplicação em que o erro ocorre.

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.
- Alterar as definições de componentes individuais das aplicações, que não estão disponíveis através dos elementos padrão da interface.
- 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\Traces.

Os ficheiros de rastreio são designados da seguinte maneira: KES<service version number_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.

Kaspersky Endpoint Security guarda palavras-passe de utilizadores num ficheiro de rastreio apenas de forma encriptada.

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 dos 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<version number_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 `shelllex.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 13 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:

- Palavra-passe do utilizador KLAdmin para desbloqueio da interface Kaspersky Endpoint Security ([Proteção por palavra-passe](#)).
- Palavra-passe temporária para desbloqueio da interface Kaspersky Endpoint Security ([Proteção por palavra-passe](#)).
- Nome de utilizador e palavra-passe para o servidor de [e-mail](#) SMTP.
- Nome de utilizador e palavra-passe para o [servidor proxy](#).
- Nome de utilizador e password para a [tarefa Change application components](#).
- 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 de informação de volume de sistema e é designado da seguinte maneira: `KLFD E . {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 ocorreram durante a operação da aplicação.

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 é aberta, 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 **Rastreios**, selecione um modo de rastreio de aplicação:
 - **Com rotação**. 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 número máximo de ficheiros para rotação e o tamanho máximo para cada ficheiro.
 - **Gravar num único ficheiro**. Guarde um ficheiro de rastreio (sem limite de tamanho).
5. Na lista pendente **Nível**, selecione o nível de rastreio:

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 (500)**.
6. Reiniciar o Kaspersky Endpoint Security.
7. 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, é criado um ficheiro de rastreio de desempenho na pasta %ProgramData%\Kaspersky Lab\KES\Traces. Após a criação do ficheiro de rastreio, envie o ficheiro 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 é aberta, 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 **Rastreios**, selecione um modo de rastreio de aplicação:
 - **Com rotação**. 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.
 - **Gravar num único ficheiro**. Guarde um ficheiro de rastreio (sem limite de tamanho).
5. Na lista pendente **Nível**, selecione o nível de rastreio:
 - **Leve**. 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 deteção**, 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\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\Traces.

Para ativar ou desativar a gravação de descarga:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, seleccione **Definições gerais** → **Definições da aplicação**.
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 protecção de ficheiros de descarga e de rastreio.

Se a protecção 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.

Para ativar ou desativar a protecção de ficheiros de descarga e de rastreio:

1. Na janela principal da aplicação, clique no botão .
2. Na janela de definições da aplicação, seleccione **Definições gerais** → **Definições da aplicação**.
3. No bloco **Informações de depuração**, utilize a caixa de verificação **Ativar protecção de ficheiros de descarga e de rastreio** para ativar ou desativar a protecção de ficheiros.
4. Guarde as suas alterações.

Os ficheiros de descarga e de rastreio que foram editados enquanto a protecção estava ativa permanecem protegidos mesmo depois de esta ser desativada.

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).
- Ao tentar instalar qualquer versão do Módulo de Encriptação AES num computador com o Kaspersky Endpoint Security for Windows 11.8.0, mas nenhum componente de encriptação instalado, a instalação do Módulo de Encriptação terminará com uma mensagem de erro a informar de que está instalada uma versão mais recente da aplicação. A partir do Kaspersky Endpoint Security 10 for Windows Service Pack 2 (versão 10.3.0.6294), não existe nenhum ficheiro de instalação separado para o Módulo de Encriptação. As bibliotecas de encriptação estão incluídas no kit de distribuição do pacote. O Kaspersky Endpoint Security 11.8.0 é incompatível com os módulos de encriptação AES. As bibliotecas necessárias para a encriptação são instaladas automaticamente quando o componente Encriptação de Disco Completa (Full Disk Encryption – FDE) ou Encriptação ao Nível dos Ficheiros (File Level Encryption – FLE) é selecionado.
- 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 da aplicação, inicie sua recuperação após a reinicialização do computador.
- 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](#).
- Se estiver a atualizar uma versão anterior da aplicação para a versão 11.8.0, para instalar o Kaspersky Endpoint Agent, reinicie o computador e inicie sessão no sistema utilizando uma conta com direitos de administrador local. Caso contrário, o Kaspersky Endpoint Agent não será instalado durante o procedimento de atualização.
- 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.

[Atualizar a aplicação](#)

- Ao atualizar do Kaspersky Endpoint Security 10 Service Pack 2 for Windows (compilação 10.3.0.6294), o [componente Prevenção contra invasões é ativado](#).
- Ao atualizar o Kaspersky Endpoint Security 10 for Windows Service Pack 2 (compilação 10.3.0.6294), os ficheiros que estavam na Cópia de Segurança ou Quarentena na versão anterior da aplicação serão transferidos para a Cópia de Segurança na nova versão da aplicação. Esses ficheiros não são transferidos para versões anteriores ao Kaspersky Endpoint Security 10 for Windows Service Pack 2 (compilação 10.3.0.6294). Para os guardar, terá de restaurar os ficheiros da Quarentena e da Cópia de Segurança antes de atualizar a aplicação. Após a conclusão da atualização, verifique novamente os ficheiros restaurados.
- 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 de *Atualização*, *Verificação de Áreas Críticas*, *Verificação Personalizada* e *Verificação de integridade* 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](#).
- Se estiver a atualizar uma versão anterior da aplicação para a versão 11.8.0, para instalar o Kaspersky Endpoint Agent, reinicie o computador e inicie sessão no sistema utilizando uma conta com direitos de administrador local. Caso contrário, o Kaspersky Endpoint Agent não será instalado durante o procedimento de atualização.
- Se está a atualizar o Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 4 com o componente Encriptação ao Nível dos Ficheiros (FLE) instalado em computadores com o Windows 10 versão 1809, 1903 e 1909, os controladores FDE não serão instalados na imagem WinRE.
- 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 *Crítico* no Kaspersky Security Center; é recebido o evento os *servidores da KSN estão indisponíveis*. 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 a aplicação ser atualizada de versões anteriores ao Kaspersky Endpoint Security 11 for Windows, o computador tem de ser reiniciado.

- 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 tarefa de verificação de vírus funciona corretamente.
 - Depois de a verificação antivírus do servidor ser iniciada, as exclusões de verificação 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 Modo Central 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 e Anti-Bridging.
 - 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.
- A sessão múltipla do Windows 10 Enterprise é suportada com limitações:
 - O Kaspersky Endpoint Security desinfecta as ameaças ativas sem notificar o utilizador, tal como quando [desinfecta 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 gestão 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 [Garantir 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 original 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\**\*"
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.

[Compatibilidade com o Kaspersky Security Center](#)

- Só é possível gerir o componente Controlo de Anomalias Adaptativo na versão Kaspersky Security Center 11 ou posterior.
- O relatório de ameaças do Kaspersky Security Center 11 poderá não apresentar informações sobre a ação realizada face a ameaças que foram detetadas pelo componente AMSI.
- O estado de funcionamento dos componentes Proteção AMSI e Controlo de Anomalias Adaptativo só está disponível no Kaspersky Security Center versão 11 ou posterior. É possível ver o estado de funcionamento na Consola do Kaspersky Security Center nas propriedades do computador, na secção **Tarefas**. Os relatórios para estes componentes estão também disponíveis apenas no Kaspersky Security Center versão 11 ou posterior.

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.
- A aplicação não pode ser ativada através da subscrição do Kaspersky Security Center se a licença tiver expirado ou se existir uma licença de avaliação ativa no computador. Para substituir uma licença de avaliação ou uma licença prestes a expirar por uma licença de subscrição, [utilize a tarefa de distribuição de licenças](#).
- 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. Isso ocorre porque a aplicação instala primeiro e tenta ativar a licença de avaliação incorporada, o que requer acesso à Internet para ativação durante o procedimento de instalação.
- 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. Isso ocorre porque, uma vez mais, a aplicação instala-se e tenta ativar a licença de avaliação incorporada, o que requer acesso à Internet para ativação ao instalar uma atualização.
- 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 11.8.0, os relatórios de desempenho dos componentes poderão funcionar incorretamente. Se tiver instalado componentes do Kaspersky Endpoint Protection 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.

[Motor de remediação](#)

- A aplicação restaura ficheiros apenas em dispositivos que têm o sistema de ficheiros NTFS ou FAT32.
- A aplicação pode restaurar ficheiros com as seguintes extensões: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls,xlsx, xslm, xlsx, xlb, 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.
- A aplicação não monitoriza modificações efetuadas em ficheiros através de uma interface de rede (por exemplo, se um ficheiro estiver guardado numa pasta partilhada e um processo for iniciado remotamente a partir de outro computador).

Firewall

- 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.
- Nas versões da aplicação 11.0.0 e 11.0.1, os endereços MAC definidos são aplicados incorretamente. As definições de endereço MAC para as versões 11.0.0, 11.0.1 e 11.1.0 ou posteriores não são compatíveis. Depois de atualizar a aplicação ou o plug-in dessas versões para a versão 11.1.0 ou posterior, deve verificar e reconfigurar os endereços MAC definidos nas regras de Firewall.
- Ao atualizar a aplicação das versões 11.1 e 11.2.0 para a versão 11.8.0, os estados das permissões para as regras de Firewall que se seguem não são migrados:
 - Pedidos para o servidor de DNS por TCP.
 - Pedidos para o servidor de DNS por UDP.
 - Qualquer atividade de rede.
 - Respostas recebidas de ICMP Destination Unreachable.
 - Fluxo ICMP de entrada.
- 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 fiável. 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.

[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](#).

[Controlo das Aplicações](#)

- São suportados apenas os arquivos ZIP com menos de 104 MB na gestão das regras de Controlo de Aplicações na Consola Web do Kaspersky Security Center. 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 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.
- 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 adicionar 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 adicionar 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.

Controlo de Dispositivos

- 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.
- 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.

Controlo de Internet

- Os formatos OGV e WEBM não são suportados.
- O protocolo RTMP não é suportado.

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.
- Um [relatório de Regras de Controlo de Anomalias Adaptativo não pode ser gerado](#) se a amostra incluir mesmo que seja um só 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](#).

Encriptação de Unidades (FDE)

- 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 o desempenho do computador ideal após a encriptação, é necessário que o processador suporte o conjunto de instruções AES-NI (Novas Instruções do Padrão de Encriptação Avançado da Intel). 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.
- Para obter detalhes sobre como restaurar um sistema operativo a partir de uma cópia de segurança para um dispositivo GPT encriptado, visite a [Base de Conhecimento de Suporte Técnico](#).
- Não é possível a coexistência de vários agentes de transferência num computador encriptado.

- 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 <domínio>/<nome de conta do Windows>, 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 descriptar 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 descriptado com êxito. Nesse caso, deve reiniciar o procedimento de recuperação de dados para descriptar 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 e pastas não é suportada nos sistemas operativos da família Microsoft Windows Embedded.
- Depois de instalar a aplicação, é necessário reiniciar o sistema operativo para que a encriptação de ficheiros e pastas funcione devidamente.
- 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 descriptada para um computador que não possui a funcionalidade de encriptação disponível.
- Recomendamos que descripte 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.
- 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. 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. Para obter detalhes sobre o suporte para Client-Side Caching (CSC) ao utilizar encriptação, consulte a [Base de Conhecimento de Suporte Técnico](#).
- [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 palavra-passe para um arquivo encriptado de autoextração fique suspensa. Para resolver este problema, feche a janela de entrada da palavra-passe, mude para o esquema de teclado no seu sistema operativo e volte a introduzir a palavra-passe 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 (Subsistema Windows para 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](#).
- Depois de atualizar o Kaspersky Endpoint Security for Windows versão 11.0.1 ou anterior, para aceder a ficheiros encriptados após reiniciar o computador, confirme que o Agente de Rede está em execução. O Agente de Rede tem um arranque atrasado, pelo que não pode aceder aos ficheiros encriptados imediatamente após o carregamento do sistema operativo. Não precisa de esperar que o Agente de Rede seja iniciado após o próximo arranque do computador.

[Outras limitações](#)

- 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.
- 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.
- Monitorização do Sistema. As informações completas sobre os processos não são apresentadas.
- 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.
- Ao verificar correio com a [extensão Mail Threat Protection para Microsoft Outlook](#), é aconselhável utilizar o Modo Exchange em Cache (a opção Utilizar o Modo Exchange em Cache).
- A [tarefa Verificação de vírus](#) não suporta a versão de 64 bits do Microsoft Outlook. Isto significa que o Kaspersky Endpoint Security não verifica ficheiros do MS Outlook (ficheiros PST e OST), se uma versão de 64 bits do MS Outlook estiver instalada no computador, mesmo se [o correio estiver incluído no âmbito de verificação](#).
- No Kaspersky Security Center, ao passar da Kaspersky Security Network global para uma Kaspersky Security Network privada, 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.
- 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 do produto e no relatório do Kaspersky Security Center.
- O componente [Endpoint Sensor](#) não pode ser instalado no Microsoft Windows Server 2008.
- 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 modo de segurança.
- Para garantir que as versões 11.5.0 e 11.6.0 do Kaspersky Endpoint Security for Windows funcionam corretamente com o software Cisco AnyConnect, tem de instalar o Módulo de Conformidade versão 4.3.183.2048 ou posterior. Saiba mais sobre compatibilidade com o Motor de Serviços de Identidade da Cisco na [documentação da Cisco](#).
- 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.

- A tarefa de verificação de disponibilidade da KSN já não é suportada.
- 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:\pasta1\pasta2, a verificação será executada para o caminho C:\pasta1\.
- Ao atualizar a aplicação da versão 11.1.0 para a versão 11.8.0, as definições de proteção de AMSI são repostas nos seus valores predefinidos.
- Se estiver a utilizar políticas de restrição de software (SRP), o computador pode não conseguir carregar (ecrã preto). Recomendamos que altere as definições das SRP da seguinte forma: defina **Todos os ficheiros de software exceto as bibliotecas (como DLL)** para o parâmetro **Aplicar Políticas de Restrição de Software nos seguintes objetos** e adicione o nível de segurança **Sem restrições** aos caminhos dos ficheiros da aplicação (C:\Program Files\Common Files\Kaspersky Lab e C:\Program Files\Kaspersky Lab). Para obter mais informações sobre a utilização das SRP, consulte a [documentação da Microsoft](#).
- Se o computador pertencer a um domínio sob o Objeto da Política de Grupo do Windows (GPO) com o parâmetro DriverLoadPolicy definido para 8 (Apenas bom), 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 (Bom e desconhecido). As definições do ELAM estão localizadas na política em: **Configuração do computador** → **Modelos administrativos** → **Sistema** → **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 palavra-passe.
- 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.
- Não pode verificar um objeto colocado em quarentena como resultado da tarefa [Move file to Quarantine](#).
- O Kaspersky Endpoint Security não executa as tarefas [Verificação IOC](#) 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 *Verificação IOC* em unidades de rede. Por exemplo, \\server\shared_folder.

- 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 configuração, ative o Kaspersky Sandbox.
- Quando for detetado um indicador de comprometimento ao executar uma tarefa [Verificação IOC](#), 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.
- Não é possível colocar em quarentena um Fluxo de Dados Alternativo (ADS) maior do que 4 MB. O Kaspersky Endpoint Security ignora esse ADS sem notificar o utilizador.
- Para gerir os detalhes do alerta, irá precisar do plug-in Web do Kaspersky Endpoint Security for Windows 11.7.0 ou posterior. Os detalhes do alerta são necessários pela solução [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.
- 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).

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.

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 adicional

Uma chave que certifica o direito de utilizar a aplicação, mas que não está a ser atualmente utilizada.

Chave ativa

Uma chave atualmente utilizada pela aplicação.

Desinfeção

Um método de processamento de objetos infetados que resulta numa recuperação total ou parcial dos dados. Nem todos os objetos infetados podem ser desinfectados.

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

Um indicador de comprometimento é um conjunto de dados sobre um objeto ou atividade maliciosa.

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:\Pasta***.txt` incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas designadas Pasta e nas suas subpastas. 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 caracteres.

Objeto OLE

Um ficheiro anexado ou um ficheiro incorporado noutra 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.

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 prevenir a infeção do sistema de ficheiros do computador. Por predefinição, o componente Proteção contra ameaças de ficheiros reside permanentemente na RAM do computador. O componente verifica ficheiros em todas as unidades do computador, bem como nas unidades ligadas. 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 pelo utilizador ou a aplicação. Se for detetado um ficheiro malicioso, o Kaspersky Endpoint Security bloqueará a operação do ficheiro. A aplicação desinfecta 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 na 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 <i>(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)</i>	<p>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 <i>níveis de segurança</i>.</p> <ul style="list-style-type: none">• 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.

<p>Tipos de ficheiros</p> <p><i>(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)</i></p>	<p>Todos os ficheiros. Se esta definição estiver ativada, o Kaspersky Endpoint Security verifica todos os ficheiros sem exceção (todos os formatos e extensões).</p> <p>Ficheiros verificados por formato. Se esta configuração estiver ativada, o Kaspersky Endpoint Security 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.</p> <p>Ficheiros verificados por extensão. Se esta configuração estiver ativada, o Kaspersky Endpoint Security verifica apenas ficheiros infetáveis. O formato do ficheiro é então determinado com base na extensão do ficheiro.</p>
<p>Âmbito de verificação</p>	<p>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.</p> <p>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. Também não é possível excluir um objeto (como unidades amovíveis) das verificações.</p>
<p>Aprendizagem automática e análise de assinaturas</p> <p><i>(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)</i></p>	<p>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.</p> <p>Com base nas recomendações dos especialistas da Kaspersky, a aprendizagem automática e a análise de assinaturas estão sempre ativadas.</p>
<p>Análise heurística</p> <p><i>(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)</i></p>	<p>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.</p> <p>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.</p>
<p>Ação após deteção de ameaças</p>	<p>Desinfetar; eliminar 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 apaga os ficheiros.</p> <p>Desinfetar; bloquear se a desinfeção falhar. Se esta opção estiver selecionada, o Kaspersky Endpoint Security tenta automaticamente desinfetar todos os ficheiros infetados detetados. Se a desinfeção não for possível, o Kaspersky Endpoint Security adiciona a informação sobre os ficheiros infetados que são detetados à lista de ameaças ativas.</p> <p>Bloquear. Se esta opção estiver selecionada, o componente Proteção contra ameaças de ficheiros bloqueia automaticamente todos os ficheiros infetados sem tentar desinfetá-los.</p>

	<p>Antes de tentar desinfetar ou eliminar um ficheiro infetado, o Kaspersky Endpoint Security 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.</p>
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 formatos de arquivo. O Kaspersky Endpoint Security verifica arquivos não só pela extensão, mas também pelo formato.
Verificar pacotes de distribuição	Esta caixa de verificação ativa/desativa a verificação de pacotes de distribuição 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.
Não descompactar ficheiros compostos extensos	<p>Se esta caixa de verificação estiver selecionada, o Kaspersky Endpoint Security não verifica ficheiros compostos se o tamanho destes exceder o valor especificado.</p> <p>Se esta caixa de verificação for desmarcada, o Kaspersky Endpoint Security verifica ficheiros compostos de todos os tamanhos.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>O Kaspersky Endpoint Security verifica ficheiros grandes que são extraídos dos arquivos, independentemente de a caixa de verificação estar marcada ou não.</p> </div>
Descompactar ficheiros compostos em 2.º plano	<p>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.</p> <p>O Kaspersky Endpoint Security apenas fornece acesso a ficheiros compostos que são menores do que o valor após descompactar e verificar esses ficheiros.</p> <p>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.</p>
Modo de verificação <i>(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)</i>	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>O Kaspersky Endpoint Security verifica os ficheiros acedidos pelo utilizador, o sistema operativo ou uma aplicação em execução na conta do utilizador.</p> </div> <p>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.</p>

	<p>No momento de acesso e alteração. Neste modo, a Proteção contra ameaças de ficheiros verifica os objetos sem que há uma tentativa para os abrir ou modificar.</p> <p>No momento de acesso. Neste modo, a Proteção contra ameaças de ficheiros verifica os objetos apenas aquando de uma tentativa para os abrir.</p> <p>No momento de execução. Neste modo, a Proteção contra ameaças de ficheiros verifica os objetos aquando de uma tentativa para os executar.</p>
<p>Tecnologia iSwift</p> <p><i>(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)</i></p>	<p>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 considera a data de lançamento das bases de dados do Kaspersky Endpoint Security, a data da última verificação do ficheiro e quaisquer modificações nas definições da verificação. A tecnologia iSwift é um avanço da tecnologia iChecker para o sistema de ficheiros NTFS.</p>
<p>Tecnologia iChecker</p> <p><i>(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)</i></p>	<p>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).</p>
<p>Pôr a proteção contra ameaças de ficheiros em pausa</p> <p><i>(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)</i></p>	<p>Isto interrompe temporariamente e automaticamente a operação da Proteção Contra Ameaças de Ficheiros no horário especificado ou ao trabalhar com as aplicações especificadas.</p>

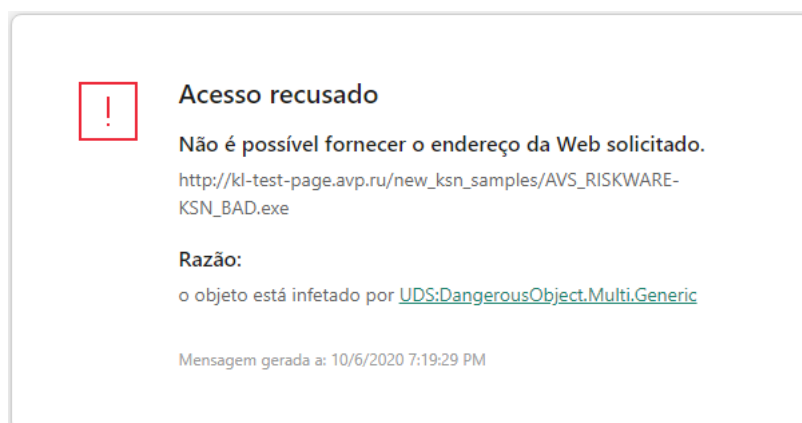
Proteção contra ameaças da Web

O componente Proteção contra Ameaças da Web impede a transferência de ficheiros maliciosos da Internet e também bloqueia 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. Pode [especificar as portas que o Kaspersky Endpoint Security irá monitorizar](#) ou selecionar todas as portas.

Para monitorização do tráfego HTTPS, precisa de [ativar a verificação de ligações encriptadas](#).

Quando um utilizador tenta abrir um website de phishing ou malicioso, o Kaspersky Endpoint Security bloqueia o acesso e apresenta um aviso (consulte a figura abaixo).



Mensagem de acesso negado ao site

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)	<p>Para Proteção contra ameaças da Web, o Kaspersky Endpoint Security pode aplicar diferentes grupos de definições. Estes grupos de definições armazenados na aplicação chamam-se <i>níveis de segurança</i>.</p> <ul style="list-style-type: none">• Alto. O nível de segurança utilizado pelo componente Proteção contra ameaças da Web para efetuar a verificação máxima do tráfego de Internet que o computador recebe através dos protocolos 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 Kaspersky Endpoint Security 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 médio de verificação.
Ação após deteção de ameaças	<p>Bloquear transferência. 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.</p> <p>Notificar. 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.</p>
Verificar o endereço da Internet na base de dados de endereços	<p>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.</p>

<p>da Internet maliciosos</p> <p><i>(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)</i></p>	
<p>Utilizar análise heurística</p> <p><i>(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)</i></p>	<p>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.</p> <p>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.</p>
<p>Verificar o endereço da Internet na base de dados de endereços da Internet de phishing</p> <p><i>(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)</i></p>	<p>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.</p>
<p>Não verificar tráfego de Internet de URL fiáveis</p>	<p>Se a caixa de verificação 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.</p>

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
- Microsoft Outlook Express
- Windows Mail

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 operações com o Outlook 2010, 2013, 2016 e 2019.

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 muda o nome do assunto da mensagem: [A mensagem necessita da sua participação no processamento] <assunto da mensagem> ou [A mensagem foi processada] <assunto da mensagem>.

Definições do componente Proteção contra ameaças de correio

Parâmetro	Descrição
Nível de segurança <i>(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)</i>	<p>Para a Proteção contra ameaças de correio, o Kaspersky Endpoint Security aplica diferentes grupos de definições. Estes grupos de definições armazenados na aplicação chamam-se <i>níveis de segurança</i>:</p> <ul style="list-style-type: none"> • 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 do Kaspersky Endpoint Security 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	<p>Desinfetar, eliminar se a desinfeção falhar. Quando um objeto infetado é detetado numa mensagem de entrada ou saída, o Kaspersky Endpoint Security tenta desinfetar o objeto detetado. O utilizador poderá aceder à mensagem com um anexo seguro. Se não for possível desinfetar o objeto, o Kaspersky Endpoint Security elimina o objeto infetado. O</p>

	<p>Kaspersky Endpoint Security adiciona as informações sobre a ação executada ao assunto da mensagem: [A mensagem foi processada] <assunto da mensagem>.</p> <p>Desinfetar, bloquear se a desinfecção falhar. Quando um objeto infetado é detetado numa mensagem de entrada, o Kaspersky Endpoint Security tenta desinfetar o objeto detetado. O utilizador poderá aceder à mensagem com um anexo seguro. Se não for possível desinfetar o objeto, o Kaspersky Endpoint Security adiciona um aviso ao assunto da mensagem: [A mensagem necessita da sua participação no processamento] <assunto da mensagem>. O utilizador poderá aceder à mensagem com o anexo original. Quando um objeto infetado é detetado numa mensagem de saída, o Kaspersky Endpoint Security tenta desinfetar o objeto detetado. Se não for possível desinfetar o objeto, o Kaspersky Endpoint Security bloqueia a transmissão da mensagem e o cliente de e-mail apresenta um erro.</p> <p>Bloquear. Se for detetado um objeto infetado numa mensagem de entrada, o Kaspersky Endpoint Security adiciona um aviso ao assunto da mensagem: [A mensagem necessita da sua participação no processamento] <assunto da mensagem>. O utilizador poderá aceder à mensagem com o anexo original. Se for detetado um objeto infetado numa mensagem de saída, o Kaspersky Endpoint Security bloqueia a transmissão da mensagem e o cliente de e-mail apresenta um erro.</p>
<p>Âmbito de proteção <i>(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)</i></p>	<p>O <i>Âmbito de proteção</i> inclui objetos que o componente verifica quando está em execução: Mensagens de entrada e de saída ou Apenas mensagens de entrada.</p> <p>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.</p>
<p>Verificar tráfego POP3, SMTP, NNTP e IMAP</p>	<p>A caixa de verificação ativa/desativa a verificação pelo componente Proteção contra ameaças de correio do tráfego transferido através dos protocolos POP3, SMTP, NNTP e IMAP.</p>
<p>Ligar a extensão do Microsoft Outlook</p>	<p>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.</p> <p>Se o correio for verificado utilizando a extensão do Microsoft Outlook, recomenda-se a utilização do Modo Exchange em Cache. Para obter informações mais detalhadas sobre o Modo Exchange em Cache e recomendações sobre a sua utilização, consulte a Base de Conhecimentos da Microsoft.</p>
<p>Análise heurística <i>(disponível apenas na Consola de Administração (MMC) e na interface do Kaspersky Endpoint Security)</i></p>	<p>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.</p> <p>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.</p>
<p>Verificar arquivos anexados</p>	<p>A verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros formatos de arquivo.</p>

	<p>Se, durante a análise, o Kaspersky Endpoint Security detetar uma password para um arquivo no texto da mensagem, esta password será usada para analisar o conteúdo do arquivo relativamente a 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.</p>
<p>Analisar ficheiros anexados com formatos do Microsoft Office</p>	<p>Verifica ficheiros do Microsoft Office (DOC, DOCX, XLS, PPT e outras extensões da Microsoft). Ficheiros de formato do Office incluem objetos OLE também.</p>
<p>Não verificar arquivos com tamanho superior a N MB</p>	<p>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.</p>
<p>Limite o tempo de verificação de arquivos a N seg</p>	<p>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.</p>
<p>Filtro de anexos</p>	<div data-bbox="375 1131 1497 1220" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>A filtragem de anexos não é aplicada às mensagens de e-mail enviadas.</p> </div> <p>Desativar filtragem. Se esta opção estiver selecionada, o componente Proteção contra ameaças de correio não filtra ficheiros anexados a mensagens de e-mail.</p> <p>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.</p> <p>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.</p> <p>Na lista de máscaras de ficheiros, pode especificar os tipos de ficheiros anexados para mudar o nome ou eliminar mensagens de e-mail.</p>

Proteção contra ameaças de Rede

O componente Proteção contra ameaças de Rede verifica o tráfego de rede de entrada quanto à existência de atividades típicas de ataques de rede. Quando o Kaspersky Endpoint Security deteta uma tentativa de ataque à rede no computador do utilizador, bloqueia a ligação da rede a o computador atacante. As bases de dados do Kaspersky Endpoint Security 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](#).

Definições do componente Proteção contra ameaças de Rede

Parâmetro	Descrição
<p>Tratar a análise de portas e o congestionamento de rede como ataques</p>	<p>A <i>saturação de redes</i> 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.</p> <p>Um ataque de <i>mapeamento de portas</i> 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.</p> <p>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.</p> <p>Pode desativar a deteção 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.</p>
<p>Adicionar um computador de ataque à lista de computadores bloqueados durante N min</p>	<p>Se a caixa de verificação estiver selecionada, o componente Proteção contra ameaças de Rede adiciona o computador atacante 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 32 768 minutos.</p> <p>Pode ver a lista do bloco na janela da ferramenta Monitor de Rede.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>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.</p> </div>
<p>Exclusões</p>	<p>Esta lista contém os endereços IP a partir dos quais a Proteção contra ameaças de Rede não bloqueia ataques de rede.</p> <p>A aplicação não regista informação sobre os ataques de rede dos endereços IP que estejam na lista de exclusões.</p>
<p>Proteção contra ataques de MAC Spoofing</p>	<p>Um <i>ataque de simulação MAC</i> 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.</p>

Firewall

A Firewall bloqueia ligações não autorizadas ao computador enquanto trabalha na Internet ou na 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 impõem 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 usando 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 fiáveis*: Fiável/Restrições baixas/Restrições altas/Não fiável.

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 de Intrusão do Host.

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 Alta Restrição 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 da seguinte maneira: uma regra de rede para aplicações inclui regras de acesso com base no estado da rede: *pública*, *local* ou *fiável*. Por exemplo, por predefinição, não é permitida nenhuma atividade de rede das aplicações no grupo fiável Alta Restrição 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.

Estados da ligação de rede

A Firewall permite controlar a atividade da rede, dependendo do estado da ligação de rede. O Kaspersky Endpoint Security recebe o estado da ligação de rede a partir do sistema operativo do computador. O estado da ligação de rede no sistema operacional é definido pelo utilizador ao configurar a ligação. Pode [alterar o estado da ligação de rede nas definições do Kaspersky Endpoint Security](#). A Firewall monitoriza a atividade da rede, dependendo do estado da rede nas definições do Kaspersky Endpoint Security, e não do sistema operativo.

A ligação de rede pode ter um dos seguintes tipos de estado:

- **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 estado *Rede pública* à Internet. Não é possível alterar o estado 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 o 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 de rede	<p>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.</p> <p>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.</p> <p>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.</p> <p>As regras de pacotes de rede têm uma prioridade mais elevada do que as regras de rede para aplicações.</p>
Ligações de rede	<p>Esta tabela contém informações sobre as ligações de rede que a Firewall deteta no computador.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Por predefinição, é atribuído o estado <i>Rede pública</i> à Internet. Não é possível alterar o estado da Internet.</p> </div>
Regras de rede	<p>Anexos</p> <p>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.</p> <p>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.</p> <p>Regras de rede</p> <p>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.</p> <p>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.</p>

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 ao 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.

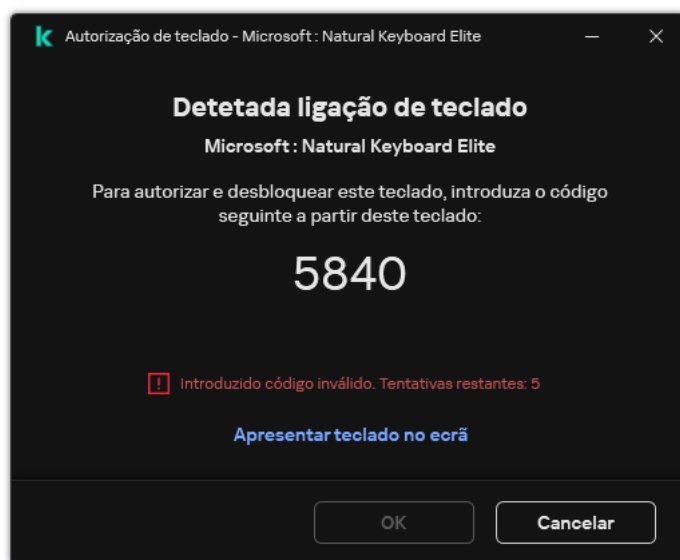
Se o código tiver sido introduzido corretamente, a aplicação guarda os parâmetros de identificação – VID/PID do teclado e o número da porta à qual foi ligado – na lista de teclados autorizados. A autorização de teclado não precisa de ser repetida quando o teclado voltar a ser ligado ou depois de o sistema operativo ser reiniciado.

Quando o teclado autorizado é ligado ao computador numa porta USB diferente, a aplicação volta a mostrar uma solicitação para 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.

Por predefinição, o componente Prevenção de ataques BadUSB não está instalado. Se precisar do componente Prevenção de ataques BadUSB, pode adicionar o componente nas propriedades do [pacote de instalação](#) antes de instalar a aplicação ou [alterar os componentes disponíveis da aplicação](#) depois da instalação da aplicação.



Autorização de teclado

Definições do componente de Prevenção de ataques BadUSB

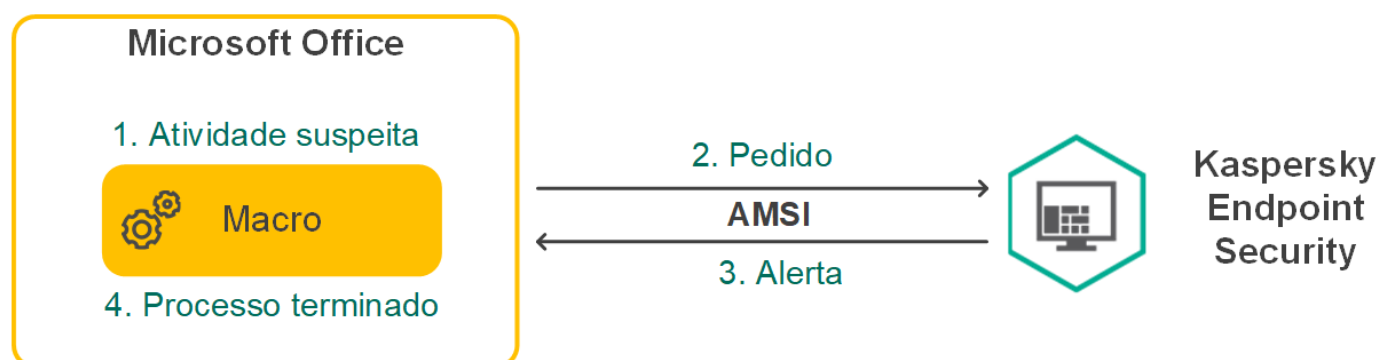
Parâmetro	Descrição

Proibir a utilização do Teclado no ecrã para autorização de dispositivos USB	Se a caixa de verificação estiver selecionada, 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.
Número máximo de tentativas de autorização do dispositivo	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 5 tentativas de introdução do código de autorização, o dispositivo USB será bloqueado após a quinta tentativa falhada. O Kaspersky Endpoint Security apresenta a duração do bloqueio do dispositivo USB. Após decorrido este tempo, tem 5 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 falhadas de introdução do 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. A aplicação de terceiros depois de receber uma notificação de uma ameaça não permite a realização de ações maliciosas (por exemplo, terminação).



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;
- Windows 11;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

Definições de Proteção AMSI

Parâmetro	Descrição
Verificar arquivos	A verificar ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e outros formatos de arquivo.
Verificar pacotes de distribuição	Esta caixa de verificação ativa/desativa a verificação de pacotes de distribuição 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.
Não descompactar ficheiros compostos extensos	<p>Se esta caixa de verificação estiver selecionada, o Kaspersky Endpoint Security não verifica ficheiros compostos se o tamanho destes exceder o valor especificado.</p> <p>Se esta caixa de verificação for desmarcada, o Kaspersky Endpoint Security verifica ficheiros compostos de todos os tamanhos.</p> <p>O Kaspersky Endpoint Security verifica ficheiros grandes que são extraídos dos arquivos, independentemente de a caixa de verificação estar marcada ou não.</p>

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.

Definições do componente Prevenção de explorações

Parâmetro	Descrição

<p>Ao detetar exploração</p>	<p>Bloquear operação. 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.</p> <p>Notificar. 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.</p>
<p>Ativar proteção da memória de processos do sistema</p>	<p>Se este botão estiver ativado, o Kaspersky Endpoint Security bloqueia processos externos que tentam aceder à memória do processo de sistema.</p>

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 com base em assinaturas de fluxos de comportamento proporciona defesa proativa ao computador.

Definições do componente Deteção de comportamento

Parâmetro	Descrição
<p>Ao detetar atividade de software malicioso</p>	<ul style="list-style-type: none"> • Delete file. 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. • Terminar a aplicação. Se esta opção estiver selecionada, ao detetar atividade maliciosa, o Kaspersky Endpoint Security encerra a aplicação em questão. • Notificar. 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.
<p>Ativar a proteção de pastas partilhadas contra encriptação externa</p>	<p>Se o botão estiver ativado, o Kaspersky Endpoint Security analisa a atividade nas 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.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>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.</p> </div> <ul style="list-style-type: none"> • Notificar. Se esta opção estiver selecionada, o Kaspersky Endpoint Security, ao detetar uma tentativa de modificar ficheiros em pastas partilhadas, adiciona informação sobre esta tentativa de modificar ficheiros em pastas partilhadas à lista de ameaças ativas. • Bloquear ligação durante N minutos. Se esta opção for selecionada, quando o Kaspersky Endpoint Security detetar uma tentativa de modificação dos ficheiros nas

	<p>pastas partilhadas, bloqueia a atividade da rede do computador que está a tentar modificar os ficheiros e cria cópias de segurança dos ficheiros modificados.</p> <p>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.</p>
Exclusões	<p>A lista de computadores a partir dos quais as tentativas de encriptar pastas partilhadas não serão monitorizadas.</p> <p>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.</p>

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 (como ficheiros e aplicações)

A atividade de rede das aplicações é controlada pela [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 usando 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 fiáveis*: Fiável/Restrições baixas/Restrições altas/Não fiável.

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 de Intrusão do Host.

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.

Definições de componente Prevenção contra invasões do anfitrião

Parâmetro	Descrição
Direitos de aplicações	<p>Anexos</p> <p>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.</p> <p>Pode seleccionar 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.</p> <p>Os direitos de acesso à aplicação são apresentados nas seguintes tabelas:</p> <ul style="list-style-type: none">• Ficheiros e registo do sistema. Esta tabela contém os direitos de aplicações num grupo fiável para aceder aos recursos do sistema operativo e aos dados pessoais.• Direitos. Esta coluna apresenta os direitos de aplicações num grupo fiável para aceder aos processos e recursos do sistema operativo.• 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	<p>Nome</p> <p>A tabela contém recursos do computador categorizados. O componente Prevenção contra invasões monitoriza as tentativas de outras aplicações de aceder aos recursos na tabela.</p> <p>Um recurso pode ser uma categoria de registo, ficheiro ou pasta, ou chave de registo.</p> <p>Anexos</p> <p>Tabela de aplicações monitorizadas pelo componente Prevenção de Intrusão do Host para o recurso seleccionado. 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.</p>

<p>Grupo fiável para aplicações iniciadas antes do Kaspersky Endpoint Security for Windows começar a trabalhar</p>	<p>Um grupo fiável no qual o Kaspersky Endpoint Security colocará aplicações iniciadas antes do Kaspersky Endpoint Security.</p>
<p>Atualizar direitos para as aplicações previamente desconhecidas das bases de dados da KSN</p>	<p>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.</p>
<p>Confiar nas aplicações assinadas digitalmente</p>	<p>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.</p> <p><i>Fornecedores fiáveis</i> são os fornecedores de software considerados fiáveis pela Kaspersky. Pode também adicionar manualmente um certificado de fornecedor ao arquivo de certificado fiável.</p> <p>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.</p>
<p>Eliminar regras para as aplicações que não são iniciadas há mais de (dias, 1 a 90)</p>	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>Na próxima vez que iniciar essa aplicação, o Kaspersky Endpoint Security analisa a aplicação como se fosse iniciada pela primeira vez.</p>
<p>Grupo fiável para aplicações que não foi possível adicionar a grupos existentes</p>	<p>Os itens nesta lista pendente determinam a que grupo fiável o Kaspersky Endpoint Security atribuirá uma aplicação desconhecida.</p> <p>Pode selecionar um dos itens seguintes:</p> <ul style="list-style-type: none"> • Restrições baixas. • Restrições altas. • Não fiáveis.

Motor de remediação

O 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 um [scan de vírus](#).

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 *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 categoria e reputação dos ficheiros verificados bem como informações sobre a reputação dos endereços da Web verificados.

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.

Para reduzir a sobrecarga nos servidores da KSN, os peritos da Kaspersky podem laçar atualizações da aplicação que desativam temporariamente ou restringem em parte os pedidos à Kaspersky Security Network. Neste caso, o estado da ligação à KSN na interface local da aplicação é *Ativado com restrições*.

Infraestrutura da KSN

O Kaspersky Endpoint Security suporta as seguintes soluções infraestruturais da KSN:

- *KSN Global* é a solução usada pela maioria das aplicações da Kaspersky. Os participantes na KSN recebem informações da Kaspersky Security Network 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.
- *Private KSN* 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 KSN Privado 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.

Por predefinição, o Kaspersky Security Center usa a KSN Global. Pode configurar a utilização do KSN Privado na Consola de Administração (MMC), na Consola Web do Kaspersky Security Center e na [Command line](#). Não é possível configurar a utilização da KSN Privada na Consola de Nuvem do Kaspersky Security Center.

Para obter mais informações detalhadas sobre o KSN Privado, consulte a *documentação sobre a Kaspersky Private Security Network*.

KSN Proxy

Os computadores de utilizador geridos pelo Servidor de Administração do Kaspersky Security Center podem interagir com a KSN através do serviço KSN Proxy.

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.

Para obter mais informações no serviço KSN Proxy, consulte a [Ajuda do Kaspersky Security Center](#).

Definições da Kaspersky Security Network

Parâmetro	Descrição
Ativar o modo KSN alargado	<p><i>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.</i></p>
Ativar o modo de nuvem	<p><i>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.</i></p> <p>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.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"><p>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.</p></div> <p>Se o botão estiver desativado, o Kaspersky Endpoint Security utiliza a versão completa das bases de dados de antivírus.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"><p>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.</p></div>
Estado do computador quando os servidores da KSN não estão disponíveis <i>(disponível apenas na Consola do Kaspersky Security Center)</i>	<p>Os itens nesta lista pendente determinam o estado de um computador no Kaspersky Security Center quando os servidores da KSN estão indisponíveis.</p>

<p>Utilizar proxy da KSN</p> <p><i>(disponível apenas na Consola do Kaspersky Security Center)</i></p>	<p>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.</p>
<p>Utilizar os servidores da KSN quando o proxy da KSN não está disponível</p> <p><i>(disponível apenas na Consola do Kaspersky Security Center)</i></p>	<p>Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security utiliza os servidores da KSN quando o serviço de proxy da KSN estiver indisponível. Os servidores da KSN podem estar localizados quer na Kaspersky (quando a KSN Global é utilizada) quer em terceiros (quando a KSN Privada é utilizada).</p>

Controlo de Internet

O Controlo de Internet gere o acesso dos utilizadores 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).

O Kaspersky Endpoint Security monitoriza apenas os tráfegos HTTP e HTTPS.

Para monitorização do tráfego HTTPS, precisa de [ativar a verificação de ligações encriptadas](#).

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 dos utilizadores aos dados num site e ocultar imagens gráficas, 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 "Ficheiros 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 do Office» apenas para a categoria do site «Correio eletrónico baseado na Internet».

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.



A página da Internet solicitada não pode ser apresentada.

Endereço: <http://kaspersky.ru/>.

A página da Internet foi bloqueada pela regra kasp.

Razão: o recurso da Internet pertence à(s) categoria(s) de conteúdo Indeterminado e à(s) categoria(s) de tipo de dados Indeterminado.

Este recurso da Internet é proibido na empresa. Se considerar o bloqueio incorreto ou se necessitar de aceder a este recurso da Internet, queira contactar o administrador da rede local da empresa ([Solicitar acesso](#)).

Mensagem gerada a: 10/14/2020 3:55:16 AM



A página da Internet solicitada pode não ser segura ou ser proibida pela política da empresa.

Endereço: <http://kaspersky.ru/>.

A página da Internet foi bloqueada pela regra kasp.

Razão: o recurso da Internet pertence à(s) categoria(s) de conteúdo Indeterminado e à(s) categoria(s) de tipo de dados Indeterminado.

Clique na ligação <http://kaspersky.ru/> para abrir a página da Internet solicitada.

Clique na ligação http://kaspersky.ru/* para obter acesso a todos os conteúdos do site no qual a página da Internet solicitada se encontra.

Clique na ligação */*.kaspersky.ru/* para obter acesso a todos os domínios existentes de nível inferior ou igual com o marcado com \"*\".

O acesso aos recursos da Internet referidos acima será concedido durante a sessão atual do Kaspersky Endpoint Security. Em caso de um aviso incorreto, contacte o administrador da rede local da empresa ([Solicitar acesso](#)).

Mensagem gerada a: 10/14/2020 3:56:21 AM

Mensagens do Controlo de Internet

Definições do componente 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	<p>A <i>Regra predefinida</i> é uma regra para aceder a recursos da Web que não são cobertos por nenhuma outra regra. Estão disponíveis as seguintes opções:</p> <ul style="list-style-type: none">• 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.

<p>Modelos de mensagem</p>	<ul style="list-style-type: none"> • 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.
<p>Registar a abertura de páginas permitidas</p>	<p>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.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Monitorizar a atividade da Internet do utilizador pode exigir mais recursos do computador ao descriptar o tráfego HTTPS.</p> </div>

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.

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 – 🚫.
- Depende do barramento de ligação (exceto para 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). Como tal, o utilizador pode restringir a ligação de todos os dispositivos, por exemplo, a 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.

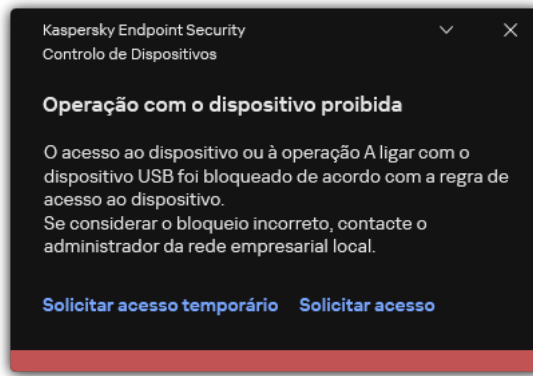
Pode adicionar dispositivos fiáveis com base nos seguintes dados:

- **Dispositivos por ID.** Cada dispositivo possui um identificador exclusivo (ID do hardware ou HWID). Pode ver a ID nas propriedades de dispositivo utilizando ferramentas do sistema operativo. Exemplo de 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 ID do fornecedor (VID) e um ID do produto (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 carácter `*` substitui qualquer conjunto de caracteres. O Kaspersky Endpoint Security não suporta o carácter `?` 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 carácter `*` substitui qualquer conjunto de caracteres. O Kaspersky Endpoint Security não suporta o carácter `?` 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.

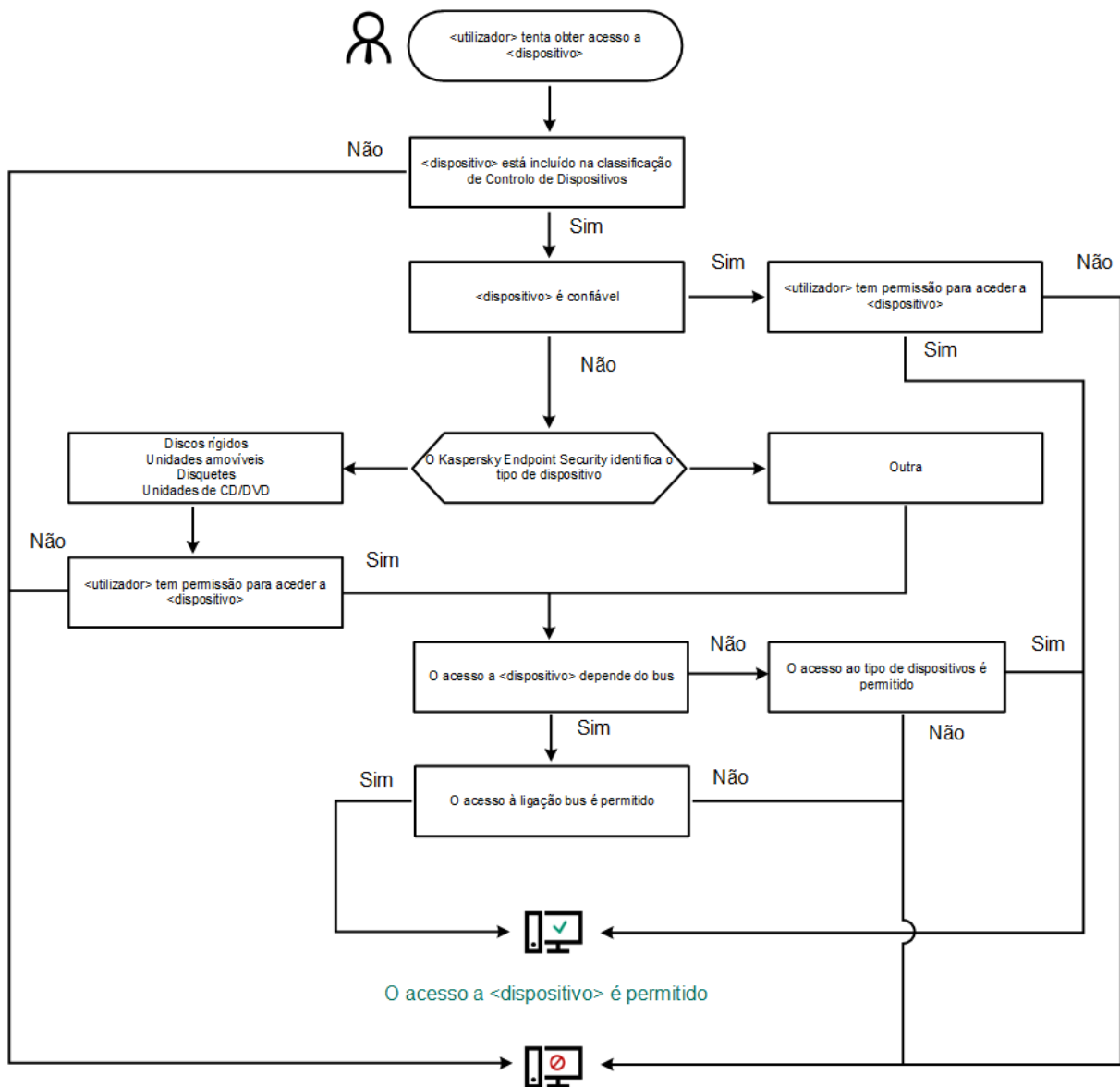
Quando um dispositivo que está bloqueado pelo Controlo de Dispositivos é ligado ao computador, o Kaspersky Endpoint Security bloqueará o acesso e apresentará uma notificação (ver a figura abaixo).



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).



O acesso a <dispositivo> está bloqueado

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](#).

Definições do componente Controlo de Dispositivos

Parâmetro	Descrição
<p>Permitir pedido de acesso temporário</p> <p><i>(disponível apenas na Consola do Kaspersky Security Center)</i></p>	<p>Se a caixa de verificação estiver seleccionada, o botão Solicitar acesso está disponível na interface local do Kaspersky Endpoint Security. Clique neste botão para abrir a janela Solicitar acesso ao dispositivo. Nesta janela, o utilizador pode solicitar o acesso temporário a um dispositivo bloqueado.</p>
<p>Dispositivos e redes Wi-Fi</p>	<p>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.</p>
<p>Barramentos de ligação</p>	<p>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.</p>
<p>Dispositivos fiáveis</p>	<p>Lista de dispositivos fiáveis e utilizadores com acesso a estes dispositivos.</p>
<p>Anti-Bridging</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>O Anti-Bridging suporta a operação com os seguintes tipos de dispositivos: adaptador de rede, Wi-Fi e modem.</p>
<p>Modelos de mensagem</p>	<ul style="list-style-type: none"> • 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.

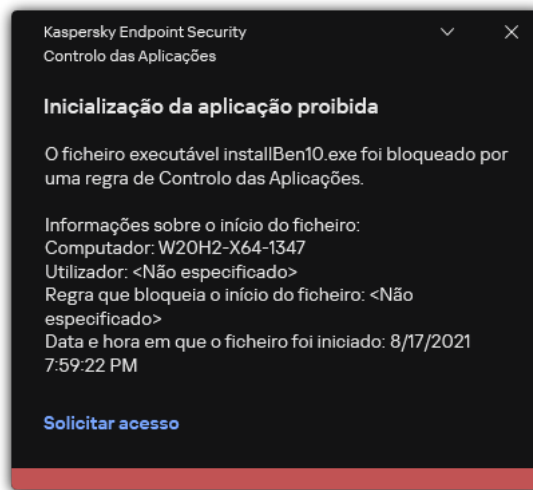
3. [Selecionar o modo de Controlo das Aplicações.](#)

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](#).

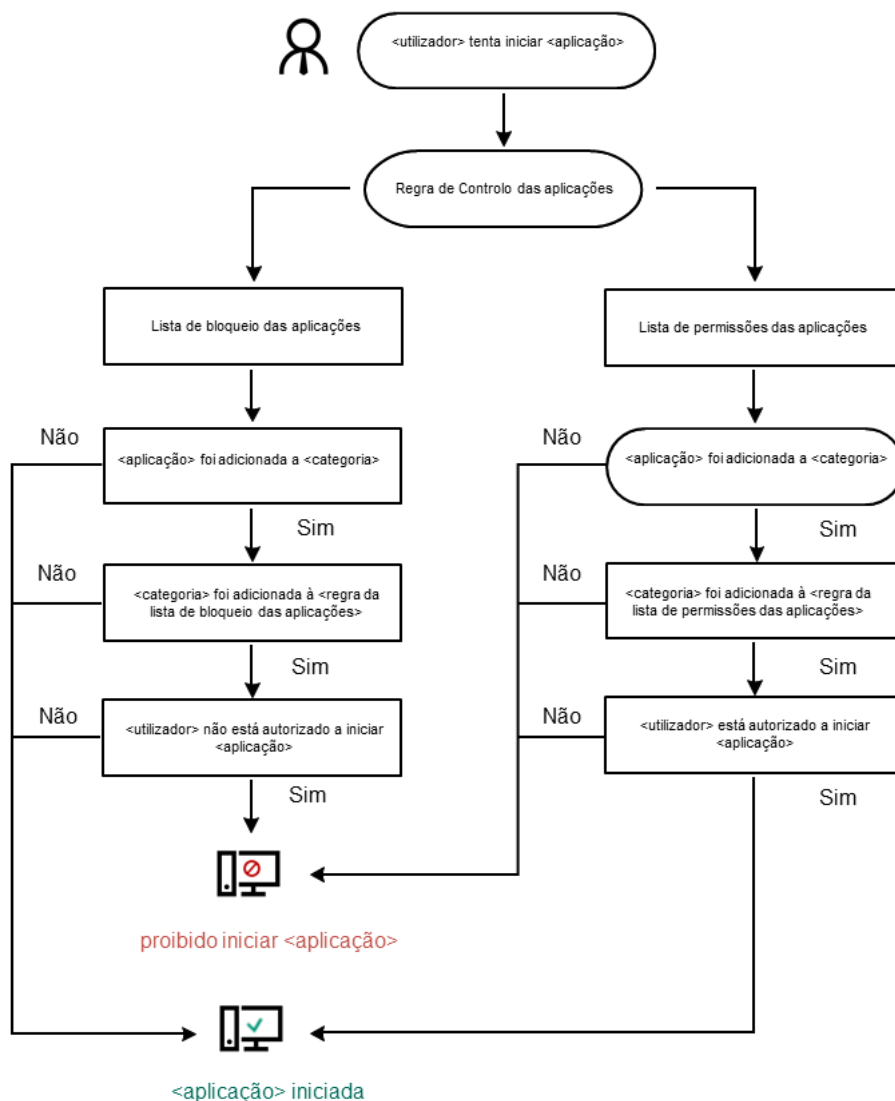
As Regras de Controlo das aplicações criadas na Consola de Administração do Kaspersky Security Center baseiam-se nas suas categorias de aplicações personalizadas e não nas condições de inclusão ou de exclusão, como na interface local do Kaspersky Endpoint Security.

- [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

Definições do componente Controlo das Aplicações

Parâmetro	Descrição
Test mode	Se este botão estiver ativado, 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.
Application Control Mode	<p>Pode seleccionar um das itens opções:</p> <ul style="list-style-type: none"> Lista de bloqueio. Se esta opção estiver seleccionada, 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 seleccionada, o Controlo das Aplicações bloqueia todos os utilizadores de iniciarem qualquer tipo de aplicação, exceto nos

	<p>casos em que satisfazem as condições das regras de permissão do Controlo das Aplicações.</p> <p>Quando o modo Lista de permissão está selecionado, são automaticamente criadas duas regras de Controlo das Aplicações:</p> <ul style="list-style-type: none"> • Golden Image. • Atualizadores fiáveis. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Não pode editar as definições nem eliminar as regras automaticamente criadas. Pode ativar ou desativar estas regras.</p> </div>
<p>Control DLL modules load (significantly increases the load on the system)</p>	<p>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.</p> <div style="background-color: #f8d7da; padding: 10px; margin-top: 10px;"> <p>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 "Certificados fiáveis", 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.</p> </div> <p>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.</p>
<p>Message templates</p>	<p>Message about blocking. Modelo da mensagem que é apresentada quando é acionada uma regra de Controlo das Aplicações que bloqueia o início de uma aplicação.</p> <p>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. 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.</p>

Controlo de Anomalias Adaptativo

Este componente está disponível apenas para o Kaspersky Endpoint Security for Business Advanced e para o Kaspersky Total Security for Business. Para obter mais informações sobre o Kaspersky Endpoint Security for Business, visite o [site da Kaspersky](#).

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 do *Início do Microsoft PowerShell a partir de uma aplicação do escritório*). 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 de regras](#) e no repositório do **Triggering of rules in Smart Training state**.

2. A analisar o relatório de acionamento de regras.

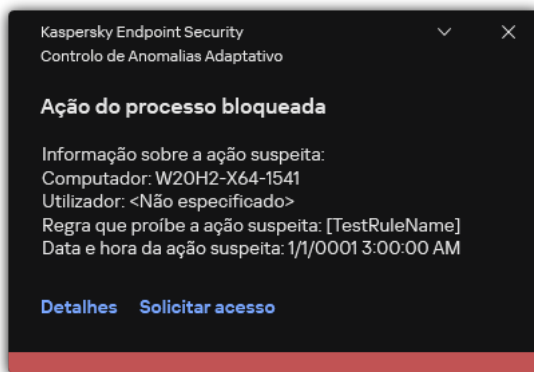
O administrador analisa o [relatório de acionamento de regras](#) ou o conteúdo do repositório do **Triggering of rules in Smart Training state**. O administrador pode então selecionar o comportamento do Controlo de Anomalias Adaptativo quando a regra é acionada: bloquear ou permitir. O administrador 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. O Controlo de Anomalias Adaptativo é configurado 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 **Triggering of rules in Smart Training state**.

Recomenda-se a verificação do relatório de acionamento de regras e o conteúdo do repositório de **Triggering of rules in Smart Training state**.

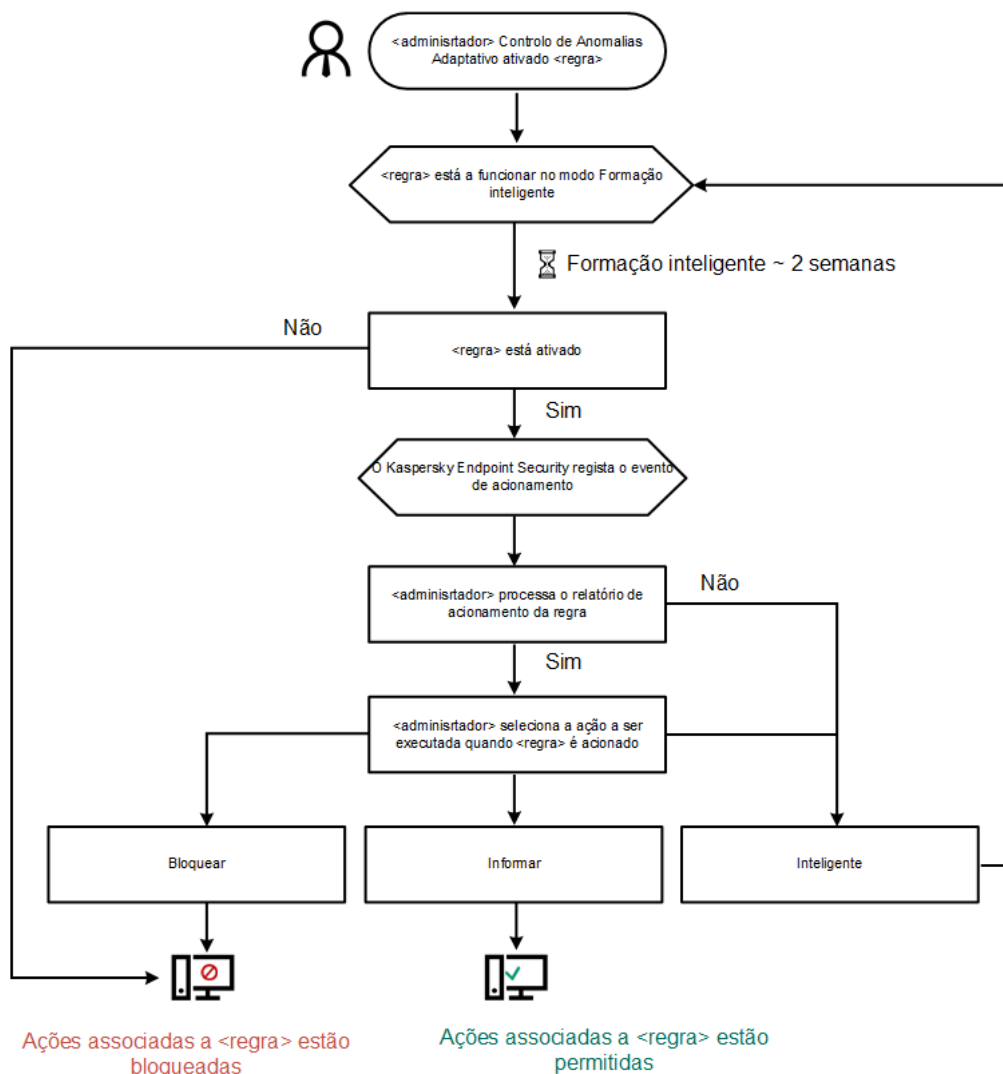
Quando uma aplicação maliciosa tentar realizar uma ação, o Kaspersky Endpoint Security irá bloquear a ação e exibir uma notificação (ver figura abaixo).



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

Parâmetro	Descrição
<p>Reportar o estado das regras do Controlo de anomalias adaptativo</p> <p><i>(disponível apenas na Consola do Kaspersky Security Center)</i></p>	<p>Este relatório contém informações sobre o estado das regras de deteção do Controlo de Anomalias Adaptativo (por exemplo, <i>Desligado</i> ou <i>Bloquear</i>). O relatório é gerado para todos os grupos de administração.</p>
<p>Report on triggered rules of Adaptive Anomaly Control</p> <p><i>(disponível apenas na Consola do Kaspersky Security Center)</i></p>	<p>Este relatório contém informações sobre ações não típicas detetadas pelo Controlo de Anomalias Adaptativo. O relatório é gerado para todos os grupos de administração.</p>
<p>Regras</p>	<p>Tabela de regras do Controlo de Anomalias Adaptativo. As regras são criadas pelos especialistas da Kaspersky com base em cenários típicos de atividade potencialmente maliciosa.</p>
<p>Modelos</p>	<ul style="list-style-type: none"> • 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.

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 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. Kaspersky Anti Targeted Attack Platform inclui dois blocos funcionais: Kaspersky Anti Targeted Attack (daqui em diante também designada por "KATA") e Kaspersky Endpoint Detection and Response (doravante denominado "KEDR"). Pode comprar o KEDR 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 Professional / Enterprise;
- Windows 10 RS3 Home / Professional / Education / Enterprise;
- Windows 10 RS4 Home / Professional / Education / Enterprise;
- Windows 10 RS5 Home / Professional / Education / Enterprise;
- Windows 10 RS6 Home / Professional / Education / Enterprise;
- Windows Server 2008 R2 Foundation / Standard / Enterprise (64 bits);
- Windows Server 2012 Foundation / Standard / Enterprise (64 bits);
- Windows Server 2012 R2 Foundation / Standard / Enterprise (64 bits);
- Windows Server 2016 Essentials / Standard (64 bits).

Para obter informações detalhadas sobre o funcionamento da KATA, consulte a [Ajuda da Kaspersky Anti Targeted Attack Platform](#).

Kaspersky Sandbox

O Kaspersky Endpoint Security 11.7.0 possui agora um agente integrado para integração com a solução Kaspersky Sandbox. A *solução Kaspersky Sandbox* deteta e bloqueia automaticamente ameaças avançadas em computadores. O Kaspersky Sandbox analisa o comportamento do objeto para detetar atividades maliciosas e atividades características de ataques direcionados à infraestrutura de TI da organização. O Kaspersky Sandbox analisa e verifica objetos em servidores especiais com imagens virtuais implementadas de sistemas operativos Microsoft Windows (servidores do Kaspersky Sandbox). Para obter mais informações sobre a solução, consulte a [Ajuda do Kaspersky Sandbox](#).

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 Kaspersky Sandbox

Parâmetro	Descrição
Server TLS certificate	Para configurar uma ligação fiável com os servidores do Kaspersky Sandbox, deve preparar um certificado TLS. Em seguida, deve adicionar o certificado aos servidores do Kaspersky Sandbox e à política do Kaspersky Endpoint Security. Para obter mais informações sobre como preparar o certificado e adicionar o certificado aos servidores, consulte a Ajuda do Kaspersky Sandbox .
Tempo limite	Tempo limite de ligação para o servidor Kaspersky 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 Kaspersky Sandbox se a velocidade da sua ligação for baixa ou instável. O tempo limite recomendado do pedido é de 0,5 segundos ou menos.
Fila de pedidos do Kaspersky Sandbox	Tamanho da pasta da fila de pedidos. Quando um objeto é acedido no computador (ficheiro executável iniciado ou documento aberto, por exemplo, em formato DOCX ou PDF), o Kaspersky Endpoint Security também pode enviar o objeto para ser verificado pelo Kaspersky Sandbox. Se houver vários pedidos, 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 Kaspersky 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.
Servidores do Kaspersky Sandbox	Definições de ligação do servidor do Kaspersky 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.
Ação após deteção de ameaças	<p>Mova a cópia para a Quarentena, elimine o objeto. 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.</p> <p>Executar verificação de áreas críticas. Se esta opção for selecionada, o Kaspersky Endpoint Security executa a tarefa 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.</p> <p>Crie uma tarefa de verificação IOC. Se esta opção for selecionada, o Kaspersky Endpoint Security cria automaticamente uma tarefa Verificação IOC (<i>tarefa de verificação IOC autónoma</i>). Para esta tarefa, pode configurar o modo de execução, âmbito de verificação e ação na deteção de IOC: eliminar objeto, executar a tarefa Verificação de Áreas Críticas. Para modificar outras definições da tarefa Verificação IOC, aceda às definições da tarefa.</p>

Âmbito da Verificação IOC	<p>Áreas críticas do ficheiro. 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.</p> <p>Áreas do ficheiro nas unidades de sistema do computador. Se esta opção for selecionada, o Kaspersky Endpoint Security fará uma verificação IOC na unidade de sistema do computador.</p>
Execute a tarefa de verificação IOC	<p>Manualmente. Modo de execução no qual pode iniciar a tarefa <i>Verificação IOC</i> manualmente num momento à sua escolha.</p> <p>Após deteção da ameaça. Modo de execução no qual o Kaspersky Endpoint Security executa a tarefa <i>Verificação IOC</i> automaticamente sempre que uma ameaça é detetada.</p> <p>Executar apenas quando o computador está inativo. Modo de execução no qual o Kaspersky Endpoint Security executa a tarefa <i>Verificação IOC</i> 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.</p>

Endpoint Detection and Response

O Kaspersky Endpoint Security 11.7.0 agora tem um agente integrado para a solução Kaspersky Endpoint Detection and Response Optimum (doravante também referida como "EDR Optimum"). O Kaspersky Endpoint Security 11.8.0 agora 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 *personal 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. 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 EDR Optimum na Consola Web e na Cloud Console. As definições dos componentes para o EDR Expert estão disponíveis apenas na Cloud Console.

Definições do Endpoint Detection and Response

Parâmetro	Descrição
Isolamento da rede	<p>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:</p> <ul style="list-style-type: none"> • Ligações listadas em Network isolation exclusions. • Ligações iniciadas pelos serviços do Kaspersky Endpoint Security. • Ligações iniciadas pelo agente de Administração do Kaspersky Security Center.

Desbloqueia automaticamente o computador isolado em N horas	<p>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.</p>
Network isolation exclusions	<p>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.</p> <p>Para configurar as exclusões de isolamento da rede, pode utilizar uma lista de <i>perfis de rede padrão</i>. 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.</p> <div style="background-color: #f8d7da; padding: 10px; margin-top: 10px;"> <p>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.</p> </div>
Prevenção da execução	<p>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.</p>
Action on execution or opening of forbidden object	<p>Block and write to report. 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.</p> <p>Log events only. 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. Este modo está selecionado por predefinição.</p>
Regras de bloqueio de execução	<p>Lista de regras de bloqueio de execução de um objeto. As <i>Regras de bloqueio de execução</i> são um conjunto de critérios que são tidos em consideração para o bloqueio. A aplicação identifica ficheiros pelos seus caminhos ou somas de verificação calculadas utilizando algoritmos hash MD5 e SHA256.</p>

Encriptação de disco completa

Pode seleccionar uma tecnologia de encriptação: Encriptação de disco Kaspersky ou Encriptação de Unidade BitLocker (aqui também referida simplesmente como "BitLocker").

Encriptação de disco Kaspersky

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 palavra-passe do token ou smart card ligado ao computador ou o nome de utilizador e a palavra-passe da conta do Agente de Autenticação criada pelo administrador da rede local, utilizando a tarefa [Gestão de contas do 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 de autenticação única \(SSO\)](#), 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 o Kaspersky Security Center. O BitLocker encripta volumes lógicos. Não pode utilizar o BitLocker para encriptação de unidades removíveis. Para obter mais informações sobre o BitLocker, consulte a [documentação da Microsoft](#).

O BitLocker fornece armazenamento seguro de chaves de acesso utilizando um módulo de plataforma fiável. Um *Módulo de plataforma fiável (TPM)* 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 uma unidade, o BitLocker cria uma chave mestra. O Kaspersky Endpoint Security envia a chave mestra 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 [informações sobre a encriptação do disco ao Kaspersky Security Center](#). No entanto, o Kaspersky Endpoint Security não enviará a chave mestra ao Kaspersky Security Center, por isso será impossível restaurar o acesso ao disco utilizando o Kaspersky Security Center. Para que o BitLocker funcione corretamente com o Kaspersky Security Center, [desencripte a unidade](#) e [volte a encriptar a unidade](#) utilizando uma política. Pode desencriptar uma unidade localmente ou utilizando uma política.

Depois de encriptar o disco rígido do sistema, o utilizador precisa passar pela autenticação do BitLocker para inicializar o sistema operativo. Depois do procedimento de autenticação, o BitLocker permitirá aos utilizadores iniciarem sessão. O BitLocker não oferece suporte à tecnologia de início de sessão único (SSO).

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	<p>Encriptar todas as unidades de discos rígido. Se este item estiver seleccionado, a aplicação encripta todas as unidades de disco rígido quando a política é aplicada.</p> <div style="border: 1px solid #f08080; padding: 5px; margin: 10px 0;"> <p>Se o computador tiver vários sistemas operativos instalados, após a encriptação apenas poderá carregar o sistema operativo com a aplicação instalada.</p> </div> <p>Desencriptar todas as unidades de discos rígido. Se este item estiver seleccionado, a aplicação desencripta todas as unidades de disco rígido previamente encriptadas quando a política é aplicada.</p> <p>Manter inalterado. Se este item estiver seleccionado, 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 seleccionado.</p>
Durante a encriptação, criar automaticamente contas do Agente de Autenticação para utilizadores do Windows	<p>Se esta caixa de verificação estiver seleccionada, 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.</p>
Def. criação conta de Agente de Autenticação	<p>Todas as contas no computador. Se esta caixa de verificação estiver seleccionada, ao executar a tarefa de encriptação de disco completo, o Kaspersky Endpoint Security cria contas de Agente de autenticação para todas as contas de computador que já estiveram ativas.</p> <p>Todas as contas de domínio no computador. Se esta caixa de verificação estiver seleccionada, ao executar a tarefa de encriptação de disco completo, o Kaspersky Endpoint Security cria contas de Agente de autenticação para todas as contas de computador pertencentes a um determinado domínio que já estiveram ativas.</p> <p>Todas as contas locais no computador. Se esta caixa de verificação estiver seleccionada, ao executar a tarefa de encriptação de disco completo, o Kaspersky Endpoint Security cria contas de Agente de autenticação para todas as contas de computador local que já estiveram ativas.</p> <p>Administrador local. Se esta caixa de verificação estiver seleccionada, ao executar a tarefa de encriptação de disco completo, o Kaspersky Endpoint Security cria uma conta de administrador local.</p> <p>Gestor do computador. Se esta caixa de verificação estiver seleccionada, ao executar a tarefa de encriptação de disco completo, o Kaspersky Endpoint Security cria uma conta de Agente de autenticação para a conta cujas propriedades no Active Directory indicam que se trata de uma conta de gestão.</p>

	<p>Conta ativa. Se esta caixa de verificação estiver selecionada, ao executar a tarefa de encriptação de disco completo, o Kaspersky Endpoint Security cria automaticamente uma conta de Agente de autenticação para a conta de computador que está ativa durante a tarefa.</p>
<p>Criar automaticamente contas do Agente de Autenticação para todos os utilizadores deste computador ao iniciar sessão</p>	<p>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 palavra-passe e alteração da palavra-passe na primeira autenticação. Como tal, não é necessário adicionar manualmente contas do Agente de Autenticação através da tarefa <i>Gestão de contas do Agente de Autenticação</i> para computadores com unidades já encriptadas.</p>
<p>Guardar o nome de utilizador introduzir no Agente de Autenticação</p>	<p>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.</p>
<p>Encriptar apenas espaço de disco utilizado</p>	<p>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.</p> <div data-bbox="443 920 1493 1115" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Ativar ou desativar a funcionalidade Encriptar apenas espaço utilizado do disco (Windows 8 e versões mais recentes) após o início da encriptação não altera esta definição até que os discos rígidos sejam desencriptados. Tem de seleccionar ou desmarcar a caixa de verificação antes de iniciar a encriptação.</p> </div> <p>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.</p> <p>Se a caixa de verificação estiver selecionada, é encriptado o disco rígido completo, incluindo os fragmentos residuais de ficheiros anteriormente eliminados e modificados.</p> <div data-bbox="443 1420 1493 1646" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>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.</p> </div> <p>Esta caixa de verificação está desmarcada por predefinição.</p>
<p>Utilizar Legacy USB Support</p>	<p>Esta caixa de verificação ativa/desativa a função Suporte USB de Legado. O <i>Suporte de USB legado</i> 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). Legacy USB Support não afeta o suporte para dispositivos USB após iniciar o sistema operativo.</p> <p>Se a caixa de verificação estiver selecionada, o suporte de dispositivos USB durante o arranque inicial do computador é ativado.</p>

	<p>Quando a função Suporte de USB de Legado 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.</p>
Definições de password	<p>Definições de segurança da password da conta do Agente de Autenticação. Pode ativar também a utilização da tecnologia de autenticação única (SSO).</p> <p>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.</p> <p>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.</p> <p>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.</p>
Help texts	<p>Autenticação. Texto de ajuda que aparece na janela Agente de autenticação ao inserir as credenciais da conta.</p> <p>Alterar password. Texto de ajuda que aparece na janela Agente de autenticação ao alterar a password da conta do Agente de Autenticação.</p> <p>Recuperar password. Texto de ajuda que aparece na janela Agente de autenticação ao recuperar a password da conta do Agente de Autenticação.</p>

Definições do componente Encriptação de Unidade BitLocker

Parâmetro	Descrição
Modo de encriptação	<p>Encriptar todas as unidades de discos rígido. Se este item estiver selecionado, a aplicação encripta todas as unidades de disco rígido quando a política é aplicada.</p> <p>Se o computador tiver vários sistemas operativos instalados, após a encriptação apenas poderá carregar o sistema operativo com a aplicação instalada.</p> <p>Desencriptar todas as unidades de discos rígido. Se este item estiver selecionado, a aplicação desencripta todas as unidades de disco rígido previamente encriptadas quando a política é aplicada.</p> <p>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.</p>
Ativar utilização de autenticação BitLocker que exija introdução por teclado de pré-arranque em tablets	<p>Esta caixa de verificação ativa / desativa a utilização da autenticação com 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).</p> <p>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.</p>

	<p>Se a caixa de verificação estiver selecionada, é permitida a utilização da autenticação com entrada de pré-arranque. Recomenda-se 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.</p> <p>Se a caixa de verificação estiver desmarcada, não é possível executar a Encriptação de Unidade BitLocker em tablets.</p>
<p>Utilizar a encriptação de hardware</p>	<p>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.</p>
<p>Encriptar apenas espaço utilizado do disco (Windows 8 e versões mais recentes)</p>	<p>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.</p> <div data-bbox="416 602 1493 795" style="border: 1px solid black; padding: 5px;"> <p>Ativar ou desativar a funcionalidade Encriptar apenas espaço utilizado do disco (Windows 8 e versões mais recentes) após o início da encriptação não altera esta definição até que os discos rígidos sejam desencriptados. Tem de seleccionar ou desmarcar a caixa de verificação antes de iniciar a encriptação.</p> </div> <p>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.</p> <p>Se a caixa de verificação estiver selecionada, é encriptado o disco rígido completo, incluindo os fragmentos residuais de ficheiros anteriormente eliminados e modificados.</p> <div data-bbox="416 1064 1493 1288" style="border: 1px solid black; padding: 5px;"> <p>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.</p> </div> <p>Esta caixa de verificação está desmarcada por predefinição.</p>
<p>Definições de autenticação</p>	<p>Utilizar password (Windows 8 e versões mais recentes)</p> <p>Se esta opção estiver selecionada, o Kaspersky Endpoint Security pede uma password ao utilizador quando este tenta aceder a unidade encriptada.</p> <p>Esta opção pode ser selecionada quando um Trusted Platform Module (TPM) não está a ser utilizado.</p> <p>Utilizar Trusted Platform Module (TPM)</p> <p>Se esta opção estiver selecionada, o BitLocker utiliza um Trusted Platform Module (TPM).</p> <p>Um <i>Módulo de plataforma fiável (TPM)</i> 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.</p> <div data-bbox="416 1951 1493 2143" style="border: 1px solid black; padding: 5px;"> <p>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.</p> </div>

Um dispositivo equipado com um Trusted Platform Module pode criar chaves de encriptação que apenas podem ser descriptadas 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:

- **Use PIN for 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. Pode permitir que o utilizador utilize o PIN avançado. O *PIN avançado* permite a utilização de outros caracteres além dos caracteres numéricos: letras latinas maiúsculas e minúsculas, caracteres especiais e espaços.
- **Utilizar Trusted Platform Module (TPM); se não estiver disponível - utilizar password.** Se a caixa de verificação 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.

Encriptação ao nível dos ficheiros

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 descripta os seguintes ficheiros:

- ficheiros adicionados individualmente a listas de encriptação e descriptação;
- ficheiros armazenados em pastas adicionados a listas de encriptação e descriptação;
- ficheiros criados por aplicações separadas.

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/descripta ficheiros em pastas predefinidas apenas para perfis de utilizadores locais do sistema operativo. O Kaspersky Endpoint Security não encripta ou descripta 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	<p>Manter inalterado. Se este item estiver selecionado, os ficheiros e as pastas permanecem inalterados pelo Kaspersky Endpoint Security, sem encriptação nem desencriptação.</p> <p>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.</p> <p>Desencriptar tudo. Se este item estiver selecionado, o Kaspersky Endpoint Security desencripta todos os ficheiros e pastas desencriptados.</p>
Regras de encriptação	<p>Este separador apresenta as regras de encriptação para ficheiros armazenados em unidades locais. Pode adicionar ficheiros da seguinte maneira:</p> <ul style="list-style-type: none">• Pastas predefinidas. O Kaspersky Endpoint Security permite adicionar as seguintes áreas:<ul style="list-style-type: none">Documentos. Ficheiros na pasta <i>Documentos</i> padrão do sistema operativo e as respetivas subpastas.Favoritos. Ficheiros na pasta <i>Favoritos</i> padrão do sistema operativo e respetivas subpastas.Ambiente de Trabalho. Ficheiros na pasta <i>Ambiente de trabalho</i> 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:<ul style="list-style-type: none">Use uma variável de ambiente (por exemplo, %FOLDER%\UserFo1der\). Pode usar uma variável de ambiente apenas uma vez e só no início do caminho.Não use caminhos relativos. Pode usar o conjunto \. . \ (p. ex. C:\Users\.. \UserFo1der\). O conjunto \. . \ indica a transição para a pasta principal.Não use os caracteres * e ?.Não use caminhos UNC.Use ; ou , como um carácter separador.• Ficheiros por extensão. Pode seleccionar grupos de extensões da lista, como o grupo de extensões <i>Ficheiros</i>. Pode também adicionar manualmente a extensão

	do ficheiro.
Regras de descriptação	Este separador apresenta as regras de descriptação 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.
Definições da password do pacote encriptado	Requisitos de segurança da password a serem cumpridos ao criar pacotes encriptados.

Encriptação de unidades amovíveis

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:

- Encriptação Completa do Disco (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).

- Encriptação ao Nível dos Ficheiros (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 subseqüentes 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
Gerir 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**.

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.

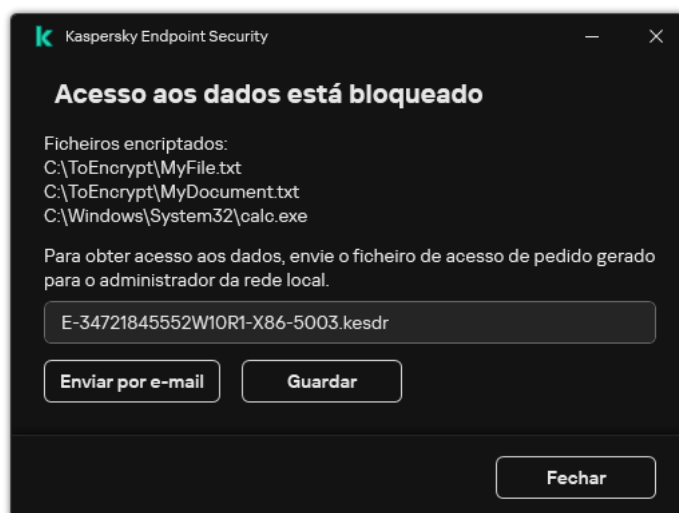
A capacidade de encriptar apenas o espaço ocupado só está disponível para o modo **Encriptar unidade amovível completa**.

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 de encriptação para os dispositivos selecionados	<p>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:</p> <ul style="list-style-type: none"> • Adicione uma unidade amovível da lista de dispositivos fiáveis para Controlo de Dispositivos. • Adicione manualmente uma unidade amovível: <ul style="list-style-type: none"> • Por ID do dispositivo (ID do hardware ou HWID) • Por ID do dispositivo: ID do fornecedor (VID) e ID do produto (PID)
Permitir encriptação de unidades amovíveis no modo offline	<p>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.</p> <p>Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security não encripta unidades amovíveis sem uma ligação ao Kaspersky Security Center.</p>
Definições da password do modo portátil	<p>Definições da segurança da password para o Gestor de ficheiros portátil.</p>

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.** 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.

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. Embora não tenham funções maliciosas, estas aplicações podem ser exploradas por intrusos. Para mais informações sobre software legal que pode ser utilizado por criminosos para danificar o computador ou os dados pessoais dos utilizadores, visite o [website da Kaspersky IT Encyclopedia](#)¹².

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.](#)
- [Tarefas de verificação.](#)

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 verifica 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. Contudo, uma aplicação que tenha sido adicionada à lista de aplicações fiáveis fica excluída das verificações pelo Kaspersky Endpoint Security.


Por exemplo, se considerar como seguros, sem verificação, 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. Deste modo, a verificação ignora objetos utilizados por esta aplicação.

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.

A exclusão de aplicações fiáveis da verificação permite evitar conflitos de compatibilidade entre o Kaspersky Endpoint Security e outros programas (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), bem como aumentar o desempenho do computador, o que é fundamental ao utilizar aplicações de servidor.

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.

Definições de exclusões

Parâmetro	Descrição
Tipos de objetos detetados	<p>Independentemente das definições da aplicação configuradas, o Kaspersky Endpoint Security deteta e bloqueia sempre vírus, worms e Trojans. Estes podem causar danos significativos no computador.</p> <ul style="list-style-type: none"> • Vírus e worms 

Subcategoria: vírus e worms (Viruses_and_Worms)

Nível de ameaça: alto

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 de *substituição* 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 *parasitas* modificam ficheiros, deixando-os total ou parcialmente funcionais. Os *vírus de companhia* 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: *vírus de ligação*, *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	Nome	Descrição
Worm de e-mail	Worm de e-mail	Disseminam-se por e-mail.

		<p>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.</p>
IM-Worm	Worms de cliente de MI	<p>Estes disseminam-se através de clientes de MI.</p> <p>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.</p>
IRC-Worm	Worms de salas de conversação	<p>Estes disseminam-se através de salas de conversação (IRC), sistemas de serviços que permitem comunicar com outras pessoas, em tempo real, através da Internet.</p> <p>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.</p>
Net-Worm	Worms de rede	<p>Estes worms disseminam-se através de redes de computadores.</p> <p>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.</p>
P2P-Worm	Worms de rede de partilha de ficheiros	<p>Disseminam-se em redes de partilha de ficheiros peer-to-peer.</p> <p>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.</p> <p>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.</p>
Worm	Outros tipos de worms	<p>Outros tipos de worms incluem:</p>

- | | | |
|--|--|--|
| | | <ul style="list-style-type: none">• 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 ameaça: alto

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	Nome	Descrição
Trojan-ArcBomb	Trojans – "arquivos bomba"	<p>Uma vez descompactados, a dimensão destes arquivos aumenta de tal forma que o funcionamento do computador é afetado.</p> <p>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.</p>
Backdoor	Trojans para administração remota	<p>São considerados o tipo de programa Trojan mais perigoso. Em termos de funções, são semelhantes às aplicações de administração remota instaladas nos computadores.</p> <p>Estes programas instalam-se no computador sem serem detetados pelo utilizador, permitindo ao intruso gerir remotamente o computador.</p>
Trojan	Trojans	<p>Estes incluem as seguintes aplicações maliciosas:</p> <ul style="list-style-type: none">• 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

		<p>contrário dos outros tipos de Trojans descritos na tabela.</p> <ul style="list-style-type: none"> • Trojans versáteis. Estes programas têm as características avançadas típicas de vários tipos de Trojans.
Trojan-Ransom	Trojans de resgate	<p>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.</p>
Trojan-Clicker	Trojans de comandos	<p>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.</p> <p>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).</p>
Trojan-Downloader	Trojans de transferências	<p>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.</p>
Trojan-Dropper	Trojans instaladores	<p>Estes contêm outros Trojans que instalam no disco rígido.</p> <p>Os intrusos podem utilizar programas do tipo Trojan Dropper com os objetivos seguintes:</p> <ul style="list-style-type: none"> • 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	<p>Estes informam um intruso de que um computador infetado está acessível, enviando-lhe informação sobre o</p>

		<p>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.</p> <p>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.</p>
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	<p>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.</p> <p>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).</p>
Trojan-Spy	Trojans espões	Estes espiam o utilizador, recolhendo informações sobre as ações do utilizador enquanto trabalha no computador. Estes podem interceptar 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.
Processo oculto (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: meio

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	Nome	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).
Exploração de vulnerabilidades	Exploração 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".

		<p>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 um 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.</p> <p>Os worms de rede (Net-Worms) disseminam-se nas redes através da exploração de vulnerabilidades. <i>O exploit Nuker</i> é constituído por pacotes de rede que desativam os computadores.</p>
FileCryptor	Encriptadores	Estes encriptam outras aplicações maliciosas, para os ocultarem das aplicações antivírus.
Flooder	Programas para "contaminar" redes	<p>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).</p> <p>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).</p>
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 intercepção de passwords. Os programas farejadores são programas que permitem visualizar o tráfego de rede.
Programas de engodo (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.
Spoofers	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 ameaça: 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 criminosos para danificar o computador ou os dados pessoais do utilizador.

Nível de perigo: meio

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	Nome	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.
Dialer	Auto-dialers	Estes conseguem estabelecer ligações telefónicas através de um modem, de forma oculta.
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 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 de 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 de 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 de 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 rede	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	Clientes de rede peer-to-peer (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 ferramentas para 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 desinfectam qualquer ameaça.
------------------	------------------	---

- Detetar outro software que pode ser utilizado por intrusos para danificar o seu computador ou dados pessoais 

Subcategoria: software legal que pode ser utilizado por criminosos para danificar o computador ou os dados pessoais do utilizador.

Nível de perigo: meio

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	Nome	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.
Dialer	Auto-dialers	Estes conseguem estabelecer ligações telefónicas através de um modem, de forma oculta.
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 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 de 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 de 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 de 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 rede	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	Cientes de rede peer-to-peer (P2P)	Estes permitem trabalhar em redes Peer-to-Peer. Podem ser utilizados pelos intrusos para espalhar software malicioso.
Client-SMTP	Cientes SMTP	Enviaram 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 ferramentas para 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 desinfectam qualquer ameaça.
------------------	------------------	---

- [Objetos comprimidos, cuja compactação pode ser utilizada para proteger um código malicioso](#) 

O Kaspersky Endpoint Security verifica objetos comprimidos e o módulo de descompressão com arquivos SFX (extração automática).

Para ocultar programas perigosos das aplicações antivírus, os intrusos arquivam os mesmos utilizando Ficheiros comprimidos especiais ou criando ficheiros multi-comprimidos.

Os analistas de vírus da Kaspersky identificaram os Ficheiros comprimidos mais populares entre os hackers.

Se o Kaspersky Endpoint Security detetar algum desses utilitários de compressão num ficheiro, o mais provável é que esse ficheiro contenha uma aplicação maliciosa ou um aplicação que pode ser utilizado por criminosos para danificar o computador ou os dados pessoais do utilizador.

O Kaspersky Endpoint Security isola os tipos de programas seguintes:

- *Ficheiros comprimidos que podem provocar danos* – utilizados para comprimir software malicioso, como vírus, worms, e Trojans.
- *Ficheiros multi-comprimidos* (nível de ameaça médio) – o objeto foi comprimido três vezes, por um ou mais ficheiros de compressão.

- [Objetos multicomprimidos](#) 

O Kaspersky Endpoint Security verifica objetos comprimidos e o módulo de descompressão com arquivos SFX (extração automática).

Para ocultar programas perigosos das aplicações antivírus, os intrusos arquivam os mesmos utilizando Ficheiros comprimidos especiais ou criando ficheiros multi-comprimidos.

Os analistas de vírus da Kaspersky identificaram os Ficheiros comprimidos mais populares entre os hackers.

Se o Kaspersky Endpoint Security detetar algum desses utilitários de compressão num ficheiro, o mais provável é que esse ficheiro contenha uma aplicação maliciosa ou um aplicação que pode ser utilizado por criminosos para danificar o computador ou os dados pessoais do utilizador.

O Kaspersky Endpoint Security isola os tipos de programas seguintes:

- *Ficheiros comprimidos que podem provocar danos* – utilizados para comprimir software malicioso, como vírus, worms, e Trojans.
- *Ficheiros multi-comprimidos* (nível de ameaça médio) – o objeto foi comprimido três vezes, por um ou mais ficheiros de compressão.

Exclusões

Esta tabela contém informações sobre as exclusões de verificação.

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:\Pasta***.txt** incluirá todos os caminhos para ficheiros com a extensão TXT encontrados nas pastas designadas **Pasta** e nas suas subpastas. 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 caracteres.

	<ul style="list-style-type: none"> • 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 carácter ? (substitui qualquer carácter único) e o carácter * (substitui qualquer número de caracteres). Por exemplo, se a máscara do Cliente* for especificada, o Kaspersky Endpoint Security exclui os objetos Client-IRC, Client-P2P e Client-SMTP das verificações.
Aplicações fiáveis	<p>Esta tabela indica as aplicações fiáveis cuja atividade não é monitorizada pelo Kaspersky Endpoint Security durante o seu funcionamento.</p> <p>O componente Controlo das Aplicações regula o arranque de cada uma das aplicações, independentemente de a aplicação estar incluída na tabela de aplicações fiáveis.</p>
Unir valores ao herdar <i>(disponível apenas na Consola do Kaspersky Security Center)</i>	<p>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.</p> <p>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.</p> <p>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.</p> <p>Se os itens nas listas das políticas subordinada e principal corresponderem, esses itens serão apresentados como o mesmo item da política principal.</p> <p>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.</p>
Permitir a utilização de exclusões locais/Permitir a utilização de aplicações fiáveis locais <i>(disponível apenas na Consola do Kaspersky Security Center)</i>	<p><i>Exclusões locais e aplicações fiáveis locais (zona fiável local)</i> – 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.</p> <p>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.</p> <p>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. Se tiverem sido geradas listas locais, depois de esta funcionalidade ser desativada, o Kaspersky Endpoint Security continua a excluir os objetos listados das verificações.</p>
Arquivo de certificados do sistema fiável	<p>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 <i>fiáveis</i>.</p> <p>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.</p>

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

Definições da aplicação

Parâmetro	Descrição
Iniciar o Kaspersky Endpoint Security for Windows no arranque do computador	<p>Quando a caixa de verificação está selecionada, o Kaspersky Endpoint Security é iniciado após o carregamento do sistema operativo, protegendo o computador durante toda a sessão.</p> <p>Quando a caixa de verificação 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.</p>
Utilizar a tecnologia de Desinfeção Avançada (requer recursos do computador consideráveis)	<p>Se a caixa de verificação estiver selecionada, uma notificação pop-up aparece no ecrã quando a atividade maliciosa for detetada no sistema operativo. Nesta notificação, o Kaspersky Endpoint Security oferece ao utilizador a possibilidade de executar a desinfeção Avançada do computador. Após a aprovação deste procedimento pelo utilizador, o Kaspersky Endpoint Security neutraliza a ameaça. Após concluir o procedimento de desinfeção avançada, o Kaspersky Endpoint Security reinicia o computador. A tecnologia de desinfeção avançada utiliza recursos consideráveis do computador, o que poderá tornar outras aplicações mais lentas.</p> <p>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.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"><p>Se o Kaspersky Endpoint Security for instalado num computador com o Windows para servidores, o Kaspersky Endpoint Security não apresenta a notificação. Como tal, o utilizador 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 <i>Verificação de vírus</i>. Depois, tem de iniciar uma tarefa <i>Verificação do vírus</i>.</p></div>
Utilizar o Kaspersky Security Center como servidor de proxy para ativação	<p>Se esta caixa de verificação estiver selecionada, o Servidor de administração do Kaspersky Security Center é utilizado como um servidor proxy ao ativar a aplicação.</p>

<i>(disponível apenas na Consola do Kaspersky Security Center)</i>	
Ativar Autodefesa	Quando esta caixa de verificação está selecionada, 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.
Permitir a gestão das definições do Kaspersky Endpoint Security através de aplicações de controlo remotas	Se esta caixa de verificação for selecionada, as aplicações de controlo remoto fiáveis (como TeamViewer, LogMeln Pro e Remotely Anywhere) podem modificar as definições do Kaspersky Endpoint Security. As aplicações de administração remota não fiáveis estão proibidas de modificar as definições do Kaspersky Endpoint Security mesmo quando a caixa de verificação está selecionada.
Ativar controlo externo de serviços	Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security permite a gestão de serviços da aplicação a partir de um computador remoto. Quando é efetuada uma tentativa de gerir remotamente os serviços da aplicação, 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).
Adiar as tarefas agendadas quando o computador estiver ligado com bateria	Se a caixa de verificação estiver selecionada, o modo de poupança de energia está ativado. O Kaspersky Endpoint Security adia as tarefas agendadas. O utilizador pode iniciar as tarefas de verificação e de atualização manualmente, se necessário.
Conceder recursos para outras aplicações	Quando o Kaspersky Endpoint Security executa tarefas agendadas, pode ocorrer uma sobrecarga da CPU e dos subsistemas do disco, tornando mais lento o desempenho de outras aplicações. Quando a caixa de verificação está selecionada, o Kaspersky Endpoint Security suspende as tarefas agendadas quando deteta uma carga acrescida e liberta recursos do sistema operativo para as aplicações do utilizador.
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 verificação 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 verificação estiver desmarcada, qualquer utilizador pode aceder a ficheiros de descarga e de rastreio.
Estado do computador quando são	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. Os estados <i>OK</i> , <i>Aviso</i> e <i>Crítico</i> estão disponíveis.

aplicadas
definições

(disponível
apenas na
Consola do
Kaspersky
Security
Center)

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\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\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

A *Quarentena* é um armazenamento local especial no computador para onde os ficheiros infetados por vírus ou não desinfetáveis são movidos. Os ficheiros na quarentena são armazenados num estado encriptado e não põem em risco a segurança do dispositivo. O Kaspersky Endpoint Security apenas utiliza a Quarentena ao trabalhar com as soluções Kaspersky Sandbox e Kaspersky Endpoint 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](#).

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
Guardar relatórios até N dias	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.
Limitar o tamanho do ficheiro de relatório a N 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.
Armazenar objetos no máximo durante N dias	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.
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 100 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.
Limitar o tamanho da Quarentena a N MB <i>(apenas disponível na Consola Web)</i>	Tamanho máximo da quarentena em MB. Por exemplo, pode definir o tamanho máximo da quarentena como 200 MB. Quando a Quarentena atinge o tamanho máximo, o Kaspersky Endpoint Security envia o evento correspondente ao 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.
Notificar quando o armazenamento da Quarentena alcançar N por cento <i>(apenas disponível na Consola Web)</i>	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 <i>(disponível apenas no Kaspersky Security Center)</i>	As categorias de eventos nos computadores do cliente cuja informação deve ser enviada para o Servidor de administração.

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	<p>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 Wi-Fi como uma ligação ilimitada.</p> <p>O Rede com Controlo de Custos funciona em computadores com o Windows 8 ou posterior.</p>
Injetar script no tráfego de Internet para interagir com páginas de Internet	<p>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 monitorização da atividade do utilizador na Internet.</p> <div style="background-color: #f8d7da; padding: 10px; margin-top: 10px;"> <p>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.</p> </div>
Servidor de proxy	<p>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.</p> <p>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, o Kaspersky Endpoint Security utiliza o endereço do servidor de proxy especificado nas definições do navegador Microsoft Internet Explorer.</p>
Ignorar o servidor de proxy nos endereços locais	<p>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.</p>
Portas monitorizadas	<p>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, Proteção contra ameaças de correio) monitorizam fluxos de dados transmitidos através de qualquer porta de rede aberta no computador.</p> <p>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.</p> <p>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.</p> <p>Monitorizar todas as portas das aplicações especificadas. Esta ação utiliza uma lista de aplicações cujas portas de rede são monitorizadas pelo Kaspersky Endpoint Security.</p>

Verificar as 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 de Ficheiros, 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.

Ao visitar um domínio com um certificado não fiável

- **Permitir.** Se esta opção estiver selecionada, 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. 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.

Bloquear ligação. Se este item estiver selecionado, 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.

Ao ocorrerem erros de verificação de ligação encriptada

- **Bloquear ligação.** Se este item estiver selecionado, quando ocorre um erro de verificação das ligações encriptadas, o Kaspersky Endpoint Security bloqueia a ligação de rede.
- **Adicionar domínio às exclusões.** Se este item estiver selecionado, quando ocorre 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

	<p>encriptadas apenas na interface local da aplicação. Para limpar o conteúdo da lista, deve seleccionar Bloquear ligação.</p>
<p>Bloquear ligações SSL 2.0 (recomendado)</p>	<p>Se a caixa de verificação estiver seleccionada, o Kaspersky Endpoint Security bloqueia as ligações de rede estabelecidas através do protocolo SSL 2.0.</p> <p>Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security não bloqueia as ligações de rede estabelecidas através do protocolo SSL 2.0 e não monitoriza o tráfego de rede transmitido através destas ligações.</p>
<p>Desencriptar ligações encriptadas com websites que utilizem certificados EV</p>	<p>Certificados EV (Extended Validation Certificates) 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 endereços a verde.</p> <p>Se a caixa de verificação estiver seleccionada, o Kaspersky Endpoint Security desencripta e monitoriza as ligações encriptadas com sites que utilizem um certificado EV.</p> <p>Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security 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, <code>https://google.com</code>.</p> <p>Se estiver a abrir um site com um certificado EV pela primeira vez, a ligação encriptada será desencriptada, independentemente de a caixa de verificação estar seleccionada ou não.</p>
<p>Endereços fiáveis</p>	<p>Esta ação utiliza uma lista de URL para os quais o Kaspersky Endpoint Security não verifica ligações de rede. Pode introduzir um nome de domínio ou endereço IP. O Kaspersky Endpoint Security suporta o caractere <code>*</code> para a introdução de uma máscara no nome de domínio.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>O Kaspersky Endpoint Security não suporta máscaras para endereços IP. Pode introduzir um intervalo de endereços IP na interface local da aplicação (por exemplo, 198.51.100.0/24). Não é possível introduzir um intervalo de endereços IP na Consola do Kaspersky Security Center.</p> </div> <p>Exemplos:</p> <ul style="list-style-type: none"> • <code>domain.com</code> - o registo inclui os seguintes endereços: <code>https://domain.com</code>, <code>https://www.domain.com</code>, <code>https://domain.com/page123</code>. O registo não inclui subdomínios (por exemplo, <code>subdomain.domain.com</code>) • <code>subdomain.domain.com</code> - o registo inclui os seguintes endereços: <code>https://subdomain.domain.com</code>, <code>https://subdomain.domain.com/page123</code>. O registo não inclui o domínio <code>dominio.com</code>. • <code>*.domain.com</code> - o registo inclui os seguintes endereços: <code>https://movies.domain.com</code>, <code>https://images.domain.com/page123</code>. O registo não inclui o domínio <code>dominio.com</code>.
<p>Aplicações fiáveis</p>	<p>Lista de aplicações cuja atividade não é monitorizada pelo Kaspersky Endpoint Security durante o seu funcionamento. Pode seleccionar os tipos de atividade da aplicação que o Kaspersky Endpoint Security não irá monitorizar (por exemplo, não verificar o tráfego da</p>



	rede). O Kaspersky Endpoint Security suporta variáveis de ambiente e os caracteres * e ? ao inserir uma máscara.
<p>Utilize o armazenamento de certificados selecionado para verificar as ligações encriptadas em aplicações do Mozilla</p> <p><i>(disponível apenas na interface do Kaspersky Endpoint Security)</i></p>	<p>Se esta caixa de verificação estiver selecionada, o Kaspersky Endpoint Security 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.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>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, o Kaspersky Endpoint Security não verifica o tráfego no navegador Mozilla Firefox e no cliente de e-mail Thunderbird.</p> </div> <p>O Kaspersky Endpoint Security usa o certificado raiz da Kaspersky para descriptar e analisar o tráfego encriptado. Pode seleccionar o armazenamento de certificados que irá conter o certificado raiz da Kaspersky.</p> <ul style="list-style-type: none"> • Utilizar o armazenamento de certificados do Windows (recomendado). O certificado raiz da Kaspersky é adicionado a este armazenamento durante a instalação do Kaspersky Endpoint Security. • Utilizar o armazenamento de certificados do Mozilla. 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
<p>Interação com o utilizador</p> <p><i>(disponível apenas na Consola do Kaspersky Security Center)</i></p>	<p>With simplified interface. 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 apresenta também notificações acima do ícone da aplicação.</p> <p>With full interface. 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.</p> <p>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 <i>Monitor de Atividade das Aplicações</i> é uma ferramenta concebida para visualizar informações sobre a atividade das aplicações no computador de um utilizador em tempo real.</p> <p>No 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.</p>
Definições	Uma tabela com as definições de notificações sobre eventos de diferentes níveis de

de notificação	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.
Definições de notificações por e-mail	As definições do servidor SMTP para entrega de notificações sobre eventos registados durante a operação da aplicação.
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 de antivírus local	As definições de notificações sobre bases de dados de antivírus desatualizadas utilizadas pela aplicação.
Proteção por password	<p>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.</p> <p>Depois de a Proteção por password estar ativada, o Kaspersky Endpoint Security solicita a configuração de uma password para realizar operações.</p>
Technical Support web resources <i>(disponível apenas na Consola do Kaspersky Security Center)</i>	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.
Message to user <i>(disponível apenas na Consola do Kaspersky Security Center)</i>	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 12 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 recomendadas pela Kaspersky para o Kaspersky Endpoint Security 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.

As atualizações regulares requerem uma licença válida. Se não existir uma licença atual, só poderá executar uma atualização uma vez.

A principal origem de atualização do Kaspersky Endpoint Security são os servidores de atualização da Kaspersky.

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 respectivas versões atualizadas, só será instalada no computador a parte das atualizações em falta.

Os ficheiros de ajuda de contexto podem ser atualizados juntamente com as atualizações dos módulos da aplicação.

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](#).

Definições do módulo da aplicação e de atualização da base de dados

Parâmetro	Descrição
Agendamento de atualização de bases de dados	<p>Automaticamente. Neste modo, o Kaspersky Endpoint Security 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.</p> <p>Manualmente. Este modo de execução da tarefa de atualização permite iniciar manualmente a tarefa de atualização.</p> <p>Por agendamento. 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.</p>
Run missed tasks	<p>Se a caixa de verificação estiver selecionada, o Kaspersky Endpoint Security inicia a tarefa de atualização ignorada assim que possível. A tarefa de atualização pode ser ignorada, por exemplo, se o computador tiver sido desligado no momento de início da tarefa de atualização.</p> <p>Se a caixa de verificação estiver desmarcada, o Kaspersky Endpoint Security não inicia tarefas de atualização ignoradas. Em alternativa, executa a tarefa de atualização seguinte, em conformidade com o agendamento atual.</p>
Origem da atualização	<p><i>Uma origem de atualização é um recurso que contém atualizações para as bases de dados e os módulos da aplicação do Kaspersky Endpoint Security.</i></p> <p>As origens de atualização incluem o servidor do Kaspersky Security Center, os servidores de atualização da Kaspersky e as pastas de rede ou locais.</p> <p>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.</p>

	<p>O Kaspersky Endpoint Security não suporta atualizações de servidores HTTPS, exceto se forem servidores de atualização da Kaspersky.</p> <p>Se forem selecionados vários recursos como origens de atualização, o Kaspersky Endpoint Security tentará 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.</p>
<p>Executar atualizações da base de dados como</p>	<p>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 do Kaspersky Endpoint Security, pode especificar um utilizador que tenha esses direitos e iniciar a tarefa de atualização do Kaspersky Endpoint Security com essa conta de utilizador.</p>
<p>Transferir atualizações dos módulos da aplicação</p>	<p>Esta caixa de verificação ativa / desativa as transferências de atualizações de módulos da aplicação e de atualizações da base de dados antivírus.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>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.</p> <p>Esta caixa de verificação está selecionada por predefinição.</p>
<p>Copiar atualizações para a pasta</p>	<p>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\Update distribution\.</p>

<p>Servidor de proxy para atualizações</p> <p><i>(disponível apenas na interface do Kaspersky Endpoint Security)</i></p>	<p>Definições do servidor de proxy para acesso à Internet de utilizadores de computadores clientes para atualizar módulos de aplicações e bases de dados.</p> <p>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, o Kaspersky Endpoint Security utiliza o endereço do servidor de proxy especificado nas definições do navegador Microsoft Internet Explorer.</p>
<p>Ignorar o servidor de proxy nos endereços locais</p> <p><i>(disponível apenas na interface do Kaspersky Endpoint Security)</i></p>	<p>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.</p>

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 aplicações 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 aplicações no 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 aplicações no 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 aplicações ao grupo Não fiáveis.

Todas as operações estão bloqueadas para estas 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

eml — mensagem de e-mail do Microsoft Outlook Express

nws — nova mensagem de e-mail do Microsoft Outlook Express

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, xlsx 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

eml – mensagem de e-mail do Microsoft Outlook Express

nws – nova mensagem de e-mail do Microsoft Outlook Express

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, xlsx para modelos do Microsoft Office Excel 2007 com suporte para macros e xlsm 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 utiliza as seguintes definições de rede para interagir com serviços externos.

Definições de Rede

Endereço	Descrição
activation- v2.kaspersky.com/activation-service/activation-service.svc Protocolo: HTTPS Port: 443	Ativar a aplicação
s00.upd.kaspersky.com s01.upd.kaspersky.com s02.upd.kaspersky.com s03.upd.kaspersky.com s04.upd.kaspersky.com s05.upd.kaspersky.com	Atualização de bases de dados e módulos de aplicação

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

downloads.upd.kaspersky.com

Protocolo: HTTPS

Port: 443

- Atualização de bases de dados e módulos de aplicação

- Verificação se os servidores da Kaspersky estão acessíveis. Se o acesso aos servidores que utilizam 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 o nível de segurança é mantido para o computador. O Kaspersky Endpoint Security utiliza a seguinte lista de servidores DNS públicos na seguinte ordem:

1. DNS Público da 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).

	<p>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 dos dados é regido pela política de privacidade do serviço relevante. Se quiser impedir que o Kaspersky Endpoint Security utilize um servidor DNS público, contacte o Suporte Técnico para uma correção privada.</p>
<p>touch.kaspersky.com Protocolo: HTTP</p>	<ul style="list-style-type: none"> • Receber o tempo fiável para verificar o período de validade do certificado (ligação TLS). • Aviso sobre a recusa de acesso a um recurso Web no navegador (Proteção contra ameaças da Web e Controlo de Internet).
<p>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</p>	<p>Atualização de bases de dados e módulos de aplicação</p>

<p>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</p> <p>Protocolo: HTTP Port: 80</p>	
<p>ds.kaspersky.com</p> <p>Protocolo: HTTPS Port: 443</p>	Utilização da Kaspersky Security Network.
<p>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</p> <p>Protocolo: Any Port: 443, 1443</p>	Utilização da Kaspersky Security Network.
<p>click.kaspersky.com redirect.kaspersky.com</p> <p>Protocolo: HTTPS</p>	Seguir as ligações da interface
<p>cr1.kaspersky.com ocsp.kaspersky.com</p> <p>Protocolo: HTTP Port: 80</p>	Infraestrutura de chave pública (PKI)

Anexo 6. Eventos da aplicação no Registo de eventos do Windows

As informações sobre o funcionamento de cada componente do Kaspersky Endpoint Security, os eventos de encriptação de dados, o desempenho de cada tarefa de verificação, 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 Windows.

[Auditoria do sistema](#) 

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
201		Contrato de Licença do Utilizador Final violado.	✓
203		A licença está quase a expirar.	–
206		As bases de dados estão em falta ou corrompidas.	–
207		As bases de dados estão extremamente desatualizadas.	–
209		A execução automática da aplicação está desativada.	–
229		Erro de ativação.	✓
231		Deteção de ameaça ativa. Deve ser iniciada uma Desinfecção Avançada.	✓
2023		Servidores KSN indisponíveis.	–
343		Não há espaço suficiente no armazenamento da Quarentena.	✓
346		Objeto não restaurado da Quarentena.	✓
348		Objeto não eliminado da Quarentena.	✓
212		A tarefa não pode ser executada.	–
237		Falha da aplicação durante a sessão anterior.	✓
204		A licença expira em breve.	–
208		As bases de dados estão desatualizadas.	–
210		As atualizações automáticas estão desativadas.	–
211		A autodefesa está desativada.	–
214		Os componentes de proteção estão desativados.	–
215		O computador está a ser executado em modo segurança.	–
216		Existem ficheiros não processados.	–
219		Política de grupo aplicada.	✓
222		Tarefa parada.	–
224		Reinicie a aplicação para concluir a atualização.	–
225		É necessário reiniciar o computador para concluir a atualização.	✓
226		A licença permite a utilização de componentes que não foram instalados.	–
232		Desinfecção avançada iniciada.	–
233		Desinfecção avançada concluída.	–
230		Chave de reserva incorreta.	–
240		A subscrição expira em breve.	✓
336		Não foi possível restaurar o objeto da cópia de segurança.	–
2001		Atividade de rede suspeita detetada.	–

250		Ligação encriptada terminada.	✓
2021		A participação na KSN está desativada.	–
245		O processamento de algumas funções do SO está desativado.	✓
344		O armazenamento da Quarentena está quase sem espaço.	✓
235		Aplicação iniciada.	✓
236		Aplicação parada.	✓
213		A operação com os recursos da aplicação está bloqueada pela Autodefesa.	–
217		Relatório apagado.	✓
220		Política de grupo desativada.	–
218		Definições da aplicação alteradas.	✓
221		Tarefa iniciada.	–
223		Tarefa concluída.	–
227		Todos os componentes da aplicação definidos pela licença foram instalados e executados no modo normal.	–
238		As definições de subscrição foram alteradas.	✓
239		A subscrição foi renovada.	✓
335		Objeto restaurado da cópia de segurança.	–
2000		Digite um nome de utilizador e uma password.	–
2020		A participação na KSN está ativada.	–
2022		Servidores KSN disponíveis.	–
2024		A aplicação funciona e processa dados no âmbito da legislação vigente e utiliza as infraestruturas adequadas.	✓
345		Objeto restaurado da Quarentena.	✓
347		Objeto eliminado da Quarentena.	✓

Detecção de comportamento

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
302		Objeto malicioso detetado.	–
313		Não pode ser eliminado.	–
452		Processo terminado.	–
453		Não foi possível terminar o processo.	–
455		Reversão concluída.	–
331		Bloqueado.	–
307		Objeto eliminado.	–
323		O objeto será eliminado ao reiniciar.	–
311		Não foi possível criar uma cópia de segurança.	–
303		Foi detetado software legítimo que pode ser utilizado por intrusos para danificar o seu computador ou dados pessoais.	–
457		Ficheiro restaurado.	–
308		Foi criada uma cópia de segurança do objeto.	–
458		Valor de registo restaurado.	–
459		Valor de registo eliminado.	–
329		Nome do objeto mudado.	–

[Prevenção de explorações](#)

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
302		Objeto malicioso detetado.	–
331		Bloqueado.	–
455		Reversão concluída.	–
307		Objeto eliminado.	–
323		O objeto será eliminado ao reiniciar.	–
457		Ficheiro restaurado.	–
458		Valor de registo restaurado.	–
459		Valor de registo eliminado.	–
329		Nome do objeto mudado.	–

[Prevenção contra invasões](#)














Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
302		Objeto malicioso detetado.	✓
312		Não foi possível executar a desinfecção.	–
313		Não pode ser eliminado.	–
317		Erro de processamento.	–
452		Processo terminado.	–
453		Não foi possível terminar o processo.	–
310		Não foi possível criar uma cópia de segurança.	–
314		Objeto não processado.	–
320		Objeto encriptado.	–
321		Objeto corrompido.	–
323		O objeto será eliminado ao reiniciar.	–
324		O objeto será desinfetado ao reiniciar.	–
303		Foi detetado software legítimo que pode ser utilizado por intrusos para danificar o seu computador ou dados pessoais.	–
336		Não foi possível restaurar o objeto da cópia de segurança.	–
307		Objeto eliminado.	–
306		Objeto desinfetado.	–
301		Objeto processado.	–
308		Foi criada uma cópia de segurança do objeto.	–
315		Objeto ignorado.	–
318		Arquivo detetado.	–
319		Objeto comprimido detetado.	–
327		Substituído por uma cópia que foi desinfetada anteriormente.	–
332		Informação sobre objeto detetado.	–
322		Arquivo de proteção de password detetado.	–
335		Objeto restaurado da cópia de segurança.	–
401		Aplicação colocada num grupo fiável.	–
402		Aplicação colocada num grupo restrito.	–
403		A Prevenção contra invasões do anfitrião foi ativada.	–
340		O objeto está na lista de permissão do KSN Privado.	✓

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
302		Objeto malicioso detetado.	✓
312		Não foi possível executar a desinfecção.	–
313		Não pode ser eliminado.	–
317		Erro de processamento.	✓
452		Processo terminado.	–
453		Não foi possível terminar o processo.	–
310		Não foi possível criar uma cópia de segurança.	–
314		Objeto não processado.	–
320		Objeto encriptado.	–
321		Objeto corrompido.	–
323		O objeto será eliminado ao reiniciar.	–
324		O objeto será desinfetado ao reiniciar.	–
303		Foi detetado software legítimo que pode ser utilizado por intrusos para danificar o seu computador ou dados pessoais.	–
336		Não foi possível restaurar o objeto da cópia de segurança.	–
307		Objeto eliminado.	–
306		Objeto desinfetado.	–
455		Reversão concluída.	–
301		Objeto processado.	–
308		Foi criada uma cópia de segurança do objeto.	–
315		Objeto ignorado.	–
318		Arquivo detetado.	–
319		Objeto comprimido detetado.	–
325		Substituído por uma cópia que foi desinfetada anteriormente.	–
322		Arquivo de proteção de password detetado.	–
332		Informação sobre objeto detetado.	–
335		Objeto restaurado da cópia de segurança.	–
340		O objeto está na lista de permissão do KSN Privado.	✓

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
302		Objeto malicioso detetado.	✓
362		Ligação perigosa bloqueada.	✓
363		Ligação perigosa aberta.	✓
1201		Ligação perigosa aberta anteriormente detetada.	✓
317		Erro de processamento.	✓
303		Foi detetado software legítimo que pode ser utilizado por intrusos para danificar o seu computador ou dados pessoais.	–
331		Bloqueado	–
341		A transferência do objeto foi bloqueada.	–
321		Objeto corrompido.	–
301		Objeto processado.	–
301		Ligação processada	–
332		Informação sobre objeto detetado.	–
319		Objeto comprimido detetado.	–
318		Arquivo detetado.	–
322		Arquivo de proteção de password detetado.	–
370		A ligação está na lista de permissão do KSN Privado.	✓
370		O objeto está na lista de permissão do KSN Privado.	✓



[Proteção contra ameaças de correio](#)

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
302		Objeto malicioso detetado.	✓
312		Não foi possível executar a desinfecção.	–
317		Erro de processamento.	✓
314		Objeto não processado.	–
303		Foi detetado software legítimo que pode ser usado por intrusos para danificar o seu computador.	–
321		Objeto corrompido.	–
336		Não foi possível restaurar o objeto da cópia de segurança.	–
307		Objeto eliminado.	–
342		Objeto eliminado de acordo com as definições.	–
306		Objeto desinfetado.	–
301		Objeto processado.	–
308		Foi criada uma cópia de segurança do objeto.	–
318		Arquivo detetado.	–
319		Objeto comprimido detetado.	–
329		Nome do objeto mudado.	–
332		Informação sobre objeto detetado.	–
322		Arquivo de proteção de password detetado.	–
335		Objeto restaurado da cópia de segurança.	–
340		O objeto está na lista de permissão do KSN Privado.	✓


Firewall 

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
602		Atividade de rede bloqueada.	✓
601		Atividade de rede permitida.	–




Proteção contra ameaças de Rede 

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
651		Ataque de rede detetado.	–
















Prevenção de ataques BadUSB

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
2051		Teclado não autorizado.	✓
2052		Erro de autorização de teclado.	✓
2050		Teclado autorizado.	–

Proteção AMSI

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
302		Objeto malicioso detetado.	✓
2200		Pedido de AMSI bloqueado.	✓
317		Erro de processamento.	✓
314		Objeto não processado.	–
320		Objeto encriptado.	–
321		Objeto corrompido.	–
303		Foi detetado software legítimo que pode ser utilizado por intrusos para danificar o seu computador ou dados pessoais.	–
1512		O resultado da verificação do objeto foi enviado para uma aplicação de terceiros.	–
301		Objeto processado.	–
315		Objeto ignorado.	–
318		Arquivo detetado.	–
319		Objeto comprimido detetado.	–
322		Arquivo de proteção de password detetado.	–
332		Informação sobre objeto detetado.	–
340		O objeto está na lista de permissão do KSN Privado.	✓

Controlo das Aplicações

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
702		Início de aplicação proibido.	–
710		O processo proibido foi iniciado antes de o Kaspersky Endpoint Security for Windows ter sido iniciado.	–
707		Erro nas definições da tarefa. Definições de tarefa não aplicadas.	–
708		Definições de tarefa aplicadas com sucesso.	–
701		Início de aplicação permitido.	–
703		Início de aplicação proibido no modo de teste.	–
704		Início de aplicação permitido no modo de teste.	–

Controlo de Dispositivos

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
802		Operação com o dispositivo proibida.	–
809		Ligação de rede bloqueada.	–
803		Acesso temporário ao dispositivo ativado.	
801		Operação com o dispositivo permitida.	–
808		Operação de ficheiro executada.	–



Controlo de Internet

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
752		Acesso negado.	–
753		Aviso sobre conteúdo indesejável.	–
754		Conteúdo indesejável foi acedido depois de um aviso.	–
751		Acesso permitido.	–
751		Página permitida aberta.	–

Controlo de Anomalias Adaptativo

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
2200		Ação de processo bloqueada.	✓
2201		Ação de processo ignorada.	–

[Encriptação de dados](#) 

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
904		Erro ao aplicar regras de encriptação/desencriptação de ficheiros.	✓
912		Erro de encriptação/desencriptação de ficheiros.	✓
940		Acesso ao ficheiro bloqueado.	✓
951		Erro ao ativar o modo portátil.	✓
953		Erro ao desativar o modo portátil.	✓
931		Erro ao criar pacote encriptado.	✓
1305		Erro ao encriptar/desencriptar o dispositivo.	✓
1311		Falha ao carregar o módulo de encriptação.	✓
1340		A tarefa de gestão das contas de Agente de Autenticação terminou com um erro.	✓
1312		Não foi possível aplicar a política.	✓
1342		Falha na atualização da FDE.	✓
1344		Reversão da atualização da Encriptação de disco completa concluída com um erro.	✓
903		Interrupção da aplicação de regras de encriptação/desencriptação de ficheiros.	–
914		Interrupção da encriptação/desencriptação de ficheiros.	–
1303		Interrupção da encriptação/desencriptação do dispositivo.	–
1306		Utilizador não aceitou a política de encriptação.	–
1345		Falha ao instalar ou ao atualizar os controladores da Encriptação de disco Kaspersky na imagem WinRE.	✓
901		Início da aplicação de regras de encriptação/desencriptação de ficheiros.	–
902		Fim da aplicação de regras de encriptação/desencriptação de ficheiros.	–
905		Retoma da aplicação de regras de encriptação/desencriptação de ficheiros.	–
910		Início da encriptação/desencriptação de ficheiros.	–
911		Conclusão da encriptação/desencriptação de ficheiros.	–
913		O ficheiro não foi encriptado, porque é uma exclusão.	–
950		Modo portátil ativado.	–
952		Modo portátil desativado.	–
1301		Início da encriptação/desencriptação do dispositivo.	–
1302		Conclusão da encriptação/desencriptação do dispositivo.	–
1304		Retoma da encriptação/desencriptação do dispositivo.	–

1310		Módulo de encriptação carregado.	–
1307		O dispositivo não está encriptado.	–
1308		O processo de encriptação/desencriptação do dispositivo foi alterado para o modo ativo.	–
1309		O processo de encriptação/desencriptação do disco foi alterado para o modo passivo.	–
1330		Conta de novo Agente de Autenticação criada.	–
1331		Conta do Agente de Autenticação eliminada.	–
1332		Password da conta do Agente de Autenticação alterada.	–
1333		Início de sessão no Agente de Autenticação realizado com sucesso.	–
1334		Falha ao iniciar sessão no Agente de Autenticação.	–
1335		Disco rígido acedido através da solicitação de acesso a dispositivos encriptados.	–
1336		Falha ao tentar aceder ao disco rígido através do procedimento de solicitação de acesso a dispositivos encriptados.	–
1337		Conta não adicionada. Esta conta já existe.	–
1338		Conta não modificada. Esta conta não existe.	–
1339		Conta não eliminada. Esta conta não existe.	–
1341		Atualização da FDE bem-sucedida.	✓
1343		Reversão da atualização da FDE bem-sucedida.	✓
1346		Falha ao desinstalar os controladores da Encriptação de disco Kaspersky na imagem WinRE.	✓
1370		A chave de recuperação do BitLocker foi alterada.	✓
1371		A password/PIN do BitLocker foi alterada.	✓
1372		A chave de recuperação do BitLocker foi guardada na unidade amovível.	✓

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
2100		Servidor da Kaspersky Anti Targeted Attack Platform indisponível.	–
2105		A inicialização da aplicação foi bloqueada.	✓
2106		A abertura do documento foi bloqueada.	✓
2112		Todos os processos iniciados a partir da imagem ou do fluxo do ficheiro foram terminados.	✓
2113		Aplicação iniciada.	✓
2111		O ficheiro ou o fluxo foi eliminado pelo administrador do servidor do Kaspersky Anti Targeted Attack Platform.	✓
2110		O ficheiro foi restaurado da quarentena pelo administrador no servidor do Kaspersky Anti Targeted Attack Platform.	✓
2109		O ficheiro foi movido para a quarentena pelo administrador no servidor do Kaspersky Anti Targeted Attack Platform.	✓
2107		A atividade de rede de todas as aplicações de terceiros está bloqueada.	✓
2108		Tráfego de rede desbloqueado.	✓
2104		As tarefas do servidor da Kaspersky Anti Targeted Attack Platform estão a ser processadas.	–
2103		O processamento de tarefas do servidor da Kaspersky Anti Targeted Attack Platform está inativo.	–
2101		Endpoint Sensors ligados ao servidor.	–
2102		Ligação ao servidor da Kaspersky Anti Targeted Attack Platform retomada.	–


[Scan de vírus](#)

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
302		Objeto malicioso detetado.	✓
312		Não foi possível executar a desinfecção.	–
313		Não pode ser eliminado.	–
317		Erro de processamento.	–
452		Processo terminado.	–
453		Não foi possível terminar o processo.	–
310		Não foi possível criar uma cópia de segurança.	–
314		Objeto não processado.	–
320		Objeto encriptado.	–
321		Objeto corrompido.	–
323		O objeto será eliminado ao reiniciar.	–
324		O objeto será desinfetado ao reiniciar.	–
303		Foi detetado software legítimo que pode ser utilizado por intrusos para danificar o seu computador ou dados pessoais.	–
336		Não foi possível restaurar o objeto da cópia de segurança.	✓
307		Objeto eliminado.	–
306		Objeto desinfetado.	–
455		Reversão concluída.	–
301		Objeto processado.	–
308		Foi criada uma cópia de segurança do objeto.	–
315		Objeto ignorado.	–
318		Arquivo detetado.	–
319		Objeto comprimido detetado.	–
327		Substituído por uma cópia que foi desinfetada anteriormente.	–
332		Informação sobre objeto detetado.	–
322		Arquivo de proteção de password detetado.	–
335		Objeto restaurado da cópia de segurança.	✓
329		Nome do objeto mudado.	–
340		O objeto está na lista de permissão do KSN Privado.	✓

[Verificação de integridade](#) 

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
2002		Falha ao verificar a assinatura do módulo do sistema.	–




[Atualização da base de dados](#) 

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
1011		Erro na atualização de componente.	–
1012		Erro na distribuição de atualizações dos componentes.	–
1014		Erro de atualização local.	–
1015		Erro de atualização da rede.	–
1017		Não pode iniciar duas tarefas em simultâneo.	–
1018		Erro na verificação das bases de dados e módulos das aplicações.	–
1019		Erro na interação com o Kaspersky Security Center.	–
1021		Nem todos os componentes foram atualizados.	–
1023		Atualização concluída com êxito, falha na distribuição de atualização.	–
101		Ocorreu um erro interno.	✓
2153		Falha na instalação do patch.	–
2156		Falha na reversão do patch.	–
1016		Operação cancelada pelo utilizador.	–
1001		Origem da atualização selecionada.	–
1002		Servidor de proxy selecionado.	–
1003		Transferência de ficheiro.	–
1004		Ficheiro transferido.	–
1005		Ficheiro instalado.	–
1006		Ficheiro atualizado.	–
1007		Ficheiro revertido devido a um erro de atualização.	–
1008		A atualizar ficheiros.	–
1009		A distribuir atualizações.	–
1010		A reverter ficheiros.	–
1013		A criar lista de ficheiros para transferência.	–
1020		Não existem atualizações disponíveis.	–
1022		Distribuição de atualização concluída com êxito.	–
2150		A transferir patches.	–
2151		A instalar patches.	–
2152		Patch instalado.	–
2154		A reverter patch.	–
2155		Patch revertido.	–
















[Eliminar dados](#)

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
2252		Não pode ser eliminado.	–
2253		Estatísticas de limpeza de tarefa.	–
2251		Objeto eliminado.	–

[Endpoint Detection and Response](#)

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
2551		Arranque do objeto bloqueado.	✓
2552		Arranque do processo bloqueado.	✓
2559		Execução do script bloqueada.	✓
2556		Objeto não está em quarentena (Endpoint Detection and Response).	✓
2651		IOC encontrado.	✓
2553		Arranque do objeto permitido. Evento registrado.	✓
2554		Arranque do processo permitido. Evento registrado.	✓
2560		Execução do script permitida. Evento registrado.	✓
2558		O objeto será eliminado após o reinício (Endpoint Detection and Response).	✓
2700		Isolamento da rede	✓
2701		Fim do isolamento da rede	✓
2555		Objeto em quarentena (Endpoint Detection and Response)	✓
2557		Objeto eliminado (Endpoint Detection and Response)	✓
2652		Verificação IOC iniciada	✓
2653		Verificação IOC concluída	✓

[Kaspersky Sandbox](#)

Códigos de eventos

ID do evento		Descrição	Por predefinição, ativado
2603		Objeto não está em quarentena (Kaspersky Sandbox).	✓
2607		Ocorreu um erro interno.	✓
2611		Erro ao enviar a tarefa de verificação para o Kaspersky Sandbox.	✓
2613		Certificado do servidor do Kaspersky Sandbox inválido.	✓
2614		O nó do Kaspersky Sandbox não está disponível.	✓
2615		Foi detetada uma ameaça durante o processamento assíncrono de tarefas.	✓
2617		Falha ao processar um objeto no Kaspersky Sandbox.	✓
2618		Foi alcançada a carga máxima para o Kaspersky Sandbox.	✓
2651		IOC encontrado.	✓
2620		A verificação da licença do Kaspersky Sandbox falhou .	✓
2605		O objeto será eliminado após reiniciar (Kaspersky Sandbox).	✓
2612		O tamanho total das tarefas de verificação excedeu o limite.	✓
308		Foi criada uma cópia de segurança do objeto.	–
2602		Objeto em quarentena (Kaspersky Sandbox).	✓
2604		Objeto eliminado (Kaspersky Sandbox).	✓
2606		Decidiu enviar a tarefa de verificação para o Kaspersky Sandbox.	✓
2609		A cache local foi limpa.	✓
2610		Não foi enviada uma tarefa de verificação para o Kaspersky Sandbox.	✓
2616		Não foram encontradas ameaças durante o processamento assíncrono de tarefas.	✓
2652		Verificação IOC iniciada.	✓
2653		Verificação IOC concluída.	✓
2608		Foi encontrado um resultado na cache durante o processamento síncrono de objetos	✓

Anexo 7. Eventos da aplicação no Registo de eventos do Kaspersky Security Center

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, 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.

O Kaspersky Endpoint Security gera eventos dos seguintes tipos: eventos genéricos 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 – Mensagem informativa (i), 2 – Aviso (⚠), 3 – Falha funcional (⚠), 4 – Crítico (⚠).
- 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 genéricos 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 genéricos têm um ID mais complexo, como GNRL_EV_VIRUS_FOUND. Para além das definições necessárias, os eventos genéricos contêm definições avançadas.

[Lista de eventos específicos do Kaspersky Endpoint Security for Windows](#) 















ID do evento		Descrição	Por predefinição, ativado
00000065		Erro interno da tarefa.	–
000000cb		A licença está quase a expirar.	–
000000cc		A licença expira em breve.	✓
000008cd		Estatísticas de limpeza de tarefa.	✓
000000ce		As bases de dados estão em falta ou corrompidas.	–
000000cf		As bases de dados estão extremamente desatualizadas.	✓
000000d0		As bases de dados estão desatualizadas.	✓
000000d1		A execução automática da aplicação está desativada.	✓
000000d2		As atualizações automáticas estão desativadas.	✓
000000d3		A autodefesa está desativada.	✓
000000d4		A tarefa não pode ser executada.	✓
000000d5		A operação com os recursos da aplicação está bloqueada pela Autodefesa.	✓
000000d6		Os componentes de proteção estão desativados.	✓
000000d7		O computador está a ser executado em modo segurança.	–
000000d8		Existem ficheiros não processados.	✓
000000d9		Relatório apagado.	✓
000000da		Definições da aplicação alteradas.	✓
000000db		Política de grupo aplicada.	✓
000000dc		Política de grupo desativada.	✓
000000dd		Tarefa iniciada.	✓
000000de		Tarefa parada.	✓
000000df		Tarefa concluída.	✓
000000e1		É necessário reiniciar o computador para concluir a atualização.	✓
000000e2		A licença permite a utilização de componentes que não foram instalados.	✓
000000e3		Todos os componentes da aplicação definidos pela licença foram instalados e executados no modo normal.	–
000000e6		Chave de reserva incorreta.	✓
000000e7		Deteção de ameaça ativa. Deve ser iniciada uma Desinfecção Avançada.	✓
000000e8		Desinfecção avançada iniciada.	✓
000000e9		Desinfecção avançada concluída.	✓
000000ee		As definições de subscrição foram alteradas.	✓
000000ef		A subscrição foi renovada.	✓

000000f0		A subscrição expira em breve.	✓
000000f5		O processamento de algumas funções do SO está desativado.	✓
00000134		Foi criada uma cópia de segurança do objeto.	✓
00000136		Não foi possível criar uma cópia de segurança.	✓
00000139		Não pode ser eliminado.	✓
0000013a		Objeto não processado.	✓
0000013d		Erro de processamento.	✓
00000140		Objeto encriptado.	–
00000141		Objeto corrompido.	–
00000143		O objeto será eliminado ao reiniciar.	✓
00000144		O objeto será desinfetado ao reiniciar.	✓
00000147		Substituído por uma cópia que foi desinfetada anteriormente.	–
00000149		Nome do objeto mudado.	✓
0000014c		Informação sobre objeto detetado.	✓
0000014f		Objeto restaurado da cópia de segurança.	✓
00000150		Não foi possível restaurar o objeto da cópia de segurança.	✓
00000154		O objeto está na lista de permissão do KSN Privado.	✓
00000157		Não há espaço suficiente no armazenamento da Quarentena.	✓
00000158		O armazenamento da Quarentena está quase sem espaço.	✓
00000159		Objeto restaurado da Quarentena.	✓
0000015a		Objeto não restaurado da Quarentena.	✓
0000015b		Objeto eliminado da Quarentena.	✓
0000015c		Objeto não eliminado da Quarentena.	✓
00000172		A ligação está na lista de permissão do KSN Privado.	✓
00000191		Aplicação colocada num grupo fiável.	✓
00000192		Aplicação colocada num grupo restrito.	✓
00000193		A Prevenção contra invasões do anfitrião foi ativada.	✓
000001c4		Processo terminado.	✓
000001c5		Não foi possível terminar o processo.	–
000001c7		Reversão concluída.	✓
000001c9		Ficheiro restaurado.	✓
000001ca		Valor de registo restaurado.	✓
000001cb		Valor de registo eliminado.	–
000002c3		Erro nas definições da tarefa. Definições de tarefa não aplicadas.	✓
000002c4		Definições de tarefa aplicadas com sucesso.	✓

000002c6		O processo proibido foi iniciado antes de o Kaspersky Endpoint Security for Windows ter sido iniciado.	✓
000002f2		Conteúdo indesejável foi acessado depois de um aviso.	–
000002f4		Página permitida aberta.	–
00000321		Operação com o dispositivo permitida.	–
00000323		Acesso temporário ao dispositivo ativado.	✓
00000329		Ligação de rede bloqueada.	✓
00000385		Início da aplicação de regras de encriptação/desencriptação de ficheiros.	✓
00000386		Fim da aplicação de regras de encriptação/desencriptação de ficheiros.	✓
00000388		Erro ao aplicar regras de encriptação/desencriptação de ficheiros.	✓
000003a3		Erro ao criar pacote encriptado.	✓
000003b7		Erro ao ativar o modo portátil.	✓
000003b9		Erro ao desativar o modo portátil.	✓
000003f3		Erro na atualização de componente.	✓
000003f4		Erro na distribuição de atualizações dos componentes.	–
000003f7		Erro de atualização da rede.	–
000003f8		Operação cancelada pelo utilizador.	✓
000003f9		Não pode iniciar duas tarefas em simultâneo.	✓
000003fa		Erro na verificação das bases de dados e módulos das aplicações.	✓
000003fb		Erro na interação com o Kaspersky Security Center.	✓
000003fc		Não existem atualizações disponíveis.	–
000003fd		Nem todos os componentes foram atualizados.	✓
000003fe		Distribuição de atualização concluída com êxito.	–
000003ff		Atualização concluída com êxito, falha na distribuição de atualização.	–
00000519		Erro ao encriptar/desencriptar o dispositivo.	✓
0000051a		Utilizador não aceitou a política de encriptação.	✓
0000051e		Módulo de encriptação carregado.	–
0000051f		Falha ao carregar o módulo de encriptação.	✓
00000520		Não foi possível aplicar a política.	✓
00000532		Conta de novo Agente de Autenticação criada.	–
00000533		Conta do Agente de Autenticação eliminada.	–
00000534		Password da conta do Agente de Autenticação alterada.	–
00000535		Início de sessão no Agente de Autenticação realizado com sucesso.	–
00000536		Falha ao iniciar sessão no Agente de Autenticação.	–



00000539		Conta não adicionada. Esta conta já existe.	–
0000053a		Conta não modificada. Esta conta não existe.	–
0000053b		Conta não eliminada. Esta conta não existe.	–
0000053c		A tarefa de gestão das contas de Agente de Autenticação terminou com um erro.	✓
0000053d		Atualização da FDE bem-sucedida.	✓
0000053e		Falha na atualização da FDE.	✓
0000053f		Reversão da atualização da FDE bem-sucedida.	✓
00000540		Reversão da atualização da encriptação concluída com um erro (para mais detalhes, consulte a Ajuda online do Kaspersky Endpoint Security for Windows).	✓
00000541		Falha ao instalar ou ao atualizar os controladores da Encriptação de disco Kaspersky na imagem WinRE.	✓
00000542		Falha ao desinstalar os controladores da Encriptação de disco Kaspersky na imagem WinRE.	✓
0000055a		A chave de recuperação do BitLocker foi alterada.	✓
0000055b		A password/PIN do BitLocker foi alterada.	✓
0000055c		A chave de recuperação do BitLocker foi guardada numa unidade amovível.	✓
00000579		Erro ao alterar componentes da aplicação.	✓
0000057a		Componentes da aplicação alterados com sucesso.	✓
0000057b		É necessário reiniciar para concluir a tarefa.	✓
000007d0		Digite um nome de utilizador e uma password.	✓
000007d1		Atividade de rede suspeita detetada.	✓
000007d2		Falha ao verificar a assinatura do módulo do sistema.	✓
000007d3		Ligação encriptada terminada.	–
000007e4		A participação na KSN está ativada.	✓
000007e5		A participação na KSN está desativada.	✓
000007e6		Servidores KSN disponíveis.	✓
000007e7		Servidores KSN indisponíveis.	✓
000007e8		A aplicação funciona e processa dados no âmbito da legislação vigente e utiliza as infraestruturas adequadas.	✓
00000802		Teclado autorizado.	✓
00000803		Teclado não autorizado.	✓
00000804		Erro de autorização de teclado.	✓
00000834		Servidor da Kaspersky Anti Targeted Attack Platform indisponível.	✓
00000835		Endpoint Sensor ligado ao servidor.	✓
00000836		Ligação ao servidor da Kaspersky Anti Targeted Attack Platform retomada.	✓

00000837		O processamento de tarefas do servidor da Kaspersky Anti Targeted Attack Platform está inativo.	✓
00000838		As tarefas do servidor da Kaspersky Anti Targeted Attack Platform estão a ser processadas.	✓
00000839		A inicialização da aplicação foi bloqueada.	✓
0000083a		A abertura do documento foi bloqueada.	✓
0000083b		A atividade de rede de todas as aplicações de terceiros está bloqueada.	✓
0000083c		Tráfego de rede desbloqueado.	✓
0000083d		O ficheiro foi movido para a quarentena pelo administrador no servidor do Kaspersky Anti Targeted Attack Platform.	✓
0000083e		O ficheiro foi restaurado da quarentena pelo administrador no servidor do Kaspersky Anti Targeted Attack Platform.	✓
0000083f		O ficheiro ou o fluxo foi eliminado pelo administrador do servidor do Kaspersky Anti Targeted Attack Platform.	✓
0000083e		O ficheiro foi restaurado da quarentena pelo administrador no servidor do Kaspersky Anti Targeted Attack Platform.	✓
00000840		Todos os processos iniciados a partir da imagem ou do fluxo do ficheiro foram terminados.	✓
00000841		Aplicação iniciada.	✓
00000869		Falha na instalação do patch.	✓
0000086c		Falha na reversão do patch.	✓
00000898		Pedido de AMSI bloqueado.	✓
000008cc		Erro ao eliminar um objeto.	✓
000009f8		Processo permitido para ser executado, evento registado.	✓
000009f9		Arranque do objeto bloqueado.	✓
000009fa		Objeto permitido para ser executado, evento registado.	✓
000009fb		Objeto em quarentena (Endpoint Detection and Response).	✓
000009fc		Objeto não está em quarentena (Endpoint Detection and Response).	✓
000009fd		Objeto eliminado (Endpoint Detection and Response).	✓
000009fe		O objeto será eliminado após o reinício (Endpoint Detection and Response).	✓
00000a2a		Objeto em quarentena (Kaspersky Sandbox).	✓
00000a2b		Objeto não está em quarentena (Kaspersky Sandbox).	✓
00000a2d		O objeto será eliminado após reiniciar (Kaspersky Sandbox).	✓
00000a2f		Ocorreu um erro interno.	✓
00000a34		O tamanho total das tarefas de verificação excedeu o limite.	✓
00000a35		Certificado do servidor do Kaspersky Sandbox inválido.	✓
00000a36		O nó do Kaspersky Sandbox não está disponível.	✓



00000a39		Falha ao processar um objeto no Kaspersky Sandbox.	
00000a3c		A verificação da licença do Kaspersky Sandbox falhou .	
00000a5b		IOC encontrado.	
00000a5c		Verificação IOC iniciada.	
00000a5d		Verificação IOC concluída.	
00000a8c		Isolamento da rede.	
00000a8d		Fim do isolamento da rede.	

[Lista de eventos genéricos](#) 

ID do evento		Descrição	
GNRL_EV_VIRUS_FOUND	❗	Objeto malicioso detetado.	<ul style="list-style-type: none"> • GNRL_EA_PAR (SHA256). • GNRL_EA_PAR • GNRL_EA_PAR de acordo com por exemplo, E • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR por exemplo, T • GNRL_EA_PAR adicionais sob Componente c Tecnologia de (método). Ameaça detet (denylist): t Versão EDR. Identificador d Hash MD5 do c
GNRL_EV_VIRUS_FOUND_BY_KSN	❗	Objeto malicioso detetado (KSN).	<ul style="list-style-type: none"> • GNRL_EA_PAR (SHA256). • GNRL_EA_PAR • GNRL_EA_PAR de acordo com por exemplo, E • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR por exemplo, T • GNRL_EA_PAR adicionais sob Componente c Tecnologia de (método). Ameaça detet (denylist): t Versão EDR. Identificador d Hash MD5 do c
GNRL_EV_VIRUS_FOUND_AND_BLOCKED	❗	Ligação perigosa bloqueada	

		(Proteção contra ameaças da Web).	<ul style="list-style-type: none"> • GNRL_EA_PAR objeto. • GNRL_EA_PAR de acordo com • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR por exemplo, T • GNRL_EA_PAR adicionais sob Componente c Tecnologia de (método). Ameaça detet (denylist): t
GNRL_EV_VIRUS_FOUND_AND_REPORTED		Ligação perigosa aberta (Proteção contra ameaças da Web).	<ul style="list-style-type: none"> • GNRL_EA_PAR objeto. • GNRL_EA_PAR de acordo com • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR por exemplo, T • GNRL_EA_PAR adicionais sob Componente c Tecnologia de (método). Ameaça detet (denylist): t
GNRL_EV_VIRUS_FOUND_AND_PASSED		Detetada ligação perigosa aberta anteriormente (Proteção contra ameaças da web).	<ul style="list-style-type: none"> • GNRL_EA_PAR objeto. • GNRL_EA_PAR de acordo com • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR por exemplo, T • GNRL_EA_PA adicionais sob Componente c Tecnologia de (método).







			Ameaça detetada (denylist): t
GNRL_EV_SUSPICIOUS_OBJECT_FOUND	⚠	Foi detetado software legítimo que pode ser usado por criminosos para danificar o seu computador ou dados pessoais	<ul style="list-style-type: none"> • GNRL_EA_PAR (SHA256). • GNRL_EA_PAR • GNRL_EA_PAR de acordo com por exemplo, E • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR por exemplo, T
GNRL_EV_OBJECT_CURED	⚠	Objeto desinfetado.	<ul style="list-style-type: none"> • GNRL_EA_PAR (SHA256). • GNRL_EA_PAR • GNRL_EA_PAR do objeto (opc • GNRL_EA_PAR de acordo com por exemplo, E • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR por exemplo, T • GNRL_EA_PAR adicionais sob Componente c Tecnologia de (método). • Ameaça detetada (denylist): t Versão EDR. Identificador d Hash MD5 do c
GNRL_EV_OBJECT_DELETED	⚠	Objeto eliminado.	<ul style="list-style-type: none"> • GNRL_EA_PAR (SHA256). • GNRL_EA_PAR • GNRL_EA_PAR do objeto (opc • GNRL_EA_PAR de acordo com







			<p>por exemplo, E</p> <ul style="list-style-type: none"> • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR por exemplo, T • GNRL_EA_PAR adicionais sob Componente c Tecnologia de (método). Ameaça detet (denylist): t Versão EDR. Identificador d Hash MD5 do c
GNRL_EV_OBJECT_NOTCURED		Não foi possível executar a desinfecção.	<ul style="list-style-type: none"> • GNRL_EA_PAR (SHA256). • GNRL_EA_PAR • GNRL_EA_PAR do objeto (opc • GNRL_EA_PAR de acordo con por exemplo, E • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR adicionais sob Componente c Tecnologia de (método). Ameaça detet (denylist): t Versão EDR. Identificador d Hash MD5 do c
GNRL_EV_OBJECT_BLOCKED		A transferência do objeto foi bloqueada.	<ul style="list-style-type: none"> • GNRL_EA_PAR (SHA256). • GNRL_EA_PAR • GNRL_EA_PAR de acordo con por exemplo, E • GNRL_EA_PAR utilizador da se





			<ul style="list-style-type: none"> • GNRL_EA_PAR por exemplo, T • GNRL_EA_PAR adicionais sob Componente c Tecnologia de (método). Ameaça detet (denylist): t Versão EDR. Identificador d Hash MD5 do c
GNRL_EV_OBJECT_REPORTED	⚠	<p>Objeto não processado (Proteção contra ameaças de correio).</p> <p>O resultado da verificação do objeto foi enviado para uma aplicação de terceiros (Proteção AMSI).</p>	<ul style="list-style-type: none"> • GNRL_EA_PAR (SHA256). • GNRL_EA_PAR • GNRL_EA_PAR de acordo com por exemplo, E • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR por exemplo, T • GNRL_EA_PAR adicionais sob Componente c Tecnologia de (método). Ameaça detet (denylist): t Versão EDR. Identificador d Hash MD5 do c
GNRL_EV_PASSWD_ARCHIVE_FOUND	🔍	Arquivo de proteção de password detetado.	<ul style="list-style-type: none"> • GNRL_EA_PAR • GNRL_EA_PAR do objeto (opc • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR adicionais sob Componente c Tecnologia de (método). Ameaça detet (denylist): true
GNRL_EV_ATTACK_DETECTED	🚨	Ataque de rede detetado (Proteção contra ameaças	<ul style="list-style-type: none"> • GNRL_EA_PAR

		de rede).	<ul style="list-style-type: none"> • GNRL_EA_PAR • GNRL_EA_PAR do computador do ataque de r indicado na or Por exemplo, 2 172.16.0.20 • GNRL_EA_PAR • GNRL_EA_PAR por exemplo, 12B012B012B • GNRL_EA_PAR do computador O endereço de bytes do anfitri 2886729929 p
GNRL_EV_LICENSE_EXPIRATION	⚠	Contrato de Licença do Utilizador Final violado.	
GNRL_EV_APPLICATION_LAUNCHED	🕒	Início da aplicação permitido (Controlo das Aplicações).	<ul style="list-style-type: none"> • GNRL_EA_PAR início da aplica Kaspersky Sec • GNRL_EA_PAR vezes que a ap • GNRL_EA_PAR segurança da c • GNRL_EA_PAR aplicação (opc • GNRL_EA_PAR utilizador da se
GNRL_EV_APPLICATION_LAUNCH_DENIED	⚠	Início da aplicação proibido (Controlo das Aplicações).	<ul style="list-style-type: none"> • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR categoria criac • GNRL_EA_PAR aplicação (opc • GNRL_EA_PAR relativa à assin • GNRL_EA_PAR executável da chrome.exe).

			<ul style="list-style-type: none"> • GNRL_EA_PAR ficheiro execut • GNRL_EA_PAR (SHA256). • GNRL_EA_PAR aplicação que executar.
GNRL_EV_APP_INCIDENT_OCCURED	ⓘ	Alerta assíncrono do Kaspersky Sandbox.	<ul style="list-style-type: none"> • GNRL_EA_PAR componente K • GNRL_EA_PAR objeto. • GNRL_EA_PAR • GNRL_EA_PAR (SHA256).
GNRL_EV_APP_LAUNCH_TESTED_DENIED	ⓘ	Início de aplicação proibido no modo de teste (Controlo das Aplicações).	<ul style="list-style-type: none"> • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR categoria criac • GNRL_EA_PAR segurança da c • GNRL_EA_PAR relativa à assin • GNRL_EA_PAR executável da chrome.exe). • GNRL_EA_PAR ficheiro execut • GNRL_EA_PAR (SHA256). • GNRL_EA_PAR aplicação que executar.
GNRL_EV_APP_LAUNCH_TESTED_ALLOW	ⓘ	Início de aplicação permitido no modo de teste (Controlo das Aplicações).	<ul style="list-style-type: none"> • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR categoria criac • GNRL_EA_PAR segurança da c

			<ul style="list-style-type: none"> • GNRL_EA_PAR aplicação (opc
GNRL_EV_AC_USER_REQUEST		Mensagem de bloqueio do início da aplicação para o administrador (Controlo das Aplicações).	<ul style="list-style-type: none"> • GNRL_EA_DES para o utilizador • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR executável da chrome.exe). • GNRL_EA_PAR ficheiro execut • GNRL_EA_PAR (SHA256). • GNRL_EA_PAR aplicação que executar.
GNRL_EV_WEB_URL_BLOCKED		Acesso negado (Controlo de Internet).	<ul style="list-style-type: none"> • GNRL_EA_PAR • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR Controlo de In
GNRL_EV_WEB_URL_BLOCKED_BY_KSN		Acesso negado por KSN (Controlo de Internet).	<ul style="list-style-type: none"> • GNRL_EA_PAR • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR Controlo de In
GNRL_EV_WEB_URL_WARNING		Aviso sobre conteúdo indesejável (Controlo de Internet).	<ul style="list-style-type: none"> • GNRL_EA_PAR • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR Controlo de In
GNRL_EV_WC_USER_REQUEST		Mensagem de bloqueio de acesso à página da Internet para o administrador (Controlo de Internet).	<ul style="list-style-type: none"> • GNRL_EA_DES para o utilizador • GNRL_EA_PAR • GNRL_EA_PAR utilizador da se
GNRL_EV_DC_USER_REQUEST		Mensagem de bloqueio de acesso ao dispositivo para o	<ul style="list-style-type: none"> • c_er_descr é utilizador.

		administrador (Controlo de Dispositivos).	<ul style="list-style-type: none"> • GNRL_EA_PAR (HWID). • GNRL_EA_PAR utilizador da se
GNRL_EV_DEVCTRL_DEV_PLUGGED		Dispositivo ligado (Controlo de Dispositivos).	<ul style="list-style-type: none"> • GNRL_EA_PAR (HWID). • GNRL_EA_PAR utilizador da se
GNRL_EV_DEVCTRL_DEV_UNPLUGGED		Dispositivo removido (Controlo de Dispositivos).	<ul style="list-style-type: none"> • GNRL_EA_PAR (HWID). • GNRL_EA_PAR utilizador da se
GNRL_EV_DEVCTRL_DEV_PLUG_DENIED		Dispositivo ligado bloqueado (Controlo de Dispositivos).	<ul style="list-style-type: none"> • GNRL_EA_PAR (HWID). • GNRL_EA_PAR utilizador da se
GNRL_EV_ADSEC_DETECT	 / 	Ação de processo bloqueada/Ação de processo ignorada (Controlo de Anomalias Adaptativo).	<ul style="list-style-type: none"> • GNRL_EA_PAR Controlo de A • GNRL_EA_PAR heurística. • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR • GNRL_EA_PAR • GNRL_EA_PAR destino. • GNRL_EA_PAR • GNRL_EA_PAR adicionais sob • Hashes do pro • processo/obje • Processo bloq • true ou fals • ID de seguranc
GNRL_EV_ADSEC_USER_REQUEST		Mensagem de bloqueio de atividade de aplicação para o administrador (Controlo de Anomalias Adaptativo).	<ul style="list-style-type: none"> • GNRL_EA_DES para o utilizad • GNRL_EA_PAR Controlo de A

			<ul style="list-style-type: none"> • GNRL_EA_PAR heurística. • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR • GNRL_EA_PAR • GNRL_EA_PAR destino. • GNRL_EA_PAR • GNRL_EA_PAR adicionais sob Hashes do pro processo/obje Processo bloq true ou fals ID de seguranc
GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION		Acesso ao ficheiro bloqueado.	<ul style="list-style-type: none"> • GNRL_EA_PAR • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR executável (po aplicação, que ao ficheiro.
GNRL_EV_ENCRYPTION_ERROR		Erro de encriptação/descriptação de ficheiros.	<ul style="list-style-type: none"> • GNRL_EA_PAR ficheiro. • GNRL_EA_PAR • GNRL_EA_PAR dispositivo.
GNRL_EV_DEVCTRL_DEV_PLUG_DENIED		Operação com o dispositivo proibida	<ul style="list-style-type: none"> • GNRL_EA_PAR (HWID). • GNRL_EA_PAR utilizador da se
GNRL_EV_USB_FILE_OPERATION		Operação de ficheiro executada (Controlo de Dispositivos).	<ul style="list-style-type: none"> • GNRL_EA_PAR ficheiro (escrit • GNRL_EA_PAR ficheiro. • GNRL_EA_PAR dispositivo.

			<ul style="list-style-type: none"> • GNRL_EA_PAR utilizador da se • GNRL_EA_PAR (HWID).
GNRL_EV_HST_CMD_RESULT	①	Resultados da tarefa.	<ul style="list-style-type: none"> • GNRL_EA_PAR • GNRL_EA_PAR execução do c 1 significa que com êxito 2 significa que executado 3 significa que com êxito 4 significa que eliminado • GNRL_EA_PAR resultado do c falhas.

Informação acerca de código de terceiros

A informação acerca de código de terceiros está incluída no ficheiro legal_notices.txt, na pasta de instalação da aplicação.

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 Systems Incorporated nos Estados Unidos e/ou noutros países.

Apple, FireWire, iTunes e Safari são marcas comerciais de Apple Inc. registadas nos Estados Unidos e 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.

Android e Google Chrome são marcas comerciais da Google, Inc.

Citrix e Citrix Provisioning Services e XenDesktop são marcas comerciais de Citrix Systems, Inc. e/ou de uma ou mais das suas subsidiárias e podem estar registadas no Escritório de Marcas e Patentes dos Estados Unidos e noutros países.

Dell é uma marca comercial da Dell, Inc. ou das suas subsidiárias.

o dBase é uma marca comercial da dataBased Intelligence, Inc.

EMC é uma marca comercial ou marca comercial registada da EMC Corporation nos Estados Unidos e/ou noutros países.

Radmin é uma marca registrada da Famatech.

IBM é uma marca comercial de International Business Machines Corporation, registada em várias jurisdições em todo o mundo.

ICQ é uma marca comercial e/ou marca de serviço da ICQ LLC.

Intel é uma marca comercial de Intel Corporation nos EUA e/ou noutros países.

IOS é uma marca registada da Cisco Systems, Inc. e/ou dos seus afiliados nos Estados Unidos e outros países.

Lenovo e 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 registada da Mail.Ru, LLC.

McAfee é uma marca comercial ou marca comercial registada da McAfee, Inc. nos Estados Unidos e noutros países.

Microsoft, Access, Active Directory, ActiveSync, BitLocker, Excel, Internet Explorer, LifeCam Cinema, MSDN, MultiPoint, Outlook, PowerPoint, PowerShell, Visual Basic, Visual FoxPro, Windows, Windows PowerShell, Windows Server, Windows Store, MS-DOS, Surface e Hyper-V são marcas comerciais da Microsoft Corporation nos Estados Unidos e noutros países.

Mozilla, Firefox e Thunderbird são as marcas comerciais da Mozilla Foundation.

Java e JavaScript são marcas comerciais registadas de Oracle Corporation e/ou das suas filiais.

VERISIGN é uma marca comercial registada ou não registada da VeriSign, Inc. e das suas subsidiárias nos Estados Unidos e noutros países.

VMware e VMware ESXi são marcas comerciais registadas ou marcas comerciais de VMware, Inc. nos Estados Unidos e/ou noutras jurisdições.

Thawte é uma marca comercial ou marca comercial registada da Symantec Corporation ou das suas filiais nos EUA e noutros países.

SAMSUNG é uma marca comercial da SAMSUNG nos Estados Unidos e noutros países.