kaspersky

Kaspersky Endpoint Security 10 Service Pack 2 for Windows

Conteúdos

Sobre o Kaspersky Endpoint Security 10 Service Pack 2 for Windows

Esta secção descreve as funções, os componentes e o kit de distribuição do Kaspersky Endpoint Security e fornece uma lista dos requisitos de hardware e de software do Kaspersky Endpoint Security.

Novidades

O Kaspersky Endpoint Security 10 Service Pack 2 for Windows disponibiliza as seguintes funcionalidades e melhoramentos:

1. Controlo de Arranque das Aplicações:
   - Suporta sistemas operativos de servidor.
   - Controla as transferências de módulos DLL e módulos e controladores.
   - Gere a lista de objetos na tarefa de inventário (módulos DLL e ficheiros de script)
   - Controla objetos com base num novo critério - por atributos dos certificados da assinatura digital.
   - Gera um relatório sobre inícios de teste de aplicações bloqueadas.
   - Suportes dois modos operativos para Controlo de Arranque das Aplicações: "Lista Negra" e "Lista Branca".
   - Utiliza o hash SHA256 para o controlo e inventário de objetos.
   - Controla a execução de scripts do interpretador PowerShell.
   - Utiliza armazenamento de certificados de sistema confiáveis.
2. A administração do Microsoft BitLocker ativa a encriptação de discos rígidos com a ajuda da tecnologia BitLocker da Microsoft:
   - Gestão remota da encriptação.
   - Monitorização de dispositivos encriptados.
   - Criação de relatórios de encriptação de dispositivos.
   - Restauro do acesso a dispositivos encriptados.
3. Encriptação de disco Kaspersky:
   - Suporte para introdução de credenciais no ambiente de pré-carregamento do Agente de Autenticação que utiliza um teclado virtual.
   - Suporte do modo de encriptação para encriptar apenas o espaço ocupado num dispositivo.
   - Suporte para encriptação em tablets (MS Surface versão 3 e 4).
4. Controlo de Privilégios das Aplicações:
   - Controla o acesso de aplicações em dispositivos de gravação de áudio e vídeo.

5. Controlo de Internet:

   - Configura as regras de acesso a recursos da Internet para categorias adicionais de recursos da Internet.

6. Controlo de dispositivos:

   - Regista eventos associados à eliminação e gravação de ficheiros em dispositivos USB.
   - Gera uma lista de redes Wi-Fi confiáveis com base nas seguintes definições: nome, tipo de encriptação e tipo de autenticação.
   - Gere direitos de acesso de utilizador para o ficheiro lido e operações de escrita em unidades de CD/DVD.

7. Antivírus de E-mail:

   - Capaz de eliminar e mudar o nome de tipos específicos de ficheiros dentro de arquivos para verificação pelo Antivírus de E-mail.

8. Kaspersky Security Network:

   - Apresenta o KSN como uma razão para uma decisão quanto ao método de processamento de objetos em relatórios do Kaspersky Endpoint Security e relatórios do Kaspersky Security Center.
   - Envia uma consulta ao KSN quanto à reputação de um ficheiro selecionado.
   - Apresenta o estado de disponibilidade dos servidores de KSN para computadores cliente que tenham o Kaspersky Endpoint Security instalado.

Kit de distribuição

O kit de distribuição do Kaspersky Endpoint Security contém os seguintes ficheiros:

- Os ficheiros necessários para instalar a aplicação utilizando qualquer um dos métodos disponíveis:
- Os ficheiros do pacote de atualização utilizados durante a instalação da aplicação.
- O ficheiro klcfginst.msi para instalar o administration plug-in do Kaspersky Endpoint Security através do Kaspersky Security Center.
- O ficheiro ksn_<ID do idioma>.txt, com o qual pode visualizar os termos de da participação na Kaspersky Security Network.
- O ficheiro license.txt, com o qual pode visualizar o Contrato de Licença do Utilizador Final.
- O ficheiro incompatible.txt que contém uma lista do software incompatível.
- O ficheiro installer.ini que contém as definições internas do kit de distribuição.

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

Tem de descompactar o kit de distribuição para aceder aos ficheiros.

Organizar a proteção do computador

O Kaspersky Endpoint Security fornece uma proteção abrangente do computador contra vários tipos de ameaças, ataques de rede e de phishing.

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.

Adicionalmente à proteção em tempo real que os componentes da aplicação permitem, é recomendado *verificar* regularmente a presença de vírus e outras ameaças no computador. Deste modo 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.

Para manter o Kaspersky Endpoint Security atualizado, tem de *Atualização* as bases de dados e os módulos utilizados pela aplicação. A aplicação é atualizada automaticamente por defeito, mas se necessário, pode atualizar as bases de dados e os módulos da aplicação manualmente.

Os seguintes componentes da aplicação são componentes de controlo:

- **Controlo de Arranque das Aplicações**. Este componente permite controlar as tentativas do utilizador de iniciar aplicações e regula o arranque das aplicações.
- **Controlo de Privilégios das Aplicações**. Este componente regista as ações das aplicações no sistema operativo e regula a atividade da aplicação, conforme o grupo confiável de uma determinada aplicação. Para cada grupo de aplicações é especificado um conjunto de regras. Estas regras regulam o acesso das aplicações aos dados do utilizador e aos recursos do sistema operativo. Tais dados incluem ficheiros de utilizador (a pasta Os meus documentos, cookies, informação de atividade do utilizador) e ficheiros, pastas e chaves de registo que contêm definições e informações importantes das aplicações utilizadas mais frequentemente.
- **Monitor de Vulnerabilidades**. O componente Monitor de Vulnerabilidades executa uma verificação de vulnerabilidade em tempo real das aplicações iniciadas ou que estão em execução no computador do utilizador.
- **Controlo de dispositivos**. Este componente permite definir restrições flexíveis de acesso a dispositivos de armazenamento de dados (tais como discos rígidos, unidades amovíveis, unidades de banda e unidades de CD/DVD), equipamento de transmissão de dados (tais como modems), equipamento que converte informações em cópias impressas (tais como impressoras), ou interfaces para ligar dispositivos a computadores (tais como USB, Bluetooth e Infravermelhos).
- **Controlo de Internet**. Este componente permite definir restrições flexíveis de acesso a recursos da Internet para grupos de utilizadores diferentes.

O funcionamento dos componentes de controlo baseia-se nas regras seguintes:

- O Controlo de Arranque das Aplicações utiliza as regras de Controlo de Arranque das Aplicações.
- O Controlo de Privilégios das Aplicações utiliza as regras de Controlo das Aplicações.
- O Controlo de Dispositivos utiliza as regras de acesso a dispositivo e as regras de acesso a barramentos de ligação.
- O Controlo de Internet utiliza as regras de acesso de recursos da Internet.

Os seguintes componentes da aplicação são componentes de proteção:

- **Antivírus de Ficheiros**. Este componente protege o sistema de ficheiros do computador de infeções. O Antivírus de Ficheiros é iniciado juntamente como o Kaspersky Endpoint Security e permanece ativo na memória do computador, verificando todos os ficheiros abertos, guardados ou iniciados no computador e em todas as unidades ligadas. O Antivírus de Ficheiros intercepta todas as tentativas de acesso a ficheiros e verifica a existência de vírus e outras ameaças nos ficheiros.

- **Monitorização do Sistema**. Este componente mantém um registo da atividade da aplicação no computador e fornece esta informação a outros componentes, de modo a garantir uma proteção mais eficaz do computador.

- **Antivírus de E-mail**. Este componente verifica a existência de vírus e outras ameaças nas mensagens de e-mail de entrada e de saída.

- **Antivírus de Internet**. Este componente verifica o tráfego recebido no computador do utilizador através dos protocolos HTTP e FTP, e verifica se os URLs estão identificados como endereços maliciosos ou de phishing.

- **Antivírus de MI**. Este componente verifica o tráfego recebido no computador através de protocolos de cliente de MI. O componente permite-lhe utilizar os clientes de MI de forma segura.

- **Firewall**. Este componente protege os dados armazenados no computador e bloqueia a maioria das ameaças possíveis ao sistema operativo enquanto o computador está ligado à Internet ou a uma rede local. O componente filtra todas as atividades de rede segundo dois tipos de regras: regras de rede de aplicações e regras de pacotes de rede.

- **Monitor de Rede**. Este componente permite ver a atividade de rede do computador em tempo real.

- **Bloqueio de Ataques de Rede**. Este componente inspeciona a atividade do tráfego de rede de entrada, típica de ataques de rede. Mediante a deteção de uma tentativa de ataque de rede dirigida ao computador, o Kaspersky Endpoint Security bloqueia a atividade de rede do computador atacante.

O Kaspersky Endpoint Security permite as tarefas seguintes:

- **Verificação completa**. O Kaspersky Endpoint Security verifica o sistema operativo, incluindo a RAM, os objetos carregados no arranque, os armazenamentos de cópias de segurança do sistema operativo e todas as unidades de discos rígidos e unidades amovíveis.

- **Verificação personalizada**. O Kaspersky Endpoint Security verifica os objetos selecionados pelo utilizador.

- **Verificação de áreas críticas**. O Kaspersky Endpoint Security verifica objetos carregados no arranque do sistema operativo, a RAM, e objetos alvos dos processos ocultos (rootkits).

- **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.

- **Verificação de Vulnerabilidade**. O Kaspersky Endpoint Security verifica a existência de vulnerabilidades no sistema operativo e no software instalado. Esta verificação garante a deteção e a remoção atempada de potenciais problemas que os intrusos podem explorar.

A funcionalidade de encriptação de ficheiros permite encriptar ficheiros e pastas localizados em unidades de leitura locais. A funcionalidade de encriptação da unidade permite encriptar unidades de disco rígido e unidades amovíveis.

Administração remota através do Kaspersky Security Center

O Kaspersky Security Center permite iniciar e parar o Kaspersky Endpoint Security remotamente num computador cliente e permite também gerir e configurar as definições da aplicação de forma remota.

Funções de serviço da aplicação

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

- **Relatórios**. Durante o seu funcionamento, a aplicação mantém um relatório de cada tarefa e componente da aplicação. O relatório contém uma lista dos eventos do Kaspersky Endpoint Security e de todas as operações efetuadas 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.

- **Armazenamento de dados**. Se a aplicação detetar ficheiros infetados ou provavelmente infetados ao verificar a existência de vírus e outras ameaças no computador, estes ficheiros são bloqueados. O Kaspersky Endpoint Security move os ficheiros provavelmente infetados para um armazenamento especial denominado *Quarentena*. O Kaspersky Endpoint Security armazena cópias de ficheiros desinfetados e apagados na *Cópia de segurança*. O Kaspersky Endpoint Security move os ficheiros que, por algum motivo, não são processados para a *lista de ficheiros não processados*. Pode verificar ficheiros, repor ficheiros nas pastas originais e apagar todos os conteúdos do armazenamento de dados.

- **Serviço de notificação**. O serviço de notificação mantém o utilizador informado sobre o estado atual da proteção do computador e sobre o funcionamento 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 eficácia da proteção informática através da recolha em tempo real de informações sobre a reputação de ficheiros, recursos da Internet e software 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 a partir da conta My Kaspersky para o site da Internet de Suporte Técnico ou receber assistência dos técnicos de suporte por telefone.

Se a aplicação devolve um erro 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.

A aplicação recebe informações sobre os erros recorrentes e suspende o funcionamento utilizando algoritmos específicos definidos por peritos da Kaspersky.

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
- Processador com uma velocidade de relógio de 1 GHz (que suporta o conjunto de instruções SSE2)
- RAM:
  - 1 GB (para sistema operativo de 32 bits);
  - 2 GB (para sistema operativo de 64 bits).

Sistemas operativos suportados para computadores pessoais:

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

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

Sistemas operativos suportados para servidores de ficheiros:

- Windows Small Business Server 2008 Standard/Premium (64 bits);
- Windows Small Business Server 2011 Essentials/Standard (64 bits);
- Windows MultiPoint Server 2011 (64 bits);
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2 ou posterior;
- 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.

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.

Instalar e remover a aplicação

Esta secção guia-o na instalação do Kaspersky Endpoint Security no computador, na configuração inicial, na atualização de uma versão anterior da aplicação e na remoção da aplicação do computador.

Instalar a aplicação

Esta secção descreve como instalar o Kaspersky Endpoint Security no computador e executar a configuração inicial da aplicação.

Sobre as formas de instalar a aplicação

O Kaspersky Endpoint Security 10 for Windows pode ser instalado localmente (diretamente no computador do utilizador) ou remotamente, a partir da estação de trabalho do administrador.

A instalação local do Kaspersky Endpoint Security 10 for Windows pode ser executada num dos seguintes modos:

- Em modo interativo, através da utilização do Assistente de Instalação da Aplicação.

  Este modo interativo requer a sua participação no processo de configuração.

- No modo não assistido, a partir da linha de comandos.

  Depois de a instalação ser iniciada no modo não assistido, o seu envolvimento no processo de instalação deixa de ser necessário.

A aplicação pode ser instalada remotamente em computadores de rede utilizando as ferramentas seguintes:

- Software do Kaspersky Security Center (consulte o *Guia de Implementação do Kaspersky Security Center*).
- Editor de Políticas de Grupo do Microsoft Windows (consulte os ficheiros de ajuda do sistema operativo).
- System Center Configuration Manager.

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

Instalar a aplicação utilizando o Assistente de Instalação

A interface do Assistente de Instalação da aplicação consiste numa sequência de janelas que correspondem aos passos de instalação da aplicação. Pode navegar entre as páginas do Assistente de Instalação, utilizando os botões **Anterior** e **Seguinte**. Para fechar o Assistente de Instalação após a conclusão da tarefa, clique no botão **Terminar**. Para parar o Assistente de Instalação em qualquer etapa, clique no botão **Cancelar**.

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

1. Execute o ficheiro setup.exe incluído no kit de distribuição.

O Assistente de Instalação é iniciado.

2. Siga as instruções do Assistente de Instalação.

Quando o ficheiro setup.exe é iniciado, o Kaspersky Endpoint Security verifica no computador a existência de qualquer software incompatível. Por predefinição, mediante a deteção de software incompatível, o processo de instalação é cancelado e a lista de aplicações incompatíveis com o Kaspersky Endpoint Security aparece no ecrã. Para continuar a instalação, remova estas aplicações do computador.

Passo 1. Certificar-se de que o computador cumpre os requisitos de instalação

Antes de instalar o Kaspersky Endpoint Security 10 for Windows num computador ou de atualizar uma versão anterior da aplicação, são verificadas as condições seguintes:

- Se o sistema operativo e o service pack cumprem os requisitos de software para a instalação do produto.
- 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 10 Service Pack 2 for Windows e a versão anterior da aplicação é automaticamente removida. Isto aplica-se às seguintes versões da aplicação:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1/MP4 CF2
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4/MP4 CF2
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows

Passo 2. Página inicial do procedimento de instalação

Se todos os requisitos para a instalação da aplicação forem cumpridos, é apresentada uma página inicial após iniciar o pacote de instalação. A página inicial notifica o utilizador do início da instalação do Kaspersky Endpoint Security no computador.

Para prosseguir com o Assistente de Instalação, clique no botão **Seguinte**.

Passo 3. Visualização do Acordo de Licença

Neste passo, recomendamos que verifique o contrato de licença celebrado entre o cliente e a Kaspersky.

Leia atentamente o Contrato de Licença e, se aceitar todos os termos, selecione a caixa de verificação **Aceito os termos do Contrato de Licença**.

Para regressar ao passo anterior do Assistente de Instalação, clique no botão **Anterior**. Para prosseguir com o Assistente de Instalação, clique no botão **Seguinte**. Para parar o Assistente de Instalação, clique no botão **Cancelar**.

Passo 4. Selecionar o tipo de instalação

Neste passo, pode selecionar o tipo de instalação mais adequado do Kaspersky Endpoint Security:

- **Instalação básica**. Se escolher este tipo de instalação, os componentes de proteção, Controlo de Privilégios das Aplicações e Monitor de Vulnerabilidades estão instalados no computador com as definições recomendadas pelos peritos da Kaspersky.
- **Instalação padrão**. Se selecionar este tipo de instalação, os componentes de proteção e controlo com definições recomendadas pela Kaspersky são instalados no computador.
- **Instalação personalizada**. Se selecionou este tipo da instalação, é-lhe solicitado que selecione os componentes a instalar e especifique a pasta de destino da aplicação.

  Este tipo de instalação permite instalar componentes que não estão incluídos nas instalações básicas e padrão.

A seleção padrão está selecionada por defeito.

Para regressar ao passo anterior do Assistente de Instalação, clique no botão **Anterior**. Para prosseguir com o Assistente de Instalação, clique no botão **Seguinte**. Para parar o Assistente de Instalação, clique no botão **Cancelar**.

Passo 5. Selecionar os componentes da aplicação a instalar

Este passo é executado se selecionar a *Instalação personalizada* da aplicação.

Neste passo, pode selecionar os componentes do Kaspersky Endpoint Security que pretende instalar. O Antivírus de Ficheiros é um componente obrigatório da instalação. Não pode cancelar a sua instalação.

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

- Prevenção de ataques BadUSB.
- Encriptação de unidades.
- Encriptação de ficheiros.
- Microsoft BitLocker Manager.

- KATA Endpoint Sensor.

O *Microsoft BitLocker Manager* executa as seguintes funções:

- Gere a encriptação do BitLocker integrada no sistema operativo do Windows.
- Configura as definições da política de encriptação e verifica a sua aplicabilidade para o computador gerido.
- Inicia os processos de encriptação e de desencriptação.
- Monitoriza o estado de encriptação no computador gerido.
- Armazena centralmente chaves de recuperação no Servidor de administração do Kaspersky Security Center.

O KATA Endpoint Sensor é um componente da Kaspersky Anti Targeted Attack Platform. Esta solução destina-se à deteção rápida de ameaças como, por exemplo, ataques direcionados. O componente monitoriza constantemente os processos, as ligações de rede ativas e ficheiros que são alterados e volta a transmitir esta informação para a Kaspersky Anti Targeted Attack Platform.

Para selecionar um componente para instalar, clique no ícone junto ao nome do componente para apresentar o menu de contexto e selecione a **O recurso será instalado na unidade de disco rígido local**. Para obter mais detalhes sobre as tarefas executadas pelo componente selecionado e o espaço em disco necessário para instalar o componente, consulte a secção inferior da página atual do Assistente de Instalação.

Para ver informações detalhadas sobre o espaço disponível nas unidades de disco rígido locais, clique no botão **Volume**. As informações são apresentadas na janela apresentada **Espaço em disco disponível**.

Para cancelar a instalação do componente, selecione a opção **O recurso estará indisponível** no menu de contexto.

Para voltar à lista de componentes instalados por predefinição, clique no botão **Repor**.

Para regressar ao passo anterior do Assistente de Instalação, clique no botão **Anterior**. Para prosseguir com o Assistente de Instalação, clique no botão **Seguinte**. Para parar o Assistente de Instalação, clique no botão **Cancelar**.

Passo 6. Selecionar a pasta de destino

Este passo está disponível se selecionar a *Instalação personalizada* da aplicação.

Durante este passo, pode especificar o caminho para a pasta de destino na qual a aplicação será instalada. Para selecionar a pasta de destino da aplicação, clique no botão **Procurar**.

Para ver informações sobre o espaço disponível nas unidades de disco rígido locais, clique no botão **Volume**. As informações são apresentadas na janela **Requisitos de espaço em disco** que é aberta.

Para regressar ao passo anterior do Assistente de Instalação, clique no botão **Anterior**. Para prosseguir com o Assistente de Instalação, clique no botão **Seguinte**. Para parar o Assistente de Instalação, clique no botão **Cancelar**.

Passo 7. Adicionar exclusões ao scan de vírus

Este passo está disponível se selecionar a *Instalação personalizada* da aplicação.

Nesta fase pode especificar quais as exclusões ao scan de vírus que pretende adicionar às definições da aplicação.

As caixas de verificação **Excluir áreas recomendadas pela Microsoft do âmbito de verificação de vírus** / **Excluir áreas recomendadas pela Kaspersky do âmbito de verificação de vírus** excluem, respetivamente, áreas recomendadas pela Microsoft e pela Kaspersky da zona confiável ou inclui-as na mesma.

Se uma destas caixas de verificação estiver selecionada, o Kaspersky Endpoint Security inclui na zona confiável, respetivamente, as áreas que a Microsoft ou a Kaspersky recomendam. O Kaspersky Endpoint Security não verifica a existência de vírus e de outras ameaças nessas áreas.

A caixa de verificação **Excluir áreas recomendadas pela Microsoft do âmbito de verificação de vírus** está disponível quando o Kaspersky Endpoint Security está instalado num computador com o Microsoft Windows para servidores de ficheiros.

Para regressar ao passo anterior do Assistente de Instalação, clique no botão **Anterior**. Para prosseguir com o Assistente de Instalação, clique no botão **Seguinte**. Para parar o Assistente de Instalação, clique no botão **Cancelar**.

Passo 8. Preparar a instalação da aplicação

É recomendada a proteção do processo de instalação, uma vez que o computador pode estar infetado com programas maliciosos que podem interferir com a instalação do Kaspersky Endpoint Security 10 for Windows.

A proteção do processo de instalação está ativada por defeito.

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. Se este for o caso, interrompa a instalação e inicie novamente o Assistente de Instalação da aplicação. No passo "Preparar a instalação da aplicação", desmarque a caixa de verificação **Proteger o processo de instalação**.

A caixa de verificação **Assegurar a compatibilidade com os PVS da Citrix** ativa/desativa a função que instala os controladores no modo de compatibilidade com os PVS da Citrix.

Selecione esta caixa de verificação apenas se estiver a trabalhar com Serviços de aprovisionamento da Citrix.

A caixa de verificação **Adicione o caminho para o ficheiro avp.com à variável de sistema %PATH%** ativa/desativa uma opção que adiciona o caminho ao ficheiro avp.com à variável de sistema %PATH%.

Se a caixa de verificação estiver selecionada, ao iniciar o Kaspersky Endpoint Security ou qualquer uma das suas tarefas a partir da linha de comandos não é necessário introduzir o caminho para o ficheiro executável. É suficiente introduzir o nome do ficheiro executável e o comando para iniciar uma determinada tarefa.

Para regressar ao passo anterior do Assistente de Instalação, clique no botão **Anterior**. Para instalar o programa, clique no botão **Instalar**. Para parar o Assistente de Instalação, clique no botão **Cancelar**.

As ligações de rede atuais podem ser terminadas enquanto a aplicação está a ser instalada no computador. A maior parte de ligações de rede terminadas são restauradas após a conclusão da instalação da aplicação.

Passo 9. Instalar a aplicação

A instalação da aplicação pode demorar algum tempo. Aguarde até que esteja concluída.

Se estiver a atualizar uma versão anterior da aplicação, este passo também inclui a migração das definições e a remoção da versão anterior da aplicação.

Após a instalação do Kaspersky Endpoint Security terminar, é iniciado o Assistente de Configuração Inicial.

Instalar a aplicação a partir da linha de comandos

O Kaspersky Endpoint Security pode ser instalado a partir da linha de comando num dos seguintes modos:

- Em modo interativo, através da utilização do Assistente de Instalação da Aplicação.
- Em modo silencioso. 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 silencioso, use as teclas `/ s` e `/ qn`.

Para instalar a aplicação ou atualizar a versão 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|0] [/pADDLOCAL=<componente>] [/pSKIPPRODUCTCHECK=1|0] [/pSKIPPRODUCTUNINSTALL=1|0] [/pKLLOGIN=<user name> /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 | 0] [ADDLOCAL = <componente>] [SKIPPRODUCTCHECK = 1 | 0] [SKIPPRODUCTUNINSTALL = 1 | 0] [KLLOGIN = <nome do utilizador> KLPASSWD = <password> KLPASSWDAREA = <escopo da password>] [ENABLETRACES = 1 | 0 TRACESLEVEL = <nível de rastreamento>] / qn
   ```

`EULA`	Aceitar ou recusar os termos do Contrato de Licença do Utilizador Final. Valores disponíveis: • `1` – aceitação dos termos do Contrato de Licença do Utilizador Final. • `0` – rejeição dos termos do Contrato de Licença do Utilizador Final. O texto do Contrato de Licença está incluído no kit de distribuição do Kaspersky Endpoint Security. É necessário aceitar os termos do Contrato de Licença do Utilizador Final para instalar a aplicação ou para atualizar a versão da aplicação.
`PRIVACYPOLICY`	Aceitação ou rejeição da Privacy Policy. Valores disponíveis: • `1` – aceitação da Privacy Policy. • `0` – rejeição da Privacy Policy.

	O texto da Privacy Policy encontra-se incluído no kit de distribuição do Kaspersky Endpoint Security. Para instalar a aplicação ou atualizar a versão da aplicação, tem de aceitar a Privacy Policy.
KSN	Aceitar ou recusar participar na Kaspersky Security Network. Se nenhum valor for definido para este parâmetro, o Kaspersky Endpoint Security solicitará a confirmação do seu consentimento ou recusa em participar no KSN, quando o Kaspersky Endpoint Security for iniciado pela primeira vez. Valores disponíveis: • `1` - acordo para participar no KSN. • `0` – Recusar participar na KSN (valor predefinido). O pacote de distribuição do Kaspersky Endpoint Security está otimizado para utilização com a Kaspersky Security Network. Se optou por não participar na Kaspersky Security Network, deve atualizar o Kaspersky Endpoint Security imediatamente após concluir a instalação.
ALLOWREBOOT	Reinício automático do computador, se necessário após a instalação ou atualização da aplicação. Valores disponíveis: • `1` - reinicialização automática do computador, se necessário. • `0` - a reinicialização automática do computador está bloqueada (valor padrão). Um reinicio não é necessário ao instalar o Kaspersky Endpoint Security. Reinicio é necessário apenas se tiver de remover aplicativos incompatíveis antes da instalação. Um reinício pode também ser necessário ao atualizar a versão da aplicação.
ADDLOCAL	Selecione componentes adicionais para instalação. Por predefinição, todos os componentes da aplicação estão selecionados para instalação, exceto os seguintes componentes: Prevenção de Ataque BadUSB, Encriptação de Nível de Ficheiro, Criptografia de Disco Cheio, Gestão de BitLocker do BitLocker e KATA Sensor de Ponto de Extremidade. Valores disponíveis: • `MSBitLockerFeature`. É instalado o componente Microsoft BitLocker Manager. • `AntiAPTFeature`. É instalado o componente KATA Endpoint Sensor.
SKIPPRODUCTCHECK	A verificar software incompatível. A lista de softwares incompatíveis está disponível no ficheiro incompatible.txt que está incluído no kit de distribuição. Valores disponíveis: • `1` - a verificação de software incompatível está ativada (valor padrão). • `0` - a verificação de software incompatível está desativada.
SKIPPRODUCTUNINSTALL	Remover automaticamente o software incompatível detetado. Valores disponíveis: • `1` - O Kaspersky Endpoint Security tenta remover software incompatível (valor predefinido). • `0` - a remoção automática de software incompatível é proibida.

KLLOGIN	Defina o nome de utilizador para aceder aos recursos e configurações do Kaspersky Endpoint Security (o componente Proteção de password). O nome do utilizador é definido com as definições de KLPASSWD e KLPASSWDAREA. O nome de utilizador predefinido é KLAdmin.
KLPASSWD	Especificar uma password para aceder às funcionalidades e definições do Kaspersky Endpoint Security (a password é especificada juntamente com os parâmetros KLLOGIN de sessão e KLPASSWDAREA). Se tiver especificado uma password mas não especificou um nome de utilizador com o parâmetro KLLOGIN, o nome de utilizador KLAdmin é utilizado por predefinição.
KLPASSWDAREA	Especificar o âmbito da password para aceder às funcionalidades e definições do Kaspersky Endpoint Security. Quando um utilizador tenta executar uma ação incluída neste âmbito, o Kaspersky Endpoint Security solicita as credenciais da conta do utilizador (parâmetros KLLOGIN e KLPASSWD). Utilize o caráter ";" para especificar vários valores. Valores disponíveis: • CONJUNTO - modificar as configurações da aplicação. • SAIR – sair da aplicação. • DESPROTEGER – desativar componentes de proteção e parar tarefas de verificação. • DESATIVAR POLÍTICA – desativar política do Kaspersky Security Center. • DESINSTALAR – remover a aplicação do computador. • DISCRRL - desativar os componentes de controlo. • REMOVELIC - remover a chave. • RELATÓRIOS - visualizar relatórios.
ENABLETRACES	Ativar ou desativar os rastreios da aplicação. O Kaspersky Endpoint Security guarda ficheiros de rastreio na pasta %ProgramData%/Kaspersky Lab depois de iniciar. Valores disponíveis: • 1 – os rastreios são ativados. • 0 – os rastreios são desativados (valor padrão).
TRACESLEVEL	Nível de detalhe do rastreio. Valores disponíveis: • 100 (crítico). Apenas as mensagens de erro crítico. • 200 (alto). Mensagens sobre todos os erros, incluindo erros fatais. • 300 (diagnóstico). Mensagens sobre todos os erros e uma seleção de mensagens contendo avisos. • 400 (importante). Todos os avisos e mensagens sobre erros comuns e críticos e uma seleção de mensagens que contêm informações adicionais.

- `500` (normal). Todos os avisos e mensagens sobre erros normais e fatais, e também mensagens contendo informações detalhadas sobre a operação da aplicação no modo normal (valor predefinido).
- `600` (baixo). Todas as mensagens possíveis.

Exemplo:

```
setup.exe / pEULA = 1 / pPRIVACYPOLICY = 1 /
pKSN = 1 / pALLOWREBOOT = 1 / s

msiexec / i kes_win.msi EULA = 1 PRIVACYPOLICY
= 1 KSN = 1 KLLOGIN = Admin KLPASSWD = Password
KLPASSWDAREA = SAIR; DISPOL.; DESINSTALAR / qn

setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Após a instalação da aplicação, o Kaspersky Endpoint Security ativa a licença de avaliação, a não ser que indique 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, tem de ativar uma licença comercial.

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 de configuração da aplicação;
- install.cfg – definições locais do Kaspersky Endpoint Security;
- setup.reg - chaves do registo.

  As chaves de registo do ficheiro setup.reg são escritas no registo apenas se o valor de `setup.reg` for estabelecido para o parâmetro `SetupReg` no ficheiro setup.ini. O ficheir setup.reg é gerado pelos peritos da Kaspersky. Não se recomenda modificar os 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.

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**, selecione **Pacotes**.
3. Na parte superior da consola, no painel de controlo, clique no botão **Criar pacote**.

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 kit de distribuição do Kaspersky Endpoint Security.

   b. Na secção **Tipo de Aplicação**, selecione a opção **Aplicação Padrão**.

   c. Na secção **Aplicação Padrão**:

   - No campo **Nome**, introduza o nome único do pacote de instalação (por exemplo, o nome da aplicação incluindo a versão).
   - No campo **Linha de comandos**, especifique as opções de instalação do Kaspersky Endpoint Security da linha de comandos.
   - 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 de administrador** selecionado.

   d. Na secção **Requisitos**:

   - Selecione a caixa de verificação **Iniciar outra aplicação em primeiro lugar** se pretender que seja iniciada uma aplicação diferente antes de instalar o Kaspersky Endpoint Security.

     Selecione a aplicação na lista pendente **Aplicação** ou especifique o caminho para o ficheiro executável desta aplicação clicando no **Botão Procurar**.

   - Selecione a opção **Esta aplicação pode ser iniciada apenas nas plataformas especificadas** na secção **Requisitos de plataformas** 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 linha de comandos 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.

O ficheiro setup.ini consiste nas seguintes secções:

- `[Setup]` – opções gerais de 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. O Antivírus de Ficheiros é um componente obrigatório e é instalado no computador, independentemente das definições indicadas nesta secção.
- `[Tarefas]` – 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
`[Configuração]`	`InstallDir`	Caminho para a pasta de instalação da aplicação.
	`ActivationCode`	Código de ativação do Kaspersky Endpoint Security.
	`Eula`	Aceitar ou recusar os termos do Contrato de Licença do Utilizador Final. Valores disponíveis: • `1` – aceitação dos termos do Contrato de Licença do Utilizador Final. • `0` – rejeição dos termos do Contrato de Licença do Utilizador Final.

		O texto do Contrato de Licença está incluído no kit de distribuição do Kaspersky Endpoint Security. É necessário aceitar os termos do Contrato de Licença do Utilizador Final para instalar a aplicação ou para atualizar a versão da aplicação.
	`Política de Privacidade`	Aceitação ou rejeição da Privacy Policy. Valores disponíveis: • `1` – aceitação da Privacy Policy. • `0` – rejeição da Privacy Policy. O texto da Privacy Policy encontra-se incluído no kit de distribuição do Kaspersky Endpoint Security. Para instalar a aplicação ou atualizar a versão da aplicação, tem de aceitar a Privacy Policy.
	`KSN`	Aceitar ou recusar participar na Kaspersky Security Network. Se nenhum valor for definido para este parâmetro, o Kaspersky Endpoint Security solicitará a confirmação do seu consentimento ou recusa em participar no KSN, quando o Kaspersky Endpoint Security for iniciado pela primeira vez. Valores disponíveis: • `1` - acordo para participar no KSN. • `0` – Recusar participar na KSN (valor predefinido). O pacote de distribuição do Kaspersky Endpoint Security está otimizado para utilização com a Kaspersky Security Network. Se optou por não participar na Kaspersky Security Network, deve atualizar o Kaspersky Endpoint Security imediatamente após concluir a instalação.
	`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 predefinido é KLAdmin.
	`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 nesse escopo, o Kaspersky Endpoint Security solicita as credenciais da conta do utilizador (parâmetros `Iniciar sessão` e `Password`). Utilize o caráter "`;`" para especificar vários valores. Valores disponíveis: • `CONJUNTO` - modificar as configurações da aplicação. • `SAIR` – sair da aplicação. • `DESPROTEGER` – desativar componentes de proteção e parar tarefas de verificação. • `DESATIVAR POLÍTICA` – desativar política do Kaspersky Security Center. • `DESINSTALAR` – remover a aplicação do computador. • `DISCRRL` - desativar os componentes de controlo. • `REMOVELIC` - remover a chave. • `RELATÓRIOS` - visualizar relatórios.
	`Auto-proteção`	Ativação ou desativação do mecanismo de proteção de instalação da aplicação. Valores disponíveis: • `1` – o mecanismo de proteção de instalação de aplicação é ativado. • `0` – o mecanismo de proteção de instalação de aplicação é desativado. Pode desativar a proteção de instalação. A proteção de instalação inclui a proteção contra o spoofing do pacote de distribuição com software malicioso, bloqueando o acesso à pasta de instalação do Kaspersky Endpoint Security, e bloqueando o acesso ao núcleo 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.
	`Reinicialização=1`	Reinício automático do computador, se necessário após a instalação ou atualização da aplicação. Se nenhum valor for definido para este parâmetro, a reinicialização automática do computador será bloqueada.

		Um reinicio não é necessário ao instalar o Kaspersky Endpoint Security. Reinicio é necessário apenas se tiver de remover aplicativos incompatíveis antes da instalação. Um reinício pode também ser necessário ao atualizar a versão da aplicação.
	`AddEnvironment`	Complemente a variável de sistema %PATH% com o caminho para os ficheiros executáveis localizados na pasta de instalação do Kaspersky Endpoint Security. Valores disponíveis: • `1` – a variável de sistema %PATH% é complementada com o caminho para os ficheiros executáveis localizados na pasta de instalação do Kaspersky Endpoint Security. • `0` – a variável de sistema %PATH% não é complementada com o caminho para os ficheiros executáveis localizados na pasta de instalação do Kaspersky Endpoint Security.
	`AMPPL`	Ativa ou desativa a proteção do serviço Kaspersky Endpoint Security utilizando a tecnologia AM-PPL (Antimalware Protected Process Light). Valores disponíveis: • `1` – a proteção do serviço Kaspersky Endpoint Security utilizando a tecnologia AM-PPL é ativada. • `0` – a proteção do serviço Kaspersky Endpoint Security utilizando a tecnologia AM-PPL é desativada.
	`SetupReg`	Ativa a escrita das chaves de registo do ficheiro setup.reg para o registo. Valor do parâmetro `SetupReg: setup.reg`.
	`EnableTraces`	Ativar ou desativar os rastreios da instalação da aplicação. O Kaspersky Endpoint Security guarda ficheiros de rastreamento na pasta %ProgramData%/Kaspersky Lab. Valores disponíveis: • `1` – os rastreios de instalação da aplicação são ativados. • `0` - os rastreios de instalação da aplicação estão desativados (valor padrão).
	`TracesLevel`	Nível de detalhe do rastreio. Valores disponíveis: • `100` (crítico). Apenas as mensagens de erro crítico. • `200` (alto). Mensagens sobre todos os erros, incluindo erros fatais.

		• `300` (diagnóstico). Mensagens sobre todos os erros e uma seleção de mensagens contendo avisos. • `400` (importante). Todos os avisos e mensagens sobre erros comuns e críticos e uma seleção de mensagens que contêm informações adicionais. • `500` (normal). Todos os avisos e mensagens sobre erros normais e fatais, e também mensagens contendo informações detalhadas sobre a operação da aplicação no modo normal (valor predefinido). • `600` (baixo). Todas as mensagens possíveis.
`[Componentes]`	`TODOS`	Instalar todos os componentes. Se o valor do parâmetro `1` for especificado, todos os componentes serão instalados independentemente das definições de instalação dos componentes individuais.
	`MailAntiVirus`	Antivírus de E-mail.
	`IMAntiVirus`	Antivírus de MI.
	`WebAntiVirus`	Antivírus de Internet.
	`ApplicationPrivilegeControl`	Controlo de Privilégios das Aplicações.
	`SystemWatcher`	Monitorização do Sistema.
	`Firewall`	Firewall.
	`NetworkAttackBlocker`	Bloqueio de Ataques de Rede.
	`WebControl`	Controlo de Internet.
	`DeviceControl`	Controlo de dispositivos.
	`ApplicationStartupControl`	Controlo de Arranque das Aplicações.
	`FileEncryption`	Bibliotecas de encriptação ao nível dos ficheiros.
	`DiskEncryption`	Bibliotecas de Full Disk Encryption.
	`VulnerabilityAssessment`	Monitor de Vulnerabilidades.
	`KeyboardAuthorization`	Prevenção de ataques BadUSB.
	`AntiAPT`	KATA Endpoint Sensor.
	`MSBitLocker`	Microsoft BitLocker Manager.
	`AdminKitConnector`	Conector do Agente de Rede para administração remota da aplicação através do Kaspersky Security Center. Valores disponíveis: • `1` – o Conector do Agente de Rede é instalado. • `0` – o Conector do Agente de Rede não é instalado.

[Tarefas]	ScanMyComputer	Tarefa de Verificação Completa. Valores disponíveis: • 1 – A tarefa não é incluída na lista de tarefas do Kaspersky Endpoint Security. • 0 – A tarefa não é incluída na lista de tarefas do Kaspersky Endpoint Security.
	ScanCritical	Tarefa de Verificação de Áreas Críticas. Valores disponíveis: • 1 – A tarefa não é incluída na lista de tarefas do Kaspersky Endpoint Security. • 0 – A tarefa não é incluída na lista de tarefas do Kaspersky Endpoint Security.
	Atualização	Tarefa de atualização. Valores disponíveis: • 1 – A tarefa não é incluída na lista de tarefas do Kaspersky Endpoint Security. • 0 – A tarefa não é incluída na lista de tarefas do Kaspersky Endpoint Security.

Assistente de Configuração Inicial

O Assistente de Configuração Inicial do Kaspersky Endpoint Security é iniciado no final do procedimento de instalação da aplicação. O Assistente de Configuração Inicial permite ativar a aplicação e recolhe informações sobre as aplicações incluídas no sistema operativo. Estas aplicações são adicionadas à lista de aplicações confiáveis cujas ações no sistema operativo não estão sujeitas a quaisquer restrições.

A interface do Assistente de Configuração Inicial é constituída por uma sequência de páginas (passos). Pode navegar pelas páginas do Assistente de Configuração Inicial, utilizando os botões **Anterior** e **Seguinte**. Para concluir o procedimento do Assistente de Configuração Inicial, clique no botão **Terminar**. Para parar o procedimento do Assistente de Configuração Inicial em qualquer fase, clique em **Cancelar**.

Se o Assistente de Configuração Inicial for interrompido por algum motivo, as definições já especificadas não são guardadas. Quanto voltar a tentar utilizar a aplicação, o Assistente de Configuração Inicial será iniciado novamente e terá de configurar as definições novamente.

Ativar a aplicação

É necessário que a aplicação esteja ativada num computador com a data e hora de sistema atuais. Se a data e a hora do sistema forem alteradas após a ativação da aplicação, não é possível utilizar a chave. A aplicação muda para um modo de funcionamento sem atualizações e o Kaspersky Security Network fica indisponível. A chave pode ser novamente utilizada apenas se reinstalar o sistema operativo.

Neste passo, selecione uma das seguintes opções de ativação do Kaspersky Endpoint Security:

- **Ativar com um código de ativação**. Para ativar a aplicação com um código de ativação, selecione esta opção e introduza um código de ativação.
- **Ativar com um ficheiro-chave**. Selecione esta opção para ativar a aplicação com um ficheiro-chave.
- **Ativar a versão de avaliação**. Para ativar a versão de avaliação da aplicação, selecione esta opção. O utilizador pode utilizar a versão com todas as funcionalidades da aplicação durante o período limitado pela licença para a versão de avaliação da aplicação. Após a licença expirar, as funcionalidades da aplicação são bloqueadas e não poderá ativar a versão de avaliação novamente.
- **Ativar mais tarde**. Selecione esta opção para ignorar a fase de ativação do Kaspersky Endpoint Security. O utilizador poderá utilizar apenas os componentes Antivírus de Ficheiros e Firewall. Pode atualizar as bases de dados de antivírus e os módulos da aplicação do Kaspersky Endpoint Security apenas uma vez após a instalação. A opção **Ativar mais tarde** está disponível apenas na primeira inicialização do Assistente de Configuração Inicial, imediatamente após a instalação da aplicação.

É necessária uma ligação à Internet para ativar a versão de avaliação da aplicação com um código de ativação.

Para prosseguir com o Assistente de Configuração Inicial, selecione uma opção de ativação e clique no botão **Seguinte**. Para parar o Assistente de Configuração Inicial, clique no botão **Cancelar**.

Ativar com um código de ativação

Este passo está disponível apenas ao ativar a aplicação através de um código de ativação. Este passo é ignorado se ativar uma versão de avaliação da aplicação ou ativar a aplicação através de um ficheiro-chave.

Durante este passo, o Kaspersky Endpoint Security envia dados ao servidor de ativação de modo a validar o código de ativação introduzido:

- Se a verificação do código de ativação for bem-sucedida, o Assistente de Configuração Inicial avança automaticamente para a janela seguinte.
- Se a validação do código de ativação falhar, é apresentada uma mensagem correspondente. Neste caso, deve procurar aconselhamento junto do fornecedor de software que lhe vendeu a licença do Kaspersky Endpoint Security.
- Se o número de ativações com o código de ativação for excedido, é apresentada uma notificação correspondente. O Assistente de Configuração Inicial é interrompido e a aplicação sugere-lhe que contacte o Suporte Técnico da Kaspersky.

Para regressar ao passo anterior do Assistente de Configuração Inicial, clique no botão **Anterior**. Para parar o Assistente de Configuração Inicial, clique no botão **Cancelar**.

Ativar com um ficheiro-chave

Este passo está disponível apenas ao ativar a aplicação através de um ficheiro-chave.

Neste passo, especifique o caminho para o ficheiro-chave. Para tal, clique no botão **Procurar** e selecione um ficheiro-chave no formulário `<ID do ficheiro>.key`.

Depois de selecionar um ficheiro-chave, são apresentadas as seguintes informações na parte inferior da janela:

- Chave
- O tipo de licença (comercial ou de avaliação) e o número de computadores abrangidos por esta licença
- Data de ativação da aplicação no computador
- Data de validade da licença
- Funcionalidade da aplicação disponível ao abrigo da licença
- Notificações sobre problemas de chave, caso existam. Por exemplo, *Lista negra de chaves corrompida*.

Para regressar ao passo anterior do Assistente de Configuração Inicial, clique no botão **Anterior**. Para prosseguir com o Assistente de Configuração Inicial, clique no botão **Seguinte**. Para parar o Assistente de Configuração Inicial, clique no botão **Cancelar**.

Selecionar funções para ativar

Este passo está disponível apenas ao ativar a versão de avaliação da aplicação.

Neste passo, pode selecionar a funcionalidade que ficará disponível depois da ativação da aplicação:

- **Instalação básica**. Se esta opção estiver selecionada, apenas os componentes de proteção, Controlo de Privilégios das Aplicações e Monitor de Vulnerabilidades estão disponíveis após a ativação da aplicação.
- **Instalação padrão**. Se esta opção for selecionada, apenas os componentes de proteção e controlo da aplicação estarão disponíveis após a ativação.
- **Instalação completa**. Se esta opção estiver selecionada, todos os componentes de aplicações instalados, incluindo a funcionalidade de encriptação de dados, estarão disponíveis após a ativação da aplicação.

Se selecionou mais componentes do que os que a licença adquirida permite durante a instalação, após a ativação da aplicação os componentes que estão indisponíveis de acordo com a licença serão instalados, mas não estarão operacionais. Se a licença adquirida permite utilizar mais componentes do que os atualmente instalados, após a aplicação ser ativada os componentes que não foram instalados são apresentados na secção **Licenciamento**.

A seleção padrão está selecionada por defeito.

Para regressar ao passo anterior do Assistente de Configuração Inicial, clique no botão **Anterior**. Para prosseguir com o Assistente de Configuração Inicial, clique no botão **Seguinte**. Para parar o Assistente de Configuração Inicial, clique no botão **Cancelar**.

Concluir ativação

Durante este passo, o Assistente de Configuração Inicial informa-o da ativação com êxito do Kaspersky Endpoint Security. São fornecidas as seguintes informações sobre a licença:

- O tipo de licença (comercial ou de avaliação) e o número de computadores abrangidos por esta licença
- Data de validade da licença
- Funcionalidade da aplicação disponível ao abrigo da licença

Para prosseguir com o Assistente de Configuração Inicial, clique no botão **Seguinte**. Para parar o Assistente de Configuração Inicial, clique no botão **Cancelar**.

Analisar o sistema operativo

Durante este passo, é recolhida informação sobre aplicações incluídas no sistema operativo. Estas aplicações são adicionadas à lista de aplicações confiáveis cujas ações no sistema operativo não estão sujeitas a quaisquer restrições.

Outras aplicações são analisadas ao serem iniciadas pela primeira vez após a instalação do Kaspersky Endpoint Security.

Para parar o Assistente de Configuração Inicial, clique no botão **Cancelar**.

A concluir a configuração inicial da aplicação

A janela de conclusão do Assistente de Configuração Inicial contém informações sobre a conclusão do processo de instalação do Kaspersky Endpoint Security.

Se pretender iniciar o Kaspersky Endpoint Security, clique no botão **Concluir**.

Se pretender sair do Assistente de Configuração Inicial sem iniciar o Kaspersky Endpoint Security, desmarque a caixa de verificação **Iniciar o Kaspersky Endpoint Security 10 for Windows** e clique em **Concluir**.

Declaração de Recolha de Dados da KSN

Durante este passo, é convidado a participar na Kaspersky Security Network.

Reveja a Declaração de Recolha de Dados da KSN:

- Se aceitar todos os termos, selecione a opção **Aceito os termos de participação no Kaspersky Security Network** na janela do Assistente de Configuração Inicial.
- Se não aceitar os termos de participação no Kaspersky Security Network, selecione a opção **Não aceito os termos de participação no Kaspersky Security Network** na janela do Assistente de Configuração Inicial.

Para continuar com o Assistente de Configuração Inicial, clique em **OK**.

Sobre as formas de atualizar uma versão anterior da aplicação

Para atualizar uma versão anterior da aplicação para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows, desencripte todas as unidades de disco rígido encriptadas.

Pode atualizar as seguintes aplicações para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1 (compilação 6.0.4.1424) / MP4 CF2 (compilação 6.0.4.1611)
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 (compilação 6.0.4.1424) / MP4 CF2 (compilação 6.0.4.1611)
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows (compilação 10.2.2.10535)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows (compilação 10.2.2.10535(MR1))
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows (compilação 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows (compilação 10.2.5.3201).

Quando qualquer uma das aplicações anteriormente indicadas é atualizada para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows, os conteúdos em Quarentena e Cópia de Segurança não são transferidos.

Pode atualizar a versão antiga da aplicação da seguinte forma:

- Localmente, no modo interativo, através da utilização do Assistente de Instalação da Aplicação.
- No modo não interativo, a partir da linha de comandos
- Utilizar o complexo de software do Kaspersky Security Center remotamente (consulte o *Manual de Implementação do Kaspersky Security Center*)
- Remotamente, através do Editor de Políticas de Grupo do Microsoft Windows (consulte os ficheiros de ajuda do sistema operativo)

Ao atualizar uma versão anterior da aplicação para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows, não é necessário remover a versão anterior da aplicação. É recomendado fechar todas as aplicações ativas antes de atualizar uma versão anterior da aplicação.

Remover a aplicação

Esta secção descreve como remover o Kaspersky Endpoint Security do computador.

Sobre as formas de 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 removido do computador de várias formas:

- Localmente em modo interativo, através do Assistente de Instalação
- No modo não interativo, a partir da linha de comandos
- Utilizar o complexo de software do Kaspersky Security Center remotamente (consulte o *Guia de Implementação do Kaspersky Security Center* para obter detalhes)
- Remotamente, através do Editor de Políticas de Grupo do Microsoft Windows (consulte os ficheiros de ajuda do sistema operativo)

Remover a aplicação utilizando o Assistente de Instalação

Para remover o Kaspersky Endpoint Security através do Assistente de Instalação:

1. No menu **Iniciar**, selecione **Aplicações → Kaspersky Endpoint Security 10 for Windows → Modificar, Reparar ou Remover**.

   O Assistente de Instalação é iniciado.

2. Na janela **Modificar, Reparar ou Remover a aplicação** do Assistente de Instalação, clique no botão **Remover**.

3. Siga as instruções do Assistente de Instalação.

Passo 1. Guardar dados da aplicação para utilização futura

Neste passo pode especificar quais os dados utilizados pela aplicação que pretende guardar para utilização futura, durante a próxima instalação da aplicação (por exemplo, ao instalar uma versão mais recente). Se não especificar quaisquer dados, a aplicação será totalmente removida.

Para guardar dados da aplicação para utilização futura,

selecione as caixas de verificação junto aos tipos de dados que pretende guardar:

- **Dados de ativação** - dados que eliminam a necessidade de ativar a aplicação que instalar no futuro. É ativada automaticamente com a licença atual, desde que a licença não tenha expirado na data da instalação.
- **Criar cópia de segurança e colocar ficheiros em quarentena** - ficheiros verificados pela aplicação e colocados na Cópia de Segurança ou Quarentena.

Os ficheiros de Cópia de segurança e Quarentena guardados após a remoção da aplicação podem ser acedidos apenas a partir da mesma versão da aplicação que foi usada para guardar esses ficheiros.

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

- **Configurações operacionais da aplicação** – valores das definições da aplicação selecionados durante a configuração da aplicação.
- **Armazenamento local das chaves de encriptação** – dados que fornecem acesso direto a ficheiros e dispositivos que foram encriptados antes da remoção da aplicação. É possível aceder diretamente a ficheiros e unidades encriptados depois de a aplicação ser reinstalada com a funcionalidade de encriptação.

  Esta caixa de verificação está selecionada por defeito.

Para prosseguir com o Assistente de Instalação, clique no botão **Seguinte**. Para parar o Assistente de Instalação, clique no botão **Cancelar**.

Passo 2. Confirmar a remoção da aplicação

Uma vez que a remoção da aplicação coloca em perigo a segurança do seu computador, é-lhe solicitado que confirme que pretende remover a aplicação. Para tal, clique no botão **Remover**.

Para parar a remoção da aplicação em qualquer altura, pode cancelar esta operação clicando no botão **Cancelar**.

Passo 3. Remover a aplicação. Concluir a remoção

Durante este passo, o Assistente de Instalação remove a aplicação do computador. Aguarde até a remoção da aplicação estar concluída.

Ao remover a aplicação, pode ser necessário reiniciar o sistema operativo. Se optar por não reiniciá-lo imediatamente, a conclusão da remoção da aplicação é adiada até que o sistema operativo seja reiniciado ou até que o computador seja desligado e novamente ligado.

Remover a aplicação a partir da linha de comandos

Pode iniciar o processo de desinstalação da aplicação a partir da linha de comandos. A desinstalação é executada no modo interativo ou não assistido (sem iniciar o Assistente de Instalação da Aplicação).

Para iniciar o processo de desinstalação da aplicação no modo interativo,

escreva na linha de comandos `setup.exe /x` ou `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

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

Para iniciar o processo de desinstalação da aplicação no modo não assistido,

escreva na linha de comandos `setup.exe /s /x` ou `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} /qn`.

Esta ação inicia o processo de desinstalação da aplicação no modo não assistido (sem iniciar o Assistente de Instalação).

Se a operação de desinstalação da aplicação estiver protegida por password, o nome de utilizador e a password correspondente têm de ser introduzidos na linha de comandos.

Para remover a aplicação a partir da linha de comandos no modo interativo quando o nome de utilizador e a password para autenticação da remoção, modificação ou reparação do Kaspersky Endpoint Security estão estabelecidos:

Na linha de comandos, escreva `setup.exe /pKLLOGIN=<Nome de utilizador> /pKLPASSWD=***** /x` ou

`msiexec.exe KLLOGIN=<User name> KLPASSWD=***** /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

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

Para remover a aplicação a partir da linha de comandos no modo não assistido quando o nome de utilizador e a password para autenticação da remoção, modificação ou reparação do Kaspersky Endpoint Security estão estabelecidos:

Na linha de comandos, escreva `setup.exe /pKLLOGIN=<User name> /pKLPASSWD=***** /s /x` ou

`msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} KLLOGIN=<User name> KLPASSWD=***** /qn`.

Remover objetos e dados restantes após a operação de teste 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 de duas formas:

- Utilizando a política do Kaspersky Security Center.
- Utilizando o Ferramenta de Restauro.

Para utilizar uma política do Kaspersky Security Center para remover os objetos e os dados restantes após a operação de teste do Agente de Autenticação:

1. Aplicar uma política do Kaspersky Security Center com as definições configuradas para desencriptar todas as unidades de disco rígido no computador.

2. Iniciar o Kaspersky Endpoint Security.

Para utilizar a Ferramenta de Restauro para remover os objetos e os dados restantes após a operação de teste do Agente de Autenticação:

1. Inicie a Ferramenta de Restauro ao executar o ficheiro executável fdert.exe criado com o Kaspersky Endpoint Security no computador com a unidade de disco rígido do sistema ligada na qual permanecem os objetos e os dados após a operação de teste do agente de autenticação.

2. Na lista suspensa **Selecionar dispositivo** na janela do Ferramenta de Restauro, selecione a unidade de disco rígido do sistema com os objetos e os dados a serem removidos.

3. Clique no botão **Verificar**.

4. Clique no botão **Eliminar artefactos do Agente de Autenticação**.

   Tal inicia o processo de remoção dos objetos e dos dados que restaram após a operação de teste do Agente de Autenticação.

Após remover os objetos e os dados que restaram depois da operação de teste do Agente de Autenticação, poderá ser também necessário remover adicionalmente a informação sobre a incompatibilidade da aplicação com o Agente de Autenticação.

Para remover a informação sobre a incompatibilidade da aplicação com o Agente de Autenticação,

introduza o comando `avp pbatestreset` na linha de comandos.

Os componentes de encriptação têm de estar instalados para que o comando `avp pbatestreset` seja executado.

Interface da aplicação

Esta secção descreve os elementos principais da interface da aplicação.

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.

Indicar a atividade da aplicação

O ícone da aplicação é um indicador da atividade da aplicação:

- O ícone significa que todos os componentes de proteção da aplicação estão ativados.
- O ícone significa que ocorreram eventos importantes que necessitam de atenção no funcionamento do Kaspersky Endpoint Security. Por exemplo, o Antivírus de Ficheiros está desativado ou as bases de dados da aplicação estão desatualizadas.
- O ícone significa que ocorreram eventos críticos no funcionamento do Kaspersky Endpoint Security. Por exemplo, uma falha no funcionamento de um componente ou a corrupção das bases de dados da aplicação.

Menu de contexto do ícone da aplicação

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

- **Kaspersky Endpoint Security 10 for Windows**. Abre o separador **Proteção e Controlo** na janela principal da aplicação. O separador **Proteção e Controlo** permite ajustar o funcionamento dos componentes e das tarefas da aplicação e ver as estatísticas dos ficheiros processados e das ameaças processadas.
- **Configuração**. Abre o separador **Configuração** na janela principal da aplicação. O separador **Configuração** permite alterar as definições da aplicação.
- **Pausar proteção e controlo**/**Retomar proteção e controlo**. Pausa/retoma temporariamente o funcionamento dos componentes de proteção e controlo. Este item do menu de contexto não afeta a tarefa de atualização nem as tarefas de verificação, ficando disponível apenas quando a política do Kaspersky Security Center está desativada.
- **Desativar política**/**Ativar política**. Desativa/ativa a política do Kaspersky Security Center. Este item de menu de contexto está disponível quando o Kaspersky Endpoint Security funciona com uma política e quando foi definida uma password para desativar a política do Kaspersky Security Center.
- **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 de contexto retira a aplicação da memória RAM do computador.

Menu de contexto do ícone da aplicação

Pode abrir o menu de contexto do ícone da aplicação colocando o ponteiro do rato sobre o ícone da aplicação na área de notificação da barra de tarefas do Microsoft Windows e clicando com o botão direito do rato.

Janela principal da aplicação

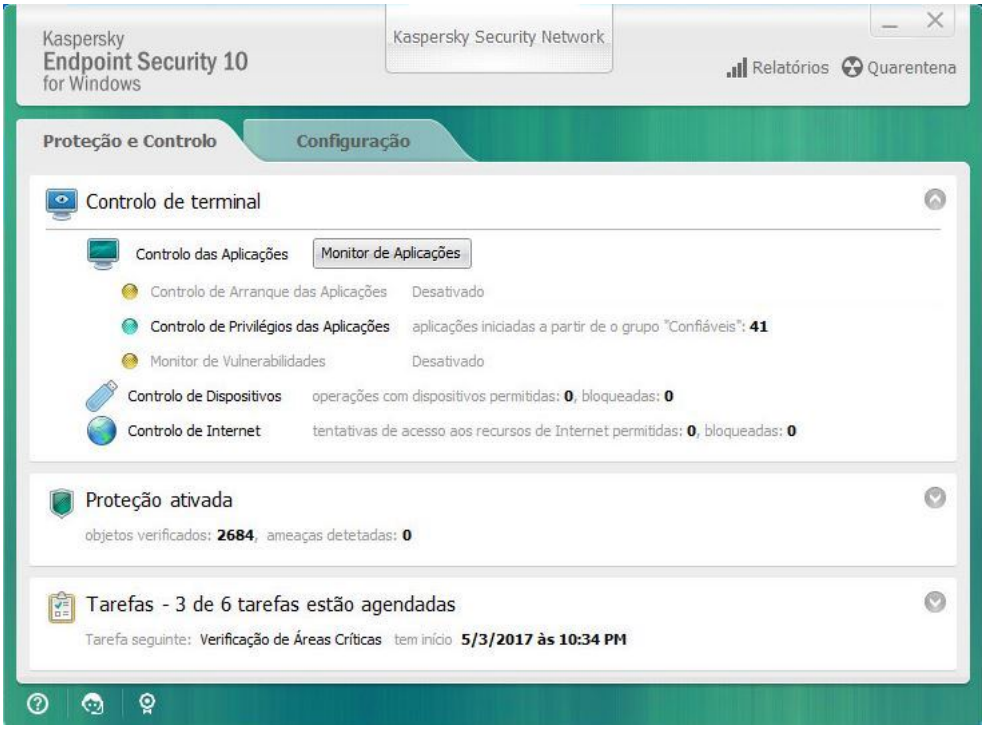
A janela principal do Kaspersky Endpoint Security contém elementos da interface que facultam acesso às funções principais da aplicação.

A janela principal de aplicações está dividida em quatro partes (consulte a imagem seguinte):

- Os elementos da interface estão situados na área superior da janela e permitem-lhe visualizar as informações seguintes:
  - Detalhes da aplicação
  - Estatísticas da Kaspersky Security Network
  - Lista de ficheiros não processados
  - Lista de vulnerabilidades detetadas
  - Lista de ficheiros em quarentena
  - Armazenamento das cópias dos ficheiros infetados apagados pela aplicação
  - Relatórios de eventos ocorridos durante o funcionamento geral da aplicação ou dos seus componentes individuais ou durante a realização de tarefas
- O separador **Proteção e Controlo** permite ajustar o funcionamento dos componentes e conclusão de tarefas. O separador **Proteção e Controlo** é apresentado ao abrir a janela principal da aplicação.
- O separador **Configuração** permite editar as configurações predefinidas da aplicação.
- A parte mais baixa da janela contém os seguintes elementos:
  - **Botão**. Ao clicar neste botão será direcionado para o sistema de ajuda do Kaspersky Endpoint Security.
  - **Botão**. Clicar neste botão abre a janela **Suporte**, que contém informações do sistema operativo, a versão atual do Kaspersky Endpoint Security, e ligações para os recursos de informação da Kaspersky.
  - **Botão**/. Clicar neste botão abre a janela **Licenciamento**, que contém informações sobre a licença atual.

- **Botão** / / Ao clicar neste botão, abre a janela **Eventos** que contém informações sobre as atualizações disponíveis, bem como pedidos de acesso a ficheiros e dispositivos encriptados.

  O botão só está disponível quando há pedidos para aceder ou atualizações desinstaladas.



Janela principal da aplicação

Para abrir a janela principal do Kaspersky Endpoint Security, execute uma das seguintes ações:

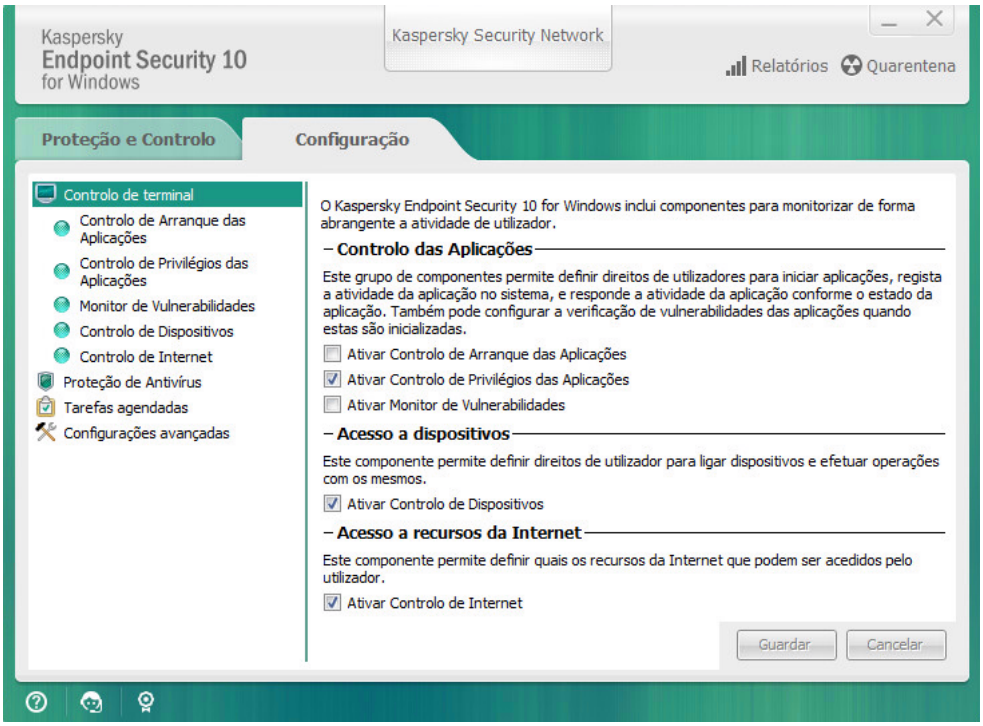
- Clicar no ícone de aplicação na área de notificação de barra de tarefas do Microsoft Windows.
- Selecione **Kaspersky Endpoint Security 10 for Windows** no menu de contexto do ícone da aplicação.

Separador Configurar Definições da Aplicação

O separador de configuração do Kaspersky Endpoint Security permite configurar as definições globais da aplicação, os componentes individuais, os relatórios e armazenamento, as tarefas de verificação, as tarefas de atualização, as tarefas de verificação de vulnerabilidade e a comunicação com os servidores da Kaspersky Security Network.

O separador de definições da aplicação é constituído por duas partes (consulte a imagem seguinte):

- A parte esquerda contém componentes da aplicação, tarefas e uma secção de configurações avançadas composta por várias subsecções.
- A parte direita contém elementos de controlo que pode utilizar para configurar as definições do componente ou da tarefa selecionada na parte esquerda da janela, bem como as configurações avançadas.



Separador Configurar Definições da Aplicação

Para abrir o separador de configurações da aplicações, execute uma das seguintes ações:

- Na janela principal da aplicação, selecione o separador **Configuração**.
- No menu de contexto do ícone da aplicação, selecione **Configuração**.

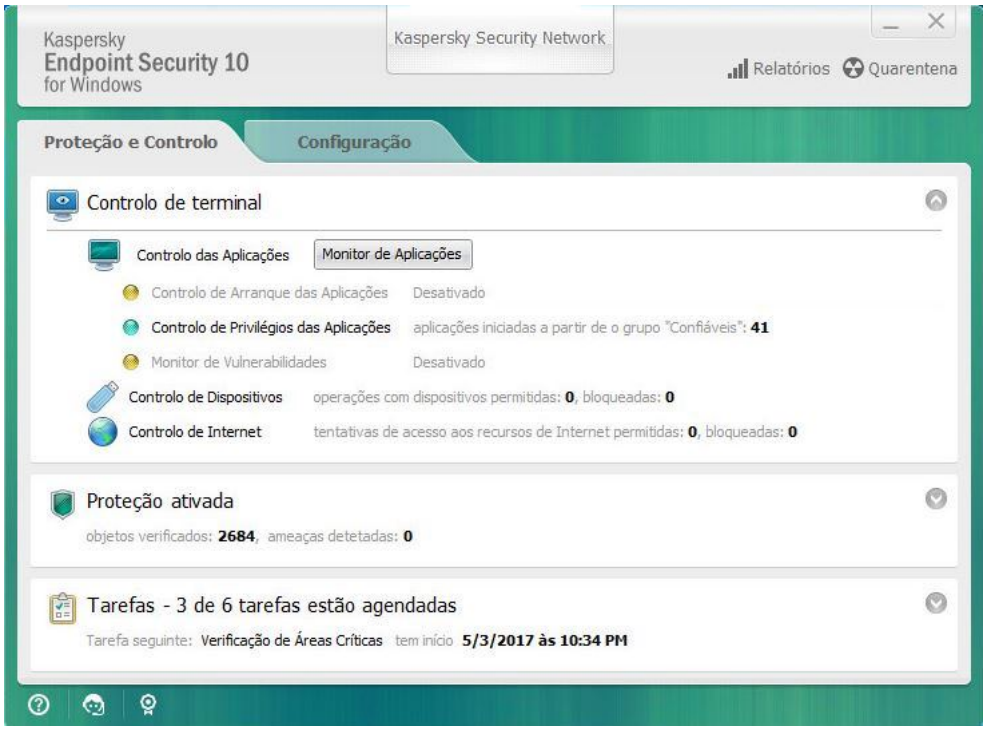
Separador Proteção e Controlo de Aplicações

O separador Proteção e Controlo de Aplicações do Kaspersky Endpoint Security destina-se a fornecer a informações gerais sobre o desempenho de todas as tarefas e a operação de todos os componentes da aplicação. Neste separador, também pode controlar o funcionamento de componentes e o desempenho das tarefas.

O separador Proteção e Controlo de Aplicações é composto por três partes (ver a imagem abaixo):

- A secção **Controlo de terminal** contém uma lista dos componentes de controlo.
- A **Gerir proteção** contém uma lista dos componentes de proteção de Antivírus.
- A secção **Tarefas** contém uma lista das tarefas locais que são executadas no computador.

Cada secção contém elementos de controlo que pode utilizar para ativar ou desativar o funcionamento de um componente, aceda às definições do componente ou tarefa selecionado e visualize as estatísticas de funcionamento do componente selecionado ou tarefa selecionado.



Separador Proteção e Controlo de Aplicações

Para abrir o separador Proteção e Controlo de Aplicações, execute uma das seguintes ações:

- Na janela de aplicação principal, selecione o separador **Proteção e Controlo**.
- Clicar no ícone de aplicação na área de notificação de barra de tarefas do Microsoft Windows.
- Selecione **Kaspersky Endpoint Security 10 for Windows** no menu de contexto do ícone da aplicação.

Licenciamento da aplicação

Esta secção fornece informações sobre conceitos gerais relativos às licenças da aplicação.

Sobre o 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 da aplicação.

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.

Uma licença válida confere ao utilizador o direito de utilização dos seguintes tipos de serviços:

- Uso da aplicação conforme os termos do Contrato de Licença do Utilizador Final
- Suporte Técnico

O âmbito dos serviços 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:

- Número de encomenda
- 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 (data de validade da subscrição, 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, é necessário renovar a subscrição. A subscrição ilimitada é renovada automaticamente se os serviços do fornecedor tiverem sido atempadamente pré-pagos.

No caso de uma subscrição limitada, ao expirar pode ter acesso a um período de tolerância para renovar a subscrição, durante o qual a aplicação mantém as suas funcionalidades. O fornecedor de serviços decide a atribuição ou não atribuição de um período de tolerância e determina também a duração do mesmo.

Para utilizar o Kaspersky Endpoint Security com subscrição, é necessário aplicar o código de ativação recebido do fornecedor de serviços. Após aplicar o código de ativação, a chave ativa é instalada. A chave ativa define a licença para utilizar a aplicação com subscrição. Pode ser instalada uma chave adicional utilizando apenas um código de ativação e não pode ser instalada utilizando um ficheiro-chave ou com subscrição.

A funcionalidade de aplicação disponível com subscrição pode corresponder à funcionalidade da aplicação para os seguintes tipos de licenças comerciais: Standard, Kaspersky Business Space Security, Kaspersky Enterprise Space Security. As licenças deste tipo são concebidas para proteger servidores de ficheiros, estações de trabalho e dispositivos móveis e suportam a utilização de componentes de controlo em estações de trabalho e dispositivos móveis.

As opções possíveis de gestão da subscrição podem variar conforme o fornecedor de serviços. O fornecedor de serviços pode não conceder um período de carência para renovar a subscrição, durante o qual a aplicação mantém as suas funcionalidades.

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

Sobre o código de ativação

Um *código de ativação* é uma sequência alfanumérica única de vinte letras latinas e algarismos que recebe ao comprar uma licença comercial 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 instalada. Pode ser instalada uma chave adicional utilizando apenas um código de ativação e não pode ser instalada utilizando um ficheiro-chave ou com subscrição.

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. Para restaurar um código de ativação, deve contactar com o Suporte técnico da Kaspersky.

Sobre a chave

A *chave* é uma sequência alfanumérica única. Uma chave permite utilizar a aplicação nos termos indicados no Certificado de Licença (tipo de licença, período de validade da licença, restrições da licença).

Um certificado de licença não é fornecido para uma chave instalada com subscrição.

É possível adicionar uma chave à aplicação utilizando um código de ativação ou um ficheiro-chave.

É possível adicionar, editar ou eliminar chaves. A chave pode ser bloqueada pela Kaspersky se os termos do Contrato de Licença do Utilizador Final forem violados. Se a chave tiver sido adicionada à lista negra, tem de adicionar uma chave diferente para continuar a utilizar a aplicação.

Se uma chave para uma licença expirada tiver sido apagada, a funcionalidade da aplicação não está disponível. Não pode adicionar tal chave novamente depois de ter sido eliminada.

Existem dois tipos de chave: ativo e adicional.

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 adicional* é uma chave que permite ao utilizador utilizar a aplicação, mas que não está atualmente a ser utilizada. Aquando da expiração da chave ativa, uma chave adicional torna-se automaticamente ativa. É apenas possível adicionar uma chave adicional 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 chave adicional. Uma chave de licença de avaliação não pode substituir a chave ativa para uma licença comercial.

Se a chave for adicionada à lista negra, as funcionalidades da aplicação definidas pela licença utilizada para ativar a aplicação permanecem disponíveis durante oito dias. O Kaspersky Security Network e as atualizações das bases de dados e dos módulos da aplicação permanecem disponíveis sem restrições. A aplicação notifica o utilizador que a chave que foi adicionada à lista negra. Após oito dias, as funcionalidades da aplicação ficam limitadas ao nível de funcionalidades disponível após a licença expirar; a aplicação funciona sem atualizações e o Kaspersky Security Network fica indisponível.

Sobre o ficheiro-chave

Um *ficheiro-chave* é um ficheiro com a extensão .key que recebe da Kaspersky depois de comprar o Kaspersky Endpoint Security. O objetivo de um ficheiro-chave é adicionar uma chave que ativa a aplicação.

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 fornecedor da licença.
- Obtenha um ficheiro-chave no site da Kaspersky com base no seu código de ativação existente.

Acerca da provisão de dados

Na aceitação do Contrato de Licença do Utilizador Final, aceita transferir automaticamente as informações sobre a sua utilização do produto, bem como o tipo, a versão e a localização linguística do programa instalado, o identificador único do instalador do programa e tipo da instalação, assim como os dados sobre chaves ativas e adicionais (incluindo o tipo de licença, período de validade, a data de ativação do programa e a data em que a licença expira, o número da licença, o estado atual da licença e a versão do protocolo de interação do servidor de ativação).

Caso o programa seja ativado com um código de ativação, para receber informações estatísticas sobre a distribuição e a utilização dos produtos do Detentor da Licença, aceita facultar automaticamente a versão do programa a ser utilizado (incluindo informações sobre atualizações do programa instaladas, o identificador de instalação do programa e informações sobre licenças), a versão do sistema operativo e os identificadores de componentes de programa ativos no momento em que as informações são facultadas.

A informação recebida está protegida pela Kaspersky conforme a lei e os requisitos, bem como as regulamentações aplicáveis da Kaspersky.

A Kaspersky utiliza a informação recebida de modo inteiramente anónimo e apenas sob a forma de dados estatísticos gerais. As estatísticas gerais são criadas automaticamente utilizando informações recolhidas originalmente e não contêm quaisquer dados pessoais ou outras informações confidenciais. A informação recolhida originalmente é destruída à medida que se vai acumulando (uma vez por ano). Os dados estatísticos gerais são armazenados indefinidamente.

Leia o Contrato de Licença do Utilizador Final e visite o site da Kaspersky para obter mais informações sobre a recolha, processamento, armazenamento e eliminação de informações sobre a utilização das aplicações, após aceitar o Contrato de Licença do Utilizador Final e concordar com a Declaração da KSN. Os ficheiros license.txt e ksn.txt contêm o Contrato de Licença do Utilizador Final e a Declaração da KSN e fazem parte do pacote de distribuição do programa.

Ver informação sobre a licença

Para ver informação sobre a licença:

1. Abra a janela principal da aplicação.
2. Clique no botão / na parte inferior da janela principal da aplicação.

   É aberta a janela **Licenciamento**. A informação sobre a licença é apresentada na secção localizada na parte superior da janela **Licenciamento**.

Adquirir 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 comprar uma licença:

1. Abra a janela principal da aplicação.
2. Clique no botão / na parte inferior da janela principal da aplicação.

   É aberta a janela **Licenciamento**.
3. Na secção **Licenciamento**, execute uma das seguintes ações:

   - 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 licença

Quando a licença estiver prestes expirar, pode renová-la. Assim, assegura que o seu computador permanece protegido após a licença atual expirar e até ativar a aplicação com uma nova licença.

Para renovar uma licença:

1. Receber um novo código de ativação da aplicação ou ficheiro-chave.
2. Adicionar uma chave adicional com o código de ativação ou o ficheiro-chave que recebeu.

   Como resultado, é adicionada uma chave adicional. Esta fica ativa até à licença expirar.

Poderá demorar algum tempo para que a chave seja atualizada de adicional para ativa devido à distribuição de carga entre os servidores de ativação da Kaspersky.

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 utilizar a aplicação com subscrição limitada, no dia em que a subscrição (ou o período de tolerância após o fim da subscrição durante o qual é possível a renovação da subscrição) expira, o Kaspersky Endpoint Security apresenta uma notificação e deixa de tentar a renovação automática da subscrição. 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.

Pode atualizar o estado da subscrição manualmente na janela **Licenciamento**. Tal poderá ser necessário se a subscrição tiver sido renovada após o fim do período de tolerância e a aplicação não tiver atualizado o estado da subscrição automaticamente.

Visitar o sítio da Web do fornecedor de serviços

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

1. Abra a janela principal da aplicação.
2. Clique no botão / na parte inferior da janela principal da aplicação.

   É aberta a janela **Licenciamento**.
3. Na janela **Licenciamento**, clique em **Contacte o seu fornecedor de subscrição**.

Sobre os métodos de ativação da aplicação

A *Ativação* é o processo de ativação de uma licença, que permite utilizar uma versão com todas as funcionalidades da aplicação até a licença expirar. O processo de ativação da aplicação implica a adição de uma chave.

Pode ativar a aplicação através de uma das seguintes formas:

- Ao instalar a aplicação, com a ajuda do Assistente de Configuração Inicial. É possível adicionar a chave ativa desta forma.
- Localmente a partir da interface da aplicação, utilizando o Assistente de Ativação pode adicionar tanto a chave ativa como a chave adicional deste modo.
- Remotamente com o software do Kaspersky Security Center criando e depois iniciando uma tarefa de inclusão da chave. É possível adicionar a chave ativa e a chave adicional desta forma.
- Remotamente, através da distribuição de chaves e códigos de ativação armazenados no armazenamento de chaves do Servidor de administração do Kaspersky Security Center para computadores cliente (consulte o *Manual do Administrador do Kaspersky Security Center* para obter detalhes). É possível adicionar a chave ativa e a chave adicional desta forma.

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

- Utilização da linha de comandos.

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

Utilizar o Assistente de Ativação para ativar a aplicação

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

1. Clique no botão / na parte inferior da janela principal da aplicação.

   É aberta a janela **Licenciamento**.

2. Na janela **Licenciamento**, clique no botão **Ativar a aplicação com uma nova licença**.

   Arranque do Assistente de Ativação da Aplicação.

3. Siga as instruções do Assistente de Ativação.

Para obter informações mais detalhadas sobre o procedimento de ativação de aplicações, consulte a secção do Assistente de Configuração Inicial.

Ativar a aplicação a partir da linha de comandos

Para ativar a aplicação a partir da linha de comandos,

introduza `avp.com license /add <activation code or key file> /password=<password>` na linha de comandos.

Iniciar e parar a aplicação

Esta secção descreve como pode configurar o arranque automático da aplicação, iniciar ou parar a aplicação manualmente e pausar e retomar os componentes de proteção e controlo.

Ativar e desativar o arranque automático da aplicação

Arranque automático significa que o Kaspersky Endpoint Security é iniciado imediatamente após o arranque do sistema operativo, sem intervenção do utilizador. Esta opção de arranque da aplicação está ativada por defeito.

Após a instalação, o Kaspersky Endpoint Security inicia automaticamente pela primeira vez. Subsequentemente a aplicação inicia automaticamente após o arranque do sistema operativo.

A transferência das bases de dados de antivírus do Kaspersky Endpoint Security depois de o sistema operativo iniciar podem 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 carregado não causa uma redução do nível de proteção do computador.

Para ativar ou desativar o arranque automático da aplicação:

1. Abra a janela de definições da aplicação.
2. Selecione a secção **Proteção de Antivírus** à esquerda.

   As definições da Proteção de Antivírus são apresentadas na parte direita da janela.
3. Execute uma das seguintes ações:
   - Se pretende ativar o arranque automático da aplicação, selecione a caixa de verificação **Iniciar o Kaspersky Endpoint Security 10 for Windows no arranque do computador**.
   - Se pretende desativar o arranque automático da aplicação, desmarque a caixa de verificação **Iniciar o Kaspersky Endpoint Security 10 for Windows no arranque do computador**.
4. Para guardar as alterações, clique no botão **Guardar**.

Iniciar e parar manualmente a aplicação

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.

O Kaspersky Endpoint Security tem de ser iniciado manualmente se tiver desativado anteriormente o arranque automático da aplicação.

Para iniciar a aplicação manualmente,

No menu **Iniciar**, selecione **Aplicações→ Kaspersky Endpoint Security 10 for Windows**.

Para parar a aplicação manualmente:

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 **Sair**.

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 desativadas.

Pausar ou retomar a proteção e controlo do computador não afeta as tarefas de verificação ou atualização.

Se já estiverem estabelecidas ligações de rede no momento em que a proteção e controlo do computador são colocadas em pausa ou retomadas, é apresentada uma notificação relativa à interrupção destas ligações de rede.

Para pausar a proteção e controlo do computador:

1. Clique com o botão direito do rato para visualizar o menu de contexto do ícone da aplicação na área de notificação da barra de tarefas.
2. No menu de contexto, selecione **Pausar proteção e controlo**.

   É aberta a janela **Pausar proteção**.
3. Selecione uma das seguintes opções:

   - **Pausar durante o tempo especificado** - A proteção e controlo do computador são retomados após o período de tempo especificado na lista pendente abaixo.
   - **Pausar até reiniciar**- A proteção e controlo do computador são retomadas depois de sair da aplicação e reabri-la 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 são retomadas quando decidir reativá-las.
4. Se selecionou a opção **Pausar durante o tempo especificado** durante o passo anterior, selecione o intervalo necessário na lista pendente.

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 e controlo**.

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.

Proteger o sistema de ficheiros do computador. Antivírus de Ficheiros

Esta secção contém informações sobre o Antivírus de Ficheiros e instruções sobre como configurar as definições do componente.

Sobre o Antivírus de Ficheiros

O Antivírus de Ficheiros previne a infeção do sistema de ficheiros do computador. Por defeito, o Antivírus de Ficheiros é iniciado juntamente com o Kaspersky Endpoint Security, permanecendo ativo na memória do computador e verificando a existência de vírus e de outras ameaças em todos os ficheiros abertos, guardados ou iniciados no computador e em todas as unidades a ele ligadas.

Ao detetar uma ameaça num ficheiro, o Kaspersky Endpoint Security efetua o seguinte:

1. Deteta o tipo de objeto detetado no ficheiro (tal como um *vírus* ou *programa Trojan*).
2. Identifica o ficheiro como *provavelmente infetado* se a verificação não determinar se o ficheiro está ou não infetado. O ficheiro pode conter uma sequência de código comum em vírus ou outro software malicioso ou código modificado de um vírus conhecido.
3. A aplicação apresenta uma notificação sobre um objeto malicioso detetado no ficheiro (se as notificações estiverem configuradas) e processa o ficheiro através da ação especificada nas definições de Antivírus de Ficheiros.

Ativar e desativar o Antivírus de Ficheiros

Por defeito, o Antivírus de Ficheiros está ativado, em execução no modo recomendado pelos peritos da Kaspersky. Pode desativar o Antivírus de Ficheiros, se necessário.

Existem duas formas para ativar ou desativar o componente:

- No separador **Proteção e Controlo** na janela principal da aplicação
- Na janela de definições da aplicação

Para ativar ou desativar o Antivírus de Ficheiros no separador Proteção e Controlo da janela principal da aplicação:

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Proteção**.

   É aberta a secção **Proteção**.
4. Clique com o botão direito do rato para visualizar o menu de contexto da linha que contém as informações sobre o componente Antivírus de Ficheiros.

   É aberto um menu para selecionar ações no componente.
5. Execute uma das seguintes ações:

- Para ativar o Antivírus de Ficheiros, selecione **Iniciar** no menu.

  O ícone de estado do componente , que é apresentado à esquerda na linha do **Antivírus de Ficheiros**, é alterado para o ícone .

- Para desativar o Antivírus de Ficheiros, selecione **Parar** no menu.

  O ícone de estado do componente , que é apresentado à esquerda na linha do **Antivírus de Ficheiros**, é alterado para o ícone .

Para ativar ou desativar o Antivírus de Ficheiros a partir da janela de definições da aplicação:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de Ficheiros**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de Ficheiros.
3. Execute uma das seguintes ações:

   - Se pretender ativar o Antivírus de Ficheiros, selecione a caixa de verificação **Ativar Antivírus de Ficheiros**.
   - Se pretender desativar o Antivírus de Ficheiros, desmarque a caixa de verificação **Ativar Antivírus de Ficheiros**.
4. Para guardar as alterações, clique no botão **Guardar**.

Pausar automaticamente o Antivírus de Ficheiros

Pode configurar o Antivírus de Ficheiros para pausar automaticamente a uma hora especificada ou ao processar programas específicos.

Pausar o Antivírus de Ficheiros em caso de conflito com determinados programas é uma medida de emergência. Em caso de conflitos durante o funcionamento de um componente, é recomendado contactar o Suporte Técnico da Kaspersky (https://companyaccount.kaspersky.com). Os especialistas de suporte irão ajudá-lo a configurar o Antivírus de Ficheiros para executar em simultâneo com outros programas no computador.

Para configurar a pausa automática do Antivírus de Ficheiros:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de Ficheiros**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de Ficheiros.
3. Na secção **Nível de segurança**, clique no botão **Configuração**.

   É aberta a janela **Antivírus de Ficheiros**.
4. Na janela **Antivírus de Ficheiros**, selecione o separador **Adicional**.
5. Na secção **Pausar a tarefa**:

   - Para configurar a pausa automática do Antivírus de Ficheiros a uma hora especificada, selecione a caixa de verificação **Planificadas** e clique no botão **Agendamento**.

É aberta a janela **Pausar a tarefa**.

- Para configurar a pausa automática do Antivírus de Ficheiros no arranque das aplicações especificadas, selecione a caixa de verificação **Com a inicialização da aplicação** e clique no botão **Selecionar**.

  É aberta a janela **Aplicações**.

6. Execute uma das seguintes ações:

   - Se estiver a configurar a pausa automática do Antivírus de Ficheiros numa hora especificada, na janela **Pausar a tarefa**, utilize os campos **Pausar tarefa às** e **Continuar tarefa às** para especificar o período (no formato HH:MM) durante o qual o Antivírus de Ficheiros deve estar em pausa. Clique em **OK**.

   - Se estiver a configurar a pausa automática do Antivírus de Ficheiros no arranque das aplicações especificadas, utilize os botões **Adicionar**, **Editar** e **Remover** na janela **Aplicações** para criar uma lista de aplicações durante o funcionamento das quais o Antivírus de Ficheiros é colocado em pausa. Clique em **OK**.

7. Na janela **Antivírus de Ficheiros**, clique **OK**.

8. Para guardar as alterações, clique no botão **Guardar**.

Configurar o Antivírus de Ficheiros

Pode efetuar as seguintes operações para configurar o Antivírus de Ficheiros:

- Alterar o nível de segurança.

  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.

- Alterar a ação executada pelo Antivírus de Ficheiros ao detetar um ficheiro infetado.

- Editar o âmbito de proteção do Antivírus de Ficheiros.

  Pode alargar ou restringir o âmbito de proteção, adicionando ou removendo objetos de verificação ou alterando o tipo de ficheiros a verificar.

- Configurar o Analisador heurístico.

  O Antivírus de Ficheiros utiliza uma técnica denominada análise de assinaturas. Durante a análise de assinaturas, o Antivírus de Ficheiros procura correspondências do objeto detetado com registos nas suas bases de dados de antivírus da aplicação. De acordo com as recomendações dos especialistas da Kaspersky, a análise de assinaturas está sempre ativada.

  Para aumentar a eficácia da proteção, pode utilizar a análise heurística. Durante a análise heurística, o Antivírus de Ficheiros analisa a atividade de objetos no sistema operativo. A análise heurística permite a deteção de objetos maliciosos para os quais não existem registos disponíveis nas bases de dados de antivírus da aplicação.

- Otimizar a verificação.

  Pode otimizar a verificação de ficheiros realizada pelo Antivírus 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 última verificação anterior.

- Configurar a verificação de ficheiros compostos.
- Alterar o modo de verificação de ficheiros.

Alterar o nível de segurança

Para proteger o sistema de ficheiros do computador, o Antivírus de Ficheiros aplica vários grupos de configurações. Estes grupos de definições são denominados *níveis de segurança*. Existem três níveis de segurança predefinidos: **Elevado**, **Recomendado** e **Baixo**. Considera-se que as definições de nível de segurança **Recomendadas** são as definições ideais recomendadas pelos especialistas da Kaspersky.

Para alterar um nível de segurança:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de Ficheiros**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de Ficheiros.
3. Na secção **Nível de segurança**, execute uma das seguintes ações:
   - Se quiser definir um dos níveis de segurança predefinidos (**Elevado**, **Recomendado** ou **Baixo**), selecione-o com o controlo de deslize.
   - Se pretender configurar um nível de segurança personalizado, clique no botão **Configuração** e introduza as definições personalizadas na janela **Antivírus de Ficheiros** apresentada.

     Depois de configurar um nível de segurança personalizado, o nome do nível de segurança de e-mail na secção **Nível de segurança** é alterado para **Configurações Personalizadas**.
   - Se pretender alterar o nível de segurança para **Recomendado**, clique no botão **Predefinições**.
4. Para guardar as alterações, clique no botão **Guardar**.

Alterar a ação que Antivírus de Ficheiros aplica a ficheiros infetados

Para alterar a ação que Antivírus de Ficheiros aplica a ficheiros infetados:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de Ficheiros**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de Ficheiros.
3. Na secção **Ação após deteção de ameaças**, selecione a opção desejada:
   - **Selecionar ação automaticamente**.
   - **Realização ação: Desinfetar. Eliminar se a desinfeção falhar**.
   - **Realização ação: Desinfetar**.

Mesmo que esta opção esteja selecionada, o Kaspersky Endpoint Security aplica a ação **Remover** aos ficheiros que pertencem à aplicação Windows Store.

- **Realização ação: Remover**.
- **Realização ação: Bloquear.**

4. Para guardar as alterações, clique no botão **Guardar**.

Editar o âmbito de proteção do Antivírus 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 serem verificados são propriedades do âmbito de proteção do Antivírus de Ficheiros. Por defeito, o Antivírus de Ficheiros verifica apenas ficheiros infetáveis armazenados em discos rígidos, unidades de rede ou discos amovíveis.

Para criar o âmbito de proteção:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de Ficheiros**.
   Na parte direita da janela, são apresentadas as definições do componente Antivírus de Ficheiros.
3. Na secção **Nível de segurança**, clique no botão **Configuração**.
   É aberta a janela **Antivírus de Ficheiros**.
4. Na janela **Antivírus de Ficheiros**, selecione o separador **Geral**.
5. Na secção **Tipos de ficheiros**, especifique o tipo de ficheiros que pretende que o Antivírus de Ficheiros verifique:
   - Se pretender verificar todos os ficheiros, selecione **Todos os ficheiros**.
   - Se pretender verificar os ficheiros com os formatos mais vulneráveis a infeção, selecione **Ficheiros verificados por formato**.
   - Se pretender verificar os ficheiros com as extensões mais vulneráveis a infeção, selecione **Ficheiros verificados por extensão**.

   Ao selecionar o tipo de ficheiros as verificar, tenha em atenção as informações seguintes:

   - Existem alguns formatos de ficheiro (tais como .txt) nos quais a probabilidade de intrusão de código malicioso e subsequente ativação é bastante baixa. Por outro lado, existem formatos de ficheiro que contêm ou podem conter código executável (tais como .exe, .dll e .doc). O risco de intrusão e ativação de código malicioso nesses ficheiros é bastante elevado.
   - Um intruso pode enviar um vírus ou outro programa malicioso para o computador num ficheiro executável cujo nome tenha sido mudado para a extensão .txt. Se selecionar a verificação de ficheiros por extensão, a verificação ignoraria tal ficheiro. Se selecionar a verificação de ficheiros por formato, o Antivírus de Ficheiros analisa o cabeçalho do ficheiro, independentemente da extensão. Esta análise poderá revelar que o

ficheiro está no formato .exe. Esse ficheiro seria minuciosamente verificado quanto à existência de vírus e de outro software malicioso.

6. Na lista **Âmbito de proteção**, execute uma das seguintes ações:

   - Se pretender adicionar um novo objeto ao âmbito de verificação, clique no botão **Adicionar**.
   - Se pretender alterar a localização de um objeto, selecione o objeto no âmbito de verificação e clique no botão **Editar**.

   É apresentada a janela **Selecionar âmbito de verificação**.

   - Se pretender remover um objeto da lista de objetos a verificar, selecione um objeto na lista de objetos a verificar e clique no botão **Remover**.

     É aberta uma janela para confirmar a eliminação.

7. Execute uma das seguintes ações:

   - Se pretender adicionar um novo objeto ou alterar a localização de um objeto na lista de objetos a verificar, selecione o objeto na janela **Selecionar âmbito de verificação** e clique no botão **Adicionar**.

     Todos os objetos selecionados na janela **Selecionar âmbito verificação** são apresentados na janela **Antivírus de Ficheiros**, na lista **Âmbito de proteção**.

     Clique em **OK**.

   - Se pretender remover um objeto, clique no botão **Sim** da janela para confirmar a remoção.

8. Se necessário, repita os passos 6-7 para adicionar, mover ou remover objetos da lista de objetos a verificar.

9. Para excluir um objeto da lista de objetos a verificar, desmarque a caixa de verificação junto ao objeto na lista **Âmbito de proteção**. Contudo, o objeto permanece na lista de objetos a verificar, embora tenha sido excluído da verificação pelo Antivírus de Ficheiros.

10. Na janela **Antivírus de Ficheiros**, clique **OK**.

11. Para guardar as alterações, clique no botão **Guardar**.

Utilizar o Analisador Heurístico com o Antivírus de Ficheiros

Para configurar a utilização do Analisador heurístico no funcionamento do Antivírus de Ficheiros:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de Ficheiros**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de Ficheiros.

3. Na secção **Nível de segurança**, clique no botão **Configuração**.

   É aberta a janela **Antivírus de Ficheiros**.

4. Na janela **Antivírus de Ficheiros**, selecione o separador **Desempenho**.

5. Na secção **Métodos de verificação**:

- Se pretender que o Antivírus de Ficheiros utilize análise heurística, selecione a caixa de verificação **Análise heurística** e utilize a barra indicadora para definir o nível da análise heurística: **Nível superficial**, **Nível médio**, ou **Nível aprofundado**.
- Se não pretender que o Antivírus de Ficheiros utilize a análise heurística, desmarque a caixa de verificação **Análise heurística**.

6. Clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

Utilizar tecnologias de verificação no funcionamento do Antivírus de Ficheiros

Para configurar a utilização das tecnologias de verificação no funcionamento do Antivírus de Ficheiros:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de Ficheiros**.
   Na parte direita da janela, são apresentadas as definições do componente Antivírus de Ficheiros.
3. Na secção **Nível de segurança**, clique no botão **Configuração**.
   É aberta a janela **Antivírus de Ficheiros**.
4. Na janela **Antivírus de Ficheiros**, selecione o separador **Adicional**.
5. Na secção **Tecnologias de verificação**:
   - Selecione as caixas de verificação junto aos nomes das tecnologias que pretende utilizar com o Antivírus de Ficheiros.
   - Desmarque as caixas de verificação junto aos nomes das tecnologias que não pretende utilizar com o Antivírus de Ficheiros.
6. Clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

Otimizar a verificação de ficheiros

Para otimizar a verificação de ficheiros:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de Ficheiros**.
   Na parte direita da janela, são apresentadas as definições do componente Antivírus de Ficheiros.
3. Clique no botão **Configuração**.

É aberta a janela **Antivírus de Ficheiros**.

4. Na janela **Antivírus de Ficheiros**, selecione o separador **Desempenho**.
5. Na secção **Otimização da verificação**, selecione a caixa de verificação **Verificar apenas os ficheiros novos e modificados**.
6. Clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

Verificação de ficheiros compostos

Uma técnica comum para ocultar vírus e outro software malicioso consiste em integrar os mesmos em ficheiros compostos como, por exemplo, arquivos ou bases de dados de e-mail. 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 conjunto de ficheiros compostos a verificar, aumentando assim a velocidade da verificação.

O método utilizado para processar um ficheiro composto infetado (desinfeção ou eliminação) depende do tipo do ficheiro.

O Antivírus de Ficheiros desinfeta os ficheiros compostos nos formatos RAR, ARJ, ZIP, CAB e LHA e elimina os ficheiros em todos outros formatos (exceto bases de dados de correio).

Para configurar a verificação de ficheiros compostos:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de Ficheiros**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de Ficheiros.
3. Na secção **Nível de segurança**, clique no botão **Configuração**.

   É aberta a janela **Antivírus de Ficheiros**.
4. Na janela **Antivírus de Ficheiros**, selecione o separador **Desempenho**.
5. Na secção **Verificação de ficheiros compostos**, especifique os tipos de ficheiros compostos que pretende verificar: arquivos, pacotes de instalação ou ficheiros em formatos do office.
6. Para verificar apenas ficheiros compostos novos e modificados, selecione a caixa de verificação **Verificar apenas os ficheiros novos e modificados**.

   O Antivírus de Ficheiros irá verificar apenas os ficheiros compostos novos e modificados de todos os tipos.
7. Clique no botão **Adicional**.

   É aberta a janela **Ficheiros compostos**.
8. Na secção **Verificação em 2.º plano**, execute uma das seguintes ações:

- Se não pretender que o Antivírus de Ficheiros descompacte os ficheiros compostos no modo de segundo plano, desmarque a caixa de verificação **Descompactar ficheiros compostos em 2.° plano**.

- Se pretender que o Antivírus de Ficheiros descompacte ficheiros compostos em segundo plano, selecione a caixa de verificação **Descompactar ficheiros compostos em 2.° plano** e especifique o valor pretendido no campo **Tamanho mínimo dos ficheiros**.

9. Na secção **Limite de tamanho**, execute uma das seguintes ações:

   - Se não pretender que o Antivírus de Ficheiros descompacte ficheiros compostos de grandes dimensões, selecione a caixa de verificação **Não descompactar ficheiros compostos extensos** e especifique o valor desejado no campo **Tamanho máximo dos ficheiros**. O Antivírus de Ficheiros não descompacta ficheiros compostos com dimensões superiores ao tamanho especificado.

   - Se pretender que o Antivírus de Ficheiros descompacte ficheiros compostos de grandes dimensões, desmarque a caixa de verificação **Não descompactar ficheiros compostos extensos**.

     Um ficheiro é considerado extenso se o respetivo tamanho exceder o valor especificado no campo **Tamanho máximo dos ficheiros**.

   O Antivírus de Ficheiros verifica ficheiros de grandes dimensões extraídos de arquivos, independentemente de a caixa de verificação **Não descompactar ficheiros compostos extensos** estar ou não selecionada.

10. Clique em **OK**.

11. Na janela **Antivírus de Ficheiros**, clique **OK**.

12. Para guardar as alterações, clique no botão **Guardar**.

Alterar o modo de verificação

Modo de verificação significa a forma que o Antivírus de Ficheiros utiliza para iniciar a verificação dos ficheiros. Por defeito, o Kaspersky Endpoint Security verifica os ficheiros no modo inteligente. Neste modo de verificação de ficheiros, o Antivírus de Ficheiros irá ou não verificar os ficheiros após analisar as operações efetuadas 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. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de Ficheiros**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de Ficheiros.

3. Na secção **Nível de segurança**, clique no botão **Configuração**.

   É aberta a janela **Antivírus de Ficheiros**.

4. Na janela **Antivírus de Ficheiros**, selecione o separador **Adicional**.

5. Na secção **Modo de verificação**, selecione o modo pretendido:

- **Modo inteligente**.
- **No momento de acesso e alteração**.
- **No momento de acesso**.
- **No momento de execução**.

6. Clique em **OK**.

7. Para guardar as alterações, clique no botão **Guardar**.

Proteção de e-mail. Antivírus de E-mail

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para estações de trabalho. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para servidores de ficheiros.

Esta secção contém informações sobre o Antivírus de E-mail e instruções sobre como configurar as definições do componente.

Sobre o Antivírus de E-mail

O Antivírus de E-mail verifica a existência de vírus e outras ameaças nas mensagens de e-mail recebidas e enviadas. É iniciado juntamente com o Kaspersky Endpoint Security, permanece ativo na memória do computador e verifica todas as mensagens enviadas ou recebidas através dos protocolos POP3, SMTP, IMAP, MAPI e NNTP. Se não for detetada nenhuma ameaça na mensagem, esta ficará disponível e/ou será processada.

Ao detetar uma ameaça numa mensagem de e-mail, o Antivírus de E-mail efetua o seguinte:

1. Identifica o tipo de objeto detetado na mensagem de e-mail (tal como um *programa trojan*).
2. A uma mensagem de e-mail é atribuído um dos seguintes estados:
   - *Provavelmente infetado*. Este estado é atribuído caso a verificação não consiga determinar se a mensagem de e-mail está ou não infetada definitivamente. A mensagem de e-mail pode conter uma secção de código comum em vírus ou outro software malicioso ou código modificado de um vírus conhecido.
   - *Infetado*. Este estado é atribuído a um objeto caso a verificação de uma mensagem de e-mail encontre uma secção de código de um vírus conhecido que esteja incluída nas bases de dados de antivírus do Kaspersky Endpoint Security.
   - *Não encontrado*. Este estado é atribuído a um objeto se a verificação de uma mensagem de e-mail não detetar vírus ou outras ameaças.

A aplicação bloqueia a mensagem de e-mail, apresenta uma notificação relativa ao objeto detetado (se isto estiver especificado nas definições de notificação) e executa a ação que está especificada nas definições do Antivírus de E-mail.

Este componente interage com os clientes de e-mail instalados no computador. Está disponível uma extensão integrada para o cliente de e-mail Microsoft Office Outlook®, que lhe permite possibilita ajustar as definições de verificação de mensagens. A extensão do Antivírus de E-mail é incorporada no cliente de correio do Microsoft Office Outlook durante a instalação do Kaspersky Endpoint Security.

O funcionamento do Antivírus de E-mail é assinalado pelo ícone da aplicação apresentado na área de notificações da barra de ferramentas. Quando o Antivírus de e-mail está a verificar uma mensagem de e-mail, o ícone da aplicação muda para .

Ativar e desativar o Antivírus de E-mail

Por defeito, o Antivírus de E-mail está ativado, em execução no modo recomendado pelos peritos da Kaspersky. Pode desativar o Antivírus de E-mail, se necessário.

Existem duas formas para ativar ou desativar o componente:

- No separador **Proteção e Controlo** na janela principal da aplicação
- Na janela de definições da aplicação

Para ativar ou desativar o Antivírus de E-mail no separador Proteção e Controlo da janela principal da aplicação:

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Proteção**.
   É aberta a secção **Proteção**.
4. Clique com o botão direito do rato para visualizar o menu de contexto da linha que contém as informações sobre o componente Antivírus de E-mail.
   É aberto um menu para selecionar ações no componente.
5. Execute uma das seguintes ações:
   - Para ativar o Antivírus de E-mail, selecione **Iniciar** no menu.
     O ícone de estado do componente , que é apresentado à esquerda na linha do **Antivírus de E-mail**, é alterado para o ícone .
   - Para desativar o Antivírus de E-mail, selecione **Parar** no menu.
     O ícone de estado do componente , que é apresentado à esquerda na linha do **Antivírus de E-mail**, é alterado para o ícone .

Para ativar ou desativar o Antivírus de E-mail a partir da janela de definições da aplicação:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de E-mail**.
   Na parte direita da janela, são apresentadas as definições do componente Antivírus de E-mail.
3. Execute uma das seguintes ações:
   - Se pretender ativar o Antivírus de E-mail, selecione a caixa de verificação **Ativar Antivírus de E-mail**.
   - Se pretender desativar o Antivírus de E-mail, desmarque a caixa de verificação **Ativar Antivírus de E-mail**.
4. Para guardar as alterações, clique no botão **Guardar**.

Configurar o Antivírus de E-mail

Pode efetuar as seguintes operações para configurar o Antivírus de E-mail:

- Alterar o nível de segurança de e-mail.
  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.

- Alterar a ação que o Kaspersky Endpoint Security executa nas mensagens infetadas.
- Editar o âmbito de proteção do Antivírus de E-mail.
- Configurar a verificação de ficheiros compostos anexados às 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.
- Configurar a filtragem por tipo de anexos das mensagens de e-mail.

  A filtragem dos anexos de mensagens por tipo possibilita a mudança de nome automática ou a eliminação de ficheiros de tipos especificados.
- Configurar o Analisador heurístico.

  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 ameaças nas mensagens para as quais não existem atualmente registos nas bases de dados do Kaspersky Endpoint Security.
- Configurar a verificação de e-mails no Microsoft Office Outlook.

  Está disponível uma extensão integrada para o cliente de e-mail Microsoft Office Outlook, que possibilita a configuração conveniente das definições de verificação de e-mail.

  Ao trabalhar com outros clientes de e-mail, incluindo o Microsoft Outlook Express®, o Windows Mail, e o Mozilla™ Thunderbird™, o componente Antivírus de E-mail verifica o tráfego dos protocolos de correio SMTP, POP3, IMAP e NNTP.

  Ao trabalhar com o cliente de correio Mozilla Thunderbird, o Antivírus de E-mail não verifica a existência de vírus e outras ameaças nas mensagens transmitidas através do protocolo IMAP, se forem usados filtros para mover as mensagens da pasta **Caixa de entrada**.

Alterar o nível de segurança de e-mail

O Antivírus de E-mail aplica vários grupos de configurações para proteger o e-mail. Os grupos de definições são denominados *níveis de segurança de e-mail*. Existem três níveis de segurança de e-mail: **Elevado**, **Recomendado** e **Baixo**. O nível de segurança de ficheiros **Recomendado** é considerado a configuração ideal e é recomendado pela Kaspersky.

Para alterar o nível de segurança de e-mail:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de E-mail**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de E-mail.
3. Na secção **Nível de segurança**, execute uma das seguintes ações:

   - Se pretender instalar um dos níveis de segurança de e-mail pré-instalados (**Elevado**, **Recomendado** ou **Baixo**), utilize a barra indicadora para selecionar um.

- Se pretender configurar um nível de segurança de e-mail personalizado, clique no botão **Configuração** e especifique as configurações na janela **Antivírus de E-mail**.

  Depois de configurar um nível de segurança de e-mail personalizado, o nome do nível de segurança de e-mail na secção **Nível de segurança** é alterado para **Configurações Personalizadas**.

- Se pretender alterar o nível de segurança de e-mail para **Recomendado**, clique no botão **Predefinições**.

4. Para guardar as alterações, clique no botão **Guardar**.

Alterar a ação a executar em mensagens de e-mail infetadas

Para alterar a ação a executar em mensagens de e-mail infetadas:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de E-mail**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de E-mail.
3. Na secção **Ação após deteção de ameaças**, selecione a ação a executar pelo Kaspersky Endpoint Security quando é detetada uma mensagem infetada:
   - **Selecionar ação automaticamente**.
   - **Realização ação: Desinfetar. Eliminar se a desinfeção falhar**.
   - **Realização ação: Desinfetar**.
   - **Realização ação: Remover**.
   - **Realização ação: Bloquear.**
4. Para guardar as alterações, clique no botão **Guardar**.

Editar o âmbito de proteção do Antivírus de E-mail

O âmbito de 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 Antivírus de E-mail incluem as definições da integração do Antivírus de E-mail nos clientes de correio e o tipo de mensagens de e-mail e os protocolos de e-mail cujo tráfego é verificado pelo Antivírus de E-mail. Por defeito, 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 criar o âmbito de proteção do Antivírus de E-mail:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de E-mail**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de E-mail.

3. Clique no botão **Configuração**.

   É aberta a janela **Antivírus de E-mail**.

4. Selecione o separador **Geral**.

5. Na secção **Âmbito de proteção**, execute uma das seguintes ações:

   - Se pretender que o Antivírus de E-mail verifique todas as mensagens de entrada e de saída do computador, selecione a opção **Mensagens de entrada e de saída**.
   - Se pretender que o Antivírus de E-mail verifique apenas as mensagens de entrada do computador, selecione a opção **Apenas mensagens de entrada**.

     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.

6. Na secção **Conetividade**, execute as seguintes ações:

   - Se pretender que o Antivírus de E-mail verifique as mensagens transmitidas através dos protocolos POP3, SMTP, NNTP e IMAP antes de estas chegarem ao computador, selecione a caixa de verificação **Tráfego de POP3 / SMTP / NNTP / IMAP**.

     Se não pretender que o Antivírus de E-mail verifique as mensagens transmitidas através dos protocolos POP3, SMTP, NNTP e IMAP antes de estas chegarem ao computador, desmarque a caixa de verificação **Tráfego de POP3 / SMTP / NNTP / IMAP**. Neste caso, as mensagens são verificadas pela extensão de Antivírus de E-mail integrada no cliente de correio do Microsoft Office Outlook depois de serem todas recebidas no computador do utilizador se a caixa de verificação **Adicional: extensão do Microsoft Office Outlook** estiver selecionada.

     Se utilizar um cliente de correio que não o Microsoft Office Outlook, as mensagens transmitidas através dos protocolos POP3, SMTP, NNTP e IMAP não são verificadas pelo Antivírus de E-mail quando a caixa de verificação **Tráfego de POP3 / SMTP / NNTP / IMAP** está desmarcada.

   - Se pretender aceder às definições de Antivírus de E-mail a partir do Microsoft Office Outlook e ativar a verificação das mensagens transmitidas através dos protocolos POP3, SMTP, NNTP, IMAP, e MAPI depois de estes chegarem ao computador através da extensão incorporada no Microsoft Office Outlook, selecione a caixa de verificação **Adicional: extensão do Microsoft Office Outlook**.

     Se pretender aceder às definições de Antivírus de E-mail a partir do Microsoft Office Outlook e desativar a verificação das mensagens transmitidas através dos protocolos POP3, SMTP, NNTP, IMAP, e MAPI depois de estes chegarem ao computador através da extensão incorporada no Microsoft Office Outlook, desmarque a caixa de verificação **Adicional: extensão do Microsoft Office Outlook**.

     A extensão do Antivírus de E-mail é incorporada no cliente de correio do Microsoft Office Outlook durante a instalação do Kaspersky Endpoint Security.

7. Clique em **OK**.

8. Para guardar as alterações, clique no botão **Guardar**.

Verificação de ficheiros compostos anexados a mensagens de e-mail

Para configurar a verificação de ficheiros compostos anexados às mensagens de e-mail:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de E-mail**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de E-mail.
3. Clique no botão **Configuração**.

   É aberta a janela **Antivírus de E-mail**.
4. Selecione o separador **Geral**.
5. Execute o seguinte na secção **Verificação de ficheiros compostos**:

   - Se pretender que o Antivírus de E-mail ignore os arquivos anexos às mensagens, desmarque a caixa de verificação **Verificar arquivos anexados**.
   - Se pretender que o Antivírus de E-mail ignore os anexos de mensagens maiores do que N megabytes, selecione a caixa de verificação **Não verificar arquivos com tamanho superior a N MB**. Se selecionar esta caixa de verificação, especifique o tamanho máximo do arquivo no campo junto ao nome da caixa de verificação.
   - Se pretender que o Antivírus de E-mail verifique os anexos de mensagem que demoram mais de N segundos a verificar, desmarque a caixa de verificação **Não verificar arquivos durante mais de N seg**.
6. Clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

Filtrar anexos de mensagens de e-mail

Os programas maliciosos podem ser distribuídos 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 um programa malicioso.

Para configurar a filtragem de anexos:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de E-mail**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de E-mail.
3. Na secção **Nível de segurança**, clique no botão **Configuração**.

   É aberta a janela **Antivírus de E-mail**.
4. Na janela **Antivírus de E-mail**, selecione o separador **Filtro de anexos**.

5. Execute uma das seguintes ações:

- Se não pretender que o Antivírus de E-mail filtre anexos de mensagens, selecione a opção **Desativar filtragem**.
- Se pretender que o Antivírus de E-mail altere o nome dos anexos de mensagens dos **tipos especificados**, selecione a opção **Renomear os anexos dos tipos especificados**.

Note que o formato real de um ficheiro poderá não corresponder à sua extensão do nome de ficheiro.

Se ativar a filtragem de objetos que estão anexados a mensagens de e-mail, o Antivírus de E-mail pode alterar o nome dos ficheiros ou eliminá-los 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 — Visual Basic® script

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 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 – extensão para e-mails guardados 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. Próxima geração de metaficheiros para o Microsoft Windows OS. Os ficheiros EMF não são suportados pelo Microsoft Windows de 16 bits.

ico — ficheiro de ícones de objetos

ov? — Ficheiros executáveis de Microsoft Office Word

xl* — documentos e ficheiros do Microsoft Office Excel como, por exemplo: xla, extensão para o Microsoft Office Excel, xlc para diagramas, xlt para modelos de documentos, xlsx para livros do Microsoft Office Excel 2007, xltm para livros do Microsoft Office Excel 2007 com suporte de macros, xlsb para livros do Microsoft Office Excel 2007 em formato binário (não XML), xltx para modelos do Microsoft Office Excel 2007, xlsm para modelos do Microsoft Office Excel 2007 com suporte para macros e xlam para plug-ins do Microsoft Office Excel 2007 com suporte para macros

pp* — documentos e ficheiros do Microsoft Office PowerPoint® como, por exemplo: pps para diapositivos do Microsoft Office PowerPoint, ppt para apresentações, pptx para apresentações do Microsoft Office PowerPoint 2007, pptm para apresentações do Microsoft Office PowerPoint 2007 com suporte para macros, potx para modelos de apresentações do Microsoft Office PowerPoint 2007, potm para modelos de apresentações do Microsoft Office PowerPoint 2007 com suporte para macros, ppsx para apresentações de diapositivos do Microsoft Office PowerPoint 2007, ppsm para apresentações de diapositivos do Microsoft Office PowerPoint 2007 com suporte para macros e ppam para plug-ins do Microsoft Office PowerPoint 2007 com suporte para macros

md* — documentos e ficheiros do Microsoft Office Access® como, por exemplo: mda para grupos de trabalho e mdb para bases de dados

sldx — diapositivo do Microsoft PowerPoint 2007

sldm — diapositivo do Microsoft PowerPoint 2007 com suporte para macros

thmx — tema do Microsoft Office 2007

- Se pretender que o Antivírus de E-mail elimine os anexos de mensagens dos tipos especificados, selecione a opção **Eliminar tipos de anexos especificados**.

6. Se selecionou a opção **Renomear os anexos dos tipos especificados** ou a opção **Eliminar tipos de anexos especificados** durante o passo anterior, selecione as caixas à frente dos tipos de ficheiro relevantes.

   Pode alterar a lista de tipos de ficheiros utilizando os botões **Adicionar**, **Editar** e **Remover**.

7. Clique em **OK**.

8. Para guardar as alterações, clique no botão **Guardar**.

Verificar e-mails no Microsoft Office Outlook

Durante a instalação do Kaspersky Endpoint Security, a extensão do Antivírus de E-mail está integrada no Microsoft Office Outlook (doravante também referido como Outlook). Esta extensão permite-lhe abrir as definições do Antivírus de E-mail 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 de Antivírus de E-mail pode verificar mensagens recebidas e enviadas que são transmitidas através dos protocolos POP3, SMTP, NNTP, IMAP e MAPI.

As definições do Antivírus de E-mail podem ser configuradas diretamente no Outlook se a caixa de verificação **Adicional: extensão do Microsoft Office Outlook** estiver selecionada na interface do Kaspersky Endpoint Security.

No Outlook, as mensagens recebidas são primeiro verificadas pelo Antivírus de E-mail (se a caixa de verificação **Tráfego de POP3 / SMTP / NNTP / IMAP** estiver selecionada na interface do Kaspersky Endpoint Security) e, em seguida, pela extensão do Antivírus de E-mail para Outlook. Se o Antivírus de E-mail detetar um objeto malicioso numa mensagem, irá alertá-lo para este evento.

A ação pela qual optar na janela de notificação determina qual o componente que elimina a ameaça na mensagem: o Antivírus de E-mail ou a extensão do Antivírus de E-mail para Outlook.

- Se selecionar **Desinfetar** ou **Remover** na janela de notificação, a eliminação da ameaça é efetuada pelo Antivírus de E-mail.
- Se selecionar **Ignorar** na janela de notificação do utilizador, a extensão do Antivírus de E-mail para Outlook elimina a ameaça.

As mensagens enviadas são, primeiro, verificadas pela extensão do Antivírus de E-mail para Outlook e, depois, pelo Antivírus de E-mail.

Configurar a verificação de correio no Outlook

Para configurar a verificação de correio no Outlook 2007:

1. Abra a janela principal do Outlook 2007.
2. Selecione **Serviço** → **Definições** da barra de menus.

   É aberta a janela **Opções**.
3. Na janela **Opções**, selecione o separador **Proteção de e-mail**.

Para configurar a verificação de correio no Outlook 2010 / 2013:

1. Abra a janela principal do Outlook.

   Selecione o separador **Ficheiro** no canto superior esquerdo.
2. Clique no botão **Opções**.

   É apresentada a janela **Opções do Outlook**.
3. Selecione a secção **Suplementos**.

As definições de plug-ins incorporados no Outlook são apresentadas na parte direita da janela.

4. Clique no botão **Opções do Suplemento**.

Configurar a verificação de correio utilizando o Kaspersky Security Center

Se o correio for verificado utilizando a extensão do Antivírus de E-mail para o Outlook, recomenda-se a utilização do Modo de intercâmbio em cache. Para obter informações mais detalhadas sobre o Modo de intercâmbio em cache e as respetivas recomendações de utilização, consulte a Base de Conhecimento da Microsoft: https://technet.microsoft.com/en-us/library/cc179175.aspx.

Para configurar o modo operativo da extensão do Antivírus de E-mail para Outlook utilizando o Kaspersky Security Center:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** na árvore da Consola de Administração, abra a pasta com o nome do grupo de administração relevante para o qual pretende configurar a verificação de correio.
3. Na área de trabalho, selecione o separador **Políticas**.
4. Selecione a política pretendida.
5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.
6. Na secção **Proteção de Antivírus**, selecione a subsecção de **Antivírus de E-mail**.
7. Na secção **Nível de segurança**, clique no botão **Configuração**.
   É aberta a janela **Antivírus de E-mail**.
8. Na secção **Conetividade**, clique no botão **Configuração**.
   É aberta a janela **Proteção de e-mail**.
9. Na **Proteção de e-mail**:
   - Selecione a caixa de verificação **Verificar ao receber** se pretender que a extensão de Antivírus de E-mail 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 de Antivírus de E-mail 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 de Antivírus de E-mail para o Outlook verifique as mensagens de saída quando estas são enviadas.
10. Na janela **Proteção de e-mail**, clique em **OK**.

11. Na janela **Antivírus de E-mail**, clique em **OK**.

12. Aplicar a política.

    Consulte o *Manual do Administrador do Kaspersky Security Center* para obter mais informações sobre a aplicação da política do Kaspersky Security Center.

Proteção do computador na Internet. Antivírus de Internet

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para estações de trabalho. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para servidores de ficheiros.

Esta secção contém informações sobre o Antivírus de Internet e instruções sobre como configurar as definições do componente.

Sobre o Antivírus de Internet

Sempre que acede à Internet, as informações armazenadas no computador são expostas a vírus e a outro software malicioso. Estes podem infiltrar-se no computador enquanto o utilizador transfere um software gratuito ou navega em sites que estão sujeitos a ataques de criminosos. Os worms de rede podem penetrar no computador assim que estabelecer uma ligação à Internet, mesmo antes de abrir uma página de Internet ou transferir um ficheiro.

O Antivírus de Internet protege dados de entrada e de saída enviados para e a partir do computador através dos protocolos HTTP e FTP e verifica URLs face à lista de endereços maliciosos ou de phishing.

O Antivírus de Internet intercepta e analisa vírus e outras ameaças em todas as páginas de Internet ou ficheiros aos quais o utilizador ou uma aplicação acede através do protocolo HTTP ou FTP. Em seguida:

- Se não for detetado código malicioso na página ou ficheiro, o utilizador obtém acesso imediato aos mesmos.
- Se um utilizador acede a uma página da Internet que contém código malicioso, a aplicação executa a ação especificada nas definições do Antivírus de Internet.

Ativar e desativar o Antivírus de Internet

Por defeito, o Antivírus de Internet está ativado, em execução no modo recomendado pelos peritos da Kaspersky. Pode desativar o Antivírus de Internet, se necessário.

Existem duas formas para ativar ou desativar o componente:

- No separador **Proteção e Controlo** da janela principal da aplicação
- Na janela de definições da aplicação

Para ativar ou desativar o Antivírus de Internet no separador Proteção e Controlo da janela principal da aplicação:

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Proteção**.
   É aberta a secção **Proteção**.

4. Clique com o botão direito do rato para visualizar o menu de contexto da linha que contém as informações sobre o componente Antivírus de Internet.

   É aberto um menu para selecionar ações no componente.

5. Execute uma das seguintes ações:

   - Para ativar o Antivírus de Internet, selecione **Iniciar** no menu.

     O ícone de estado do componente , que é apresentado à esquerda na linha do **Antivírus de Internet**, é alterado para o ícone .

   - Para desativar o Antivírus de Internet, selecione **Parar** no menu.

     O ícone de estado do componente , que é apresentado à esquerda na linha do **Antivírus de Internet**, é alterado para o ícone .

Para ativar ou desativar o Antivírus de Internet a partir da janela de definições da aplicação:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de Internet**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de Internet.

3. Execute uma das seguintes ações:

   - Se pretender ativar o Antivírus de Internet, selecione a caixa de verificação **Ativar Antivírus de Internet**.

   - Se pretender desativar o Antivírus de Internet, desmarque a caixa de verificação **Ativar Antivírus de Internet**.

4. Para guardar as alterações, clique no botão **Guardar**.

Configurar o Antivírus de Internet

Pode efetuar as seguintes operações para configurar o Antivírus de Internet:

- Alterar o nível de segurança do tráfego de Internet.

  Pode selecionar um dos níveis de segurança pré-instalados de tráfego de Internet recebido ou transmitido através dos protocolos HTTP e FTP, ou configurar um nível de segurança de tráfego de Internet personalizado.

  Se alterar as definições do nível de segurança de tráfego de Internet, pode sempre repor as definições de nível de segurança de tráfego de Internet recomendadas.

- Alterar a ação que o Kaspersky Endpoint Security executa em objetos de tráfego de Internet maliciosos.

  Se a análise de um objeto de HTTP revelar que este contém código malicioso, a resposta do Antivírus de Internet depende da ação que tiver especificado.

- Configurar a verificação de URLs do Antivírus de Internet face às bases de dados de phishing e endereços da Internet maliciosos.

- Configurar a utilização de análise heurística ao verificar a existência de vírus e outros programas maliciosos no tráfego de Internet.

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.

- Configurar a utilização de análise heurística ao verificar a existência de ligações de phishing nas páginas de Internet.
- Otimizar a verificação do Antivírus de Internet do tráfego de Internet enviado e recebido através dos protocolos HTTP e FTP.
- Criar uma lista de URLs confiáveis.

  Pode criar uma lista de URLs cujo conteúdo considera confiável. O Antivírus de Internet não analisa as informações de URLs confiáveis para verificar a existência de vírus ou de outras ameaças. Esta opção pode ser útil nos casos em que, por exemplo, o Antivírus de Internet 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.

Alterar o nível de segurança do tráfego de Internet

Para proteger os dados recebidos e transmitidos através dos protocolos HTTP e FTP, o Antivírus de Internet aplica vários grupos de definições. Estes grupos de configurações são denominados *níveis de segurança de tráfego de Internet*. Existem três níveis de segurança de tráfego de Internet pré-instalados: **Elevado**, **Recomendado** e **Baixo**. O nível de segurança de tráfego de Internet **Recomendado** é considerado a configuração ideal e é recomendado pela Kaspersky.

Para alterar o nível de segurança do tráfego de Internet:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de Internet**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de Internet.
3. Na secção **Nível de segurança**, execute uma das seguintes ações:

   - Se pretender instalar um dos níveis de segurança de tráfego de Internet pré-instalados (**Elevado**, **Recomendado** ou **Baixo**), utilize a barra indicadora para selecionar um.
   - Se pretender configurar um nível de segurança de tráfego de Internet personalizado, clique no botão **Configuração** e especifique as configurações na janela **Antivírus de Internet**.

     Depois de configurar um nível de segurança de tráfego de Internet personalizado, o nome do nível de segurança na secção **Nível de Segurança** é alterado para **Configurações Personalizadas**.
   - Se pretender alterar o nível de segurança de tráfego de Internet para **Recomendado**, clique no botão **Predefinições**.
4. Para guardar as alterações, clique no botão **Guardar**.

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

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

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de Internet**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de Internet.
3. Na secção **Ação após deteção de ameaças**, selecione a ação executada pelo Kaspersky Endpoint Security em objetos maliciosos de tráfego de Internet:
   - **Selecionar ação automaticamente**.
   - **Bloquear transferência**.
   - **Permitir transferência**.
4. Para guardar as alterações, clique no botão **Guardar**.

Verificação de URLs do Antivírus de Internet face às bases de dados de phishing e endereços de Internet 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 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 recebidos não apenas em mensagens de e-mail, mas também através de outras fontes, por exemplo, em mensagens do ICQ, o Antivírus de Internet 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 URLs de phishing no kit de distribuição do Kaspersky Endpoint Security.

Para configurar o Antivírus de Internet para verificar os URLs face às bases de dados de phishing e endereços de Internet maliciosos:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de Internet**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de Internet.
3. Clique no botão **Configuração**.

   A janela **Antivírus de Internet** abre.
4. Na janela **Antivírus de Internet**, selecione o separador **Geral**.
5. Execute as seguintes ações:

- Se pretender que o Antivírus de Internet verifique os URLs face às bases de dados de endereços de Internet maliciosos, na secção **Métodos de verificação**, selecione a caixa de verificação **Verificar se as ligações estão incluídas na base de dados de ligações maliciosas**.

- Se pretender que o Antivírus de Internet verifique os URLs face às bases de dados de endereços de Internet de phishing, na secção **Configuração do Anti-Phishing**, selecione a caixa de verificação **Verificar se as ligações estão incluídas na base de dados de ligações de phishing**.

Também pode verificar as ligações com através das bases de dados de reputação da Kaspersky Security Network.

6. Clique em **OK**.

7. Para guardar as alterações, clique no botão **Guardar**.

Utilizar o Analisador Heurístico com o Antivírus de Internet

Para configurar a utilização da análise heurística:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de Internet**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de Internet.

3. Na secção **Nível de segurança**, clique no botão **Configuração**.

   A janela **Antivírus de Internet** abre.

4. Selecione o separador **Geral**.

5. Se pretender que o Antivírus de Internet utilize a análise heurística para verificar a existência de vírus e outros programas de software malicioso no tráfego de Internet, na secção **Métodos de verificação**, selecione a caixa de verificação **Análise heurística para detetar vírus** e utilize a barra indicadora para definir o nível da análise heurística: **Nível superficial**, **Nível médio** ou **Nível aprofundado**.

6. Se quiser que o Antivírus de Internet utilize a análise heurística para verificar a existência de ligações de phishing em páginas da Internet, na secção **Configuração do Anti-Phishing**, selecione a caixa de verificação **Análise heurística para detetar ligações de phishing**.

7. Clique em **OK**.

8. Para guardar as alterações, clique no botão **Guardar**.

Editar a lista de URLs confiáveis

Para criar uma lista de URLs confiáveis:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de Internet**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de Internet.

3. Clique no botão **Configuração**.

   A janela **Antivírus de Internet** abre.

4. Selecione o separador **URLs confiáveis**.

5. Selecione a caixa de verificação **Não verificar tráfego de Internet de URLs confiáveis**.

6. Criar uma lista de URLs/páginas da Internet cujo conteúdo é confiável. Para criar uma lista:

   a. Clique no botão **Adicionar**.

      É apresentada a janela **Endereço web/Máscara de endereço web**.

   b. Introduza o endereço de um site/página de Internet ou a máscara de endereço de um site/página de Internet.

   c. Clique em **OK**.

      É apresentado um novo registo na lista de URLs confiáveis.

7. Clique em **OK**.

8. Para guardar as alterações, clique no botão **Guardar**.

Proteção de tráfego de cliente de MI. Antivírus de MI

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para estações de trabalho. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para servidores de ficheiros.

Esta secção contém informações sobre o Antivírus de MI e instruções sobre como configurar as definições do componente.

Sobre o Antivírus de MI

O Antivírus de MI verifica o tráfego dos clientes de mensagens instantâneas (os conhecidos como *clientes de MI*).

O Antivírus de MI não verifica mensagens transmitidas através de canais codificados.

As mensagens enviadas através de clientes de MI podem conter os tipos seguintes de ameaças de segurança:

- URLs que tentam transferir um programa malicioso para o computador
- URLs para programas maliciosos e sites que os intrusos usam para ataques de phishing

  O objetivo dos ataques de phishing é roubar dados pessoais dos utilizadores, como por exemplo, números de cartões bancários, detalhes do passaporte, passwords de sistemas de pagamentos bancários e outros serviços online (como sites de redes sociais ou contas de e-mail).

Os ficheiros podem ser transmitidos através dos clientes de MI. Ao tentar guardar esses ficheiros, os ficheiros são verificados pelo componente Antivírus de Ficheiros.

O Antivírus de MI intercepta todas as mensagens que o utilizador envia ou recebe através de um cliente de MI e verifica essas mensagens quanto à existência de ligações que poderão ameaçar a segurança do computador:

- Se não forem detetados URLs perigosos na mensagem, esta ficará disponível para o utilizador.
- Se forem detetadas ligações perigosas na mensagem, o Antivírus de MI substitui a mensagem por informações sobre a ameaça na janela de mensagens do cliente de MI ativo.

Ativar e desativar o Antivírus de MI

Por defeito, o Antivírus de MI está ativado, em execução no modo recomendado pelos peritos da Kaspersky. Pode desativar o Antivírus de MI, se necessário.

Existem duas formas para ativar ou desativar o componente:

- No separador **Proteção e Controlo** na janela principal da aplicação
- Na janela de definições da aplicação

Para ativar ou desativar o Antivírus de MI no separador Proteção e Controlo da janela principal da aplicação:

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Proteção**.
   É aberta a secção **Proteção**.
4. Clique com o botão direito do rato na linha **Antivírus de MI** para ver o menu de contexto das ações do componente.
5. Execute uma das seguintes ações:
   - Para ativar o Antivírus de MI, selecione **Iniciar** no menu de contexto.
     O ícone de estado do componente , que é apresentado à esquerda na linha do **Antivírus de MI**, é alterado para o ícone .
   - Para desativar o Antivírus de MI, selecione **Parar** no menu de contexto.
     O ícone de estado do componente , que é apresentado à esquerda na linha do **Antivírus de MI**, é alterado para o ícone .

Para ativar ou desativar o Antivírus de MI a partir da janela de definições da aplicação:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de MI**.
   Na parte direita da janela, são apresentadas as definições do componente Antivírus de MI.
3. Execute uma das seguintes ações:
   - Se pretender ativar o Antivírus de MI, selecione a caixa de verificação **Ativar Antivírus de MI**.
   - Se pretender desativar o Antivírus de MI, desmarque a caixa de verificação **Ativar Antivírus de MI**.
4. Para guardar as alterações, clique no botão **Guardar**.

Configurar o Antivírus de MI

Pode executar as seguintes ações para configurar o Antivírus de MI:

- Configurar o âmbito de proteção.
  Pode alargar ou reduzir o âmbito de proteção, modificando o tipo de mensagens de clientes de MI que são verificadas.
- Configure a verificação das ligações do Antivírus de MI em mensagens de clientes de MI face às bases de dados de endereços da Internet maliciosos e de phishing.

Criar o âmbito de proteção do Antivírus de MI

O âmbito de proteção refere-se aos objetos que o componente verifica quando ativado. Os âmbitos de proteção de componentes diferentes têm propriedades diferentes. O tipo de mensagens de clientes de MI verificadas, de entrada ou de saída, é uma propriedade do âmbito de proteção do Antivírus de MI. Por defeito, o Antivírus de MI verifica quer as mensagens de entrada quer as mensagens de saída. Pode desativar a verificação do tráfego de saída.

Para criar o âmbito de proteção:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de MI**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de MI.
3. Na secção **Âmbito de proteção**, execute uma das seguintes ações:
   - Se pretender que o Antivírus de MI verifique todas as mensagens de entrada e de saída dos clientes de MI, selecione a opção **Mensagens de entrada e de saída**.
   - Se pretender que o Antivírus de MI verifique apenas as mensagens clientes de MI, selecione a opção **Apenas mensagens de entrada**.
4. Para guardar as alterações, clique no botão **Guardar**.

Verificar URLs face a bases de dados de URLs maliciosos e de phishing com o Antivírus de MI

Para configurar o Antivírus de MI para verificar os URLs face às bases de dados de endereços de Internet maliciosos ou de phishing:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Antivírus de MI**.

   Na parte direita da janela, são apresentadas as definições do componente Antivírus de MI.
3. Na secção **Métodos de verificação**, selecione os métodos que pretende que o Antivírus de MI utilize:
   - Se pretender verificar as ligações nas mensagens de clientes de MI face às bases de dados de endereços da Internet maliciosos, selecione a caixa de verificação **Verificar se as ligações estão incluídas na base de dados de ligações maliciosas**.
   - Se pretender verificar as ligações nas mensagens de clientes de MI face às bases de dados de endereços da Internet de phishing, selecione a caixa de verificação **Verificar se as ligações estão incluídas na base de dados de ligações de phishing**.
4. Para guardar as alterações, clique no botão **Guardar**.

Monitorização do Sistema

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para estações de trabalho. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para servidores de ficheiros.

Esta secção contém informações sobre a Monitorização do Sistema e instruções para efetuar as configurações do componente.

Sobre a Monitorização do Sistema

A Monitorização do Sistema recolhe dados sobre as ações das aplicações no computador e transmite estas informações para outros componentes, para uma proteção mais fiável.

Assinaturas de fluxos de comportamento

As Assinaturas de Fluxos de Comportamento (BSS, "behavior stream signatures") contêm sequências de ações de aplicações que o Kaspersky Endpoint Security classifica como perigosas. Se a atividade das aplicações corresponder uma assinatura de fluxo de comportamento, o Kaspersky Endpoint Security irá executar a ação especificada. A funcionalidade do Kaspersky Endpoint Security com base em assinaturas de fluxos de comportamento proporciona defesa proativa ao computador.

Por defeito, se a atividade de uma aplicação corresponder a uma assinatura de fluxo de comportamento, a Monitorização do Sistema move o ficheiro executável da aplicação para a Quarentena.

Reverter ações executadas por software malicioso

Com base nas informações recolhidas pela Monitorização do Sistema, o Kaspersky Endpoint Security pode **reverter ações que tenham sido executadas por software malicioso no sistema operativo** ao executar a desinfeção.

Ao reverter a atividade de software malicioso no sistema operativo, o Kaspersky Endpoint Security toma medidas nos seguintes tipos de atividade de software malicioso:

- Atividade de ficheiros.

  O Kaspersky Endpoint Security elimina ficheiros executáveis que tenham sido criados por um programa malicioso e estejam localizados em qualquer meio, exceto em meios de rede.

  O Kaspersky Endpoint Security elimina os ficheiros executáveis que tenham sido criados por um programa no qual tenha penetrado um programa malicioso.

  O Kaspersky Endpoint Security não restaura ficheiros alterados ou apagados.

- Atividade de registo.

  O Kaspersky Endpoint Security elimina partições e chaves de registo que tenham sido criadas por software malicioso.

  O Kaspersky Endpoint Security não restaura partições modificadas ou apagadas e chaves de registo.

- Atividade de sistema.

  O Kaspersky Endpoint Security termina processos que tenham sido iniciados por um programa malicioso.

  O Kaspersky Endpoint Security termina processos nos quais tenha penetrado um programa malicioso.

  O Kaspersky Endpoint Security não retoma processos que tenham sido interrompidos por um programa malicioso.

- Atividade de rede.

  O Kaspersky Endpoint Security bloqueia a atividade de rede de programas maliciosos.

  O Kaspersky Endpoint Security bloqueia a atividade de rede de processos que tenham sido penetrados por um programa malicioso.

Pode ser iniciada uma reversão de ações de software malicioso pelo Antivírus de Ficheiros 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.

Ativar e desativar a Monitorização do Sistema

Por predefinição, a Monitorização do Sistema está ativada e é executada no modo recomendado pela Kaspersky. Pode desativar a Monitorização do Sistema, se necessário.

Não é recomendado desativar a Monitorização do Sistema exceto quando absolutamente necessário, uma vez que afeta o desempenho dos componentes de proteção. Os componentes de proteção podem solicitar dados recolhidos pela Monitorização do Sistema para identificar de forma mais precisa uma ameaça detetada.

Existem duas formas para ativar ou desativar a Monitorização do Sistema:

- No separador **Proteção e Controlo** da janela principal da aplicação
- Na janela de definições da aplicação

*Para ativar ou desativar a Monitorização do Sistema no separador **Proteção e Controlo** da janela principal da aplicação:*

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Proteção**.

   É aberta a secção **Proteção**.
4. Clique com o botão direito do rato para visualizar o menu de contexto da linha que contém as informações sobre o componente Monitorização do Sistema.

   É aberto um menu para selecionar ações no componente.
5. Execute uma das seguintes ações:

   - Para ativar a Monitorização do Sistema, selecione **Iniciar**.

     O ícone de estado do componente , que é apresentado à esquerda na linha **Monitorização do Sistema**, é alterado para o ícone .
   - Para desativar a Monitorização do Sistema, selecione **Parar**.

     O ícone de estado do componente , que é apresentado à esquerda na linha **Monitorização do Sistema**, é alterado para o ícone .

Para ativar ou desativar a Monitorização do Sistema a partir da janela de definições da aplicação:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Monitorização do Sistema**.

   Na parte direita da janela, são apresentadas as definições do componente **Monitorização do Sistema**.
3. Execute uma das seguintes ações:

   - Para ativar a Monitorização do Sistema, selecione a caixa de verificação **Ativar Monitorização do Sistema**
   - Para desativar a Monitorização do Sistema, desmarque a caixa de verificação **Ativar Monitorização do Sistema**.
4. Para guardar as alterações, clique no botão **Guardar**.

Configurar a Monitorização do Sistema

Pode executar as seguintes ações de modo a configurar a Monitorização do Sistema:

- ativar ou desativar a proteção contra explorações de vulnerabilidades;
- selecionar ação caso uma atividade maliciosa seja detetada num programa;
- Ativar ou desativar a reversão de ações de software malicioso durante a desinfeção.

Ativar ou desativar a proteção contra explorações de vulnerabilidades

Para ativar ou desativar a proteção contra explorações de vulnerabilidades:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Monitorização do Sistema**.

   Na parte direita da janela, são apresentadas as definições do componente **Monitorização do Sistema**.
3. Execute uma das seguintes ações:

   - Selecione a caixa de verificação **Ativar prevenção de exploração de vulnerabilidades** caso pretenda que o Kaspersky Endpoint Security monitorize os ficheiros utilizados por programas vulneráveis quando são iniciados.

     Se o Kaspersky Endpoint Security detetar que um ficheiro em utilização por um programa vulnerável foi iniciado por algo que não seja o utilizador, atuará conforme a sua seleção na lista de pop-ups **Ação após deteção de ameaças**.

   - Selecione a caixa de verificação **Ativar prevenção de exploração de vulnerabilidades** caso pretenda que o Kaspersky Endpoint Security monitorize os ficheiros utilizados por programas vulneráveis quando são iniciados.
4. Para guardar as alterações, clique no botão **Guardar**.

Selecionar ação caso uma atividade maliciosa seja detetada num programa

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

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Monitorização do Sistema**.

   Na parte direita da janela, são apresentadas as definições do componente **Monitorização do Sistema**.
3. Na secção **Ação após deteção de ameaças** na lista de pop-ups **Ao detetar atividade de software malicioso**, escolha a seguinte ação:

   - **Selecionar ação automaticamente**.
   - **Mover ficheiro para a Quarentena**.
   - **Encerrar o programa malicioso**.
   - **Ignorar**.
4. Para guardar as alterações, clique no botão **Guardar**.

Ativar ou desativar a reversão de ações de software malicioso durante a desinfeção

Para ativar ou desativar a reversão de ações de software malicioso durante a desinfeção:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Monitorização do Sistema**.

   Na parte direita da janela, são apresentadas as definições do componente **Monitorização do Sistema**.
3. Execute uma das seguintes ações:

   - Se pretender que o Kaspersky Endpoint Security reverta ações que tenham sido executadas por software malicioso no sistema operativo, durante a desinfeção, selecione a caixa de verificação **Reverter ações de software malicioso durante a desinfeção**.
   - Se pretender que o Kaspersky Endpoint Security ignore ações que tenham sido executadas por software malicioso no sistema operativo, durante a desinfeção, desmarque a caixa de verificação **Reverter ações de software malicioso durante a desinfeção**.
4. Para guardar as alterações, clique no botão **Guardar**.

Firewall

Esta secção contém informações sobre a Firewall e instruções sobre como configurar as definições do componente.

Sobre a Firewall

Durante a utilização de LANs e da Internet, um computador é exposto a vírus, outro software malicioso e a uma variedade de ataques que exploram as vulnerabilidades dos sistemas operativos e do software.

A firewall protege os dados pessoais armazenados no computador do utilizador, bloqueando a maioria das ameaças possíveis ao sistema operativo enquanto o computador estiver ligado à Internet ou a uma rede local. A Firewall deteta todas as ligações de rede do computador do utilizador e fornece uma lista de endereços IP, com uma indicação do estado da ligação de rede predefinida.

O componente Firewall filtra toda a atividade da rede de acordo com as regras de rede. A configuração de regras de rede permite especificar o nível desejado de proteção do computador, desde o bloqueio do acesso à Internet de todas as aplicações à permissão de acesso ilimitado.

Ativar ou desativar a Firewall

Por defeito, a Firewall está ativada e funciona no modo otimizado. Se necessário, pode desativar a Firewall.

Existem duas formas para ativar ou desativar o componente:

- No separador **Proteção e Controlo** na janela principal da aplicação
- Na janela de definições da aplicação

Para ativar ou desativar a Firewall no separador Proteção e Controlo da janela principal da aplicação:

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Proteção**.
   É aberta a secção **Proteção**.
4. Clique com o botão direito do rato sobre a linha **Firewall**, para abrir o menu de contexto para ações da Firewall.
5. Execute uma das seguintes ações:
   - Para ativar a Firewall, selecione **Iniciar** no menu de contexto.
     O ícone de estado do componente , que é apresentado à esquerda na linha **Firewall**, é alterado para o ícone .
   - Para desativar a Firewall, selecione **Parar** no menu de contexto.
     O ícone de estado do componente , que é apresentado à esquerda na linha **Firewall**, é alterado para o ícone .

Para ativar ou desativar a Firewall na janela de configuração da aplicação:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione **Firewall**.

   Na parte direita da janela, são apresentadas as definições do componente Firewall.
3. Execute uma das seguintes ações:
   - Para ativar a Firewall, selecione a caixa de verificação **Ativar Firewall**.
   - Para desativar a Firewall, selecione a caixa de verificação **Desativar Firewall**.
4. Para guardar as alterações, clique no botão **Guardar**.

Sobre as regras de rede

As *Regras de rede* são constituídas por ações permitidas ou bloqueadas executadas pela Firewall ao detetar uma tentativa de ligação de rede.

A firewall fornece proteção contra ataques de rede de tipos diferentes em dois níveis: ao nível da rede e ao nível de programa. A proteção ao nível da rede é efetuada com a aplicação das regras de pacotes de rede. A proteção ao nível do programa é efetuada com a aplicação de regras através das quais as aplicações instaladas podem aceder aos recursos da rede.

Com base nos dois níveis de proteção da Firewall, pode criar:

- *Regras de pacotes de rede.* As regras de pacotes de rede impõem restrições aos pacotes de rede, independentemente do programa. Estas regras restringem o tráfego de entrada e de saída de rede, através de portas específicas do protocolo de dados selecionado. A firewall especifica determinadas regras de pacotes de rede por defeito.
- *Regras de rede de aplicações*. As regras de rede de aplicações impões restrições à atividade de rede de uma aplicação especificada. Estas influenciam não só as características do pacote de rede, mas também a aplicação específica à qual este pacote de rede se destina ou que emitiu este pacote de rede. Essas regras tornam possível ajustar a filtragem da atividade da rede: por exemplo, quando um determinado tipo de ligação de rede é bloqueado para determinadas aplicações, mas é permitido para outras.

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.

Pode especificar uma prioridade de execução para cada regra de pacote de rede e para cada regra de rede para aplicações.

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 *fidedigna*. Por exemplo, por predefinição, não é permitida nenhuma atividade de rede das aplicações no grupo de confiança 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 fidedigno 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.

Sobre o estado da ligação de rede

A Firewall controla todas as ligações de rede no computador do utilizador e atribui automaticamente um estado a cada ligação de rede detetada.

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

- **Rede pública**. Este estado destina-se a redes não protegidas por quaisquer aplicações antivírus, firewalls ou filtros (por exemplo, para redes de cibercafés). 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 defeito, a Firewall atribui o estado *Rede pública* à Internet. Não é possível alterar o estado da Internet.

- **Rede local**. Este estado é atribuído às redes cujos utilizadores são confiáveis para aceder aos ficheiros e às impressoras neste computador (por exemplo, uma LAN ou uma rede doméstica).

- **Rede confiável**. Este estado destina-se a 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.

Alterar o estado da ligação de rede

Para alterar a situação da ligação de rede:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Firewall**.

   Na parte direita da janela, são apresentadas as definições do componente Firewall.
3. Clique no botão **Redes disponíveis**.

   É apresentada a janela **Firewall**.
4. Selecione a ligação de rede cujo estado pretende alterar.
5. No menu de contexto, selecione o estado da ligação de rede:

   - **Rede pública**.
   - **Rede local**.
   - **Rede confiável**.
6. Na janela **Firewall**, clique em **OK**.

7. Para guardar as alterações, clique no botão **Guardar**.

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 defeito, 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 e editar uma regra de pacotes de rede

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

Para criar ou editar uma regra de pacote de rede:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione **Firewall**.

3. Clique no botão **Regras de pacotes de rede**.

4. A janela **Firewall** é aberta no separador **Regras de pacotes de rede**.

   Este separador apresenta uma lista predefinida de regras de pacotes de rede definidas pela Firewall.

5. Execute uma das seguintes ações:

   - Para criar uma regra de pacote de rede nova, clique no botão **Adicionar**.
   - Para editar uma regra de pacote de rede, selecione a regra na lista de regras de pacotes de rede e clique no botão **Editar**.

   É aberta a janela **Regra de rede**.

6. 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**.

7. No campo **Nome**, especifique o nome do serviço de rede de uma das seguintes formas:

   - Clique no ícone à direita do campo **Nome** e selecione o nome do serviço de rede na lista suspensa.

     A lista pendente inclui os serviços de rede que definem as ligações de rede utilizadas mais frequentemente.

   - Introduza manualmente o nome do serviço de rede no campo **Nome**.

8. Especifique o protocolo de transferência de dados:

   a. Selecione a caixa de verificação **Protocolo**.

   b. Na lista suspensa, selecione o tipo de protocolo para o qual a atividade de rede deve ser monitorizada.

      A firewall monitoriza ligações de rede que utilizam os protocolos TCP, UDP, ICMP, ICMPv6, IGMP e GRE.

      Se selecionar um serviço de rede na lista suspensa **Nome**, a caixa de verificação **Protocolo** é selecionada automaticamente e a lista pendente junto à caixa de verificação contém o tipo de protocolo que corresponde ao serviço de rede selecionado. Por defeito, a caixa de verificação **Protocolo** está desmarcada.

9. Na lista suspensa **Direção**, selecione a direção da atividade de rede monitorizada.

   A firewall monitoriza ligações de rede com as seguintes direções:

   - **Entrada (pacote)**.
   - **Entrada**.
   - **Entrada/Saída**
   - **Saída (pacote)**.
   - **Saída**.

10. Se ICMP ou ICMPv6 estiver selecionado como protocolo, pode especificar o código e tipo de pacote ICMP:

a. Selecione a caixa de verificação **Tipo de ICMP** e selecione o pacote ICMP na lista suspensa.

b. Selecione a caixa de verificação **Código ICMP** e selecione o pacote ICMP na lista suspensa.

11. Se TCP ou UDP estiver selecionado como 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:

    a. Introduza as portas do computador remoto no campo **Portas Remotas**.

    b. Introduza as portas do computador local no campo **Portas Locais**.

12. Na tabela de **Adaptadores de rede**, especifique as definições de adaptadores de rede a partir dos quais os pacotes de rede podem ser enviados ou que podem receber pacotes de rede. Para tal, utilize os botões **Adicionar**, **Editar** e **Eliminar**.

13. Se pretende limitar o controlo dos pacotes de rede com base no seu tempo de vida (TTL), selecione a caixa **TTL** e o campo junto a esta, especifique o intervalo de valores de TTL para pacotes de rede de entrada e/ou de saída.

    Uma regra de rede controla a transmissão dos pacotes de rede cujo TTL não excede o valor especificado.

    Caso contrário, desmarque a caixa de verificação **TTL**.

14. Especificar os endereços da rede de computadores remotos que podem enviar e/ou receber pacotes de rede. Para tal, selecione um dos seguintes valores na lista pendente **Endereços remotos**:

    - **Qualquer endereço**. A regra de rede controla pacotes de rede enviados e/ou recebidos por computadores remotos com qualquer endereço IP.
    - **Endereços de sub-rede**. A regra de rede controla pacotes de rede enviados e/ou recebidos por computadores remotos com endereços IP associados ao tipo de rede selecionado: **Redes confiáveis**, **Redes locais** ou **Redes públicas**.
    - **Endereços da lista**. A regra de rede controla pacotes de rede enviados e/ou recebidos por computadores remotos com endereços IP que podem ser especificados na lista abaixo, utilizando os botões **Adicionar**, **Editar** e **Eliminar**.

15. Especificar os endereços de rede de computadores que têm o Kaspersky Endpoint Security instalado e podem enviar e/ou receber pacotes de rede. Para tal, selecione um dos seguintes valores na lista suspensa **Endereços locais**:

    - **Qualquer endereço**. A regra de rede controla pacotes de rede enviados e/ou recebidos por computadores com o Kaspersky Endpoint Security instalado e com qualquer endereço IP.
    - **Endereços da lista**. A regra de rede controla pacotes de rede enviados e/ou recebidos por computadores com o Kaspersky Endpoint Security instalado e com endereços IP que podem ser especificados na lista abaixo, utilizando os botões **Adicionar**, **Editar** e **Eliminar**.

    Por vezes, o endereço local não pode ser obtido para aplicações que funcionam com os pacotes de rede. Se este for o caso, o valor da definição das **Endereços locais** é ignorado.

16. Se pretender que as ações da regra de rede se reflitam no relatório, selecione a caixa de verificação **Registar eventos**.

17. Na janela **Regra de rede**, clique em **OK**.

    Se criar uma regra de rede nova, a regra é apresentada no separador **Regras de pacotes de rede** da janela **Firewall**. Por defeito, uma regra de rede nova é adicionada ao fim da lista de regras de pacotes de rede.

18. Na janela **Firewall**, clique em **OK**.
19. Para guardar as alterações, clique no botão **Guardar**.

Ativar ou desativar uma regra de pacotes de rede

Para ativar ou desativar uma regra de pacotes de rede:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Firewall**.
   Na parte direita da janela, são apresentadas as definições do componente Firewall.
3. Clique no botão **Regras de pacotes de rede**.
   A janela **Firewall** é aberta no separador **Regras de pacotes de rede**.
4. Na lista, selecione a regra de pacotes de rede necessária.
5. Execute uma das seguintes ações:
   - Para ativar a regra, selecione a caixa de verificação junto ao nome da regra de pacotes de rede.
   - Para desativar a regra, desmarque a caixa de verificação junto ao nome da regra de pacotes de rede.
6. Clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

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. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Firewall**.
   Na parte direita da janela, são apresentadas as definições do componente Firewall.
3. Clique no botão **Regras de pacotes de rede**.
   A janela **Firewall** é aberta no separador **Regras de pacotes de rede**.
4. Na lista, selecione a regra de pacotes de rede cuja ação pretende alterar.
5. Na coluna **Permissão**, clique com o botão direito do rato para visualizar o menu de contexto e selecione a ação que pretende atribuir:
   - **Permitir**
   - **Bloquear**

- **De acordo com a regra da aplicação**
- **Registar eventos**

6. Na janela **Firewall**, clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

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. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Firewall**.

   Na parte direita da janela, são apresentadas as definições do componente Firewall.
3. Clique no botão **Regras de pacotes de rede**.

   A janela **Firewall** é aberta no separador **Regras de pacotes de rede**.
4. Na lista, selecione a regra de pacotes de rede cuja prioridade pretende alterar.
5. Utilize os botões **Mover cima** e **Mover baixo** para mover a regra de pacote de rede para a localização pretendida na lista de regras de pacotes de rede.
6. Clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

Gerir regras de rede de aplicações

Por defeito, 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 de confiança. 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.

Por defeito, 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, de um modo semelhante ao componente Controlo de Privilégios das Aplicações. As regras de rede de grupo de aplicações definem os direitos que permitem às aplicações no grupo aceder a ligações de rede diferentes.

Por defeito, 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 defeito. Não pode editar, remover, desativar ou alterar a prioridade das regras de rede do grupo de aplicações criadas por defeito.

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.

Pode executar as seguintes ações ao gerir regras de rede de aplicações:

- Criar uma nova regra de rede.

  Pode criar uma nova regra de rede em conformidade com a qual a Firewall regula a atividade da rede da aplicação ou aplicações que pertencem ao grupo de aplicações selecionado.

- Ativar ou desativar uma regra de rede.

  Todas as regras de rede são adicionadas à lista de regras de rede de aplicações com o estado *Ativado*. Se uma regra de rede estiver ativada, a Firewall aplica esta regra.

  Pode desativar uma regra de rede que tenha sido criada manualmente. Se uma regra de pacotes de rede estiver desativada, a Firewall não aplica esta regra temporariamente.

- Alterar as definições de uma regra de rede.

  Depois de criar uma nova regra de rede, pode regressar sempre às respetivas definições e alterá-las, conforme necessário.

- Alterar a ação da Firewall para uma regra de rede.

  Na lista de regras de rede, pode editar a ação que a Firewall aplica à regra de rede ao detetar atividade de rede nesta aplicação ou grupo de aplicações.

- Alterar a prioridade de uma regra de rede.

  Pode aumentar ou reduzir a prioridade de uma regra de rede personalizada.

- Eliminar uma regra de rede.

  Pode eliminar uma regra de rede personalizada para que a Firewall deixe de aplicar esta regra de rede à aplicação ou grupo de aplicações selecionadas ao detetar a atividade da rede e para que esta regra deixe de ser apresentada na lista de regras de rede de aplicações.

Criar e editar uma regra de rede de aplicações

Para criar ou editar uma regra de rede para um grupo de aplicações:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Firewall**.

3. Clique no botão **Regras de rede de aplicações**.

   A janela **Firewall** é aberta no separador **Regras de controlo das 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 para abrir o menu de contexto e selecione as **Regras de aplicações** ou as **Regras de grupos** dependendo do que necessita de fazer.

   Esta ação abre as **Regras de controlo das aplicações** ou a janela **Regras de controlo de grupos de aplicações**.

6. Na janela que é aberta, selecione o separador **Regras de rede**.

7. Execute uma das seguintes ações:

   - Para criar uma regra de rede nova, clique no botão **Adicionar**.
   - Para editar uma regra de rede, selecione-a na lista de regras de rede e clique no botão **Editar**.

   É aberta a janela **Regra de rede**.

8. Na lista suspensa **Ação**, selecione a ação a ser executada pela Firewall ao detetar este tipo de atividade de rede:

   - **Permitir**
   - **Bloquear**

9. No campo **Nome**, especifique o nome do serviço de rede de uma das seguintes formas:

   - Clique no ícone à direita do campo **Nome** e selecione o nome do serviço de rede na lista suspensa.

     A lista pendente inclui os serviços de rede que definem as ligações de rede utilizadas mais frequentemente.

   - Introduza manualmente o nome do serviço de rede no campo **Nome**.

10. Especifique o protocolo de transferência de dados:

    a. Selecione a caixa de verificação **Protocolo**.

    b. Na lista suspensa, selecione o tipo de protocolo no qual pretende monitorizar a atividade de rede.

       A firewall monitoriza ligações de rede que utilizam os protocolos TCP, UDP, ICMP, ICMPv6, IGMP e GRE.

       Se selecionar um serviço de rede na lista suspensa **Nome**, a caixa de verificação **Protocolo** é selecionada automaticamente e a lista pendente junto à caixa de verificação contém o tipo de protocolo que corresponde ao serviço de rede selecionado. Por defeito, a caixa de verificação **Protocolo** está desmarcada.

11. Na lista suspensa **Direção**, selecione a direção da atividade de rede monitorizada.

    A firewall monitoriza ligações de rede com as seguintes direções:

    - **Entrada**.
    - **Entrada/Saída**.
    - **Saída**.

12. Se ICMP ou ICMPv6 estiver selecionado como protocolo, pode especificar o código e tipo de pacote ICMP:

    a. Selecione a caixa de verificação **Tipo de ICMP** e selecione o pacote ICMP na lista suspensa.

    b. Selecione a caixa de verificação **Código ICMP** e selecione o pacote ICMP na lista suspensa.

13. Se TCP ou UDP estiver selecionado como 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:

    a. Introduza as portas do computador remoto no campo **Portas Remotas**.

    b. Introduza as portas do computador local no campo **Portas Locais**.

14. Especificar os endereços da rede de computadores remotos que podem enviar e/ou receber pacotes de rede. Para tal, selecione um dos seguintes valores na lista pendente **Endereços remotos**:

    - **Qualquer endereço**. A regra de rede controla pacotes de rede enviados e/ou recebidos por computadores remotos com qualquer endereço IP.
    - **Endereços de sub-rede**. A regra de rede controla pacotes de rede enviados e/ou recebidos por computadores remotos com endereços IP associados ao tipo de rede selecionado: **Redes confiáveis**, **Redes locais** ou **Redes públicas**.
    - **Endereços da lista**. A regra de rede controla pacotes de rede enviados e/ou recebidos por computadores remotos com endereços IP que podem ser especificados na lista abaixo, utilizando os botões **Adicionar**, **Editar** e **Eliminar**.

15. Especificar os endereços de rede de computadores que têm o Kaspersky Endpoint Security instalado e podem enviar e/ou receber pacotes de rede. Para tal, selecione um dos seguintes valores na lista suspensa **Endereços locais**:

    - **Qualquer endereço**. A regra de rede controla pacotes de rede enviados e/ou recebidos por computadores com o Kaspersky Endpoint Security instalado e com qualquer endereço IP.
    - **Endereços da lista**. A regra de rede controla pacotes de rede enviados e/ou recebidos por computadores com o Kaspersky Endpoint Security instalado e com endereços IP que podem ser especificados na lista abaixo, utilizando os botões **Adicionar**, **Editar** e **Eliminar**.

    Por vezes, o endereço local não pode ser obtido para aplicações que funcionam com os pacotes de rede. Se este for o caso, o valor da definição das **Endereços locais** é ignorado.

16. Se pretender que as ações da regra de rede se reflitam no relatório, selecione a caixa de verificação **Registar eventos**.

17. Na janela **Regra de rede**, clique em **OK**.

    Se criou uma regra de rede nova, a regra é apresentada no separador **Regras de rede**.

18. Clique em **OK** na janela de **Regras de controlo de grupos de aplicações** se a regra se destinar a um grupo de aplicações, ou na janela **Regras de controlo das aplicações** se a regra se destinar a uma aplicação.

19. Na janela **Firewall**, clique em **OK**.

20. Para guardar as alterações, clique no botão **Guardar**.

Ativar e desativar uma regra de rede de aplicações

Para ativar ou desativar uma regra de rede de aplicações:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Firewall**.

   Na parte direita da janela, são apresentadas as definições do componente Firewall.
3. Clique no botão **Regras de rede de aplicações**.

   A janela **Firewall** é aberta no separador **Regras de controlo das aplicações**.
4. Na lista, selecione a aplicação ou o grupo de aplicações para o qual pretende ativar ou desativar uma regra de rede.
5. Clique com o botão direito para abrir o menu de contexto e selecione as **Regras de aplicações** ou as **Regras de grupos** dependendo do que necessita de fazer.

   Esta ação abre as **Regras de controlo das aplicações** ou a janela **Regras de controlo de grupos de aplicações**.
6. Na janela que é aberta, selecione o separador **Regras de rede**.
7. Na lista de regras de rede para um grupo de aplicações, selecione a regra de rede relevante.
8. Execute uma das seguintes ações:

   - Se pretender ativar a regra, selecione a caixa de verificação junto ao nome da regra de rede.
   - Se pretender desativar a regra, desmarque a caixa de verificação junto ao nome da regra de rede.

   > Não é possível desativar uma regra de rede de grupos de aplicações que seja criada, por defeito, pela Firewall.
9. Clique em **OK** na janela de **Regras de controlo de grupos de aplicações** se a regra se destinar a um grupo de aplicações, ou na janela **Regras de controlo das aplicações** se a regra se destinar a uma aplicação.
10. Na janela **Firewall**, clique em **OK**.
11. Para guardar as alterações, clique no botão **Guardar**.

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 defeito 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. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Firewall**.

   Na parte direita da janela, são apresentadas as definições do componente Firewall.
3. Clique no botão **Regras de rede de aplicações**.

   A janela **Firewall** é aberta no separador **Regras de controlo das aplicações**.
4. Se pretender alterar a ação da Firewall aplicada a todas as regras de rede que criadas por defeito, selecione uma aplicação ou grupo de aplicações na lista. As regras de rede criadas manualmente permanecem inalteradas.
5. Na coluna **Rede**, clique para apresentar o menu de contexto e selecione a ação que pretende atribuir:
   - **Herdar**
   - **Permitir**
   - **Bloquear**
6. Clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

Para alterar a resposta da Firewall para uma regra de rede, para uma aplicação ou grupo de aplicações:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione **Firewall**.

   Na parte direita da janela, são apresentadas as definições do componente Firewall.
3. Clique no botão **Regras de rede de aplicações**.

   A janela **Firewall** é aberta no separador **Regras de controlo das 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 para abrir o menu de contexto e selecione as **Regras de aplicações** ou as **Regras de grupos** dependendo do que necessita de fazer.

   Esta ação abre as **Regras de controlo das aplicações** ou a janela **Regras de controlo de grupos de aplicações**.
6. Na janela que é aberta, 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:
   - **Permitir**
   - **Bloquear**
   - **Registar eventos**

9. Clique em **OK** na janela de **Regras de controlo de grupos de aplicações** se a regra se destinar a um grupo de aplicações, ou na janela **Regras de controlo das aplicações** se a regra se destinar a uma aplicação.

10. Na janela **Firewall**, clique em **OK**.

11. Para guardar as alterações, clique no botão **Guardar**.

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 defeito.

Para alterar a prioridade de uma regra de rede de aplicações:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Firewall**.

   Na parte direita da janela, são apresentadas as definições do componente Firewall.

3. Clique no botão **Regras de rede de aplicações**.

   A janela **Firewall** é aberta no separador **Regras de controlo das 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 para abrir o menu de contexto e selecione as **Regras de aplicações** ou as **Regras de grupos** dependendo do que necessita de fazer.

   Esta ação abre as **Regras de controlo das aplicações** ou a janela **Regras de controlo de grupos de aplicações**.

6. Na janela que é aberta, selecione o separador **Regras de rede**.

7. Selecione a regra de rede cuja prioridade pretende editar.

8. Utilize os botões **Mover cima** e **Mover baixo** para mover a regra de rede para a localização pretendida na lista de regras de rede.

9. Clique em **OK** na janela de **Regras de controlo de grupos de aplicações** se a regra se destinar a um grupo de aplicações, ou na janela **Regras de controlo das aplicações** se a regra se destinar a uma aplicação.

10. Na janela **Firewall**, clique em **OK**.

11. Para guardar as alterações, clique no botão **Guardar**.

Monitor de Rede

Esta secção contém informações sobre o Monitor de Rede e instruções sobre como iniciar o Monitor de Rede.

Sobre o Monitor de Rede

O Monitor de Rede é uma ferramenta concebida para ver informações sobre a atividade de rede de um computador em tempo real.

Iniciar o Monitor de Rede

Para iniciar o Monitor de Rede:

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Proteção**.

   É aberta a secção **Proteção**.
4. Clique com o botão direito do rato sobre a linha **Firewall**, para abrir o menu de contexto para operações da Firewall.
5. No menu de contexto, selecione **Monitor de Rede**.

   É aberta a janela **Monitor de Rede**. 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.
   - O separador **Portas abertas** indica todas as portas de rede abertas do computador.
   - 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 Bloqueio de Ataques de Rede, após detetar tentativas de ataque de rede provenientes desses endereços IP.

Bloqueio de Ataques de Rede

Esta secção contém informações sobre o Bloqueio de Ataques de Rede e instruções sobre como configurar as definições do componente.

Sobre o Bloqueio de Ataques de Rede

O Bloqueio de Ataques de Rede verifica o tráfego de rede de entrada quanto à existência de atividades típicas de ataques de rede. Mediante a deteção de uma tentativa de ataque de rede dirigida ao computador, o Kaspersky Endpoint Security bloqueia a atividade de rede do computador atacante. O seu ecrã apresenta então um aviso que afirma que ocorreu uma tentativa de ataque à rede e apresenta informação sobre o computador de ataque.

O tráfego de rede do computador atacante é bloqueado durante uma hora. Pode editar as definições de bloqueio de um 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 Bloqueio de Ataques de Rede deteta é atualizada durante as atualizações da base de dados e do módulo de aplicação.

Ativar e desativar o Bloqueio de Ataques de Rede

Por defeito, o Bloqueio de Ataques de Rede está ativado, funcionando em modo otimizado. Se necessário, pode desativar o Bloqueio de Ataques de Rede.

Existem duas formas para ativar ou desativar o componente:

- No separador **Proteção e Controlo** na janela principal da aplicação
- Na janela de definições da aplicação

Para ativar ou desativar o Bloqueio de Ataques de Rede, proceda do seguinte modo no separador Proteção e Controlo da janela principal da aplicação:

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Proteção**.

   É aberta a secção **Proteção**.
4. Clique com o botão direito do rato na linha **Bloqueio de Ataques de Rede** para visualizar o menu de contexto das ações do Bloqueio de Ataques de Rede.
5. Execute uma das seguintes ações:

   - Para ativar o Bloqueio de Ataques de Rede, selecione **Iniciar** no menu de contexto.

     O ícone de estado do componente apresentando à esquerda da linha **Bloqueio de Ataques de Rede** é alterado para o ícone .
   - Para desativar o Bloqueio de Ataques de Rede, selecione **Parar** no menu de contexto.

O ícone de estado do componente apresentando à esquerda da linha **Bloqueio de Ataques de Rede** é alterado para o ícone .

Para ativar ou desativar o Bloqueio de Ataques de Rede na janela de definições da aplicação:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Bloqueio de Ataques de Rede**.

   As configurações do Bloqueio de Ataques de Rede são apresentadas na parte direita da janela.
3. Execute as seguintes ações:

   - Para ativar o Bloqueio de Ataques de Rede, selecione a caixa de verificação **Ativar Bloqueio de Ataques de Rede**.
   - Para desativar o Bloqueio de Ataques de Rede, desmarque a caixa de verificação **Ativar Bloqueio de Ataques de Rede**.
4. Para guardar as alterações, clique no botão **Guardar**.

Configurações de Bloqueio de Ataques de Rede

Pode executar as seguintes ações para configurar as configurações de Bloqueio de Ataques de Rede:

- Configurar as definições utilizadas para bloquear um computador atacante.
- Gerar uma lista de moradas de exclusões do bloqueio.

Editar as definições utilizadas no bloqueio de um computador atacante

Para editar as definições de bloqueio de um computador atacante:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Bloqueio de Ataques de Rede**.

   As configurações do Bloqueio de Ataques de Rede são apresentadas na parte direita da janela.
3. Selecione a caixa de verificação **Adicionar computador atacante à lista de computadores bloqueados durante**.

   Se esta caixa de verificação estiver selecionada, ao detetar uma tentativa de ataque de rede, o Bloqueio de Ataques de Rede bloqueia o tráfego de rede proveniente do computador atacante durante o período de tempo específico. Deste modo, o computador é protegido automaticamente contra eventuais futuros ataques de rede provenientes do mesmo endereço.

   Se esta caixa de verificação estiver desmarcada, ao detetar uma tentativa de ataque de rede, o Bloqueio de Ataques de Rede não ativa a proteção automática contra eventuais futuros ataques de rede provenientes do mesmo endereço.

4. Pode alterar o período de tempo durante o qual um computador atacante é bloqueado no campo junto à caixa de verificação **Adicionar computador atacante à lista de computadores bloqueados durante**.

5. Para guardar as alterações, clique no botão **Guardar**.

Configurar moradas de exclusões de bloqueio

Para configurar moradas de exclusões de bloqueio:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Bloqueio de Ataques de Rede**.

   As configurações do Bloqueio de Ataques de Rede são apresentadas na parte direita da janela.

3. Clique no botão **Exclusões**.

   É apresentada a janela **Exclusões**.

4. Execute uma das seguintes ações:

   - Se pretender adicionar um novo endereço IP, clique no botão **Adicionar**.
   - Se quiser editar um endereço IP adicionado anteriormente, selecione-a na lista de endereços e clique no botão **Editar**.

   É apresentada a janela **Endereço IP**.

5. Introduza o endereço IP do computador para o qual não devem ser bloqueados os ataques de rede.

6. Na janela **Endereço IP**, clique em **OK**.

7. Na janela **Exclusões**, clique em **OK**.

8. Para guardar as alterações, clique no botão **Guardar**.

Prevenção de ataques BadUSB

Esta secção contém informações sobre o componente Prevenção de ataques BadUSB.

Sobre a 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.

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 pela aplicação como teclado, a aplicação solicita ao utilizador que introduza um código numérico gerado pela aplicação deste teclado ou utilizando um teclado no ecrã (se estiver disponível). Este procedimento é conhecido como autorização de teclado. A aplicação permite a utilização de um teclado autorizado e bloqueia um teclado que não foi autorizado.

A prevenção de ataques BadUSB é executada em modo de segundo plano logo que este componente seja instalado. Se a aplicação não estiver sujeita a uma política do Kaspersky Security Center, pode ativar ou desativar a Prevenção de ataques BadUSB fazendo uma pausa temporária e retomando a proteção e o controlo do computador.

Instalar o componente Prevenção de ataques BadUSB

Se selecionou a instalação básica ou padrão durante a instalação do Kaspersky Endpoint Security, o componente Prevenção de ataques BadUSB não estará disponível. Para o instalar, deve alterar o conjunto de componentes da aplicação.

Para instalar o componente Prevenção de ataques BadUSB:

1. No menu **Iniciar**, selecione **Aplicações → Kaspersky Endpoint Security 10 for Windows → Modificar, Reparar ou Remover.**

   O Assistente de Instalação é iniciado.

2. Na janela **Modificar, Reparar ou Remover a aplicação** do Assistente de Instalação da Aplicação, clique no botão **Modificar**.

   Esta ação abre a janela **Instalação personalizada** do Assistente de Instalação da Aplicação.

3. No menu de contexto do ícone ao lado do nome do componente **Prevenção de ataques BadUSB**, selecione a opção **O recurso será instalado na unidade de disco rígido local**.

4. Clique no botão **Seguinte**.

5. Siga as instruções do Assistente de Instalação.

Ativar e desativar Prevenção de ataques BadUSB

Para ativar ou desativar a Proteção contra ataques BadUSB:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Prevenção de ataques BadUSB**.

   As definições da Prevenção de ataques BadUSB são apresentadas na parte direita da janela.
3. Execute uma das seguintes ações:

   - Para ativar a Prevenção de ataques BadUSB, selecione a caixa de verificação **Ativar prevenção de ataques BadUSB**.
   - Para desativar a Prevenção de ataques BadUSB, desmarque a caixa de verificação **Ativar prevenção de ataques BadUSB**.
4. Para guardar as alterações, clique no botão **Guardar**.

Permitir e proibir o uso do teclado no ecrã para autorização

O teclado no ecrã apenas deve ser usado para a autorização de dispositivos USB que não suportam a introdução de carateres aleatórios (p. ex., leitores de códigos de barras). Não se recomenda 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. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Proteção de Antivírus**, selecione a subsecção **Prevenção de ataques BadUSB**.

   As definições do componente são apresentadas na parte direita da janela.
3. Execute uma das seguintes ações:

   - Selecione a caixa de verificação **Proibir a utilização do teclado no ecrã para autorização** para bloquear a utilização do teclado no ecrã para autorização.
   - Desmarque a caixa de verificação **Proibir a utilização do teclado no ecrã para autorização** para permitir a utilização do teclado no ecrã para autorização.
4. Para guardar as alterações, clique no botão **Guardar**.

Autorização de teclado

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.

A aplicação apenas necessita da autorização do dispositivo USB ligado que foi identificado pelo sistema operativo como teclado se a solicitação de autorização do teclado USB estiver ativada. O utilizador não pode usar um teclado não autorizado até que este seja autorizado.

Se a solicitação de autorização do teclado USB estiver desativada, o utilizador pode usar todos os teclados ligados. Imediatamente após a solicitação de autorização do teclado USB ser ativada, a aplicação mostra uma solicitação para autorização de cada teclado não autorizado que está ligado.

Para autorizar um teclado:

1. Com a autorização do teclado USB ativada, ligue o teclado a uma porta USB.

   É apresentada a janela **autorização de teclado <Nome do teclado>** com os detalhes do teclado ligado e um código numérico para a respetiva autorização.

2. Introduza o código numérico gerado aleatoriamente na janela de autorização a partir do teclado ligado ou do teclado no ecrã (se disponível).

3. Clique em **OK**.

   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 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. Existem três tentativas para introduzir o código numérico. Se o código numérico for introduzido incorretamente três vezes seguidas ou a janela de **autorização de teclado <Nome do teclado>** for fechada, a aplicação bloqueia a ativação deste teclado. Quando o teclado volta a ser ligado ou o sistema operativo é reiniciado, a aplicação solicita ao utilizador que execute novamente a autorização do teclado.

Controlo de Arranque das Aplicações

Esta secção contém informações sobre o Controlo de Arranque das Aplicações e instruções para efetuar as configurações do componente.

Sobre o Controlo de Arranque das Aplicações

O componente Controlo de Arranque das Aplicações monitoriza as tentativas do utilizador de iniciar aplicações e regula o arranque de aplicações utilizando as *regras de Controlo de Arranque das Aplicações*.

O arranque das aplicações cujos parâmetros não correspondem a nenhuma das regras de Controlo de Arranque das Aplicações é regulado pelo modo operativo selecionado do componente. O *Modo Lista negra* está selecionado por defeito. Este modo permite a qualquer utilizador iniciar qualquer aplicação.

Todas as tentativas do utilizador para iniciar aplicações são registadas nos relatórios.

Ativar e desativar o Controlo de Arranque das Aplicações

Embora o Controlo de Arranque da Aplicação esteja desativado por predefinição, pode ativá-lo, se necessário.

Existem duas formas para ativar ou desativar o componente:

- No separador **Proteção e Controlo** da janela principal da aplicação
- Na janela de definições da aplicação

Para ativar ou desativar o Controlo de Arranque das Aplicações no separador Proteção e Controlo da janela principal da aplicação:

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Controlo de terminal**.

   A secção **Controlo de terminal** é apresentada.
4. Clique com o botão direito do rato para visualizar o menu da linha que contém as informações sobre o componente Controlo de Arranque das Aplicações.

   É aberto um menu para selecionar ações no componente.
5. Execute uma das seguintes ações:

   - Para ativar o Controlo de Arranque das Aplicações, selecione **Iniciar** no menu.

     O ícone de estado do componente , que é apresentado à esquerda na linha do **Controlo de Arranque das Aplicações**, é alterado para o ícone .
   - Para desativar o componente Controlo de Arranque das Aplicações, selecione **Parar** no menu.

     O ícone de estado do componente , que é apresentado à esquerda na linha do **Controlo de Arranque das Aplicações**, é alterado para o ícone .

Para ativar ou desativar o Controlo de Arranque das Aplicações na janela de configurações das aplicações:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Arranque das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Arranque das Aplicações.
3. Execute uma das seguintes ações:

   - Para ativar o Controlo de Arranque das Aplicações, selecione a caixa de verificação **Ativar Controlo de Arranque das Aplicações**.
   - Para desativar o Controlo de Arranque das Aplicações, desmarque a caixa de verificação **Ativar Controlo de Arranque das Aplicações**.
4. Para guardar as alterações, clique no botão **Guardar**.

Limitações da funcionalidade de Controlo de Arranque das Aplicações

A operação do componente Controlo de Arranque das Aplicações está limitada nos seguintes casos:

- Quando a versão da aplicação é atualizada, não é suportada a importação da definições do componente Controlo de Arranque das Aplicações.

  Para restaurar a funcionalidade do Controlo de Arranque das Aplicações, é necessário configurar novamente as definições do 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. Se as bases de dados locais não contiverem informações sobre a aplicação, a aplicação não será categorizada num grupo de confiança.

  A categorização de aplicações quando existe uma ligação aos servidores da KSN pode ser diferente da categorização quando não existe ligação com a 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 linha de comandos.

  Se o arranque de um interpretador for autorizado pelas regras de Controlo de Arranque das Aplicações, o componente não irá bloquear um script iniciado a partir deste interpretador.

- 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:

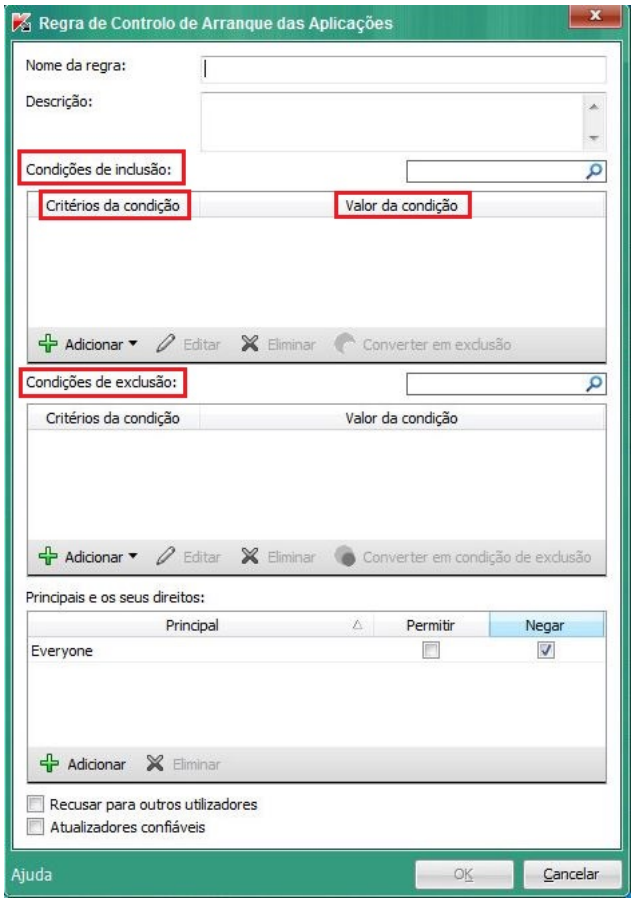
  - { cCmdLineParser::itCmd, _T("%ComSpec%") };
  - { cCmdLineParser::itReg, _T("%SystemRoot%\\system32\\reg.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedit.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\regedit.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedt32.exe") };
  - { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\cscript.exe") };
  - { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\wscript.exe") };
  - { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\system32\\msiexec.exe") };
  - { cCmdLineParser::itMmc, _T("%SystemRoot%\\system32\\mmc.exe") };
  - { cCmdLineParser::itMshta, _T("%SystemRoot%\\system32\\mshta.exe") };
  - { cCmdLineParser::itRundll, _T("%SystemRoot%\\system32\\rundll32.exe") };
  - { cCmdLineParser::itMetro, _T("%SystemRoot%\\system32\\wwahost.exe") };
  - { cCmdLineParser::itCmd, _T("%SystemRoot%\\syswow64\\cmd.exe") };
  - { cCmdLineParser::itReg, _T("%SystemRoot%\\syswow64\\reg.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedit.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedt32.exe") };
  - { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\cscript.exe") };
  - { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\wscript.exe") };
  - { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\syswow64\\msiexec.exe") };
  - { cCmdLineParser::itMmc, _T("%SystemRoot%\\syswow64\\mmc.exe") };
  - { cCmdLineParser::itMshta, _T("%SystemRoot%\\syswow64\\mshta.exe") };
  - { cCmdLineParser::itRundll, _T("%SystemRoot%\\syswow64\\rundll32.exe") };
  - { cCmdLineParser::itMetro, _T("%SystemRoot%\\syswow64\\wwahost.exe") }.

Sobre as regras de Controlo de Arranque das Aplicações

O Kaspersky Endpoint Security controla o arranque das aplicações por utilizadores por meio de regras. Uma regra de Controlo de Arranque das Aplicações especifica as condições de ativação e a ação executada pelo Controlo de Arranque das Aplicações quando a regra é ativada (permitindo ou bloqueando o arranque da aplicação por utilizadores).

Condições de ativação de regras

Uma condição de ativação de regras tem a seguinte correspondência: "tipo de condição - valor do critério - valor da condição" (consulte a figura abaixo). Com base nas condições de ativação de regras, o Kaspersky Endpoint Security aplica (ou não aplica) uma regra a uma aplicação.



Regra de Controlo de Arranque das Aplicações. Parâmetros da condição de ativação de regras

As regras usam condições de inclusão e exclusão:

- *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, principal, 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 de Arranque 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 de Arranque das Aplicações não controla o arranque da aplicação.

Decisões tomadas pelo componente Controlo de Arranque das Aplicações quando uma regra é ativada

Quando uma regra é ativada, o Controlo de Arranque 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 de Arranque das Aplicações foi configurada para um grupo de utilizadores e uma regra de bloqueio de Controlo de Arranque das Aplicações foi configurada para um utilizador do grupo, este utilizador estará impedido de iniciar a aplicação.

Estado operacional de uma regra

As regras de Controlo de Arranque das Aplicações podem ter um de dois valores de estado operacional:

- **Ativado.**

  Este estado operacional da regra significa que a regra está ativada.

- **Desativado.**

  Este estado de regra significa que a regra foi desativada.

Regras de Controlo de Arranque das Aplicações predefinidas

Por defeito, o Controlo de Arranque das Aplicações opera no modo Lista Negra. Este componente permite que todos os utilizadores iniciem todas as aplicações. Quando um utilizador tenta iniciar uma aplicação bloqueada por regras de Controlo de Arranque das Aplicações, o Kaspersky Endpoint Security bloqueia o arranque desta aplicação (se estiver selecionada a ação **Bloquear**) ou guarda informação relativa ao arranque da aplicação num relatório (se a ação **Notificar** estiver selecionada).

Gerir regras de Controlo de Arranque das Aplicações

Pode executar as seguintes ações para as regras de Controlo de Arranque das Aplicações:

- Adicionar uma nova regra
- Criar ou alterar as condições para a ativação de uma regra
- Editar o estado da regra

  Pode estar ativada uma regra de Controlo de Arranque das Aplicações (a caixa à frente da regra está selecionada) ou desativada (a caixa em frente à regra está desmarcada). Uma regra de Controlo de Arranque das Aplicações está ativada por defeito após a sua criação.
- Eliminar regra

Adicionar e editar uma regra de Controlo de Arranque das Aplicações

Para adicionar ou editar uma regra de Controlo de Arranque das Aplicações:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Arranque das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Arranque das Aplicações.
3. Selecione **Ativar Controlo de Arranque das Aplicações** para colocar as definições do componente disponíveis para edição.
4. Execute uma das seguintes ações:

   - 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**.

   É aberta a janela **Regra de Controlo de Arranque das Aplicações**.
5. Especifique ou edite as definições da regra:

   a. No campo **Nome da regra**, introduza ou edite o nome da regra.

   b. Na tabela **Condições de inclusão**, crie ou edite a lista de condições de inclusão que ativam uma regra clicando nos botões **Adicionar**, **Editar**, **Eliminar** e **Converter em exclusão**.

   c. Na tabela **Condições de exclusão**, crie ou edite a lista de condições de exclusão que ativam uma regra clicando nos botões **Adicionar**, **Editar**, **Eliminar** e **Converter em condição de exclusão**.

   d. Se for necessário, altere o tipo de condição de ativação de regras:

- Para alterar o tipo de condição de uma condição de inclusão para uma condição de exclusão, selecione uma condição na tabela **Condições de inclusão** e clique no botão **Converter em exclusão**.

- Para alterar o tipo de condição de uma condição de exclusão para uma condição de inclusão, selecione uma condição na tabela **Condições de exclusão** e clique no botão **Converter em condição de exclusão**.

e. 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 **Principais e os seus direitos**.

É aberta a janela **Selecionar Utilizadores ou Grupos** no Microsoft Windows. Esta janela permite selecionar utilizadores e/ou grupos de utilizadores.

Por defeito, 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.

f. Na tabela **Principais e os seus direitos** selecione as caixas de verificação **Permitir** ou **Bloquear** localizadas à frente dos utilizadores e/ou grupos de utilizadores para determinar o seu direito de iniciar aplicações.

A caixa que está selecionada por defeito depende do Modo operativo do Controlo de Arranque das Aplicações.

g. Selecione a caixa de verificação **Recusar para outros utilizadores** se pretender que todos os utilizadores que não são apresentados na coluna **Principal** e que não façam parte do grupo de utilizadores especificado na coluna **Principal** sejam impedidos de iniciar aplicações que cumpram as condições de ativação de regras.

> 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 **Principais e os seus direitos** e que não pertencem aos grupos de utilizadores especificados na tabela **Principais e os seus direitos**.

h. Se pretender que o Kaspersky Endpoint Security considere as aplicações correspondentes às condições de ativação de regras enquanto atualizadores confiáveis com permissão para iniciar outras aplicações para as quais não estão definidas regras do Controlo de Arranque das Aplicações, selecione a caixa de verificação **Atualizadores confiáveis**.

6. Clique em **OK**.

7. Para guardar as alterações, clique no botão **Guardar**.

Adicionar uma condição de ativação para uma regra de Controlo de Arranque das Aplicações

Adicionar uma nova condição de ativação para uma regra de Controlo de Arranque das Aplicações:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Arranque das Aplicações**.

Na parte direita da janela, são apresentadas as configurações do componente Controlo de Arranque das Aplicações.

3. Selecione **Ativar Controlo de Arranque das Aplicações** para colocar as definições do componente disponíveis para edição.

4. Execute uma das seguintes ações:

   - Se pretende criar uma nova regra e adicionar-lhe uma condição de ativação, clique no botão **Adicionar**.
   - Se pretende adicionar uma condição de ativação a uma regra existente, selecione a regra na lista de regras e clique no botão **Editar**.

   É aberta a janela **Regra de Controlo de Arranque das Aplicações**.

5. Nas **Condições de inclusão** ou na tabela **Condições de exclusão**, clique no botão **Adicionar**.

Pode usar a lista pendente do botão **Adicionar** para adicionar várias condições de ativação à regra (consulte as instruções abaixo).

Adicionar uma condição de ativação de regras baseada nas propriedades dos ficheiros na pasta especificada:

1. Na lista pendente do botão **Adicionar**, selecione **Condição(ões) das propriedades dos ficheiros na pasta especificada**.

   É aberta a janela padrão **Selecionar pasta** no Microsoft Windows.

2. Na janela **Selecionar pasta**, selecione uma pasta que contenha os ficheiros executáveis de aplicações cujas propriedades pretenda utilizar como base para uma ou várias condições de ativação de uma regra.

3. Clique em **OK**.

   É aberta a janela **Adicionar condição**.

4. Na lista pendente **Mostrar critério**, selecione o critério conforme pretenda criar uma ou várias condições de ativação de regras: **Código hash do ficheiro**, **Certificado**, **Categoria KL**, **Metadados** ou **Caminho da pasta**.

   O Kaspersky Endpoint Security não suporta um código hash do ficheiro MD5 e não controla o início das aplicações com base num hash MD5. Um hash de SHA256 é utilizado como uma condição de ativação de regras.

5. Se selecionou **Metadados** na lista pendente **Mostrar critério**, selecione as caixas de verificação à frente das propriedades do ficheiro executável que pretende utilizar na condição de ativação de regras: **Nome de ficheiro**, **Versão do ficheiro**, **Nome da aplicação**, **Versão da aplicação** e **Fornecedor**.

   Se nenhuma das propriedades especificadas estiver selecionada, a regra não pode ser guardada.

6. Se selecionou **Certificado** na lista pendente **Mostrar critério**, selecione as caixas de verificação à frente das definições que pretende utilizar na condição de ativação de regras: **Emissor**, **Principal** e **Thumbprint**.

   Se nenhuma das definições especificadas estiver selecionada, a regra não pode ser guardada.

   Não é recomendado que se utilize apenas os critérios **Emissor** e **Principal** como condições de ativação de regras. A utilização destes critérios não é segura.

7. Selecione as caixas de verificação à frente dos nomes dos ficheiros executáveis de aplicações cujas propriedades pretende incluir nas condições de ativação de regras.

8. Clique no botão **Seguinte**.

   É apresentada uma lista de condições formuladas de ativação da regra.

9. Na lista de condições formuladas de ativação da regra, selecione as caixas de verificação em frente às condições de ativação da regra que pretende adicionar à regra de Controlo de Arranque das Aplicações.

10. Clique no botão **Terminar**.

Adicionar uma condição de ativação de regras baseada nas propriedades das aplicações iniciadas no computador:

1. Na lista pendente do botão **Adicionar**, selecione **Condição(ões) das propriedades das aplicações iniciadas**.

2. Na janela **Adicionar condição**, na lista pendente **Mostrar critério**, selecione o critério conforme pretenda criar uma ou várias condições de ativação de regras: **Código hash do ficheiro**, **Certificado**, **Categoria KL**, **Metadados** ou **Caminho da pasta**.

3. Se selecionou **Metadados** na lista pendente **Mostrar critério**, selecione as caixas de verificação à frente das propriedades do ficheiro executável que pretende utilizar na condição de ativação de regras: **Nome de ficheiro**, **Versão do ficheiro**, **Nome da aplicação**, **Versão da aplicação** e **Fornecedor**.

   Se nenhuma das propriedades especificadas estiver selecionada, a regra não pode ser guardada.

4. Se selecionou **Certificado** na lista pendente **Mostrar critério**, selecione as caixas de verificação à frente das definições que pretende utilizar na condição de ativação de regras: **Emissor**, **Principal** e **Thumbprint**.

   Se nenhuma das definições especificadas estiver selecionada, a regra não pode ser guardada.

   > Não é recomendado que se utilize apenas os critérios **Emissor** e **Principal** como condições de ativação de regras. A utilização destes critérios não é segura.

5. Selecione as caixas de verificação à frente dos nomes dos ficheiros executáveis de aplicações cujas propriedades pretende incluir nas condições de ativação de regras.

6. Clique no botão **Seguinte**.

   É apresentada uma lista de condições formuladas de ativação da regra.

7. Na lista de condições formuladas de ativação da regra, selecione as caixas de verificação em frente às condições de ativação da regra que pretende adicionar à regra de Controlo de Arranque das Aplicações.

8. Clique no botão **Terminar**.

Adicionar uma condição de ativação de regras baseada numa categoria KL:

1. Na lista pendente debaixo do botão **Adicionar**, selecione **Condição(ões) "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 de "aplicações do Office" inclui as aplicações do conjunto de programas do Microsoft Office, Adobe® Acrobat® e outros.

2. Na janela **Condição(ões) "Categoria KL"**, selecione as caixas de verificação ao lado dos nomes das categorias KL com base nas quais pretende criar condições de ativação de regras.

3. Clique em **OK**.

Adicionar uma condição de ativação de regras personalizada:

1. Na lista pendente do botão **Adicionar**, selecione **Condição personalizada**.

2. Na janela **Condição personalizada**, clique no botão **Selecionar** e especifique o caminho para o ficheiro executável da aplicação.

3. Selecionar o critério no qual pretende basear a criação de uma condição de ativação de regras: **Código hash do ficheiro**, **Certificado**, **Metadados** ou **Caminho para o ficheiro ou pasta**.

   Se estiver a utilizar ligações simbólicas no campo **Caminho para o ficheiro ou pasta**, aconselhamo-lo a resolver as ligações simbólicas para o funcionamento correto da regra de Controlo de Arranque das Aplicações. Para tal, clique no botão **Resolver ligação simbólica**.

4. Se necessário, configure as definições do critério selecionado.

5. Clique em **OK**.

Adicionar uma condição de ativação de regras baseada na informação sobre a unidade que guarda o ficheiro executável de uma aplicação:

1. Na lista pendente do botão **Adicionar**, selecione **Condição por unidade de ficheiro**.

2. Na janela **Condição por unidade de ficheiro**, na lista pendente **Unidade**, selecione o tipo de unidade a partir da qual o início de aplicações irá funcionar como uma condição de ativação de regras.

3. Clique em **OK**.

Alterar o estado de uma regra de Controlo de Arranque das Aplicações

Para alterar o estado de uma regra de Controlo de Arranque das Aplicações:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Arranque das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Arranque das Aplicações.

3. Selecione **Ativar Controlo de Arranque das Aplicações** para colocar as definições do componente disponíveis para edição.

4. Selecione a regra cujo estado pretende editar.

5. Na coluna **Estado**, execute as seguintes ações:

   - Se pretender ativar a utilização de uma regra, selecione a caixa de verificação à frente da regra.
   - Se pretender desativar a utilização de uma regra, desmarque a caixa de verificação à frente da regra.

6. Para guardar as alterações, clique no botão **Guardar**.

Teste das regras de Controlo de Arranque das Aplicações

Para assegurar que as regras de Controlo de Arranque das Aplicações não bloqueiam aplicações necessárias para o trabalho, recomenda-se que as regras criadas recentemente sejam colocadas em modo de teste e que a sua operação seja analisada.

Uma análise ao funcionamento das regras do Controlo de Arranque das Aplicações requer uma revisão dos eventos do Controlo de Arranque das Aplicações reportados ao Kaspersky Security Center. Se for possível iniciar todas as aplicações necessárias ao trabalho do utilizador do computador, as regras foram criadas corretamente. Caso contrário, recomendamos a revisão das definições das regras que criou.

O modo de teste de regras de Controlo de Arranque das Aplicações está desativado por defeito.

Para testar as regras de Controlo de Arranque das Aplicações:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Arranque das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Arranque das Aplicações.
3. Selecione **Ativar Controlo de Arranque das Aplicações** para colocar as definições do componente disponíveis para edição.
4. Na lista pendente **Modo de Controlo de Arranque das Aplicações**, selecione um dos seguintes itens:

   - **Lista Negra**, se pretende permitir o arranque de todas as aplicações exceto das aplicações especificadas nas regras de bloqueio.
   - **Lista Branca**, se pretende bloquear o arranque de todas as aplicações exceto das aplicações especificadas nas regras de bloqueio.
5. Na lista pendente **Ação**, selecione **Notificar**.
6. Para guardar as alterações, clique no botão **Guardar**.

O Kaspersky Endpoint Security não irá bloquear aplicações cujo arranque é proibido pelas regras de Controlo de Arranque das Aplicações, mas enviará notificações sobre o seu arranque para o Servidor de Administração.

Editar modelos de mensagens de Controlo de Arranque das Aplicações

Quando um utilizador tenta iniciar uma aplicação bloqueada por uma regra de Controlo de Arranque das Aplicações, o Kaspersky Endpoint Security apresenta uma mensagem que declara que o início 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. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Arranque das Aplicações**.

Na parte direita da janela, são apresentadas as configurações do componente Controlo de Arranque das Aplicações.

3. Selecione **Ativar Controlo de Arranque das Aplicações** para colocar as definições do componente disponíveis para edição.

4. Clique no botão **Modelos**.

   É apresentada a janela **Modelos de mensagem**.

5. Execute uma das seguintes ações:

   - Se pretender editar o modelo da mensagem apresentada quando o início de uma aplicação está bloqueado, selecione o separador **Bloqueio**.

   - Se pretender modificar o modelo da mensagem que é enviada ao administrador da rede local, selecione o separador **Mensagem para o administrador**.

6. Alterar o modelo da mensagem que é apresentada quando o arranque de uma aplicação é bloqueado ou a mensagem enviada ao administrador. Para tal, utilize os botões **Predefinições** e **Variável**.

7. Clique em **OK**.

8. Para guardar as alterações, clique no botão **Guardar**.

Sobre os modos de funcionamento do Controlo de Arranque das Aplicações

O componente Controlo de Arranque das Aplicações funciona em dois modos:

- **Lista Negra**. Neste modo, o Controlo de Arranque das Aplicações permite que todos os utilizadores iniciem todas as aplicações, exceto as aplicações especificadas nas regras de bloqueio do Controlo de Arranque das Aplicações.

  Este modo do Controlo de Arranque das Aplicações está ativado, por defeito.

- **Lista Branca**. Neste modo, o Controlo de Arranque das Aplicações impede todos os utilizadores de iniciar quaisquer aplicações, exceto as aplicações especificadas nas regras de permissão do Controlo de Arranque das Aplicações.

  Se as regras de permissão do Controlo de Arranque 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 confiáveis das quais os utilizadores dependem para a realização das suas tarefas.

Cada modo tem duas ações que podem ser executadas em aplicações em funcionamento: o Kaspersky Endpoint Security pode bloquear o arranque das aplicações ou notificar o utilizador sobre o arranque de uma aplicação que corresponde às condições das regras do Controlo de Arranque das Aplicações.

O Controlo de Arranque das Aplicações pode ser configurado para funcionar nestes modos utilizando 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 do Controlo de Arranque das Aplicações na Consola de Administração do Kaspersky Security Center baseiam-se nas categorias de aplicações predefinidas 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.

Por este motivo, recomenda-se a utilização do Kaspersky Security Center para configurar o funcionamento do componente Controlo de Arranque das Aplicações.

Selecionar o modo de Controlo de Arranque das Aplicações

Para selecionar o modo de Controlo de Arranque das Aplicações:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Arranque das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Arranque das Aplicações.
3. Selecione **Ativar Controlo de Arranque das Aplicações** para colocar as definições do componente disponíveis para edição.
4. Na lista pendente **Modo de Controlo de Arranque das Aplicações**, selecione uma das seguintes opções:

   - **Lista Negra**, se pretende permitir o arranque de todas as aplicações exceto das aplicações especificadas nas regras de bloqueio.
   - **Lista Branca**, se pretende bloquear o arranque de todas as aplicações exceto das aplicações especificadas nas regras de bloqueio.

     Quando este modo está selecionado, são criadas por defeito duas regras de Controlo de Arranque das Aplicações: **Golden Image** e **Atualizadores Confiáveis**. Não é possível eliminar estas regras. As definições destas regras não podem ser editadas. Pode ativar ou desativar estas regras selecionando ou desmarcando a caixa de verificação à frente da regra relevante. Por defeito, a regra **Golden Image** está ativada, e a regra **Atualizadores Confiáveis** 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 reverter a utilização destas regras, tudo que necessita de fazer é selecionar o modo necessário na lista pendente do **Modo de Controlo de Arranque das Aplicações**.
5. Na lista pendente **Ação**, selecione a ação a ser executada pelo componente quando um utilizador tenta iniciar uma aplicação bloqueada pelas regras de Controlo de Arranque das Aplicações.
6. Selecione a caixa de verificação **Monitorizar DLL e controladores** se pretender que o Kaspersky Endpoint Security monitorize o carregamento de módulos DLL quando as aplicações são iniciadas por utilizadores.

   A informação sobre o módulo e a aplicação que carregou o módulo será guardada num relatório.

Se a caixa de verificação estiver selecionada, os módulos DLL e os controladores são monitorizados antes de o Kaspersky Endpoint Security ser iniciado. Para configurar a monitorização subsequente de todos os módulos DLL e controladores antes do arranque da aplicação, reinicie o computador depois de selecionar a caixa de verificação **Monitorizar DLL e controladores**. Se não conseguir reiniciar o computador, depois de selecionar a caixa de verificação **Monitorizar DLL e controladores** pode carregar módulos DLL e controladores enquanto o Kaspersky Endpoint Security está a ser executado. Neste caso, a monitorização só entra em vigor para os módulos DLL e controladores que sejam carregados enquanto o Kaspersky Endpoint Security está a ser executado.

Durante a monitorização de módulos DLL e controladores, não se recomenda a utilização de regras de Controlo de Arranque das Aplicações que tenham sido criadas com base em categorias KL. A determinação de categorias KL (incluindo nas regras "Sistema operativo e os seus componentes") para módulos DLL e controladores pode não funcionar corretamente. Em particular, a regra "Sistema operativo e os seus componentes" foi criada por predefinição e não é distribuída na execução de módulos DLL e controladores. Quando se ativar esta função, é necessário criar regras separadas de permissão para módulos DLL e controladores. Utilizar a função **Controlar DLL e controladores** se essas regras de permissão não existirem pode tornar o sistema instável.

Recomendamos que a proteção por password seja ativada para configurar as definições do programa, para que seja possível desativar regras de permissão que bloqueiam a execução de módulos DLL e controladores criticamente importantes não modificando as definições da política do Kaspersky Security Center no processo.

7. Para guardar as alterações, clique no botão **Guardar**.

Gerir regras do Controlo de Arranque das Aplicações utilizando o Kaspersky Security Center

Esta secção contém informações sobre a utilização do Kaspersky Security Center para configurar as regras de Controlo de Arranque das Aplicações e fornece recomendações sobre a utilização ótima do Controlo de Arranque das Aplicações.

Recolher informações sobre as aplicações instaladas nos computadores dos utilizadores

Para criar regras do Controlo de Arranque das Aplicações ótimas, é recomendado que primeiro tenha uma perspetiva das aplicações que são utilizadas nos computadores na rede local. 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 **Registo das aplicações** 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 Network Agent 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**.

Criar categorias de aplicações

Para mais conveniência durante a criação de regras, pode criar categorias de aplicações e utilizá-las ao criar regras de Controlo de Arranque das Aplicações.

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, selecione a pasta **Adicional** → **Gestão de aplicações** → **Categorias da aplicação**.
3. Clique no botão **Criar categoria** 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.

Criar regras do Controlo de Arranque das Aplicações utilizando o Kaspersky Security Center

Criar uma regra de Controlo de Arranque das Aplicações utilizando o Kaspersky Security Center:

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 pretendida.
5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:

- No menu de contexto da política, selecione **Propriedades**.
- Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.

6. Na secção **Controlo de terminal**, selecione a secção **Controlo de Arranque das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Arranque das Aplicações.

7. Clique no botão **Adicionar**.

   É aberta a janela **Regra de Controlo de Arranque das Aplicações**.

8. Na lista pendente **Categoria**, selecione a categoria de aplicação criada com base na qual pretende criar uma regra.

9. 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. Para tal, na tabela **Principais e os seus direitos**, clique no botão **Adicionar**.

   É aberta a janela padrão **Selecionar Utilizadores ou Grupos** no Microsoft Windows. Esta janela permite selecionar utilizadores e/ou grupos de utilizadores.

10. Na tabela **Principais e os seus direitos**:

    - Se pretender permitir que os utilizadores e / ou os grupos de utilizadores iniciem aplicações que pertencem à categoria selecionada, selecione as caixas de verificação **Permitir** à frente desses utilizadores.
    - Se pretender bloquear esses utilizadores e / ou os grupos de utilizadores de iniciar aplicações que pertencem à categoria selecionada, selecione as caixas de verificação **Bloquear** à frente desses utilizadores.

11. Selecione a caixa de verificação **Recusar para outros utilizadores** se pretender que todos os utilizadores que não são apresentados na coluna **Principal** e que não façam parte do grupo de utilizadores especificado na coluna **Principal** sejam impedidos de iniciar aplicações que pertençam à categoria selecionada.

12. Se pretender que o Kaspersky Endpoint Security considere as aplicações da categoria especificada na regra como atualizadores confiáveis com direitos a iniciar outras aplicações para as quais não foram definidas regras de Controlo de Arranque das Aplicações, selecione a caixa de verificação **Atualizadores Confiáveis**.

13. Clique em **OK**.

14. Na secção **Controlo de Arranque das Aplicações** da janela de propriedades da política, clique no botão **Aplicar**.

Alterar o estado de uma regra de Controlo de Arranque das Aplicações utilizando o Kaspersky Security Center

Para alterar o estado de uma regra de Controlo de Arranque das Aplicações:

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 pretendida.

5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.

6. Na secção **Controlo de terminal**, selecione a secção **Controlo de Arranque das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Arranque das Aplicações.

7. Selecione a regra de Controlo de Arranque das Aplicações cujo estado pretende alterar.

8. Na coluna **Estado**, execute uma das seguintes ações:

   - Se pretender ativar a utilização de uma regra, selecione a caixa de verificação à frente da regra.
   - Se pretender desativar a utilização de uma regra, desmarque a caixa de verificação à frente da regra.

9. Clique no botão **Aplicar**.

Controlo de Privilégios das Aplicações

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para estações de trabalho. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para servidores de ficheiros.

Esta secção contém informações sobre o Controlo de Privilégios das Aplicações e instruções para efetuar as configurações do componente.

Sobre o Controlo de Privilégios das Aplicações

O Controlo de Privilégios das Aplicações 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 de identidade.

Este componente controla a atividade das aplicações, incluindo o acesso a recursos protegidos (tais como ficheiros e pastas, chaves de registo), utilizando *regras de controlo das aplicações*. As regras de controlo das aplicações consistem num conjunto de restrições aplicáveis a várias ações de aplicações no sistema operativo e a direitos de acesso a recursos do computador.

A atividade de rede das aplicações é monitorizada pelo componente Firewall.

Quando uma aplicação é iniciada pela primeira vez, o Controlo de Privilégios das Aplicações verifica a aplicação e adiciona a mesma a um grupo de confiança. Um grupo de confiança define as regras de controlo das aplicações que o Kaspersky Endpoint Security aplica ao controlar a atividade das aplicações.

Recomendamos que participe na Kaspersky Security Network para melhorar o desempenho do Controlo de Privilégios das Aplicações. Os dados obtidos através da Kaspersky Security Network permitem organizar as aplicações em grupos com maior precisão e aplicar regras otimizadas de controlo das aplicações.

Quando a aplicação é iniciada novamente, o Controlo de Privilégios das Aplicações verifica a integridade da aplicação. Se a aplicação não tiver sofrido alterações, o componente aplica-lhe as regras de controlo das aplicações atuais. Se a aplicação tiver sido modificada, o Controlo de Privilégios das Aplicações verifica-a novamente, como se estivesse a ser iniciada pela primeira vez.

Limitações do controlo de dispositivos de áudio e de vídeo

Sobre a proteção do fluxo de áudio

A proteção do fluxo de áudio tem as seguintes considerações especiais:

- O componente Controlo de Privilégios das Aplicações tem de estar ativo para que esta funcionalidade seja executada.

- Se a aplicação tiver começado a receber o fluxo de áudio antes de o componente Controlo de Privilégios das Aplicações ser iniciado, o Kaspersky Endpoint Security permite à aplicação receber o fluxo de áudio e não apresenta qualquer notificação.
- Se tiver movido a aplicação para o grupo **Não confiável** ou para o grupo **Restrições altas** depois de aplicação ter começado a receber o fluxo de áudio, o Kaspersky Endpoint Security permite à aplicação receber o fluxo de áudio e não apresenta qualquer notificação.
- Após a alteração das definições de acesso da aplicação a dispositivos de gravação de som (por exemplo, se tiver sido bloqueada a receção de fluxo de áudio na aplicação na janela de definições de Controlo das Aplicações), 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 à webcam 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 fluxo 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.

Considerações especiais sobre o funcionamento de dispositivos de áudio e vídeo durante a instalação e a atualização do Kaspersky Endpoint Security

Quando executa aplicações de reprodução ou de registo de áudio e vídeo pela primeira vez desde a instalação do Kaspersky Endpoint Security, a reprodução ou o registo de áudio e vídeo podem ser interrompidos. 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.

Sobre acesso de aplicações a webcams

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.

Webcams suportadas

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.

Ativar e desativar o Controlo de Privilégios das Aplicações

Por defeito, o Controlo de Privilégios das Aplicações está ativado, sendo executado num modo recomendado pelos especialistas da Kaspersky. Se necessário, pode desativar o Controlo de Privilégios das Aplicações.

Existem duas formas para ativar ou desativar o componente:

- No separador **Proteção e Controlo** na janela principal da aplicação
- Na janela de definições da aplicação

Para ativar ou desativar o Controlo de Privilégios das Aplicações no separador Proteção e Controlo da janela principal da aplicação:

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Controlo de terminal**.

   A secção **Controlo de terminal** é apresentada.
4. Clique com o botão direito do rato para visualizar o menu da linha que contém informações sobre o componente Controlo de Privilégios das Aplicações.

   É aberto um menu para selecionar ações no componente.
5. Execute uma das seguintes ações:

   - Para ativar o Controlo de Privilégios das Aplicações, selecione **Iniciar**.

     O ícone de estado do componente , que é apresentado à esquerda na linha do Controlo de Privilégios das Aplicações, é alterado para o ícone .
   - Para desativar o componente Controlo de Privilégios das Aplicações, selecione **Parar**.

     O ícone de estado do componente , que é apresentado à esquerda na linha do Controlo de Privilégios das Aplicações, é alterado para o ícone .

Para ativar o Controlo de Privilégios das Aplicações na janela de configurações das aplicações:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Privilégios das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Privilégios das Aplicações.

3. Na parte direita da janela, execute uma das seguintes ações:

   - Para ativar o Controlo de Privilégios das Aplicações, selecione a caixa de verificação **Ativar Controlo de Privilégios das Aplicações**.
   - Para desativar o Controlo de Privilégios das Aplicações, desmarque a caixa de verificação **Ativar Controlo de Privilégios das Aplicações**.

4. Para guardar as alterações, clique no botão **Guardar**.

Gerir grupos de confiança da aplicação

Quando cada aplicação é iniciada pela primeira vez, o componente Controlo de Privilégios das Aplicações verifica a segurança da aplicação e coloca a aplicação num grupo de confiança.

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 de confiança. Sempre que a aplicação é iniciada, o Kaspersky Endpoint Security envia uma nova consulta para a base de dados da KSN e coloca a aplicação num grupo de confiança diferente se a reputação da aplicação nas bases de dados da KSN tiver sido alterada.

Pode selecionar um grupo confiável ao qual o Kaspersky Endpoint Security atribui automaticamente todas as aplicações desconhecidas. As aplicações que foram iniciadas antes do Kaspersky Endpoint Security são automaticamente movidas para o grupo confiável especificado na janela **Selecionar grupo confiável**.

O componente controla apenas a atividade de rede de aplicações iniciadas antes do Kaspersky Endpoint Security com base nas regras de rede definidas nas configurações da Firewall.

Configurar as definições de atribuição de aplicações a grupos de confiança

Se a participação no Kaspersky Security Network estiver ativada, o Kaspersky Endpoint Security envia à KSN uma consulta sobre a reputação de uma aplicação sempre que a aplicação é iniciada. Com base na resposta da KSN, a aplicação pode ser movida para um grupo de confiança diferente do especificado nas definições do Controlo de Privilégios das Aplicações.

Para configurar as definições de colocação de aplicações em grupos de confiança:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Privilégios das Aplicações**.

Na parte direita da janela, são apresentadas as configurações do componente Controlo de Privilégios das Aplicações.

3. Se pretender adicionar de forma automática aplicações assinadas digitalmente de fornecedores confiáveis ao grupo Confiáveis, selecione a caixa de verificação **Aplicações confiáveis que têm uma assinatura digital**.

   Fornecedores confiáveis são os fornecedores de software incluídos no grupo confiável pela Kaspersky. Pode também adicionar manualmente um certificado de fornecedor ao arquivo de certificados do sistema confiável.
4. Selecione a forma como as aplicações desconhecidas serão atribuídas a grupos de confiança:

   - Para utilizar a análise heurística para atribuir aplicações desconhecidas a grupos de confiança, selecione a opção **Utilizar análise heurística para definir grupo** e especifique o período de tempo destinado à verificação a aplicação iniciada no campo **Tempo máximo para definir grupo**.
   - Se pretender atribuir todas as aplicações desconhecidas a um grupo de confiança específico, selecione a opção **Mover automaticamente para o grupo** e, em seguida, selecione o grupo de confiança apropriado na lista suspensa.

     Para fins de segurança, o grupo **Confiáveis** não está incluído nos valores da definição **Mover automaticamente para o grupo**.
5. Para guardar as alterações, clique no botão **Guardar**.

Modificar um grupo de confiança

Quando uma aplicação é iniciada pela primeira vez, o Kaspersky Endpoint Security coloca automaticamente a aplicação num grupo de confiança. Se necessário, pode mover a aplicação manualmente para outro grupo de confiança.

Os especialistas da Kaspersky não recomendam a transferência de aplicações do grupo de confiança atribuído automaticamente para outro grupo de confiança. Em alternativa, pode editar as regras para uma aplicação individual.

Para alterar o grupo de confiança atribuído automaticamente a uma aplicação pelo Kaspersky Endpoint Security quando esta foi iniciada pela primeira vez:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Privilégios das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Privilégios das Aplicações.
3. Clique no botão **Aplicações**.

   É aberto o separador **Regras de controlo das aplicações** na janela **Aplicações**.
4. Selecione a aplicação pretendida no separador **Regras de controlo das aplicações**.
5. Execute uma das seguintes ações:

- Clique com o botão direito do rato para visualizar o menu de contexto da aplicação. No menu de contexto da aplicação, selecione **Mover para grupo**→ <νομε δο γρυπο>.

- Para abrir o menu de contexto, clique na ligação **Confiáveis/Restrições baixas/Restrições altas/Não confiável**. No menu de contexto, selecione o grupo de confiança pretendido.

6. Clique em **OK**.

7. Para guardar as alterações, clique no botão **Guardar**.

Selecionar um grupo de confiança para aplicações iniciadas antes do Kaspersky Endpoint Security

O componente controla apenas a atividade de rede de aplicações que tenham sido iniciadas antes do Kaspersky Endpoint Security. 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 de confiança.

Para selecionar um grupo de confiança para aplicações iniciadas antes do Kaspersky Endpoint Security:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Privilégios das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Privilégios das Aplicações.

3. Clique no botão **Editar**.

   Esta ação abre a janela **Selecionar grupo confiável**.

4. Selecione o grupo de confiança necessário.

5. Clique em **OK**.

6. Para guardar as alterações, clique no botão **Guardar**.

Gerir as regras de Controlo das aplicações

Por defeito, a atividade das aplicações é controlada pelas regras de controlo das aplicações definidas para o grupo de confiança ao qual o Kaspersky Endpoint Security atribuiu a aplicação na primeira vez em que foi iniciada. Se necessário, pode editar as regras de controlo das aplicações para um grupo de confiança completo, para uma aplicação individual ou para um grupo de aplicações dentro de um grupo de confiança.

As regras de controlo das aplicações definidas para aplicações individuais ou grupos de aplicações dentro de um grupo de confiança têm uma prioridade superior à das regras de controlo das aplicações definidas para um grupo de confiança. Por outras palavras, se as definições de regras de controlo das aplicações especificadas para uma aplicação individual ou grupo de aplicações num grupo de confiança forem diferentes das definições das regras de controlo das aplicações especificadas para o grupo de confiança, o componente Controlo de Privilégios das Aplicações controla a atividade da aplicação ou grupo de aplicações do grupo de confiança, em conformidade com as regras de controlo das aplicações definidas para a aplicação ou grupo de aplicações.

Alterar regras de controlo das aplicações para grupos de confiança e grupos de aplicações

As regras de controlo das aplicações ideais para diferentes grupos de confiança são criadas por defeito. As definições de regras para controlo de grupos de aplicações herdam valores das definições regras de controlo de grupos de confiança. Pode editar as regras de controlo de grupos de confiança e as regras de controlo de grupos de aplicações predefinidas.

Para editar as regras de controlo de grupos de confiança ou as regras de controlo de grupos de aplicações:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Privilégios das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Privilégios das Aplicações.
3. Clique no botão **Aplicações**.

   Esta ação abre o separador **Regras de controlo das aplicações** na janela **Controlo de Privilégios das Aplicações**.
4. Selecionar o grupo de confiança necessário ou grupo de aplicações.
5. No menu de contexto de um grupo de confiança ou de um grupo de aplicações, selecione **Regras de grupos**.

   É aberta a janela **Regras de controlo de grupos de aplicações**.
6. Na janela **Regras de controlo de grupos de aplicações**, execute uma das seguintes ações:

   - Para editar regras de controlo de grupos ou regras de controlo de grupos de aplicações que administrem os direitos do grupo de confiança ou grupo de aplicações para acesso ao registo do sistema operativo, a ficheiros de utilizador e configurações de aplicações, selecione o separador **Ficheiros e registo do sistema**.
   - Para editar regras de controlo de grupos de confiança ou regras de controlo de grupos de aplicações que administrem os direitos do grupo de confiança ou do grupo de aplicações para acesso a processos e objetos do sistema operativo, selecione o separador **Direitos**.
7. Para o recurso pretendido, na coluna da ação correspondente, clique com o botão direito do rato para abrir o menu de contexto.
8. No menu de contexto, selecione o item pretendido.

   - **Herdar**
   - **Permitir**

- **Bloquear**
- **Registar eventos**

> Se estiver a editar regras de controlo de grupos de confiança, o item **Herdar** não está disponível.

9. Clique em **OK**.
10. Na janela **Aplicações**, clique em **OK**.
11. Para guardar as alterações, clique no botão **Guardar**.

Editar uma regra de controlo das aplicações

Por defeito, as definições de regras de controlo das aplicações que pertençam a um grupo de aplicações ou grupo de confiança herdam os valores das definições de regras de controlo de grupos de confiança. Pode editar as definições de regras de controlo das aplicações.

Para alterar uma regra de controlo das aplicações:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Privilégios das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Privilégios das Aplicações.
3. Clique no botão **Aplicações**.

   Esta ação abre o separador **Regras de controlo das aplicações** na janela **Controlo de Privilégios das Aplicações**.
4. Selecione a aplicação necessária.
5. Execute uma das seguintes ações:

   - No menu de contexto da aplicação, selecione **Regras de aplicações**.
   - Clique no botão **Adicional** no canto inferior direito do separador **Regras de controlo das aplicações**.

   É aberta a janela **Regras de controlo das aplicações**.
6. Na janela **Regras de controlo das aplicações**, execute uma das seguintes ações:

   - Para editar regras de controlo das aplicações que administrem os direitos da aplicação para acesso ao registo do sistema operativo, a ficheiros de utilizador e a configurações da aplicação, selecione o separador **Ficheiros e registo do sistema**.
   - Para editar regras de controlo das aplicações que administrem os direitos das aplicações para acesso a processos e objetos do sistema operativo, selecione o separador **Direitos**.
7. Para o recurso pretendido, na coluna da ação correspondente, clique com o botão direito do rato para abrir o menu de contexto.

8. No menu de contexto, selecione o item pretendido.
    - **Herdar**
    - **Permitir**
    - **Bloquear**
    - **Registar eventos**
9. Clique em **OK**.
10. Na janela **Aplicações**, clique em **OK**.
11. Para guardar as alterações, clique no botão **Guardar**.

Desativar transferências e atualizações de regras de controlo das aplicações da base de dados da Kaspersky Security Network

Por defeito, quando é detetada uma nova informação sobre uma aplicação na base de dados do Kaspersky Security Network, o Kaspersky Endpoint Security aplica as regras de controlo transferidas da base de dados da KSN destinadas a esta aplicação. Pode então editar manualmente as regras de controlo para a aplicação.

Se a aplicação não estava incluída na base de dados da Kaspersky Security Network quando foi iniciada pela primeira vez, mas as informações sobre a mesma foram adicionadas à base de dados posteriormente, por defeito, o Kaspersky Endpoint Security atualiza automaticamente as regras de controlo para esta aplicação.

Pode desativar transferências de regras de controlo das aplicações da base de dados da Kaspersky Security Network e atualizações automáticas de regras de controlo para aplicações anteriormente desconhecidas.

Para desativar transferências e atualizações de regras de controlo das aplicações da base de dados da Kaspersky Security Network:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Privilégios das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Privilégios das Aplicações.
3. Desmarque a caixa de verificação **Atualizar regras de controlo para as aplicações previamente desconhecidas das bases de dados da KSN**.
4. Para guardar as alterações, clique no botão **Guardar**.

Desativar a herança de restrições do Processo-Principal

A inicialização da aplicação pode ser executada pelo utilizador ou por outra aplicação em execução. Quando a inicialização da aplicação é iniciada por outra aplicação, é criada uma sequência de arranque, constituída por processos ascendentes e descendentes.

Quando uma aplicação tenta obter acesso a um recurso protegido, o Controlo de Privilégios das Aplicações analisa todos os processos ascendentes da aplicação para determinar se estes processos têm direitos para aceder ao recurso protegido. É, então, aplicada a regra de prioridade mínima: ao comparar os direitos de acesso da aplicação aos do processo-pai, são aplicados os direitos de acesso com prioridade mínima à atividade da aplicação.

A prioridade de direitos de acesso é a seguinte:

1. **Permitir** Este direito de acesso tem a prioridade mais elevada.
2. **Bloquear** Este direito de acesso tem a prioridade mais baixa.

Este mecanismo impede que uma aplicação não confiável ou uma aplicação com direitos restritos utilize uma aplicação confiável para executar ações que requerem determinados privilégios.

Se a atividade de uma aplicação for bloqueada devido à falta de direitos concedidos a um processo ascendente, pode editar estes direitos ou desativar a herança de restrições do processo ascendente.

Para desativar a herança de restrições do processo ascendente:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Privilégios das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Privilégios das Aplicações.
3. Clique no botão **Aplicações**.

   Esta ação abre o separador **Regras de controlo das aplicações** na janela **Controlo de Privilégios das Aplicações**.
4. Selecione a aplicação necessária.
5. No menu de contexto da aplicação, selecione **Regras de aplicações**.

   É aberta a janela **Regras de controlo das aplicações**.
6. Na janela **Regras de Controlo das Aplicações**, selecione o separador **Exclusões**.
7. Selecione a caixa de verificação **Não herdar restrições do processo-pai (aplicação)**.
8. Clique em **OK**.
9. Na janela **Aplicações**, clique em **OK**.
10. Para guardar as alterações, clique no botão **Guardar**.

Excluir determinadas ações de aplicações das regras de controlo das aplicações

Para excluir determinadas ações de aplicações das regras de controlo das aplicações:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Privilégios das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Privilégios das Aplicações.

3. Clique no botão **Aplicações**.

   Esta ação abre o separador **Regras de controlo das aplicações** na janela **Controlo de Privilégios das Aplicações**.

4. Selecione a aplicação necessária.

5. No menu de contexto da aplicação, selecione **Regras de aplicações**.

   É aberta a janela **Regras de controlo das aplicações**.

6. Selecione o separador **Exclusões**.

7. Selecione caixas de verificação junto às ações de aplicações que não é necessário monitorizar.

8. Clique em **OK**.

9. Na janela **Aplicações**, clique em **OK**.

10. Para guardar as alterações, clique no botão **Guardar**.

Remoção de regras de controlo das aplicações desatualizadas

Por defeito, as regras de controlo para aplicações que não tenham sido iniciadas durante 60 dias são automaticamente apagadas. Pode alterar a duração de armazenamento de regras de controlo para aplicações não utilizadas ou desativar a eliminação automática de regras.

Para eliminar as regras de controlo das aplicações desatualizadas:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Privilégios das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Privilégios das Aplicações.

3. Execute uma das seguintes ações:

   - Se pretender que o Kaspersky Endpoint Security apague regras de controlo das aplicações não utilizadas, selecione a caixa de verificação **Eliminar regras para as aplicações que não são iniciadas há mais de** e especifique o número de dias pretendido.

   - Para desativar a eliminação automática das regras de controlo das aplicações não utilizadas, desmarque a caixa de verificação **Eliminar regras para as aplicações que não são iniciadas há mais de**.

4. Para guardar as alterações, clique no botão **Guardar**.

Proteção dos recursos do sistema operativo e de dados de identidade

O Controlo de Privilégios das Aplicações gere os direitos das aplicações para realizar ações de várias categorias de recursos do sistema operativo e de dados de identidade.

Os especialistas da Kaspersky estabeleceram categorias predefinidas de recursos protegidos. Não é possível editar ou apagar as categorias predefinidas de recursos protegidos ou dos recursos protegidos inseridos nestas categorias.

Pode executar as seguintes ações:

- Adicionar uma nova categoria de recursos protegidos.
- Adicionar um novo recurso protegido.
- Desativar a proteção de um recurso.

Adicionar uma categoria de recursos protegidos

Para adicionar uma nova categoria de recursos protegidos:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Privilégios das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Privilégios das Aplicações.
3. Clique no botão **Recursos**.

   Esta ação abre o separador **Recursos protegidos** na janela **Controlo de Privilégios das Aplicações**.
4. No lado esquerdo do separador **Recursos protegidos**, selecione uma secção ou categoria de recursos protegidos à qual pretenda adicionar uma nova categoria de recursos protegidos.
5. Clique no botão **Adicionar** e na lista pendente selecione a **Categoria**.

   É aberta a janela **Categoria de recursos protegidos**.
6. Na janela **Categoria de recursos protegidos** que é aberta, introduza um nome para a nova categoria de recursos protegidos.
7. Clique em **OK**.

   É apresentado um novo item na lista de categorias de recursos protegidos.
8. Na janela **Controlo de Privilégios das Aplicações**, clique em **OK**.
9. Para guardar as alterações, clique no botão **Guardar**.

Após adicionar uma categoria de recursos protegidos, pode editar ou remover a mesma, clicando nos botões **Editar** ou **Remover** no canto superior esquerdo do separador **Recursos protegidos**.

Adicionar um recurso protegido

Para adicionar um recurso protegido:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Privilégios das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Privilégios das Aplicações.
3. Clique no botão **Recursos**.

   Esta ação abre o separador **Recursos protegidos** na janela **Controlo de Privilégios das Aplicações**.
4. No lado esquerdo do separador **Recursos protegidos**, selecione uma categoria de recursos protegidos à qual pretende adicionar um novo recurso protegido.
5. Clique no botão **Adicionar** e na lista pendente selecione o tipo do recurso que pretende adicionar:

   - **Ficheiro ou pasta**.
   - **Chave de registo**.

   É aberta a janela **Recurso protegido**.
6. Na janela **Recurso protegido**, introduza o nome do recurso protegido no campo **Nome**.
7. Clique no botão **Procurar**.
8. Na janela que é aberta, especifique as definições necessárias, consoante o tipo de recurso protegido que pretende adicionar. Clique em **OK**.
9. Na janela **Recurso protegido**, clique em **OK**.

   É apresentado um novo item na lista de recursos protegidos da categoria selecionada no separador **Recursos protegidos**.
10. Na janela **Controlo de Privilégios das Aplicações**, clique em **OK**.
11. Para guardar as alterações, clique no botão **Guardar**.

Após adicionar um recurso protegido, pode editar ou remover o mesmo, clicando nos botões **Editar** ou **Remover** no canto superior esquerdo do separador **Recursos protegidos**.

Desativar a proteção de recursos

Para desativar a proteção de recursos:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Privilégios das Aplicações**.

   Na parte direita da janela, são apresentadas as configurações do componente Controlo de Privilégios das Aplicações.
3. Na parte direita da janela, clique no botão **Recursos**.

   Esta ação abre o separador **Recursos protegidos** na janela **Controlo de Privilégios das Aplicações**.
4. Execute uma das seguintes ações:

   - Na parte esquerda do separador, na lista de recursos protegidos, selecione o recurso para o qual pretende desativar a proteção e desmarque a caixa de verificação junto ao nome.
   - Clique em **Exclusões** e execute as seguintes ações:

     a. Na janela **Exclusões**, clique no botão **Adicionar**. Na lista pendente, selecione o tipo de recurso que pretende adicionar à lista de exclusões de proteção com o componente Controlo de Privilégios das Aplicações: **Ficheiro ou pasta** ou **Chave de registo**.

     É aberta a janela **Recurso protegido**.

     b. Na janela **Recurso protegido**, introduza o nome do recurso protegido no campo **Nome**.

     c. Clique no botão **Procurar**.

     d. Na janela que é aberta, especifique as definições necessárias, consoante o tipo de recurso protegido que pretende adicionar à lista de exclusões de proteção do componente Controlo de Privilégios das Aplicações.

     e. Clique em **OK**.

     f. Na janela **Recurso protegido**, clique em **OK**.

     É apresentado um novo elemento na lista de recursos excluídos da proteção pelo componente Controlo de Privilégios das Aplicações.

     > Após adicionar um recurso à lista de exclusões de proteção pelo componente Controlo de Privilégios das Aplicações, pode editar ou remover o mesmo, clicando nos botões **Editar** ou **Remover** no canto superior da janela **Exclusões**.

     g. Na janela **Exclusões**, clique em **OK**.
5. Na janela **Controlo de Privilégios das Aplicações**, clique em **OK**.
6. Para guardar as alterações, clique no botão **Guardar**.

Monitor de Vulnerabilidades

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para estações de trabalho. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador com o Microsoft Windows for File Servers.

Esta secção contém a informação sobre o Monitor de Vulnerabilidades e as instruções sobre como ativar ou desativar o componente.

Sobre o Monitor de Vulnerabilidades

O componente Monitor de Vulnerabilidades executa uma verificação de vulnerabilidade em tempo real das aplicações que estão em execução no computador do utilizador e que são iniciadas por este. Quando o componente Monitor de Vulnerabilidades está ativado, não é necessário iniciar a tarefa Verificação de Vulnerabilidade. Esta verificação é importante se uma Tarefa de Verificação de Vulnerabilidade das aplicações instaladas no computador do utilizador nunca tiver sido executada ou tiver sido executada há algum tempo.

Ativar e desativar o Monitor de Vulnerabilidades

Por defeito, o componente Monitor de Vulnerabilidades está desativado. Se necessário, pode ativar o Monitor de Vulnerabilidades.

Existem duas formas para ativar ou desativar o componente:

- No separador **Proteção e Controlo** na janela principal da aplicação
- Na janela de definições da aplicação

Para ativar ou desativar o Monitor de Vulnerabilidades no separador Proteção e Controlo da janela principal da aplicação:

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Controlo de terminal**.

   A secção **Controlo de terminal** é apresentada.
4. Clique com o botão direito do rato para visualizar o menu de contexto da linha que contém as informações sobre o componente Monitor de Vulnerabilidades.

   É aberto um menu para selecionar ações no componente.
5. Execute uma das seguintes ações:

   - Para ativar o Monitor de Vulnerabilidades, selecione **Iniciar**.

     O ícone de estado do componente , que é apresentado à esquerda na linha do **Monitor de Vulnerabilidades**, é alterado para o ícone .
   - Para desativar o Monitor de Vulnerabilidades, selecione **Parar**.

O ícone de estado do componente , que é apresentado à esquerda na linha do **Monitor de Vulnerabilidades**, é alterado para o ícone .

Para ativar ou desativar o Monitor de Vulnerabilidades a partir da janela de definições da aplicação:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione **Monitor de Vulnerabilidades**.

   Na parte direita da janela, são apresentadas as definições do componente Monitor de Vulnerabilidades.
3. Na parte direita da janela, execute uma das seguintes ações:

   - Se pretender que o Kaspersky Endpoint Security inicie uma verificação de vulnerabilidade das aplicações que estão em execução no computador do utilizador ou que são iniciadas pelo utilizador, selecione a caixa de verificação **Ativar Monitor de Vulnerabilidades**.
   - Se não pretender que o Kaspersky Endpoint Security inicie uma verificação de vulnerabilidade das aplicações que estão em execução no computador do utilizador ou que são iniciadas pelo utilizador, desmarque a caixa de verificação **Ativar Monitor de Vulnerabilidades**.
4. Para guardar as alterações, clique no botão **Guardar**.

Controlo de Dispositivos

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para estações de trabalho. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para servidores de ficheiros.

Esta secção contém informações sobre o Controlo de Dispositivos e instruções para efetuar as configurações do componente.

Sobre o Controlo de Dispositivos

O Controlo de Dispositivos garante a segurança de dados confidenciais ao restringir o acesso de utilizadores a dispositivos que estejam instalados no computador ou ligados ao mesmo, incluindo:

- Dispositivos de armazenamento de dados (discos rígidos, unidades amovíveis, unidades de banda, unidades de CD/DVD)
- Ferramentas de transferência de dados (modems, placas de rede externas)
- Dispositivos concebidos para converterem dados para cópias impressas (impressoras)
- Barramentos de ligação (também designados simplesmente por "barramentos"), que se referem a interfaces destinadas à ligação de dispositivos a computadores (tais como USB, FireWire e Infravermelhos)

O Controlo de Dispositivos gere o acesso de utilizadores a dispositivos através da aplicação de *regras de acesso a dispositivos* (também designadas por "regras de acesso") e de *regras de acesso a barramentos de ligação* (também designadas por "regras de acesso a barramentos").

Ativar e desativar o Controlo de Dispositivos

Por defeito, o Controlo de Dispositivos está ativado. Se necessário, pode desativar o Controlo de Dispositivos.

Existem duas formas para ativar ou desativar o componente:

- No separador **Proteção e Controlo** na janela principal da aplicação
- Na janela de definições da aplicação

*Para ativar ou desativar o Controlo de Dispositivos no separador **Proteção e Controlo** da janela principal da aplicação:*

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Controlo de terminal**.

   A secção **Controlo de terminal** é apresentada.

4. Clique com o botão direito do rato para visualizar o menu da linha que contém as informações sobre o componente Controlo de Dispositivos.

   É aberto um menu para selecionar ações no componente.

5. Execute uma das seguintes ações:

   - Para ativar o Controlo de Dispositivos, selecione **Iniciar** no menu.
   - Para desativar o Controlo de Dispositivos, selecione **Parar** no menu.

Para ativar ou desativar o Controlo de Dispositivos a partir da janela de definições da aplicação:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Dispositivos**.

   Na parte direita da janela, são apresentadas as definições do componente de Controlo de Dispositivos.

3. Execute uma das seguintes ações:

   - Se pretender ativar o Controlo de Dispositivos, selecione a caixa de verificação **Ativar Controlo de Dispositivos**.
   - Se pretender desativar o Controlo de Dispositivos, desmarque a caixa de verificação **Ativar Controlo de Dispositivos**.

4. Para guardar as alterações, clique no botão **Guardar**.

Sobre as regras de acesso a dispositivos e barramentos de ligação

Uma regra de acesso a dispositivos consiste numa combinação de parâmetros que definem as seguintes funções do componente Controlo de Dispositivos:

- Permitir que utilizadores e/ou grupos selecionados acedam a tipos específicos de dispositivos durante períodos de tempo específicos.

  Pode selecionar um utilizador e/ou grupo de utilizadores e criar um agendamento de acesso a dispositivos.

- Definir o direito de leitura do conteúdo de dispositivos de memória.
- Definir o direito de edição do conteúdo de dispositivos de memória.

Por defeito, são criadas regras de acesso para todos os tipos de dispositivos na classificação do componente Controlo de Dispositivos. Estas regras concedem a todos os utilizadores acesso total aos dispositivos, em qualquer altura, caso o acesso aos barramentos de ligação dos tipos de dispositivos correspondentes seja permitido.

A regra de acesso ao barramento de ligação permite ou impede o acesso ao barramento de ligação.

São criadas, por defeito, regras que permitem o acesso a barramentos para todos os barramentos de ligação existentes na classificação do componente Controlo de Dispositivos.

O utilizador não pode criar ou apagar regras de acesso a dispositivos ou regras de acesso a barramentos de ligação; pode apenas editá-las.

Sobre dispositivos confiáveis

Dispositivos confiáveis são dispositivos aos quais os utilizadores especificados nas definições de dispositivo confiável têm acesso total, em qualquer altura.

Estão disponíveis as seguintes ações para trabalhar com dispositivos confiáveis:

- Adicionar o dispositivo à lista de dispositivos confiáveis.
- Alterar o utilizador e/ou grupo de utilizadores com permissão para aceder ao dispositivo confiável.
- Apagar o dispositivo da lista de dispositivos confiáveis.

Se tiver adicionado um dispositivo à lista de dispositivos confiáveis e criado uma regra de acesso para este tipo de dispositivo que bloqueie ou limite o acesso, o Kaspersky Endpoint Security decide se deve ou não conceder acesso ao dispositivo com base na sua presença na lista de dispositivos confiáveis. A presença na lista de dispositivos confiáveis tem uma prioridade superior à de uma regra de acesso.

Decisões padrão de acesso aos 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.

Decisões padrão de acesso aos dispositivos

N.º	Condições iniciais	Passos intermédios a executar até ser tomada uma decisão sobre o acesso ao dispositivo			Decisão sobre o acesso ao dispositivo
		Verificar se o dispositivo é incluído na lista de dispositivos confiáveis	Testar o acesso ao dispositivo com base na regra de acesso	Testar o acesso ao barramento com base na regra de acesso	
1	O dispositivo não está presente na classificação de dispositivo do componente Controlo de Dispositivos.	Não incluído na lista de dispositivos confiáveis.	Sem regra de acesso.	Não é sujeito a verificação.	Acesso permitido.
2	O dispositivo é confiável.	Incluído na lista de dispositivos confiáveis.	Não é sujeito a verificação.	Não é sujeito a verificação.	Acesso permitido.
3	O acesso ao dispositivo é permitido.	Não incluído na lista de dispositivos confiáveis.	Acesso permitido.	Não é sujeito a verificação.	Acesso permitido.
4	O acesso ao dispositivo	Não incluído na	O acesso	Acesso	Acesso

	depende do barramento.	lista de dispositivos confiáveis.	depende do barramento.	permitido.	permitido.
5	O acesso ao dispositivo depende do barramento.	Não incluído na lista de dispositivos confiáveis.	O acesso depende do barramento.	Acesso bloqueado.	Acesso bloqueado.
6	O acesso ao dispositivo é permitido. Não foi encontrada qualquer regra de acesso a barramentos.	Não incluído na lista de dispositivos confiáveis.	Acesso permitido.	Sem regra de acesso a barramentos.	Acesso permitido.
7	O acesso ao dispositivo é bloqueado.	Não incluído na lista de dispositivos confiáveis.	Acesso bloqueado.	Não é sujeito a verificação.	Acesso bloqueado.
8	Não foi encontrada qualquer regra de acesso ao dispositivo ou regra de acesso a barramentos.	Não incluído na lista de dispositivos confiáveis.	Sem regra de acesso.	Sem regra de acesso a barramentos.	Acesso permitido.
9	Não existe regra de acesso ao dispositivo.	Não incluído na lista de dispositivos confiáveis.	Sem regra de acesso.	Acesso permitido.	Acesso permitido.
10	Não existe regra de acesso ao dispositivo.	Não incluído na lista de dispositivos confiáveis.	Sem regra de acesso.	Acesso bloqueado.	Acesso bloqueado.

Pode editar a regra de acesso ao dispositivo depois de ligar o dispositivo. Se o dispositivo estiver ligado e a regra de acesso permitir o acesso ao mesmo, mas, posteriormente, editar a regra de acesso e bloquear o acesso, o Kaspersky Endpoint Security irá bloquear o acesso na próxima vez que for solicitada uma operação com ficheiros a partir do dispositivo (ver a árvore de pastas, ler, escrever, etc.). 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.

Editar uma regra de acesso a dispositivos

Dependendo do tipo do dispositivo, pode alterar várias definições de acesso, como a lista de utilizadores que recebem acesso ao dispositivo, o agendamento de acesso e o acesso autorizado/bloqueado.

Para editar uma regra de acesso a dispositivos:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Dispositivos**.

   Na parte direita da janela, são apresentadas as definições do componente de Controlo de Dispositivos.
3. Na parte direita da janela, selecione o separador **Tipos de dispositivos**.

O separador **Tipos de dispositivos** contém regras de acesso para todos os dispositivos incluídos na classificação do componente Controlo de Dispositivos.

4. Selecione a regra de acesso que pretende editar.

5. Clique no botão **Editar**. Este botão está disponível apenas para tipos de dispositivos que têm um sistema de ficheiros.

   É aberta a janela **Configurar a regra de acesso a dispositivos**.

   Por defeito, uma regra de acesso a dispositivos atribui a todos os utilizadores acesso total ao tipo especificado de dispositivos em qualquer altura. Na lista **Utilizadores e/ou grupos de utilizadores**, esta regra de acesso contém o grupo **Todos**. Na tabela **Direitos do grupo de utilizadores selecionado por agendamentos de acesso**, esta regra de acesso contém o **Agendamento predefinido** para acesso a dispositivos, com os direitos de execução de todos os tipos de operações com dispositivos.

6. Editar as definições da regra de acesso aos dispositivos:

   a. Selecione um utilizador e/ou grupo de utilizadores na lista **Utilizadores e/ou grupos de utilizadores**.

      Para editar a lista **Utilizadores e/ou grupos de utilizadores**, utilize os botões **Adicionar**, **Editar** e **Remover**.

   b. Na tabela **Direitos do grupo de utilizadores selecionado por agendamentos de acesso**, configure o agendamento para acesso aos dispositivos para o utilizadores e/ou grupo de utilizadores. Para tal, selecione as caixas de verificação junto aos nomes dos agendamentos de acesso para os dispositivos que pretende utilizar na regra de acesso de dispositivos que será editada.

      Para editar a lista de agendamento de acesso aos dispositivos, utilize os botões **Criar**, **Editar**, **Copiar** e **Remover** na tabela **Direitos do grupo de utilizadores selecionado por agendamentos de acesso**.

   c. Para cada agendamento para acesso a dispositivos utilizados na regra que está a ser editada, especifique as operações autorizadas ao trabalhar com dispositivos. Para tal, na tabela **Direitos do grupo de utilizadores selecionado por agendamentos de acesso**, selecione as caixas de verificação nas colunas que contenham os nomes das operações relevantes.

   d. Clique em **OK**.

   Depois de editar as configurações predefinidas de uma regra de acesso a dispositivos, a definição de acesso ao tipo do dispositivo na coluna **Acesso** na tabela nos **Tipos de dispositivos** é alterada para o valor *Restringir pelas regras*.

7. Para guardar as alterações, clique no botão **Guardar**.

Adicionar ou excluir registo para ou do registo de eventos

O registo de eventos está disponível apenas para operações com ficheiros em unidades amovíveis.

Para ativar ou desativar o registo de eventos:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Dispositivos**.

   Na parte direita da janela, são apresentadas as definições do componente de Controlo de Dispositivos.

3. Na parte direita da janela, selecione o separador **Tipos de dispositivos**.

   O separador **Tipos de dispositivos** contém regras de acesso para todos os dispositivos incluídos na classificação do componente Controlo de Dispositivos.

4. Selecione **Unidades amovíveis** na tabela de dispositivos.

   O botão **Registo de dados** fica disponível na parte superior da tabela.

5. Clique no botão **Registo de dados**.

   Esta ação abre a janela **Definições de registo de dados**.

6. Execute uma das seguintes ações:

   - Se pretender ativar o registo de eliminação de ficheiros e registar operações em unidades amovíveis, selecione a caixa **Ativar registo de dados**.

     O Kaspersky Endpoint Security irá guardar um evento no ficheiro de registo e enviar uma mensagem ao Servidor de administração do Kaspersky Security Center sempre que o utilizador executa operações de escrita ou de eliminação com ficheiros em unidades amovíveis.

   - Caso contrário, desmarque a caixa de verificação **Ativar registo de dados**.

7. Especifique as operações que devem ser registadas. Para o fazer, execute uma das seguintes ações:

   - Se pretender que o Kaspersky Endpoint Security registe todos os eventos, selecione a caixa de verificação **Guardar informação sobre todos os ficheiros**.

   - Se pretender que o Kaspersky Endpoint Security registe apenas informações sobre ficheiros com um formato específico, na secção **Filtrar nos formatos de ficheiro**, selecione as caixas de verificação à frente dos formatos de ficheiro relevantes.

8. Especifique quais as ações dos utilizadores do Kaspersky Endpoint Security que devem ser registadas como eventos. Para tal:

   a. Na secção **Utilizadores**, clique no botão **Selecionar**.

      É aberta a janela padrão **Selecionar Utilizadores ou Grupos** no Microsoft Windows.

   b. Especifique ou edite a lista de utilizadores e/ou os grupos de utilizadores.

   Quando os utilizadores especificados na secção **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 uma mensagem para o Servidor de Administração do Kaspersky Security Center.

9. Na janela **Definições de registo de dados**, clique em **OK**.

10. Para guardar as alterações, clique no botão **Guardar**.

Pode ver os eventos associados a ficheiros em unidades amovíveis na Consola de Administração do Kaspersky Security Center na área de trabalho do nó **Servidor de Administração** no separador **Eventos**. Para que os eventos sejam apresentados no registo de eventos do Kaspersky Endpoint Security local, deve selecionar a caixa de verificação **Operação de ficheiro realizada** nas definições de notificação do componente Controlo de Dispositivos.

Adicionar uma rede Wi-Fi à lista confiável

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 confiáveis. O Controlo de dispositivos irá bloquear o acesso a todas as redes Wi-Fi exceto às especificadas na lista confiável.

Para adicionar uma rede Wi-Fi à lista confiável:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Dispositivos**.

   Na parte direita da janela, são apresentadas as definições do componente de Controlo de Dispositivos.
3. Na parte direita da janela, selecione o separador **Tipos de dispositivos**.

   O separador **Tipos de dispositivos** contém regras de acesso para todos os dispositivos incluídos na classificação do componente Controlo de Dispositivos.
4. Na coluna **Acesso** à frente do dispositivo **Wi-Fi**, clique com o botão direito para abrir o menu de contexto.
5. Selecione a opção **Bloquear com exceções**.
6. Na lista de dispositivos, selecione **Wi-Fi** e clique no botão **Editar**.

   Esta ação abre a janela **Redes Wi-Fi confiáveis**.
7. Clique no botão **Adicionar**.

   Esta ação abre a janela **Rede Wi-Fi confiável**.
8. Na janela **Rede Wi-Fi confiável**:

   - No campo de **Nome de rede**, especifique o nome da rede Wi-Fi que pretende adicionar à lista confiável.
   - Na lista pendente **Tipo de autenticação**, selecione o tipo da autenticação utilizado ao estabelecer ligação à rede Wi-Fi confiável.
   - Na lista pendente **Tipo de encriptação**, selecione o tipo da encriptação utilizado para assegurar o tráfego da rede Wi-Fi confiável.
   - No campo **Comentário**, pode especificar qualquer informação sobre a rede Wi-Fi adicionada.

   Uma rede Wi-Fi considera-se confiável se as suas definições corresponderem a todas as definições especificadas na regra.
9. Na janela **Rede Wi-Fi confiável**, clique em **OK**.
10. Na janela **Redes Wi-Fi confiáveis**, clique em **OK**.

Editar uma regra de acesso a barramentos de ligação

Para editar uma regra de acesso a barramentos de ligação:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Dispositivos**.

   Na parte direita da janela, são apresentadas as definições do componente de Controlo de Dispositivos.

3. Selecione o separador **Barramentos de ligação**.

   O separador **Barramentos de ligação** apresenta as regras de acesso para todos os barramentos de ligação classificados no componente Controlo de Dispositivos.

4. Selecione a regra de ligação do barramento que pretende editar.

5. Altere o valor do parâmetro de acesso:

   - Para permitir o acesso a um barramento de ligação, clique na coluna **Acesso** para abrir um menu de contexto e selecione **Permitir**.
   - Para bloquear o acesso a um barramento de ligação, clique na coluna **Acesso** para abrir um menu de contexto e selecione **Bloquear**.

6. Para guardar as alterações, clique no botão **Guardar**.

Ações com dispositivos confiáveis

Esta secção contém informações sobre ações com dispositivos confiáveis.

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

Por defeito, quando um dispositivo é adicionado à lista de dispositivos confiáveis, o acesso ao dispositivo é permitido a todos os utilizadores (no grupo de utilizadores Todos).

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

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Dispositivos**.

   Na parte direita da janela, são apresentadas as definições do componente de Controlo de Dispositivos.

3. Na parte direita da janela, selecione o separador **Dispositivos confiáveis**.

4. Clique no botão **Selecionar**.

   É aberta a janela **Selecionar dispositivos confiáveis**.

5. Selecione a caixa de verificação junto ao nome do dispositivo que pretende adicionar à lista de dispositivos confiáveis.

   A lista na coluna **Dispositivos** depende do valor selecionado na lista suspensa **Mostrar dispositivos ligados**.

6. Clique no botão **Selecionar**.

   É aberta a janela **Selecionar Utilizadores ou Grupos** no Microsoft Windows.

7. Na janela **Selecionar Utilizadores ou Grupos** no Microsoft Windows, especifique os utilizadores e/ou grupos de utilizadores para os quais o Kaspersky Endpoint Security reconhece os dispositivos selecionados como confiáveis.

   Os nomes dos utilizadores e/ou grupos de utilizadores especificados na janela **Selecione utilizadores e/ou grupos de utilizadores** no Microsoft Windows são apresentados no campo **Permitir a utilizadores e/ou grupos de utilizadores**.

8. Na janela **Selecionar dispositivos confiáveis**, clique em **OK**.

   Na tabela, no separador **Dispositivos confiáveis** da janela de definições do componente **Controlo de Dispositivos**, é apresentada uma linha e apresenta os parâmetros do dispositivo confiável adicionado.

9. Repita os passos de 4 a 7 para cada dispositivo que pretender adicionar à lista de dispositivos confiáveis para os utilizadores e/ou grupos de utilizadores especificados.

10. Para guardar as alterações, clique no botão **Guardar**.

Adicionar dispositivos à lista confiável com base no modelo ou ID do dispositivo

Por defeito, quando um dispositivo é adicionado à lista de dispositivos confiáveis, o acesso ao dispositivo é permitido a todos os utilizadores (no grupo de utilizadores Todos).

Para adicionar dispositivos à lista confiável com base no modelo ou ID do dispositivo:

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

2. Na pasta **Dispositivos geridos** na árvore da Consola de Administração, abra a pasta com o nome do grupo de administração relevante para o qual pretende criar uma lista de dispositivos confiáveis.

3. Na área de trabalho, selecione o separador **Políticas**.

4. Selecione a política pretendida.

5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.

   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.

6. Na secção **Controlo de terminal**, selecione a secção **Controlo de Dispositivos**.

7. Na parte direita da janela, selecione o separador **Dispositivos confiáveis**.

8. Clique no botão **Adicionar**.

   É apresentado o menu de contexto do botão.

9. No menu de contexto do botão **Adicionar**, execute uma das ações seguintes:

   - Selecione o botão **Dispositivos por ID** se pretender selecionar dispositivos com IDs exclusivos conhecidos para adicionar à lista de dispositivos confiáveis.

- Selecione o item **Dispositivos por modelo** para adicionar à lista aqueles dispositivos confiáveis cujos VID (ID de fornecedor) e PID (ID de produto) são conhecidos.

10. Na janela apresentada, na lista pendente **Tipo de dispositivo** selecione o tipo de dispositivos para serem apresentados na tabela abaixo.

11. Clique no botão **Atualizar**.

    A tabela apresenta uma lista de dispositivos para os quais os IDs e/ou os modelos de dispositivos são conhecidos e quais pertencem ao tipo selecionado na lista pendente **Tipo de dispositivo**.

12. Selecione as caixas de verificação junto aos nomes dos dispositivos que pretende adicionar à lista de dispositivos confiáveis.

13. Clique no botão **Selecionar**.

    É aberta a janela **Selecionar Utilizadores ou Grupos** no Microsoft Windows.

14. Na janela **Selecionar Utilizadores ou Grupos** no Microsoft Windows, especifique os utilizadores e/ou grupos de utilizadores para os quais o Kaspersky Endpoint Security reconhece os dispositivos selecionados como confiáveis.

    Os nomes dos utilizadores e/ou grupos de utilizadores especificados na janela **Selecione utilizadores e/ou grupos de utilizadores** no Microsoft Windows são apresentados no campo **Permitir a utilizadores e/ou grupos de utilizadores**.

15. Clique em **OK**.

    São apresentadas linhas juntamente com os parâmetros dos dispositivos confiáveis que foram adicionados na tabela no separador **Dispositivos confiáveis**.

16. Clique em **OK** ou **Aplicar** para guardar as alterações.

Adicionar dispositivos à lista confiável com base na máscara do ID do dispositivo

Por defeito, quando um dispositivo é adicionado à lista de dispositivos confiáveis, o acesso ao dispositivo é permitido a todos os utilizadores (no grupo de utilizadores Todos).

Podem ser adicionados dispositivos à lista confiável com base na máscara do seu ID apenas na Consola de Administração do Kaspersky Security Center.

Para adicionar dispositivos à lista confiável com base na máscara do seu ID:

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

2. Na pasta **Dispositivos geridos** na árvore da Consola de Administração, abra a pasta com o nome do grupo de administração relevante para o qual pretende criar uma lista de dispositivos confiáveis.

3. Na área de trabalho, selecione o separador **Políticas**.

4. Selecione a política pretendida.

5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:

- No menu de contexto da política, selecione **Propriedades**.
- Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.

6. Na secção **Controlo de terminal**, selecione a secção **Controlo de Dispositivos**.
7. Na parte direita da janela, selecione o separador **Dispositivos confiáveis**.
8. Clique no botão **Adicionar**.

   É apresentado o menu de contexto do botão.
9. No menu de contexto do botão **Adicionar**, selecione o item **Dispositivos por máscara de ID**.

   A janela **Adicionar dispositivos confiáveis por máscara de ID** é apresentada.
10. Na janela **Adicionar dispositivos confiáveis por máscara de ID**, introduza a máscara para os IDs dos dispositivos no campo **Máscara**.
11. Clique no botão **Selecionar**.

    É aberta a janela **Selecionar Utilizadores ou Grupos** no Microsoft Windows.
12. Na janela **Selecionar Utilizadores ou Grupos** no Microsoft Windows, especifique os utilizadores e/ou os grupos de utilizadores para os quais o Kaspersky Endpoint Security reconhece como confiáveis os dispositivos cujos modelos ou IDs correspondem à máscara especificada.

    Os nomes dos utilizadores e/ou grupos de utilizadores especificados na janela **Selecione utilizadores e/ou grupos de utilizadores** no Microsoft Windows são apresentados no campo **Permitir a utilizadores e/ou grupos de utilizadores**.
13. Clique em **OK**.

    Na tabela, no separador **Dispositivos confiáveis** na janela das definições do componente **Controlo de Dispositivos**, é apresentada uma linha com as definições da regra para adicionar dispositivos à lista de dispositivos confiáveis pela máscara dos seus IDs.
14. Para guardar as alterações, clique no botão **Guardar**.

Configurar acesso de utilizador a um dispositivo confiável

Por defeito, quando um dispositivo é adicionado à lista de dispositivos confiáveis, o acesso ao dispositivo é permitido a todos os utilizadores (no grupo de utilizadores Todos). Pode configurar o acesso de utilizadores (ou grupos de utilizadores) a um dispositivo confiável.

Configurar o acesso de utilizador a um dispositivo confiável:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Dispositivos**.

   Na parte direita da janela, são apresentadas as definições do componente de Controlo de Dispositivos.
3. Na parte direita da janela, selecione o separador **Dispositivos confiáveis**.
4. Na lista de dispositivos confiáveis, selecione um dispositivo para o qual quer editar regras de acesso.

5. Clique no botão **Editar**.

   É apresentada a janela **Configurar a regra de acesso a dispositivos confiáveis**.

6. Clique no botão **Selecionar**.

   É aberta a janela **Selecionar Utilizadores ou Grupos** no Microsoft Windows.

7. Na janela **Selecionar Utilizadores ou Grupos** no Microsoft Windows, especifique os utilizadores e/ou grupos de utilizadores para os quais o Kaspersky Endpoint Security reconhece os dispositivos selecionados como confiáveis.

8. Clique em **OK**.

   Os nomes dos utilizadores e/ou grupos de utilizadores especificados na janela **Selecione utilizadores e/ou grupos de utilizadores** do Microsoft Windows são apresentados no campo **Permitir a utilizadores e/ou grupos de utilizadores** da janela **Configurar a regra de acesso a dispositivos confiáveis**.

9. Clique em **OK**.

10. Para guardar as alterações, clique no botão **Guardar**.

Remover um dispositivo da lista de dispositivos confiáveis

Para remover um dispositivo da lista de dispositivos confiáveis:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Dispositivos**.

   Na parte direita da janela, são apresentadas as definições do componente de Controlo de Dispositivos.

3. Na parte direita da janela, selecione o separador **Dispositivos confiáveis**.

4. Selecione o dispositivo que pretende remover da lista de dispositivos confiáveis.

5. Clique no botão **Remover**.

6. Para guardar as alterações, clique no botão **Guardar**.

A decisão sobre o acesso a um dispositivo que tenha removido da lista de dispositivos confiáveis é tomada pelo Kaspersky Endpoint Security com base nas regras de acesso a dispositivos e nas regras de acesso a barramentos de ligação.

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. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Dispositivos**.

   Na parte direita da janela, são apresentadas as definições do componente de Controlo de Dispositivos.
3. Na parte direita da janela, clique no botão **Modelos**.

   É apresentada a janela **Modelos de mensagem**.
4. Execute uma das seguintes ações:

   - Para modificar o modelo da mensagem sobre acesso bloqueado a um dispositivo ou uma operação proibida com os conteúdos do dispositivo, selecione o separador **Bloqueio**.
   - Para modificar o modelo da mensagem que é enviada ao administrador da rede local, selecione o separador **Mensagem para o administrador**.
5. Editar o modelo da mensagem. Também pode utilizar os seguintes botões: **Variável**, **Predefinições** e **Ligação** (este botão está disponível apenas no separador **Bloqueio**).
6. Clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

Obter acesso a um dispositivo bloqueado

Estas instruções destinam-se a utilizadores de computadores cliente com o Kaspersky Endpoint Security instalado.

A funcionalidade do Kaspersky Endpoint Security que concede acesso temporário a um dispositivo está disponível apenas quando o Kaspersky Endpoint Security funciona com a política do Kaspersky Security Center e esta funcionalidade está ativada nas definições da política (consulte o *Manual do Administrador do Kaspersky Security Center*).

Para solicitar acesso a um dispositivo bloqueado a partir da janela de configurações do componente Controlo de Dispositivos:

1. Na janela de aplicação principal, selecione o separador **Proteção e Controlo**.
2. Clique na secção **Controlo de terminal**.

   A secção **Controlo de terminal** é apresentada.
3. Clique com o botão direito do rato para visualizar o menu da linha que contém as informações sobre o componente Controlo de Dispositivos.

   É aberto um menu para selecionar ações no componente.

4. Clique no botão **Acesso ao dispositivo**.

   É aberta a janela **Solicitar acesso ao dispositivo**.

5. Na lista de dispositivos ligados, selecione o dispositivo ao qual pretende aceder.

6. Clique no botão **Gerar ficheiro de acesso de pedido**.

   Esta ação abre a janela **A criar ficheiro de acesso de pedido**.

7. No campo **Duração do acesso**, especifique o período de tempo durante o qual pretende ter acesso ao dispositivo.

8. Clique no botão **Guardar**.

   Esta ação abre a janela padrão **Guardar ficheiro de acesso de pedido** do Microsoft Windows.

9. Na janela **Guardar ficheiro de acesso de pedido** do Microsoft Windows, selecione a pasta na qual pretende guardar o ficheiro de acesso de pedido para o dispositivo e clique no botão **Guardar**.

10. Envie o ficheiro de acesso de pedido do dispositivo ao administrador da rede local.

11. Receba o ficheiro-chave de acesso ao dispositivo proveniente do administrador da rede local.

12. Na janela **Solicitar acesso ao dispositivo**, clique no botão **Ativar chave de acesso**.

    É apresentada a janela padrão **Abrir chave de acesso** no Microsoft Windows.

13. Na janela **Abrir chave de acesso** do Microsoft Windows, selecione o ficheiro-chave de acesso do dispositivo recebido do administrador da rede local e clique em **Abrir**.

    A janela **Ativar a chave de acesso para o dispositivo** é aberta e apresenta informações sobre o acesso concedido.

14. Na janela **Ativar a chave de acesso para o dispositivo**, clique em **OK**.

Para solicitar acesso a um dispositivo bloqueado clicando na ligação na mensagem que informa que o dispositivo está bloqueado:

1. Na janela com a mensagem que informa que o dispositivo ou o barramento de ligação está bloqueado, clique na ligação **Solicitar acesso**.

   Esta ação abre a janela **A criar ficheiro de acesso de pedido**.

2. No campo **Duração do acesso**, especifique o período de tempo durante o qual pretende ter acesso ao dispositivo.

3. Clique no botão **Guardar**.

   Esta ação abre a janela padrão **Guardar ficheiro de acesso de pedido** do Microsoft Windows.

4. Na janela **Guardar ficheiro de acesso de pedido** do Microsoft Windows, selecione a pasta na qual pretende guardar o ficheiro de acesso de pedido para o dispositivo e clique no botão **Guardar**.

5. Envie o ficheiro de acesso de pedido do dispositivo ao administrador da rede local.

6. Receba o ficheiro-chave de acesso ao dispositivo proveniente do administrador da rede local.

7. Na janela **Solicitar acesso ao dispositivo**, clique no botão **Ativar chave de acesso**.

   É apresentada a janela padrão **Abrir chave de acesso** no Microsoft Windows.

8. Na janela **Abrir chave de acesso** do Microsoft Windows, selecione o ficheiro-chave de acesso do dispositivo recebido do administrador da rede local e clique em **Abrir**.

   A janela **Ativar a chave de acesso para o dispositivo** é aberta e apresenta informações sobre o acesso concedido.

9. Na janela **Ativar a chave de acesso para o dispositivo**, clique em **OK**.

O período de tempo durante o qual o acesso ao dispositivo é concedido pode ser diferente do período solicitado. O acesso ao dispositivo é concedido durante o período de tempo que o administrador da rede local especificar ao gerar a chave de acesso ao dispositivo.

Criar uma chave para aceder um dispositivo bloqueado utilizando o Kaspersky Security Center

Para atribuir a um utilizador acesso temporário a um dispositivo bloqueado, é necessária uma chave de acesso ao dispositivo. Pode criar uma chave de acesso utilizando o Kaspersky Security Center.

Para criar uma chave de acesso para um dispositivo bloqueado:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivo geridos** 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 **Dispositivos**.
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 a dispositivos e dados em modo offline**.

   É aberta a janela **Conceder acesso a dispositivos e dados em modo offline**.

6. Selecione o separador **Controlo de Dispositivos**.
7. No separador **Controlo de Dispositivos**, clique no botão **Procurar**.

   É apresentada a janela padrão **Selecionar ficheiro de acesso de pedido** no Microsoft Windows.

8. Na janela **Selecionar ficheiro de acesso de pedido** do Windows, selecione o ficheiro de acesso de pedido recebido do utilizador e clique no botão **Abrir**.

   O **Controlo de Dispositivos** mostra os detalhes do dispositivo bloqueado para o qual o utilizador solicitou acesso.

9. Especifique o valor da definição **Duração do acesso**.

   Esta definição define o período de tempo durante o qual o utilizador tem acesso ao dispositivo bloqueado. O valor predefinido é o valor especificado pelo utilizador ao criar o ficheiro de acesso de pedido.

10. Especifique o valor da definição **Período de ativação**.

    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.

11. Clique no botão **Guardar**.

    Esta ação abre a janela padrão **Guardar chave de acesso** do Microsoft Windows.

12. Selecione a pasta de destino na qual pretende guardar o ficheiro com a chave de acesso ao dispositivo bloqueado.

13. Clique no botão **Guardar**.

Controlo de Internet

Este componente está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para estações de trabalho. Este componente não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para servidores de ficheiros.

Esta secção contém informações sobre o Controlo de Internet e instruções para efetuar as configurações do componente.

Sobre o Controlo de Internet

O Controlo de Internet permite controlar ações pelos utilizadores da rede local, restringindo ou bloqueando o acesso aos recursos da Internet.

Um recurso da Internet é uma página da Internet individual ou várias páginas da Internet ou um site da Internet ou vários sites da Internet com uma característica comum.

O Controlo de Internet disponibiliza as seguintes opções:

- Poupar no tráfego.

  O tráfego é controlado através da restrição ou bloqueio das transferências de ficheiros multimédia ou através da restrição ou bloqueio do acesso a recursos da Internet que não estejam relacionados com as responsabilidades do cargo dos utilizadores.

- Delimitar o acesso por categorias de conteúdo de recursos da Internet.

  Para poupar no tráfego e reduzir potenciais perdas resultantes da má utilização do tempo dos funcionários, pode restringir ou bloquear o acesso a categorias específicas de recursos da Internet (por exemplo, bloquear o acesso a sites pertencentes à categoria "Meios de comunicação da Internet").

- Controlo centralizado de acesso a recursos da Internet.

  Ao utilizar o Kaspersky Security Center, estão disponíveis definições pessoais e de grupo de acesso a recursos da Internet.

Todas as restrições e bloqueios que forem aplicados ao acesso a recursos da Internet são implementados como regras de acesso a recursos da Internet.

Ativar e desativar o Controlo de Internet

Por defeito, o Controlo de Internet está ativado. Se necessário, pode desativar o Controlo de Internet.

Existem duas formas para ativar ou desativar o componente:

- No separador **Proteção e Controlo** na janela principal da aplicação
- Na janela de definições da aplicação

*Para ativar ou desativar o Controlo de Internet no separador **Proteção e Controlo** da janela principal da aplicação:*

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Controlo de terminal**.

   A secção **Controlo de terminal** é apresentada.
4. Clique com o botão direito do rato para visualizar o menu da linha que contém as informações sobre o componente Controlo de Internet.

   É aberto um menu para selecionar ações no componente.
5. Execute uma das seguintes ações:

   - Para ativar o Controlo de Internet, selecione **Iniciar** no menu.
   - Para desativar o Controlo de Internet, selecione **Parar** no menu.

Para ativar ou desativar o Controlo de Internet a partir da janela de definições da aplicação:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Internet**.

   Na parte direita da janela, são apresentadas as definições do componente Controlo de Internet.
3. Execute uma das seguintes ações:

   - Se pretender ativar o Controlo de Internet, selecione a caixa de verificação **Ativar Controlo de Internet**.
   - Se pretender desativar o Controlo de Internet, desmarque a caixa de verificação **Ativar Controlo de Internet**.

   Se o Controlo de Internet estiver desativado, o Kaspersky Endpoint Security não controla o acesso aos recursos da Internet.
4. Para guardar as alterações, clique no botão **Guardar**.

Categorias de conteúdo de recursos da Internet

As categorias de conteúdo de recursos da Internet indicadas (doravante também referidas como "categorias") indicadas abaixo foram selecionadas de forma a descrever com mais pormenor os blocos de dados alojados pelos recursos da Internet, considerando os respetivos aspetos funcionais e temáticos. A ordem pela qual as categorias são apresentadas nesta lista não reflete a importância relativa ou a prevalência de tais categorias na Internet. Os nomes das categorias são provisórios e utilizados apenas para os produtos e sites da Kaspersky. Os nomes não refletem necessariamente o significado implícito por lei. Um recurso da Internet pode pertencer a várias categorias em simultâneo.

Conteúdo para adultos

Esta categoria inclui os tipos seguintes de recursos da Internet:

- Os recursos da Internet com fotografias ou materiais de vídeo com conteúdos sexuais explícitos.

- Os recursos da Internet com materiais de texto, incluindo materiais literários ou artísticos, com conteúdos sexuais explícitos.
- Recursos da Internet dedicados à discussão de aspetos sexuais das relações humanas.

  Substitui a categoria "Meios de comunicação da Internet".

- Recursos da Internet com materiais eróticos, conteúdos que representam de forma realista o comportamento sexual de humanos ou conteúdos concebidos para estímulo sexual.
- Recursos da Internet de canais de comunicação e comunidades online com um público alvo definido, contendo secções especiais ou artigos individuais dedicados à vertente sexual das relações humanas.
- Recursos da Internet dedicados a perversões sexuais.
- Recursos da Internet que publicitam e comercializam artigos de teor sexual, serviços sexuais e serviços de acompanhantes, incluindo serviços sexuais online.
- Recursos da Internet com os seguintes conteúdos:
  - Artigos e blogues que abordam a educação sexual com temas científicos e populares.
  - Enciclopédias médicas, especificamente as respetivas secções sobre reprodução sexual.
  - Recursos de instituições médicas, especificamente as respetivas seções que abordam o tratamento de órgãos sexuais.

Software, áudio, vídeo

Esta categoria inclui as seguintes subcategorias que pode selecionar individualmente:

- **Áudio e vídeo**.

  Esta subcategoria inclui recursos da Internet que distribuem materiais de áudio e vídeo: filmes, gravações de emissões desportivas, gravações de concertos, canções, clipes de vídeos, gravações áudio e vídeo de apresentações, etc.

- **Torrents**.

  Esta subcategoria inclui sites de torrents que se destinam a partilhar ficheiros com tamanho ilimitado.

- **Partilha de ficheiros**.

  Esta subcategoria inclui a partilha de ficheiros independente da localização física dos ficheiros distribuídos.

Álcool, tabaco, narcóticos

Esta categoria inclui os recursos da Internet cujo conteúdo está direta ou indiretamente relacionado com produtos alcoólicos ou contendo álcool, produtos à base de tabaco e narcóticos, psicotrópicos e/ou substâncias tóxicas.

- Recursos da Internet que publicitam e comercializam tais substâncias e artigos relacionados com o seu consumo.

Substitui a categoria "Comércio eletrónico".

- Recursos da Internet com instruções sobre como consumir ou produzir substâncias narcóticas, psicotrópicas e/ou tóxicas.

Esta categoria inclui os recursos da Internet que abordam tópicos médicos e científicos.

Violência

Esta categoria inclui recursos da Internet com fotografias, vídeos ou materiais de texto que descrevam atos de violência, física ou psicológica, dirigida a humanos ou animais.

- Recursos da Internet que representam ou descrevem cenas de execuções, tortura ou abuso, ou as ferramentas para tais práticas.

  Substitui a categoria “Armas, explosivos, pirotecnia”.

- Os recursos da Internet que representam ou descrevem cenas de homicídio, luta, maus-tratos ou violação, cenas em que seres humanos, seres imaginários ou animais são abusados ou humilhados.
- Recursos da Internet com informação que incita a atos que colocam em perigo a vida ou o bem-estar, incluindo danos autoinfligidos ou suicídio.
- Recursos da Internet com informações que fundamentam ou justificam a prática de atos de violência e/ou crueldade ou que incitam atos violentos contra pessoas ou animais.
- Recursos da Internet com descrições particularmente realistas de vítimas e atrocidades de guerra, conflitos armados e confrontos militares, acidentes, catástrofes, desastres naturais, cataclismos industriais ou sociais ou sofrimento humano.
- Jogos de computador de navegador de Internet com cenas de violência e crueldade, incluindo os denominados “atiradores”, “lutadores”, “combatentes”, etc.

  Substitui a categoria “Jogos de computador”.

Armas, explosivos, pirotecnia

Esta categoria inclui recursos da Internet com informações sobre armas, explosivos e produtos pirotécnicos:

- Sites de fabricantes e lojas de armas, explosivos e produtos pirotécnicos.

  Substitui a categoria "Comércio eletrónico".

- Recursos da Internet dedicados à produção ou utilização de armas, explosivos e produtos pirotécnicos.

- Recursos da Internet com materiais de análise, histórico, de produção e informativos dedicados a armas, explosivos e produtos pirotécnicos.

O termo “armas” significa todos os dispositivos, itens e meios concebidos para ameaçar a vida ou o bem-estar de seres humanos e animais e/ou causar danos em equipamentos e estruturas.

Profanação

Esta categoria inclui os recursos da Internet em que é detetada linguagem profana.

Substitui a categoria “Conteúdo para adultos”.

Esta categoria também inclui recursos da Internet com materiais linguísticos e filológicos contendo profanação como objeto de estudo.

Jogo, lotarias, apostas

Esta categoria inclui os recursos da Internet que permitem aos utilizadores participar financeiramente em jogos, mesmo que a participação financeira não seja uma condição obrigatória para aceder ao site. Esta categoria inclui os recursos da Internet que oferecem:

- Jogos em que os participantes têm de contribuir monetariamente.

  Substitui a categoria “Jogos de computador”.

- Apostas em dinheiro.
- Lotarias que implicam a compra de bilhetes ou números.
- Informações que podem despoletar a participação em jogos, apostas e lotarias.

Substitui a categoria "Comércio eletrónico".

Esta categoria inclui jogos de participação gratuita, como modo em separado, bem como os recursos da Internet que publicitam ativamente recursos da Internet desta categoria.

Comunicações de rede

Esta categoria inclui os recursos da Internet que permitem aos utilizadores (registados ou não) enviar mensagens pessoais a outros utilizadores dos recursos da Internet relevantes ou outros serviços online e/ou adicionar conteúdo (aberto para acesso público ou restrito) para os recursos da Internet relevantes com determinadas condições. Pode selecionar individualmente as seguintes subcategorias:

- **Conversações e fóruns**.

Esta subcategoria inclui recursos da Internet para discussão pública de vários tópicos utilizando aplicações da Web especiais, bem como recursos da Internet concebidos para distribuir ou suportar aplicações de mensagens instantâneas que permitem a comunicação em tempo real.

- **Blogues**.

  Esta subcategoria inclui plataformas de blogues, ou seja, sites que fornecem serviços gratuitos ou pagos para a criação e manutenção de blogues.

- **Redes sociais**.

  Esta subcategoria inclui sites concebidos para criar, apresentar e gerir contactos entre pessoas, organizações e governos, que requerem o registo de uma conta de utilizador como condição de participação.

- **A atualizar sites**.

  Esta subcategoria inclui recursos da Internet que funcionam como várias redes sociais que fornecem serviços pagos ou gratuitos.

  Substitui as categorias "Conteúdo para adultos" e "Comércio eletrónico".

- **E-mail baseado na Internet**.

  Esta subcategoria inclui exclusivamente páginas de início de sessão de um serviço de e-mail e páginas de caixas de correio com e-mails e dados associados (tais como contactos pessoais). Esta categoria não inclui outras páginas da Internet de um fornecedor de serviços da Internet que também forneça serviços de e-mail.

Lojas online, bancos e sistemas de pagamento

Esta categoria inclui recursos da Internet concebidos para qualquer transação online em fundos monetários utilizando aplicações específicas da Web. Pode selecionar individualmente as seguintes subcategorias:

- **Compras e leilões**.

  Esta subcategoria inclui lojas online e leilões de venda de bens, trabalho ou serviços a indivíduos e/ou entidades legais, incluindo sites de lojas de vendas exclusivamente online e perfis online de lojas físicas que aceitam pagamentos online.

- **Bancos**.

  Esta subcategoria inclui páginas da Internet especializadas de bancos com banca online, incluindo transferências (eletrónicas) entre contas bancárias, realização de depósitos bancários, conversão de moeda, pagamentos de serviços de terceiros, etc.

- **Sistemas de pagamento**.

  Esta subcategoria inclui páginas da Internet de sistemas de dinheiro eletrónico que fornecem acesso à conta pessoal do utilizador.

Em termos técnicos, o pagamento pode ser efetuado utilizando cartões bancários de qualquer tipo (físico ou virtual, de débito ou crédito, local ou internacional) e dinheiro eletrónico. Os recursos da Internet podem pertencer a esta categoria independentemente de terem ou não tais aspetos técnicos, como transmissão de dados com o protocolo SSL, utilização de autenticação 3D Secure, etc.

Procura de emprego

Esta categoria inclui recursos da Internet concebidos para juntar empregadores e candidatos:

- Sites de agências de recrutamento (agências de emprego e/ou de recrutamento).
- Sites de empregadores com descrições das ofertas disponíveis e das suas vantagens.
- Portais independentes com ofertas de emprego de empregadores e agências de recrutamento.
- Redes sociais profissionais que, entre outros, permitem publicar ou procurar informação sobre especialistas que não procuram emprego ativamente.

Substitui a categoria "Meios de comunicação da Internet".

Sistemas de acesso anónimo

Esta categoria inclui recursos da Internet que funcionam como intermediários na transferência de conteúdo de outros recursos da Internet, utilizando aplicações da Web especiais com a finalidade de:

- Ignorar as restrições impostas por um administrador de rede relativamente ao acesso a endereços da Web e endereços IP;
- Aceder anonimamente a recursos da Internet, incluindo recursos da Internet que rejeitam especificamente pedidos de HTTP de determinados endereços IP ou dos seus grupos (por exemplo, endereços IP agrupados por país de origem).

Esta categoria inclui os recursos da Internet que se destinam exclusivamente às finalidades acima mencionadas (“anonymizers”) e recursos da Internet com funcionalidades tecnicamente semelhantes.

Jogos de computador

Esta categoria inclui os recursos da Internet dedicados a jogos de computador de vários géneros:

- Sites de programadores de jogos de computador.
- Recursos da Internet dedicados à discussão de jogos de computador.

Substitui a categoria "Meios de comunicação da Internet".

- Recursos da Internet que fornecem a possibilidade técnica de participação online em jogos, juntamente com outros participantes ou individualmente, com a instalação local de aplicações ou sem instalação (“jogos de navegador”).
- Recursos da Internet concebidos para publicitar, distribuir e dar suporte a software de jogos.

Substitui a categoria "Comércio eletrónico".

Religiões, associações religiosas

Esta categoria inclui recursos da Internet com materiais sobre movimentos públicos, associações e organizações com uma ideologia religiosa e/ou culto de qualquer tipo.

- Sites de organizações religiosas oficiais em diferentes níveis, incluindo religiões internacionais a comunidades religiosas locais.
- Sites de associações e sociedades religiosas não registadas que surgiram a partir de uma comunidade ou associação religiosa dominante.
- Sites de comunidades e associações religiosas que surgiram de forma independente dos movimentos religiosos tradicionais, incluindo pela iniciativa de um fundador específico.
- Sites de organizações interconfessionais que têm como objetivo a cooperação entre representantes de diferentes religiões tradicionais.
- Recursos da Internet com materiais académicos, históricos e enciclopédicos sobre religião.
- Recursos da Internet com descrições detalhadas do culto religioso, incluindo rituais envolvendo a adoração de Deus, seres e/ou itens que se crê terem poderes sobrenaturais.

Meios de comunicação social de notícias

Esta categoria inclui recursos da Internet com conteúdo de notícias públicas criado pelos meios de comunicação ou publicações online que permitem aos utilizadores adicionar as suas notícias:

- Sites de canais de comunicação.
- Sites com oferta de serviços de informação com a atribuição de fontes oficiais de informação.
- Sites que oferecem serviços agregados de conjuntos de informações noticiosas de várias fontes, oficiais e não oficiais.
- Sites em que o conteúdo noticioso é criado pelos próprios utilizadores (“sites de notícias sociais”).

Substitui a categoria "Meios de comunicação da Internet".

Banners

Esta categoria inclui os recursos da Internet com banners. A informação anunciada em banners podem distrair os utilizadores da sua atividade, ao mesmo tempo que as transferências de banners aumentam o volume de tráfego.

Sobre as regras de acesso a recursos da Internet

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 de determinadas categorias. Quando os utilizadores visitam recursos da Internet que pertençam à categoria de conteúdo e/ou categoria de tipo de dados selecionada, o Kaspersky Endpoint Security executa a ação especificada na regra.

- **Filtro por endereços de recursos da Internet**. Pode controlar o acesso de utilizadores a todos os endereços de recursos da Internet ou a endereços de recursos da Internet individuais e/ou grupos de endereços de recursos da Internet.

  Se a filtragem por conteúdo e a filtragem por endereços de recursos da Internet forem especificadas e os endereços de recursos da Internet e/ou grupos de endereços de recursos da Internet especificados pertencerem às categorias de conteúdo ou categorias de tipos de dados selecionadas, o Kaspersky Endpoint Security não controla o acesso a todos os recursos da Internet nas categorias de conteúdo e/ou tipo de dados selecionadas. Em vez disso, a aplicação controla o acesso apenas aos endereços de recursos da Internet e/ou grupos de endereços de recursos da Internet especificados.

- **Filtrar por nomes de utilizadores e grupos de utilizadores**. Pode especificar os nomes dos utilizadores e/ou dos grupos de utilizadores para os quais o acesso aos recursos da Internet é controlado de acordo com a regra.

- **Agendamento de regras**. Pode especificar o agendamento de regra. O agendamento de regra determina o período durante o qual o Kaspersky Endpoint Security monitoriza o acesso aos recursos da Internet abrangidos pela regra.

Após a instalação do Kaspersky Endpoint Security, a lista de regras do componente Controlo de Internet não está em branco. Existem duas regras predefinidas:

- A regra Tabelas de Estilo e Cenários 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.

- A "Regra predefinida", que concede a todos os utilizadores acesso a quaisquer recursos da Internet em qualquer altura.

Ações com regras de acesso a recursos da Internet

Pode executar as seguintes ações em regras de acesso a recursos da Internet:

- Adicionar uma nova regra

- Editar uma regra

- Atribuir prioridade a uma regra

  A prioridade de uma regra é definida pela posição da linha que contém uma breve descrição desta regra inserida na tabela regras de acesso na janela de definições do componente Controlo de Internet. Isto significa que uma regra que esteja numa posição superior na tabela regras de acesso tem uma prioridade superior relativamente a uma regra que esteja posicionada mais abaixo.

  Se o recurso da Internet a que o utilizador está a tentar aceder satisfizer os parâmetros de várias regras, o Kaspersky Endpoint Security executa uma ação em conformidade com a regra com a prioridade mais elevada.

- Testar uma regra.

  Pode verificar a consistência de regras utilizando a função Diagnósticos de regras.

- Ativar ou desativar uma regra.

Uma regra de acesso a recursos da Internet pode ser ativada (estado de funcionamento: *Ativado*) ou desativada (estado de funcionamento: *Desativado*). Por defeito, após a criação de uma regra, esta é ativada (estado de funcionamento: *Ativado)*. Pode desativar a regra.

- Eliminar regra

Adicionar e editar uma regra de acesso a recursos da Internet

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

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Internet**.

   Na parte direita da janela, são apresentadas as definições do componente Controlo de Internet.
3. Execute uma das seguintes ações:
   - Para adicionar uma regra, clique no botão **Adicionar**.
   - Se pretende editar uma regra existente, selecione a regra na tabela e clique no botão **Editar**.

   É apresentada a janela **Regra de acesso a recursos da Internet**.
4. Especifique ou edite as definições da regra. Para tal:
   a. No campo **Nome**, introduza ou edite o nome da regra.
   b. Na lista pendente **Conteúdo de filtro**, selecione a opção pretendida:
      - **Qualquer conteúdo**.
      - **Por categorias de conteúdo**.
      - **Por tipos de dados**.
      - **Por categorias de conteúdo e tipos de dados**.
   c. Se estiver selecionada outra opção que não **Qualquer conteúdo**, são apresentadas as secções para que sejam selecionadas categorias de conteúdo e/ou tipos de dados. Selecione as caixas de verificação junto dos nomes das categorias de conteúdo e/ou tipos de dados pretendidas.

      Selecionar a caixa de verificação junto ao nome de uma categoria de conteúdo e/ou tipo de dados significa que o Kaspersky Endpoint Security aplica a regra para controlar o acesso aos recursos da Internet que pertencem às categorias de conteúdo selecionadas e/ou categorias de tipos de dados.
   d. Na lista suspensa **Aplicar aos endereços**, selecione a opção pretendida:
      - **Para todos os endereços**.
      - **Para endereços individuais**.
   e. Se a opção **Para endereços individuais** estiver selecionada, é apresentada uma secção onde pode criar uma lista de recursos da Internet. Pode adicionar ou editar os endereços de recursos da Internet utilizando os botões **Adicionar**, **Editar**, e **Eliminar**.

f. Selecione a caixa de verificação **Especifique utilizadores e/ou grupos**.

g. Clique no botão **Selecionar**.

É aberta a janela **Selecionar Utilizadores ou Grupos** no Microsoft Windows.

h. Especifique ou edite a lista de utilizadores e/ou grupos de utilizadores para os quais o acesso aos recursos da Internet descritos pela regra deve ser permitido ou bloqueado.

i. Na lista suspensa **Ação**, selecione a opção pretendida:

- **Permitir** Se este valor for selecionado, o Kaspersky Endpoint Security permite o acesso a recursos da Internet que correspondem aos parâmetros da regra.
- **Bloquear** Se este valor for selecionado, o Kaspersky Endpoint Security impede o acesso a recursos da Internet que correspondem aos parâmetros da regra.
- **Aviso**. Se este valor estiver selecionado, 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.

j. 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:

1. Junto à lista suspensa **Agendamento de regras**, clique no botão **Configuração**.

   É aberta a janela **Agendamento de regras**.

2. Para adicionar ao agendamento de regra um intervalo de tempo durante o qual a regra não é aplicada, na tabela apresentada no agendamento de regra, clique nas células da tabela correspondentes à hora e ao dia da semana que pretende selecionar.

   A cor das células muda para cinzento.

3. Para substituir um intervalo de tempo durante o qual a regra é aplicada por um intervalo de tempo durante o qual a regra não é aplicada, clique nas células cinzentas na tabela correspondentes à hora e ao dia da semana que pretende selecionar.

   A cor das células muda para verde.

4. Clique no botão **Guardar como**.

   É aberta a janela **Nome do agendamento da regra**.

5. Introduza um Nome do agendamento da regra ou utilize o nome predefinido sugerido.

6. Clique em **OK**.

5. Na janela **Regra de acesso a recursos da Internet**, clique em **OK**.

6. Para guardar as alterações, clique no botão **Guardar**.

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. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Internet**.

   Na parte direita da janela, são apresentadas as definições do componente Controlo de Internet.
3. Na parte direita da janela, selecione a regra para a qual pretende alterar a prioridade.
4. Utilize os botões **Mover cima** e **Mover baixo** para mover a regra para a classificação pretendida na lista de regras.
5. Repita os passos 3 e 4 para as regras cuja prioridade pretende alterar.
6. Para guardar as alterações, clique no botão **Guardar**.

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. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Internet**.

   Na parte direita da janela, são apresentadas as definições do componente Controlo de Internet.
3. Na parte direita da janela, clique no botão **Diagnósticos**.

   É aberta a janela **Diagnósticos de regras**.
4. Preencha os campos na secção **Condições**:

   a. Se pretender testar as regras que o Kaspersky Endpoint Security utiliza para controlar o acesso a um recurso da Internet específico, selecione a caixa de verificação **Especifique o endereço**. Introduza o endereço do recurso da Internet no campo abaixo.

   b. 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.

   c. Se pretender testar as regras que o Kaspersky Endpoint Security utiliza para controlar o acesso aos recursos da Internet de categorias de conteúdo e/ou categorias de tipos de dados especificadas, na lista suspensa **Conteúdo de filtro**, selecione a opção pretendida (**Por categorias de conteúdo**, **Por tipos de dados** ou **Por categorias de conteúdo e tipos de dados**).

   d. 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.
5. Clique no botão **Teste**.

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 **Teste**. 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.

Ativar e desativar uma regra de acesso a recursos da Internet

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

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Internet**.

   Na parte direita da janela, são apresentadas as definições do componente Controlo de Internet.
3. Na parte direita da janela, selecione a regra que pretende ativar ou desativar.
4. Na coluna **Estado**, execute as seguintes ações:
   - Se pretender ativar a utilização da regra, selecione o valor *Ativado*.
   - Se pretender desativar a utilização da regra, selecione o valor *Desativado*.
5. Para guardar as alterações, clique no botão **Guardar**.

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

Quando o Service Pack 1 Maintenance Release 1 ou uma versão anterior da aplicação é atualizada para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows, as regras de acesso de recursos da Internet baseadas em categorias de conteúdo do recurso da Internet são migradas segundo os princípios seguintes:

- As regras de acesso de recursos da Internet baseadas em uma ou várias categorias de conteúdo de recursos da Internet das listas "Fóruns e conversações", "E-mail na Internet" e "Redes sociais" migram para a categoria de conteúdo de recursos da Internet "Meios de comunicação da Internet".
- As regras de acesso de recursos da Internet baseadas em uma ou várias categorias de conteúdo de recursos da Internet das listas "Lojas on-line" e "Sistemas de pagamentos" migram para a categoria de conteúdo de recursos da Internet "Comércio eletrónico".
- As regras de acesso de recursos da Internet baseadas na categoria de conteúdo de recursos da Internet “Jogo” migram para a categoria de conteúdo “Jogo, lotarias, apostas”.
- As regras de acesso de 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 de recursos da Internet baseadas em categorias de conteúdo que não estão enumeradas na lista acima são migradas sem alterações.

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

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Internet**.

   Na parte direita da janela, são apresentadas as definições do componente Controlo de Internet.
3. Selecione a regra cuja lista de endereços de recursos da Internet pretende exportar para um ficheiro.
4. Clique no botão **Editar**.

   É apresentada a janela **Regra de acesso a recursos da Internet**.
5. Se não pretender exportar a lista completa de endereços de recursos da Internet, mas apenas uma parte, selecione os endereços de recursos da Internet requeridos.
6. À direita do campo que contém a lista de endereços de recursos da Internet, clique no botão .

   É aberta a janela de confirmação da ação.
7. Execute uma das seguintes ações:

   - Se pretender exportar apenas os itens selecionados da lista de endereços de recursos da Internet, na janela de confirmação da ação, clique no botão **Sim**.
   - Se pretender exportar todos os itens da lista de endereços de recursos da Internet, na janela de confirmação da ação, clique no botão **Não**.

     É aberta a janela padrão **Guardar como** do Microsoft Windows.
8. Na janela **Guardar como** do Microsoft Windows, selecione o ficheiro para o qual pretende exportar a lista de endereços de recursos da Internet. Clique no botão **Guardar**.

Para importar a lista de endereços de recursos da Internet de um ficheiro para uma regra:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Internet**.

   Na parte direita da janela, são apresentadas as definições do componente Controlo de Internet.
3. Execute uma das seguintes ações:

   - Se pretender criar uma nova regra de acesso a recursos da Internet, clique no botão **Adicionar**
   - Selecione a regra de acesso a recursos da Internet que pretende editar. Em seguida, clique no botão **Editar**.

   É apresentada a janela **Regra de acesso a recursos da Internet**.

4. Execute uma das seguintes ações:

   - Se estiver a criar uma nova regra de acesso a recursos da Internet, selecione **Para endereços individuais** na lista suspensa **Aplicar aos endereços**.
   - Se estiver a editar uma regra de acesso a recursos da Internet, avance para o passo 5 destas instruções.

5. À direita do campo que contém a lista de endereços de recursos da Internet, clique no botão .

   Se estiver a criar uma nova regra, é aberta a janela padrão **Abrir ficheiro** do Microsoft Windows.

   Se estiver a editar uma regra, é aberta uma janela a solicitar a confirmação.

6. Execute uma das seguintes ações:

   - Se estiver a editar uma nova regra de acesso a recursos da Internet, avance para o passo 7 destas instruções.
   - Se estiver a editar uma regra de acesso a recursos da Internet, execute uma das seguintes ações na janela de confirmação:
     - Se pretender adicionar itens importados da lista de endereços de recursos da Internet aos existentes, clique no botão **Sim**.
     - Se pretender apagar os itens existentes da lista de endereços de recursos da Internet e adicionar os itens importados, clique no botão **Não**.

   É aberta a janela **Abrir ficheiro** no Microsoft Windows.

7. Na janela **Abrir ficheiro** do Microsoft Windows, selecione um ficheiro com uma lista de endereços de recursos da Internet a importar.

8. Clique no botão **Abrir**.

9. Na janela **Regra de acesso a recursos da Internet**, clique em **OK**.

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.

   Para incluir o carácter `*` na máscara de endereço, introduza o carácter `*` duas vezes.

2. A sequência de caracteres `www.` no início da máscara de endereço é interpretada como uma sequência `*.`

   Exemplo: a máscara de endereço www.exemplo.com é processada como *.exemplo.com.

3. Se uma máscara de endereço não começar com o carácter `*`, o conteúdo da máscara de endereço é equivalente ao mesmo conteúdo com o prefixo `*.`

4. Uma sequência de caracteres `*.` no início de uma máscara de endereço é interpretada como `*.` ou uma cadeia vazia.

   Exemplo: a máscara de endereço http://www.*.example.com abrange o endereço http://www2.example.com.

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 exemplo.com abrange os endereços http://example.com e https://example.com.

   - Se a máscara de endereço contiver um protocolo de rede, esta máscara de endereço abrange apenas endereços com o mesmo protocolo de rede que a máscara de endereço.

     Exemplo: a máscara de endereço http://*.example.com abrange o endereço http://www.example.com mas não o endereço https://www.example.com.

9. Uma máscara de endereço entre aspas é processada sem considerar quaisquer substituições adicionais, exceto o carácter `*`, se tiver sido inicialmente incluído na máscara de endereço. As regras 5 e 7 não se aplicam a máscaras de endereço entre aspas duplas (ver exemplos 14 – 18 na tabela abaixo).

10. O nome de utilizador e a password, a porta de ligação e a utilização de maiúsculas ou minúsculas nos caracteres não são tidos em consideração durante a comparação com a máscara de endereço de um recurso da Internet.

Exemplos de como utilizar regras para criar máscaras de endereço

N.º	Máscara de endereço	Endereço de recurso da Internet a verificar	O endereço é abrangido pela máscara de endereço	Comentário
1	*.exemplo.com	http://www.123exemplo.com	Não	Ver regra 1.
2	*.exemplo.com	http://www.123.exemplo.com	Sim	Ver regra 1.
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 2, 1.
7	www.exemplo.com	https://www.exemplo.com	Sim	Ver regras 2, 1.
8	http://www.*.exemplo.com	http://123.exemplo.com	Sim	Ver regras 2, 4, 1.
9	www.exemplo.com	http://www.exemplo.com/abc	Sim	Ver regras 2, 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://exemplo.com	Sim	Ver regra 7.
13	http://exemplo.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.

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 na lista pendente **Ação** 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 na lista pendente **Ação** 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. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Controlo de terminal**, selecione a subsecção **Controlo de Internet**.

   Na parte direita da janela, são apresentadas as definições do componente Controlo de Internet.
3. Na parte direita da janela, clique no botão **Modelos**.

   É apresentada a janela **Modelos de mensagem**.
4. Execute uma das seguintes ações:

   - Se pretender editar o modelo da mensagem que avisa o utilizador a não visitar um recurso da Internet, selecione o separador **Aviso**.
   - Se pretender editar o modelo da mensagem que informa o utilizador que o acesso a um recurso da Internet está bloqueado, selecione o separador **Bloqueio**.
   - Para editar o modelo da mensagem enviado ao administrador, selecione o separador **Mensagem para o administrador**.
5. Editar o modelo da mensagem. Também pode utilizar a lista pendente **Variável**, bem como os botões **Predefinições** e **Ligação** (este botão não está disponível no separador **Mensagem para o administrador**).
6. Clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

KATA Endpoint Sensor

As definições do componente KATA Endpoint Sensor estão disponíveis apenas na Consola de Administração do Kaspersky Security Center. Para utilizar este componente, tem de instalar o administration plug-in.

Esta secção contém a informação sobre o KATA Endpoint Sensor e instruções sobre como ativar ou desativar este componente.

Sobre o KATA Endpoint sensor

O KATA Endpoint Sensor é um componente da Kaspersky Anti Targeted Attack Platform. Esta solução destina-se à deteção rápida de ameaças como, por exemplo, ataques direcionados.

Este componente está instalado em computadores cliente. Nestes computadores o componente monitoriza constantemente os processos, as ligações de rede ativas e ficheiros que são alterados e volta a transmitir esta informação para a Kaspersky Anti Targeted Attack Platform.

A funcionalidade do componente está disponível nos seguintes sistemas operativos:

- Microsoft Windows 7 Professional/Enterprise/Ultimate x86 Edition SP1, Microsoft Windows 7 Professional/Enterprise/Ultimate x64 Edition SP1.
- Microsoft Windows 8.1 Enterprise x86 Edition, Microsoft Windows 8.1 Enterprise x64 Edition.
- Microsoft Windows 10 Pro/Enterprise x86 Edition, Microsoft Windows 10 Pro/Enterprise x64 Edition.
- Microsoft Windows Server 2008 R2 Standard/Enterprise x64 SP1.
- Microsoft Windows Server 2012 Standard/Foundation/Essentials x64 Edition, Microsoft Windows Server 2012 R2 Standard/Foundation/Essentials x64 Edition.
- Microsoft Windows Server 2016

Para obter mais informações sobre a Kaspersky Anti Targeted Attack Platform que não sejam facultadas neste documento, consulte a secção de ajuda da Kaspersky Anti Targeted Attack Platform.

As ligações de entrada a computadores com o componente KATA Endpoint Sensor devem ser autorizadas diretamente a partir do servidor do Kaspersky Anti Targeted Attack Platform, sem um servidor de proxy.

Ativar e desativar o componente do KATA Endpoint Sensor

Ativar ou desativar o componente KATA Endpoint Sensor:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com nome do grupo de administração relevante para o qual pretende editar as definições de políticas.

3. Na área de trabalho, selecione o separador **Políticas**.

4. Selecione a política pretendida.

5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.

6. Na secção de **Configurações avançadas**, selecione a subsecção **KATA Endpoint Sensor**.

7. Execute uma das seguintes ações:

   - Se pretender ativar o KATA Endpoint Sensor, selecione a caixa de verificação **KATA Endpoint Sensor**.
   - Se pretender desativar o KATA Endpoint Sensor, desmarque a caixa de verificação **KATA Endpoint Sensor**.

8. Se tiver selecionado a caixa de verificação **KATA Endpoint Sensor** durante o passo anterior, no campo **Endereço do Servidor**, especifique a morada de servidor da Kaspersky Anti Targeted Attack Platform composta pelas seguintes partes:

   a. Nome de Protocolo

   b. Endereço IP ou nome de domínio totalmente qualificado (FQDN) do servidor

   c. Caminho para o Windows Event Collector no servidor

9. Clique em **OK**.

10. Aplicar a política.

    Consulte o *Manual do Administrador do Kaspersky Security Center* para obter mais informações sobre a aplicação da política do Kaspersky Security Center.

Encriptação de dados

Se o Kaspersky Endpoint Security estiver instalado num computador com o Microsoft Windows para estações de trabalho, a funcionalidade de encriptação de dados está totalmente disponível. Se o Kaspersky Endpoint Security estiver instalado num computador com o Microsoft Windows for File Servers, apenas a encriptação de disco rígido com a tecnologia de Encriptação de Unidade BitLocker está disponível.

Esta secção contém informações sobre a encriptação e desencriptação de unidades de disco rígido, unidades amovíveis e ficheiros e pastas em unidades de leitura locais e faculta instruções para a configuração e execução de encriptação e desencriptação de dados com o Kaspersky Endpoint Security e o plug-in de administração do Kaspersky Endpoint Security.

Se não existir acesso aos dados encriptados, consulte as instruções especiais para trabalhar com dados encriptados (Trabalhar com ficheiros encriptados em caso de limitações da funcionalidade de encriptação de ficheiros, Trabalhar com dispositivos encriptados caso o acesso aos mesmos não exista).

Ativação da apresentação de configurações de encriptação na política do Kaspersky Security Center

Para ativar a apresentação de configurações de encriptação na política do Kaspersky Security Center:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. No menu de contexto do nó do **Servidor de Administração – <Nome do computador>** da árvore da Consola de Administração, selecione **Ver** Configurações da Interface de Utilizador.

   A janela **Configurações da Interface de Utilizador** é apresentada.
3. Na janela **Definições da interface** , selecione a caixa de verificação **Apresentar encriptação e proteção de dados**.
4. Clique em **OK**.

Sobre a 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.

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 o programa seja ativado 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, 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:

- **Encriptar ficheiros nas 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 do Kaspersky Security Center, 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.

  Consulte o *Manual do Administrador do Kaspersky Security Center* para obter mais informações sobre a aplicação da política do Kaspersky Security Center.

- **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.

A aplicação executa a ação especificada na regra de encriptação quando a política do Kaspersky Security Center é aplicada.

- **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 arquivos 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 unidades de disco rígido**. Pode selecionar uma tecnologia de encriptação: Encriptação de disco Kaspersky ou Encriptação de Unidade BitLocker (aqui também referida simplesmente como "BitLocker").

  BitLocker é uma tecnologia que faz parte do sistema operativo do 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 de encriptação de unidade de disco rígido predefinida e criar uma lista de unidades de disco rígido a serem excluídas da encriptação. O Kaspersky Endpoint Security encripta unidades de disco rígido setor 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. Consulte o *Manual do Administrador do Kaspersky Security Center* para obter mais informações sobre a aplicação da política do Kaspersky Security Center.

  Após a encriptação das unidades de disco rígido do sistema, no próximo arranque do computador, o utilizador tem de efetuar a autenticação utilizando o Agente de Autenticação antes de as unidades de disco rígido poderem ser acedidas e o sistema operativo ser carregado. Para tal é necessário introduzir a password do token ou smart card ligado ao computador ou o nome de utilizador e a password da conta do Agente de Autenticação criada pelo administrador da rede local utilizando as tarefas de gestão de conta do Agente de Autenticação. Estas contas são baseadas em contas do Microsoft Windows com as quais os utilizadores iniciam sessão no sistema operativo. Pode gerir as contas do Agente de Autenticação e utilizar 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 no *Manual do Administrador do Kaspersky Security Center*.

  Quando uma versão da aplicação é atualizada para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows, a lista de contas de Agente de Autenticação não é guardada.

  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 unidades de disco rígido 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 novos ficheiros são escritos num novo dispositivo durante a execução de uma encriptação normal com a função **Encriptar apenas espaço utilizado do disco** ativada no computador, 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 ficheiros encriptados estiver sob o controlo de outro Servidor de administração e os ficheiros encriptados nunca tiverem sido acedidos, o acesso pode ser obtido de uma das seguintes formas:

- solicitar o acesso aos objetos encriptados ou ao administrador da rede local;
- restaurar os dados em dispositivos encriptados utilizando a Ferramenta de Restauro;
- Restaurar a configuração do Servidor de Administração do Kaspersky Security Center que controlava o computador na altura da encriptação a partir de uma cópia de segurança e utilizar essa configuração no Servidor de Administração que agora controla o computador com os objetos encriptados.

A aplicação cria ficheiros de serviço durante a encriptação. São necessários cerca de dois a três porcento 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.

A compatibilidade entre a funcionalidade de encriptação do Kaspersky Endpoint Security e o Kaspersky Anti-Virus for UEFI não é suportada. A encriptação de unidades de disco rígido de computadores em que o Kaspersky Anti-Virus for UEFI está instalado causa a inoperabilidade do Kaspersky Anti-Virus for UEFI.

Limitações da funcionalidade de encriptação

Criar novas partições em unidades de disco rígido encriptadas bem como formatar as partições existentes das unidades de disco rígido encriptadas pode levar à perda de dados nestas unidades de disco rígido.

A encriptação de unidades de disco rígido utilizando a tecnologia de Encriptação de disco Kaspersky não está indisponível para unidades de disco rígido que não cumpram os requisitos de hardware e de software.

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.
- A tecnologia Rapid Start da ®Intel e as unidades que têm uma partição de hibernação mesmo quando a tecnologia Rapid Start da ®Intel está desativada.
- Unidades em formato MBR com mais de quatro partições expandidas.
- ficheiro de troca localizado numa unidade que não pertence ao sistema.
- Sistema multiboot com vários sistemas operativos instalados em simultâneo.
- Partições dinâmicas (são suportadas apenas as partições primárias).
- Unidades com menos de 2% 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.

Alterar o algoritmo de encriptação

O algoritmo de encriptação utilizado pelo Kaspersky Endpoint Security para a encriptação de dados depende das bibliotecas de encriptação que estão incluídas no kit de distribuição.

Para alterar o algoritmo de encriptação:

1. Desencriptar objetos que o Kaspersky Endpoint Security encriptou antes de começar a alterar o algoritmo de encriptação.

   Depois da alteração do algoritmo 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 kit de distribuição que contém bibliotecas de encriptação de contas de bits diferentes.

Ativação da tecnologia de autenticação única (SSO)

A tecnologia de autenticação única (SSO) não é compatível com o fornecimento de credenciais de conta por parte de terceiros.

Para ativar a tecnologia de autenticação única (SSO):

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

2. Na pasta **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração para o qual pretende ativar a tecnologia de autenticação única (SSO).

3. Na área de trabalho, selecione o separador **Políticas**.

4. Selecione a política pretendida.

5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.

6. Na secção **Encriptação de Dados**, selecione a subsecção **Definições de encriptação comuns**.

7. Na subsecção **Definições de encriptação comuns**, clique no botão **Configurar** na secção **Definições de password**.

   Será aberto o separador **agente de autenticação** da janela **Definições da password de encriptação**.

8. Selecione a caixa de verificação **Utilizar a tecnologia SSO (Single Sign-On)**.

9. Clique em **OK**.

10. Para guardar as alterações, na janela **Propriedades: <Nome da política>** clique em **OK**.

11. Aplicar a política.

    Consulte o *Manual do Administrador do Kaspersky Security Center* para obter mais informações sobre a aplicação da política do Kaspersky Security Center.

Considerações especiais para a encriptação de ficheiros

Ao utilizar a funcionalidade de encriptação de ficheiros, lembre-se dos seguintes pontos:

- A política do Kaspersky Security Center com predefinições para encriptação de unidades amovíveis é formada por um grupo específico de computadores geridos. Deste modo, o resultado da aplicação da política de encriptação / desencriptação de dados em unidades amovíveis depende do computador ao qual a unidade amovível está ligada.

- O Kaspersky Endpoint Security não encripta/desencripta ficheiros com o estado apenas de leitura que estão armazenados em unidades amovíveis.

- 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/desencripta ficheiros em pastas predefinidas de perfis de utilizadores em roaming, perfis de utilizador obrigatórios, perfis de utilizador temporários e pastas redirecionadas. A lista de pastas padrão recomendada pela Kaspersky para encriptação inclui as seguintes pastas:

  - Os Meus Documentos
  - Favoritos
  - Cookies

- Ambiente de Trabalho
- Ficheiros temporários do Internet Explorer
- Ficheiros temporários
- Ficheiros do Outlook

- O Kaspersky Endpoint Security não efetua encriptação de ficheiros e pastas quando esse procedimento pode danificar o sistema operativo e as aplicações nele instaladas. Por exemplo, os seguintes ficheiros e pastas com todas as pastas imbricadas estão na lista de exclusões da encriptação:
  - %WINDIR%.
  - %PROGRAMFILES%, %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 uma tarefa de encriptação de um ficheiro e uma pasta.
- 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 de SSD ligadas por bus USB e bus FireWire

Encriptar ficheiros nas unidades locais do computador

A encriptação de ficheiros em unidades de leitura locais está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para estações de trabalho. A encriptação de ficheiros em unidades de leitura locais está indisponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para servidores de ficheiros.

Esta secção descreve a encriptação de ficheiros em unidades de computador locais e fornece instruções para configurar e efetuar encriptação de ficheiros em unidades de computador locais com o Kaspersky Endpoint Security e o Plug-In da Consola do Kaspersky Endpoint Security.

Encriptar ficheiros nas unidades locais do computador

Para encriptar ficheiros em unidades locais:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** na árvore da Consola de Administração, abra a pasta com o nome do grupo de administração relevante para o qual pretende configurar a encriptação de ficheiros nas unidades locais.

3. Na área de trabalho, selecione o separador **Políticas**.

4. Selecione a política pretendida.

5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.

6. Na secção **Encriptação de dados**, selecione a subsecção **Encriptação de ficheiros e pastas**.

7. Na parte direita da janela, selecione o separador **Encriptação**.

8. Na lista pendente **Modo de encriptação**, selecione o item **Regras predefinidas**.

9. 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.

   A janela **Selecionar pastas predefinidas** é aberta.

   b. Selecione o item **Pasta predefinida** para adicionar um caminho de pasta introduzido manualmente para uma regra de encriptação.

   A janela **Adicionar pasta personalizada** é aberta.

   c. Selecione o item **Ficheiros por extensão** para adicionar extensões de ficheiro a uma regra de encriptação. O Kaspersky Endpoint Security encripta ficheiros com as extensões especificadas em todas as unidades locais do computador.

   É aberta a janela **Adicionar/editar uma lista de extensões de ficheiros**.

   d. Selecione o item **Ficheiros por grupo(s) de extensões** para adicionar grupos de extensões de ficheiro a uma regra de encriptação. O Kaspersky Endpoint Security encripta ficheiros que têm as extensões de ficheiro listadas nos grupos de extensões em todas as unidades locais do computador.

   É aberta a janela **Selecionar grupos de extensões de ficheiros**.

10. Para guardar as alterações, na janela **Propriedades: <Nome da política>** clique em **OK**.

11. Aplicar a política.

    Consulte o *Manual do Administrador do Kaspersky Security Center* para obter mais informações sobre a aplicação da política do Kaspersky Security Center.

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.

Se o mesmo ficheiro tiver sido adicionado à regra de encriptação e à regra de desencriptação, o Kaspersky Endpoint Security não encripta este ficheiro se este não estiver encriptado, e desencripta o ficheiro, caso este esteja encriptado.

O Kaspersky Endpoint Security encripta ficheiros não encriptados se as suas propriedades (caminho do ficheiro/nome do ficheiro/extensão do arquivo) ainda cumprirem os critérios das regras de encriptação depois de serem alterados.

O Kaspersky Endpoint Security adia a encriptação de ficheiros abertos até que estes sejam fechados.

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.

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.

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 **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração relevante para o qual pretende configurar as regras de acesso a ficheiros encriptados para aplicações.
3. Na área de trabalho, selecione o separador **Políticas**.
4. Selecione a política pretendida.
5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.
6. Na secção **Encriptação de dados**, selecione a subsecção **Encriptação de ficheiros e pastas**.
7. Na lista pendente **Modo de encriptação**, selecione o item **Regras predefinidas**.

   As regras de acesso são aplicadas apenas no modo **Regras predefinidas**. Depois de aplicar as regras de acesso no modo **Regras predefinidas**, 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.

8. Na parte direita da janela, selecione o separador **Regras de Aplicações**.
9. Se quiser selecionar aplicações exclusivamente a partir da lista do Kaspersky Security Center, clique no botão **Adicionar** e na lista pendente selecione o item **Aplicações da lista do Kaspersky Security Center**.

   É aberta a janela **Adicionar aplicações da lista do Kaspersky Security Center**.

   Execute as seguintes ações:

   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 **Aplicações**, selecione as caixas de verificação em frente às aplicações para as quais pretende formar regras de acesso aos ficheiros encriptados.

d. Na lista pendente **Regra para aplicação(ões)**, selecione a regra que determinará o acesso de aplicações a ficheiros encriptados.

e. 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.

f. Clique em **OK**.

Os detalhes de uma regra de acesso a ficheiros encriptados para aplicações são apresentados na tabela no separador **Regras de Aplicações**.

10. Se pretender selecionar manualmente aplicações, clique no botão **Adicionar** e na lista pendente selecione o item **Aplicações personalizadas**.

    É apresentada a janela **Adicionar/editar nomes dos ficheiros executáveis das aplicações**.

    Execute as seguintes ações:

    a. No campo de entrada, introduza o nome ou a lista de nomes de ficheiros de aplicações executáveis, incluindo as respetivas extensões.

    Também pode adicionar os nomes de ficheiros executáveis de aplicações a partir da lista do Kaspersky Security Center, clicando no botão **Adicionar da lista do Kaspersky Security Center**.

    b. Se necessário, no campo **Descrição**, introduza uma descrição da lista de aplicações.

    c. Na lista pendente **Regra para aplicação(ões)**, selecione a regra que determinará o acesso de aplicações a ficheiros encriptados.

    d. Clique em **OK**.

    Os detalhes de uma regra de acesso a ficheiros encriptados para aplicações são apresentados na tabela no separador **Regras de Aplicações**.

11. Clique em **OK** para guardar as 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 **Computadores geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração relevante para o qual pretende configurar a encriptação de ficheiros criados por aplicações específicas.

3. Na área de trabalho, selecione o separador **Políticas**.

4. Selecione a política pretendida.

5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.

6. Na secção **Encriptação de dados**, selecione a subsecção **Encriptação de ficheiros e pastas**.

7. Na lista pendente **Modo de encriptação**, selecione o item **Regras predefinidas**.

   As regras de encriptação são aplicadas apenas ao modo **Regras predefinidas**. Depois de aplicar as regras de encriptação no modo **Regras predefinidas**, 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.

8. Na parte direita da janela, selecione o separador **Regras de Aplicações**.

9. Se quiser selecionar aplicações exclusivamente a partir da lista do Kaspersky Security Center, clique no botão **Adicionar** e na lista pendente selecione o item **Aplicações da lista do Kaspersky Security Center**.

   É aberta a janela **Adicionar aplicações da lista do Kaspersky Security Center**.

   Execute as seguintes ações:

   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 em frente às aplicações cujos ficheiros criados necessitam de ser encriptados.

   d. Na lista pendente **Regra para aplicação(ões)**, selecione **Encriptar todos os ficheiros criados**.

   e. Na lista pendente **Ações para as aplicações selecionadas anteriormente**, selecione a ação a executar pelo Kaspersky Endpoint Security nas regras de encriptação de ficheiros formuladas anteriormente para essas aplicações.

   f. Clique em **OK**.

   A informação sobre a regra de encriptação para ficheiros criados ou alterados pelas aplicações selecionadas aparece na tabela no separador **Regras de aplicações**.

10. Se pretender selecionar manualmente aplicações, clique no botão **Adicionar** e na lista pendente selecione o item **Aplicações personalizadas**.

    É apresentada a janela **Adicionar/editar nomes dos ficheiros executáveis das aplicações**.

    Execute as seguintes ações:

a. No campo de entrada, introduza o nome ou a lista de nomes de ficheiros de aplicações executáveis, incluindo as respetivas extensões.

   Também pode adicionar os nomes de ficheiros executáveis de aplicações a partir da lista do Kaspersky Security Center, clicando no botão **Adicionar da lista do Kaspersky Security Center**.

b. Se necessário, no campo **Descrição**, introduza uma descrição da lista de aplicações.

c. Na lista pendente **Regra para aplicação(ões)**, selecione **Encriptar todos os ficheiros criados**.

d. Clique em **OK**.

A informação sobre a regra de encriptação para ficheiros criados ou alterados pelas aplicações selecionadas aparece na tabela no separador **Regras de aplicações**.

11. Clique em **OK** para guardar as alterações.

Criar uma regra de desencriptação

Para criar uma regra de desencriptação:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração para o qual pretende criar uma lista de ficheiros a desencriptar.
3. Na área de trabalho, selecione o separador **Políticas**.
4. Selecione a política pretendida.
5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.
6. Na secção **Encriptação de Dados**, selecione a subsecção **Encriptação de ficheiros e pastas**.
7. Na parte direita da janela, selecione o separador **Desencriptação**.
8. Na lista pendente **Modo de encriptação**, selecione o item **Regras predefinidas**.
9. No separador **Desencriptação**, clique no botão **Adicionar** e selecione um dos seguintes itens na lista pendente:

   a. Selecione o item **Pastas predefinidas** para adicionar ficheiros de pastas de perfis de utilizador locais sugeridos por peritos da Kaspersky para uma regra de desencriptação.

      A janela **Selecionar pastas predefinidas** é aberta.

   b. Selecione o item **Pasta predefinida** para adicionar um caminho de pasta introduzido manualmente para uma regra de desencriptação.

      A janela **Adicionar pasta personalizada** é aberta.

c. Selecione o item **Ficheiros por extensão** para adicionar extensões de ficheiro a uma regra de desencriptação. O Kaspersky Endpoint Security não encripta ficheiros com as extensões especificadas em todas as unidades locais do computador.

É aberta a janela **Adicionar/editar uma lista de extensões de ficheiros**.

d. Selecione o item **Ficheiros por grupo(s) de extensões** para adicionar grupos de extensões de ficheiro a uma regra de desencriptação. O Kaspersky Endpoint Security não encripta ficheiros que têm as extensões de ficheiro listadas nos grupos de extensões em todas as unidades locais dos computadores.

É aberta a janela **Selecionar grupos de extensões de ficheiros**.

10. Para guardar as alterações, na janela **Propriedades: <Nome da política>** clique em **OK**.

11. Aplicar a política.

Consulte o *Manual do Administrador do Kaspersky Security Center* para obter mais informações sobre a aplicação da política do Kaspersky Security Center.

Se o mesmo ficheiro tiver sido adicionado à regra de encriptação e à regra de desencriptação, o Kaspersky Endpoint Security não encripta este ficheiro se este não estiver encriptado, e desencripta o ficheiro, caso este esteja encriptado.

Desencriptar ficheiros nas unidades locais do computador

Para desencriptar ficheiros em unidades locais:

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

2. Na pasta **Dispositivos geridos** na árvore da Consola de Administração, abra a pasta com o nome do grupo de administração relevante para o qual pretende configurar a desencriptação de ficheiros nas unidades locais.

3. Na área de trabalho, selecione o separador **Políticas**.

4. Selecione a política pretendida.

5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.

   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.

6. Na secção **Encriptação de Dados**, selecione a subsecção **Encriptação de ficheiros e pastas**.

7. Na parte direita da janela, selecione o separador **Encriptação**.

8. 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 **Remover**.

   Pode apagar vários itens da lista de encriptação em simultâneo. Para o fazer, enquanto mantém premida a tecla **CTRL**, selecione os ficheiros necessários clicando o botão esquerdo do rato, e selecione o item **Eliminar regra e desencriptar ficheiros** no menu de contexto do botão **Remover**.

   Os ficheiros e as pastas removidos da lista de encriptação são automaticamente adicionados à lista de desencriptação.

9. Formar uma lista de desencriptação de ficheiros.

10. Para guardar as alterações, na janela **Propriedades: <Nome da política>** clique em **OK**.

11. Aplicar a política.

Consulte o *Manual do Administrador do Kaspersky Security Center* para obter mais informações sobre a aplicação da política do Kaspersky Security Center.

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

O Kaspersky Endpoint Security não executa a compressão de ficheiros quando cria um pacote encriptado.

Para criar um pacote encriptado:

1. Num computador com o Kaspersky Endpoint Security instalado e com a funcionalidade de encriptação ativada, utilize qualquer gestor de ficheiros para selecionar ficheiros e/ou pastas que pretende adicionar a um pacote encriptado. Clique com o botão direito do rato para abrir o menu de contexto respetivo.

2. No menu de contexto, selecione **Adicionar ao pacote encriptado**.

   É apresentado a caixa de diálogo padrão do Microsoft Windows **Selecione o caminho para guardar o pacote encriptado**.

3. Na caixa de diálogo padrão do Microsoft Windows **Selecione o caminho para guardar o pacote encriptado**, selecione o destino para guardar o pacote encriptado na unidade amovível. Clique no botão **Guardar**.

   A janela **Adicionar ao pacote encriptado** é apresentada.

4. Na janela **Adicionar ao pacote encriptado**, introduza e confirme uma password.

5. Clique no botão **Criar**.

   O processo de criação do pacote encriptado é iniciado. Quando o processo terminar, um pacote encriptado autoextraível e protegido por password é criado na pasta de destino selecionada na unidade amovível.

Se a criação de um pacote encriptado for cancelada, o Kaspersky Endpoint Security executa as seguintes operações:

1. Termina os processos de cópia dos ficheiros para o pacote e interrompe todas as operações de encriptação de pacotes em curso, se existirem.

2. Remove todos os ficheiros temporários que foram criados no processo de criação e encriptação de um pacote e do ficheiro do próprio pacote encriptado.

3. Notifica o utilizador de que o processo de criação do pacote encriptado foi forçado a terminar.

Extrair pacotes encriptados

Para extrair um pacote encriptado:

1. Em qualquer gestor de ficheiros, selecione um pacote encriptado. Clique para iniciar o assistente de descompactação.

   É apresentada a janela **Introduzir password**.

2. Introduza a password que protege o pacote encriptado.

3. Na janela **Introduzir password**, clique em **OK**.

   Se a introdução da password for bem-sucedida, a caixa de diálogo padrão do Windows **Procurar** é aberta.

4. Na caixa de diálogo padrão **Procurar** do Microsoft Windows, selecione a pasta de destino para extrair o pacote encriptado e clique em **OK**.

   O processo de extração do pacote encriptado para a pasta de destino é iniciado.

Se o pacote encriptado tiver sido extraído previamente para a pasta de destino especificada, os ficheiros existentes na pasta serão substituídos pelos ficheiros do pacote encriptado.

Se a extração de um pacote encriptado for cancelada, o Kaspersky Endpoint Security executa as seguintes operações:

1. Interrompe o processo de desencriptação do pacote e termina todas as operações de cópia de ficheiros do pacote encriptado, se essa operação estiver a decorrer.

2. Apaga todos os ficheiros temporários criados durante a desencriptação e extração do pacote encriptado, bem como de todos os ficheiros que já foram copiados do pacote encriptado para a pasta de destino.

3. Notifica o utilizador de que o processo de extração do pacote encriptado foi forçado a terminar.

Encriptação de unidades amovíveis

A encriptação de unidades amovíveis está disponível se o Kaspersky Endpoint Security estiver instalado num computador que tem o Microsoft Windows para estações de trabalho em execução. A encriptação de unidades amovíveis não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que tem o Microsoft Windows para servidores de ficheiros.

Esta secção contém informação sobre a encriptação de unidades amovíveis e instruções para a configuração e execução da encriptação de unidades amovíveis utilizando o Kaspersky Endpoint Security e o administration plug-in do Kaspersky Endpoint Security.

Iniciar a encriptação de unidades amovíveis

Para encriptar unidades amovíveis:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** na árvore da Consola de Administração, abra a pasta com o nome do grupo de administração relevante para o qual pretende configurar a encriptação de unidades amovíveis.
3. Na área de trabalho, selecione o separador **Políticas**.
4. Selecione a política pretendida.
5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.
6. Na secção **Encriptação de dados**, selecione a subsecção **Encriptação de unidades amovíveis**.
7. Na lista pendente **Modo de Encriptação**, selecione a ação predefinida a executar pelo Kaspersky Endpoint Security em todas as unidades amovíveis ligadas ao grupo de administração selecionado:
   - **Encriptar unidade amovível completa**. Se este item estiver selecionado, ao aplicar a política do Kaspersky Security Center com as configurações de encriptação especificadas para unidades amovíveis, o Kaspersky Endpoint Security encripta os conteúdos de unidades amovíveis, setor por setor. Deste modo, a aplicação encripta não apenas os ficheiros armazenados em unidades amovíveis, mas também ficheiros de sistema de unidades amovíveis, incluindo os nomes de ficheiros e as estruturas de pastas. O Kaspersky Endpoint Security não volta a encriptar unidades amovíveis que já tenham sido encriptadas.

     Este cenário de encriptação é ativado pela funcionalidade de encriptação da unidade de disco rígido do Kaspersky Endpoint Security.

   - **Encriptar todos os ficheiros**. Se este item estiver selecionado, ao aplicar a política do Kaspersky Security Center 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 volta a encriptar ficheiros já encriptados anteriormente. A aplicação não encripta os sistemas de ficheiros de unidades amovíveis, incluindo nomes de ficheiros encriptados e estruturas de pastas.
   - **Encriptar apenas os ficheiros novos**. Se este item estiver selecionado, ao aplicar a política do Kaspersky Security Center com as configurações de encriptação especificadas para unidades amovíveis, o Kaspersky Endpoint Security encripta apenas os ficheiros que foram adicionados às unidades amovíveis ou que foram armazenados em unidades amovíveis e que foram modificados após última aplicação da política do Kaspersky Security Center.
   - **Desencriptar unidade amovível completa**. Se este item selecionado, ao aplicar a política do Kaspersky Security Center com as configurações de encriptação especificadas para unidades amovíveis, o Kaspersky Endpoint Security desencripta todos os ficheiros encriptados que estão armazenados em unidades amovíveis, bem como todos os sistemas de ficheiros das unidades amovíveis, se tiverem sido encriptados anteriormente.

     Este cenário de encriptação é possibilitado pela funcionalidade de encriptação de ficheiros e pela funcionalidade de encriptação da unidade de disco rígido do Kaspersky Endpoint Security.

   - **Manter inalterado**. Se este item estiver selecionado, ao aplicar a política do Kaspersky Security Center com as configurações de encriptação especificadas para unidades amovíveis, o Kaspersky Endpoint Security

não encripta nem desencripta ficheiros armazenados em unidades amovíveis.

8. Criar regras de encriptação para ficheiros em unidades amovíveis cujos conteúdos pretende encriptar.

9. Aplicar a política.

Consulte o *Manual do Administrador do Kaspersky Security Center* para obter mais informações sobre a aplicação da política do Kaspersky Security Center.

Assim que a política for aplicada, quando o utilizador ligar uma unidade amovível ou se uma unidade amovível já estiver ligada, o Kaspersky Endpoint Security notifica o utilizador de que a unidade amovível está sujeita a uma regra de encriptação segundo a qual os dados armazenados na unidade amovível serão encriptados.

Se a regra *Manter inalterado* for especificada nos dados de encriptação de uma unidade amovível, a aplicação não apresenta qualquer notificação ao utilizador.

A aplicação avisa o utilizador de que o processo de encriptação pode demorar algum tempo.

A aplicação solicita ao utilizador que confirme a operação de encriptação e executa as seguintes ações:

- Encripta dados de acordo com as definições da política, se o utilizador consentir a encriptação.
- Deixa os dados sem encriptação se o utilizador rejeitar a encriptação e restringe o acesso a ficheiros da unidade amovível como apenas de leitura.
- Deixa os dados sem encriptação se o utilizador ignorar o aviso de encriptação, restringe o acesso aos ficheiros de unidades amovíveis como apenas de leitura, e avisa o utilizador novamente para confirmar a encriptação de dados na próxima vez que a política do Kaspersky Security Center for aplicada ou quando uma unidade amovível for ligada.

A política do Kaspersky Security Center com predefinições para encriptação de dados em unidades amovíveis é formada por um grupo específico de computadores geridos. Deste modo, o resultado da encriptação de dados em unidades amovíveis depende do computador ao qual a unidade amovível está ligada.

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.

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.

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 **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração ao qual pretende adicionar as regras de encriptação de unidades amovíveis.

3. Na área de trabalho, selecione o separador **Políticas**.

4. Selecione a política pretendida.

5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.

6. Na secção **Encriptação de dados**, selecione a subsecção **Encriptação de unidades amovíveis**.

7. Clique com o botão esquerdo do rato 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 confiáveis do componente de Controlo de Dispositivos, selecione **Na lista de dispositivos confiáveis desta política**.

     É apresentada a janela **Adicionar dispositivos da lista de dispositivos confiáveis**.

   - 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**.

     É aberta a janela **Adicionar dispositivos da lista do Kaspersky Security Center**.

8. Se selecionou **Da lista de dispositivos do Kaspersky Security Center** durante o passo anterior, especifique os filtros para apresentar dispositivos na tabela. Para tal:

   a. Especifique os valores dos parâmetros seguintes: **Apresentar os dispositivos na tabela, para os quais é definido o seguinte**, **Tipo de dispositivo**, **Nome**, **Computador** e **Encriptação de disco Kaspersky**.

   b. Clique no botão **Atualizar**.

9. Na coluna **Tipo de dispositivo**, selecione as caixas de verificação junto dos nomes das unidades amovíveis para as quais pretende criar regras de encriptação.

10. 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.

11. 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.

12. 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.

13. 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 uma regra de encriptação criada anteriormente para uma unidade amovível seja substituída pela nova regra, selecione **Atualizar**.

14. Clique em **OK**.

    As linhas que contenham os parâmetros das regras de encriptação criadas são apresentadas na tabela **Regras personalizadas**.

15. Clique em **OK** para guardar as alterações.

As regras de encriptação de unidades amovíveis adicionadas são aplicadas às unidades amovíveis que estão ligadas a quaisquer computadores controlados pela política modificada do Kaspersky Security Center.

Editar uma regra de encriptação para unidades amovíveis

Para editar uma regra de encriptação para uma unidade amovível:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração para o qual pretende editar uma regra de encriptação da unidade amovível.
3. Na área de trabalho, selecione o separador **Políticas**.
4. Selecione a política pretendida.
5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:

    - No menu de contexto da política, selecione **Propriedades**.
    - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.

6. Na secção **Encriptação de dados**, selecione a subsecção **Encriptação de unidades amovíveis**.
7. Na lista de unidades amovíveis para as quais as regras de encriptação foram configuradas, selecione uma entrada correspondente à unidade amovível de que necessita.
8. Clique no botão **Definir uma regra** para editar a regra de encriptação para a unidade amovível selecionada.

    É aberto o menu de contexto do botão **Definir uma regra**.

9. No menu de contexto do botão **Definir uma regra**, selecione a ação a executar pelo Kaspersky Endpoint Security em ficheiros armazenados na unidade amovível selecionada.
10. Clique em **OK** para guardar as alterações.

As regras de encriptação de unidades amovíveis modificadas são aplicadas às unidades amovíveis que estão ligadas a quaisquer computadores controlados pela política modificada do Kaspersky Security Center.

Ativar o modo portátil para aceder a ficheiros encriptados em unidades amovíveis

Para ativar o modo portátil para aceder a ficheiros encriptados em unidades amovíveis:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** na árvore da Consola de Administração, abra a pasta com o nome do grupo de administração para o qual pretende ativar o modo portátil para aceder a ficheiros encriptados em unidades amovíveis.
3. Na área de trabalho, selecione o separador **Políticas**.
4. Selecione a política pretendida.
5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.
6. Na secção **Encriptação de dados**, selecione a subsecção **Encriptação de unidades amovíveis**.
7. Selecione a caixa de verificação **Modo portátil**.

   O modo portátil está disponível para a encriptação de todos os ficheiros ou apenas dos ficheiros novos.

8. Clique em **OK**.
9. Aplicar a política.

   Consulte o *Manual do Administrador do Kaspersky Security Center* para obter mais informações sobre a aplicação da política do Kaspersky Security Center.
10. Ligue a unidade amovível a um dispositivo no qual a política do Kaspersky Security Center tenha sido aplicada.
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. Clique em **OK**.

    O Kaspersky Endpoint Security encripta ficheiros numa unidade amovível segundo as regras de encriptação definidas na política do Kaspersky Security Center. O Gestor de ficheiros portátil utilizado para trabalhar com ficheiros encriptados também será escrito na unidade amovível.

Após a ativação do modo portátil, pode aceder aos ficheiros encriptados em unidades amovíveis ligadas a um computador sem funcionalidade de encriptação.

Desencriptação de unidades amovíveis

Para desencriptar unidades amovíveis:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração para o qual pretende configurar a desencriptação das unidades amovíveis.
3. Na área de trabalho, selecione o separador **Políticas**.
4. Selecione a política pretendida.
5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.
6. Na secção **Encriptação de dados**, selecione a subsecção **Encriptação de unidades amovíveis**.
7. Se pretende desencriptar todos os ficheiros encriptados que estão armazenados em unidades amovíveis, na lista pendente **Modo de encriptação** selecione **Desencriptar unidade amovível completa**.
8. Para desencriptar dados armazenados em unidades amovíveis individuais, edite as regras de encriptação para unidades amovíveis cujos dados pretende desencriptar. Para tal:
   a. Na lista de unidades amovíveis para as quais as regras de encriptação foram configuradas, selecione uma entrada correspondente à unidade amovível de que necessita.
   b. Clique no botão **Definir uma regra** para editar a regra de encriptação para a unidade amovível selecionada.
      É aberto o menu de contexto do botão **Definir uma regra**.
   c. Selecione o item **Desencriptar todos os ficheiros** no menu de contexto do botão **Definir uma regra**.
9. Clique em **OK** para guardar as alterações.
10. Aplicar a política.

Consulte o *Manual do Administrador do Kaspersky Security Center* para obter mais informações sobre a aplicação da política do Kaspersky Security Center.

Após a aplicação da política, quando o utilizador liga uma unidade amovível ou se uma unidade amovível já estiver ligada, o Kaspersky Endpoint Security notifica o utilizador que a unidade amovível está sujeita a uma regra de encriptação segundo a qual os ficheiros encriptados armazenados na unidade amovível, bem como o sistema de ficheiros da unidade amovível (caso esteja encriptado), serão desencriptados. A aplicação avisa o utilizador de que o processo de desencriptação pode demorar algum tempo.

A política do Kaspersky Security Center com predefinições para encriptação de dados em unidades amovíveis é formada por um grupo específico de computadores geridos. Deste modo, o resultado da desencriptação de dados em unidades amovíveis depende do computador ao qual a unidade amovível está ligada.

Se o utilizador inicia a remoção segura de uma unidade amovível durante a desencriptação de dados, o Kaspersky Endpoint Security interrompe o processo de desencriptação de dados e permite a remoção da unidade amovível antes da conclusão da operação de desencriptação.

Se a desencriptação de uma unidade amovível falhar, consulte o relatório de **Encriptação de dados** na interface do Kaspersky Endpoint Security. O acesso aos ficheiros pode ser bloqueado por outra aplicação. Nesse caso, tente remover a unidade amovível do computador e introduzi-la novamente.

Encriptação de unidades de disco rígido

Se o Kaspersky Endpoint Security for instalado num computador com o Microsoft Windows para estações de trabalho, as tecnologias de Encriptação de Unidade BitLocker e de Encriptação de disco Kaspersky estão disponíveis para encriptação. Se o Kaspersky Endpoint Security estiver instalado num computador com o Microsoft Windows for File Servers, apenas a tecnologia de Encriptação de Unidade BitLocker está disponível.

Esta secção contém informação sobre a encriptação de unidades de disco rígido e instruções para a configuração e execução da encriptação de unidades de disco rígido com o Kaspersky Endpoint Security e o plug-in de Consola do Kaspersky Endpoint Security.

Sobre a encriptação de unidades de disco rígido

Antes de iniciar a encriptação da unidade de disco rígido, a aplicação executa várias verificações para determinar se o dispositivo pode ser encriptado, o que inclui verificar a unidade de disco rígido do sistema quanto à compatibilidade com o Agente de Autenticação e 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 do disco rígido é iniciada depois de o sistema operativo ter sido inicializado e a aplicação ter sido 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 das unidades de disco rígido 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 do tipo de encriptação da unidade de disco rígido, introduza `avp pbatestreset` na linha de comandos. 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 o início da encriptação da unidade de disco rígido, o Kaspersky Endpoint Security encripta todos os dados gravados nas unidades de disco rígido.

Se o utilizador encerra ou reinicia o computador durante a desencriptação da unidade de disco rígido, o Agente de Autenticação é carregado antes do próximo arranque do sistema operativo. O Kaspersky Endpoint Security retoma a encriptação das unidades de disco rígido 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 unidades de disco rígido, o Agente de Autenticação é carregado quando o sistema operativo sai do modo de hibernação. O Kaspersky Endpoint Security retoma a encriptação das unidades de disco rígido após a autenticação com êxito no agente de autenticação e o arranque do sistema operativo.

Se o sistema operativo entrar em modo de descanso durante a encriptação da unidade de disco rígido, o Kaspersky Endpoint Security retoma a encriptação de unidades de disco rígido 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.

O agente de autenticação suporta esquemas de teclado para os idiomas seguintes:

- Inglês (Reino Unido)
- Inglês (EUA)
- Árabe (Argélia, Marrocos, Tunísia, esquema AZERTY)
- Castelhano (América Latina)
- Italiano
- Alemão (Alemanha e Áustria)
- Alemão (Suíça)
- Português (Brasil, esquema ABNT2)
- Russo (para IBM de 105 teclas/teclados Windows com esquema QWERTY)
- Turco (esquema QWERTY)
- Francês (França)
- Francês (Suíça)
- Francês (Bélgica, esquema AZERTY)
- Japonês (para teclados de 106 teclas com esquema QWERTY)

Um esquema de teclado fica disponível no Agente de Autenticação se este esquema tiver sido adicionado nas definições de idioma e região do sistema operativo e estiver disponível no ecrã de boas-vindas do Microsoft Windows.

Se o nome da conta do Agente de Autenticação incluir símbolos que não podem ser introduzidos utilizando os esquemas do teclado disponíveis no Agente de Autenticação, as unidades de disco rígido encriptadas podem ser acedidas apenas após serem restauradas utilizando a Ferramenta de Restauro ou após o nome e a password da conta de agente de autenticação serem recuperados.

O Kaspersky Endpoint Security suporta os tokens, leitores de smart card e smart cards seguintes:

- SafeNet eToken PRO 64K (4.2b) (USB)
- SafeNet eToken PRO 72K Java (USB)
- SafeNet eToken PRO 72K Java (Smart Card)
- SafeNet eToken 4100 72K Java (Smart Card)
- SafeNet eToken 5100 (USB)
- SafeNet eToken 5105 (USB)
- SafeNet eToken 7300 (USB)
- EMC RSA SecurID 800 (USB).
- Rutoken EDS (USB)
- Rutoken EDS (Flash)
- Aladdin-RD JaCarta PKI (USB)
- Aladdin-RD JaCarta PKI (Smart Card)
- Athena IDProtect Laser (USB)
- Gemalto IDBridge CT40 (Reader)
- Gemalto IDPrime .NET 511

Encriptação de unidades de disco rígido utilizando tecnologia de Encriptação de disco Kaspersky

Antes de encriptar unidades de disco rígido num computador, recomendamos que se certifique de que o computador não está infetado. Para tal, inicie a tarefa de Verificação Completa ou Verificação de Áreas Críticas. A encriptação de uma unidade de disco rígido de um computador infetado por um processo oculto (rootkit) pode levar à respetiva inoperabilidade.

Para encriptar unidades de disco rígido utilizando a tecnologia de Encriptação de disco Kaspersky:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** na árvore da Consola de Administração, abra a pasta com o nome do grupo de administração relevante para o qual pretende configurar a encriptação de unidades de disco rígido.
3. Na área de trabalho, selecione o separador **Políticas**.
4. Selecione a política pretendida.

5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.

6. Na secção **Encriptação de dados**, selecione a subsecção **Encriptação de unidades de disco rígido**.

7. Na lista pendente da **Tecnologia de Encriptação**, selecione a opção **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.

8. Na lista pendente **Modo de Encriptação**, selecione a opção **Encriptar todas as unidades de discos rígido**.

   Se for necessário excluir algumas das unidades de disco rígido da encriptação, crie uma lista com essas unidades de disco rígido.

9. 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 de disco utilizado**.

     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 de disco utilizado**.

     Esta função é aplicável apenas a dispositivos sem encriptação. Se um dispositivo tiver sido encriptado anteriormente utilizando a função **Encriptar apenas espaço de disco utilizado**, depois de aplicar uma política no modo **Encriptar todas as unidades de discos rígido**, os seus setores que não estejam ocupados por ficheiros continuarão sem ser encriptados.

10. Clique em **OK** para guardar as alterações.

11. Aplicar a política.

    Consulte o *Manual do Administrador do Kaspersky Security Center* para obter mais informações sobre a aplicação da política do Kaspersky Security Center.

Encriptar discos rígidos utilizando a tecnologia de Encriptação de Unidade BitLocker

Antes de encriptar unidades de disco rígido num computador, recomendamos que se certifique de que o computador não está infetado. Para tal, inicie a tarefa de Verificação Completa ou Verificação de Áreas Críticas. A encriptação de uma unidade de disco rígido de um computador infetado por um processo oculto (rootkit) pode levar à respetiva inoperabilidade.

A utilização da tecnologia de Encriptação de Unidade BitLocker em computadores com um sistema operativo de servidor pode exigir a instalação do componente de **Encriptação de Unidade BitLocker** ao utilizar o assistente para adicionar componentes e funções.

Para encriptar discos rígidos utilizando a tecnologia de Encriptação de Unidade BitLocker:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** na árvore da Consola de Administração, abra a pasta com o nome do grupo de administração relevante para o qual pretende configurar a encriptação de unidades de disco rígido.
3. Na área de trabalho, selecione o separador **Políticas**.
4. Selecione a política pretendida.
5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.
6. Na secção **Encriptação de dados**, selecione a subsecção **Encriptação de unidades de disco rígido**.
7. Na lista pendente **Tecnologia de Encriptação**, selecione a opção **Encriptação de Unidade BitLocker**.
8. Na lista pendente do **Modo de encriptação**, selecione a opção **Encriptar todas as unidades de discos rígido**.
9. Se pretender utilizar um teclado do ecrã tátil para introduzir informações num ambiente de pré-carregamento, selecione a caixa de verificação **Permitir a utilização da autenticação com introdução da informação de pré-carregamento através de um teclado tátil em tablets**.

   Recomenda-se que esta definição seja utilizada apenas em dispositivos com ferramentas alternativas de introdução de dados como, por exemplo, um teclado USB num ambiente de pré-carregamento.

10. Selecione um dos seguintes tipos de encriptação:
    - Se pretender utilizar a encriptação de hardware, selecione a caixa de verificação **Utilizar encriptação hardware**.
    - Se pretender utilizar a encriptação de software, desmarque a caixa de verificação **Utilizar encriptação de software**.
11. 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 de disco utilizado**.

- Se pretender aplicar a encriptação à totalidade da unidade de disco rígido, desmarque a caixa de verificação **Encriptar apenas espaço de disco utilizado**.

  Esta função é aplicável apenas a dispositivos sem encriptação. Se um dispositivo tiver sido encriptado anteriormente utilizando a função **Encriptar apenas espaço de disco utilizado**, depois de aplicar uma política no modo **Encriptar todas as unidades de discos rígido**, os seus setores que não estejam ocupados por ficheiros continuarão sem ser encriptados.

12. Selecionar um método para aceder às unidades de disco rígido que foram encriptadas com o BitLocker.

    - Se pretender utilizar um Trusted Platform Module (TPM) para armazenar chaves de encriptação, selecione a opção **Utilizar Trusted Platform Module (TPM)**.

    - Se não estiver a utilizar o Trusted Platform Module (TPM) para encriptação de unidades de disco rígido, selecione a opção **Utilizar password** e especifique o número mínimo de caracteres que uma password tem de conter no campo **Comprimento mínimo da password**.

    A disponibilidade de um Trusted Platform Module (TPM) é obrigatória para os sistemas operativos Windows 7 e Windows 2008 R2, bem como para as versões anteriores.

13. Se selecionou a opção **Utilizar Trusted Platform Module (TPM)** durante o passo anterior:

    - Se pretender definir um código PIN que será solicitado quando o utilizador tenta aceder a uma chave de encriptação, selecione a caixa de verificação **Utilizar PIN** e no campo **Comprimento mínimo do PIN**, especifique o número mínimo de dígitos que um código PIN deve conter.

    - Caso pretenda aceder a discos rígidos encriptados sem um Trusted Platform Module (módulo de plataforma fidedigno) no computador através de uma password, selecione a caixa de verificação **Utilizar password se o Trusted Platform Module (TPM) não estiver disponível** e, no campo **Comprimento mínimo da password**, indique o número mínimo de carateres que a password deve conter.

      Neste caso, o acesso a chaves de encriptação ocorrerá ao utilizar a password indicada tal como se a caixa de verificação **Utilizar password** estivesse selecionada.

      Se a caixa de verificação **Utilizar password se o Trusted Platform Module (TPM) não estiver disponível** não estiver selecionada e o módulo de plataforma fidedigno não estiver disponível, a encriptação do disco rígido não é iniciada.

14. Clique em **OK** para guardar as alterações.

15. Aplicar a política.

    Consulte o *Manual do Administrador do Kaspersky Security Center* para obter mais informações sobre a aplicação da política do Kaspersky Security Center.

Depois de aplicar a política no computador cliente com o Kaspersky Endpoint Security instalado, as seguintes consultas serão feitas:

- Se a política de encriptação for aplicada a um disco rígido de sistema, a janela do código PIN aparecerá se o módulo de plataforma fidedigno estiver a ser utilizado ou, caso contrário, a janela de pedido de password aparecerá para a autorização de pré-carregamento.

- Se o sistema operativo do computador tiver o modo de compatibilidade da norma Federal Information Processing ativado, no Windows 8 e superior, o sistema operativo apresentará uma janela de pedido de ligação

de dispositivo de USB para guardar o ficheiro de chave de recuperação.

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 USB ou se tenha perdido).

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 **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração para o qual pretende criar uma lista de unidades de disco rígido a excluir da encriptação.
3. Na área de trabalho, selecione o separador **Políticas**.
4. Selecione a política pretendida.
5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.
6. Na secção **Encriptação de dados**, selecione a subsecção **Encriptação de unidades de disco rígido**.
7. Na lista pendente da **Tecnologia de Encriptação**, selecione a opção **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.
8. Para adicionar unidades de disco rígido à lista de unidades de disco rígido excluídas da encriptação:
   a. Clique no botão **Adicionar**.

      É aberta a janela **Adicionar dispositivos da lista do Kaspersky Security Center**.
   b. Na janela **Adicionar dispositivos da lista do Kaspersky Security Center**, especifique os valores dos seguintes parâmetros: **Nome**, **Computador**, **Tipo de disco** e **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**.

9. Se pretender remover unidades de disco rígido da tabela de exclusões, selecione uma ou várias linhas na tabela **Não encriptar as unidades de disco rígido seguintes** e clique no botão **Eliminar**.

   Para selecionar várias linhas na tabela, selecione-as mantendo premida a tecla **CTRL**.

10. Clique em **OK** para guardar as alterações.

Desencriptação de unidade de disco rígido

Pode desencriptar unidades de disco rígido mesmo que não exista nenhuma licença ativa que permita a encriptação de dados.

Para desencriptar unidades de disco rígido:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração para o qual pretende configurar a desencriptação das unidades de disco rígido.
3. Na área de trabalho, selecione o separador **Políticas**.
4. Selecione a política pretendida.
5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.
6. Na secção **Encriptação de dados**, selecione a subsecção **Encriptação de unidades de disco rígido**.
7. Na lista pendente **Tecnologia de Encriptação**, selecione a tecnologia com a qual foram encriptados os discos rígidos.
8. Execute uma das seguintes ações:
   - Na lista pendente **Modo de encriptação**, selecione a opção **Desencriptar todas as unidades de discos rígido** se pretender desencriptar todas as unidades de disco rígido encriptadas.
   - Adicione as unidades de disco rígido que pretende desencriptar à tabela **Não encriptar as unidades de disco rígido seguintes**.

     Esta opção está disponível apenas para a tecnologia de Encriptação de disco Kaspersky.

9. Clique em **OK** para guardar as alterações.
10. Aplicar a política.

Consulte o *Manual do Administrador do Kaspersky Security Center* para obter mais informações sobre a aplicação da política do Kaspersky Security Center.

Se o utilizador encerra ou reinicia o computador durante a desencriptação de unidades de disco rígido encriptadas através da tecnologia de Encriptação de disco Kaspersky, o Agente de Autenticação é carregado antes do próximo arranque do sistema operativo. O Kaspersky Endpoint Security retoma a desencriptação da unidade de disco rígido após a autenticação com êxito no agente de autenticação e arranque do sistema operativo.

Se o sistema operativo passar para o modo de hibernação durante a desencriptação de unidades de disco rígido encriptadas através da tecnologia de Encriptação de disco Kaspersky, o Agente de Autenticação é carregado quando o sistema operativo sai do modo de hibernação. O Kaspersky Endpoint Security retoma a desencriptação da unidade de disco rígido após a autenticação com êxito no agente de autenticação e arranque do sistema operativo. Após a desencriptação da unidade de disco rígido, o modo de hibernação está indisponível até o primeiro reinício do sistema operativo.

Se o sistema operativo entrar em modo de descanso durante a desencriptação da unidade de disco rígido, o Kaspersky Endpoint Security retoma a desencriptação da unidade de disco rígido quando o sistema operativo sair do modo de descanso sem carregar o Agente de Autenticação.

Gestão do Agente de Autenticação

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.

O utilizador, em alguns casos, pode não conseguir passar na autenticação. A autenticação é impossível, por exemplo, se o utilizador se tiver esquecido das credenciais da conta do Agente de Autenticação ou da password do token ou do smart-card, ou tiver perdido o token ou o smart-card.

Se o utilizador se tiver esquecido das credenciais da conta do Agente de Autenticação ou da password de um token ou smart card, tem de contactar o administrador da rede local empresarial para recuperá-las.

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 restaurar dados em dispositivos encriptados.

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, tem de adicionar o ficheiro de certificado eletrónico do token ou smart-card ao comando para criar uma conta de Agente de Autenticação.

A utilização de um token ou smart-card está disponível apenas se as unidades de disco rígido do computador tiverem sido encriptadas ao utilizar o algoritmo de encriptação AES256. Se os discos rígidos do computador foram encriptados através do algoritmo de encriptação AES56, a adição do ficheiro de certificado eletrónico ao comando será negada.

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.

  Se o certificado eletrónico do token ou do smart-card não cumprirem este requisito, o administration plug-in não carrega o ficheiro deste certificado para o comando para criar uma conta de Agente de Autenticação e apresenta uma mensagem de erro.

- O parâmetro `KeyUsage` que define a finalidade do certificado tem de ter o valor `keyEncipherment` ou `dataEncipherment`.

  Se o certificado eletrónico do token ou do smart-card não cumprirem este requisito, o administration plug-in carrega o ficheiro deste certificado para o comando para criar uma conta de Agente de Autenticação e apresenta uma mensagem de aviso.

- O certificado contém uma chave RSA com um comprimento de pelo menos 1024 bits.

  Se o certificado eletrónico do token ou do smart-card não cumprirem este requisito, o administration plug-in não carrega o ficheiro deste certificado para o comando para criar uma conta de Agente de Autenticação e apresenta uma mensagem de erro.

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.

Para editar as mensagens de ajuda do Agente de Autenticação:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Computadores geridos** da árvore da Consola de Administração, abra a pasta com nome do grupo de administração relevante para o qual pretende editar as mensagens de ajuda do Agente de Autenticação.
3. Na área de trabalho, selecione o separador **Políticas**.
4. Selecione a política pretendida.
5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.
6. Na secção **Encriptação de dados**, selecione a subsecção **Definições de encriptação comuns**.
7. Na secção **Modelos**, clique no botão **Ajuda**.

   Esta ação abre a janela **Mensagens de ajuda do Agente de Autenticação**.
8. Execute as 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.

9. Editar mensagens de ajuda.

   Se pretender restaurar o texto original, clique no botão **Predefinição**.

10. Clique em **OK**.

11. Para guardar as alterações, na janela **Propriedades: <Nome da política>** clique em **OK**.

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.

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. O ficheiro de rastreio do Agente de Autenticação pode ser muito útil quando é necessário repor dados nas unidades encriptadas.

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:

   - **Desativar o registo de depuração (predefinição)**. Se esta opção estiver selecionada, a aplicação não regista a informação sobre eventos do Agente de Autenticação no ficheiro de rastreio.

   - **Ativar o registo de depuração**. 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.

   - **Ativar o registo verboso**. 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 **Ativar o registo de depuração**. Um elevado nível de detalhe das entradas pode tornar mais lento o arranque do Agente de Autenticação e do sistema operativo.

   - **Ativar o registo de depuração e selecionar a porta série**. 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.

   - **Ativar o registo de depuração verboso e selecionar a porta série**. 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 **Ativar o registo de depuração e selecionar a porta série**. 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 ficheiros de rastreio do Agente de Autenticação se existirem unidades de disco rígido encriptadas no computador ou durante a encriptação de unidades de disco rígido.

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, o administrador do sistema pode enviar manualmente o ficheiro de rastreio do Agente de Autenticação para a Kaspersky para análise.

Gestão de contas do agente de autenticação

As seguintes ferramentas do Kaspersky Security Center estão disponíveis para a gestão das contas do Agente de Autenticação:

- Tarefa de grupo para a gestão de contas do Agente de Autenticação. Esta tarefa permite gerir as contas do Agente de Autenticação para um grupo de computadores cliente.
- Tarefa local de **Encriptação (gestão de conta)**. Esta tarefa permite gerir as contas do Agente de Autenticação para computadores cliente individuais.

Para configurar as definições da tarefa de gestão das contas do Agente de Autenticação:

1. Crie (Criação de uma tarefa local, Criação de uma tarefa de grupo) uma tarefa de gestão de conta do Agente de Autenticação.
2. Abrir a secção **Configuração** na janela **Propriedades: <Nome da tarefa de gestão da conta do Agente de Autenticação>**.
3. Adição de comandos para criação de contas do Agente de Autenticação.
4. Adição de comandos para edição de contas do Agente de Autenticação.
5. Adição de comandos para eliminação de contas de utilizador do Agente de Autenticação.
6. Se for necessário, edite os comandos adicionados para a gestão de contas do Agente de Autenticação. Para tal, selecione um comando na tabela **Comandos para gerir contas de Agente de Autenticação** e clique no botão **Editar**.
7. Se for necessário, apague os comandos adicionados para a gestão das contas do Agente de Autenticação. Para tal, selecione um ou vários comandos na tabela **Comandos para gerir contas de Agente de Autenticação** e clique no botão **Remover**.

   Para selecionar várias linhas na tabela, selecione-as mantendo premida a tecla **CTRL**.

8. Para guardar as alterações, clique em **OK** na janela de propriedades da tarefa.
9. Executar a tarefa.

Serão executados os comandos de gestão de conta do Agente de Autenticação adicionados à tarefa.

Adição de um comando para criação de uma conta de agente de autenticação

Para adicionar um comando para criação de uma conta de Agente de Autenticação:

1. Abrir a secção **Configuração** na janela **Propriedades: <Nome da tarefa de gestão da conta do Agente de Autenticação>**.

2. Clique no botão **Adicionar** e na lista pendente selecione o **Comando de adição de conta**.

   É aberta a janela **Adicionar conta de utilizador**.

3. No campo **Adicionar conta de utilizador** na janela **Conta do Windows**, especifique o nome da conta do Microsoft Windows com base na qual será criada a conta do Agente de Autenticação.

   Para tal, introduza manualmente o nome da conta ou clique no botão **Selecionar**.

4. Se já introduziu manualmente o nome de uma conta do Microsoft Windows, clique no botão **Permitir** para determinar 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.

   > A determinação do SID da conta do Microsoft Windows ao adicionar um comando para criação da conta do Agente de Autenticação é uma forma conveniente de garantir que o nome da conta de utilizador do Microsoft Windows introduzido manualmente está correto. Se a conta do Microsoft Windows introduzida não existir, pertencer a um domínio não confiável ou não estiver no computador para o qual a tarefa local de **Encriptação (gestão de conta)** está a ser modificada, a tarefa de gestão de conta do Agente de Autenticação é concluída com erro.

5. Selecione a caixa de verificação **Alterar conta existente** para que uma conta com nome idêntico e previamente criada para o Agente de Autenticação seja substituída pela conta que está a criar.

   > 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 indisponível se adicionar um comando de criação de conta do Agente de Autenticação nas propriedades de uma tarefa local de **Encriptação (gestão de conta)**.

6. 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.

7. 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.

8. Se selecionou a caixa de verificação **Permitir autenticação baseada em password** durante o passo anterior:

   a. No campo **Password**, introduza o nome da password do Agente de Autenticação que tem de ser introduzido durante a autenticação para aceder a unidades de disco rígido encriptadas.

   b. No campo **Confirmar password**, confirme a password da conta do Agente de Autenticação introduzida no passo anterior.

   c. Execute uma das seguintes ações:

   - Selecione a opção **Alterar password na primeira autenticação** se pretender que a aplicação apresente um pedido de alteração de password ao utilizador com a conta especificada no comando pela primeira vez.

   - Caso contrário, selecione a opção **Não solicitar a alteração da password**.

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.

10. Se selecionou a caixa de verificação **Permitir autenticação baseada em certificado** durante o passo anterior, clique no botão **Procurar** e selecione o ficheiro certificado eletrónico do token ou smart-card na janela **Selecionar ficheiro de certificado**.

11. Se solicitado, no campo **Descrição do comando**, introduza os detalhes da conta do Agente de Autenticação necessários para a gestão do comando.

12. Execute uma das seguintes ações:

    - Selecione a caixa de verificação **Permitir autenticação** se pretender que a aplicação permita que o utilizador com a conta especificada no comando aceda à janela de diálogo de autenticação no Agente de Autenticação.

    - Selecione a caixa de verificação **Bloquear autenticação** se pretender que a aplicação não permita que o utilizador com a conta especificada no comando aceda à janela de diálogo de autenticação no Agente de Autenticação.

13. Na janela **Adicionar conta de utilizador**, clique em **OK**.

Adicionar um comando de edição de conta do Agente de Autenticação

Para adicionar um comando para edição de uma conta do Agente de Autenticação:

1. Na secção **Configuração** da janela **Propriedades: <nome da tarefa de gestão de contas do Agente de Autenticação>**, abra o menu de contexto do botão **Adicionar** e selecione o item **Comando de edição de conta**.

   É aberta a janela **Editar conta de utilizador**.

2. No campo **Conta do Windows** da janela **Editar conta de utilizador**, especifique o nome da conta de utilizador do Microsoft Windows utilizada para criar a conta do Agente de Autenticação que pretende editar. Para tal, introduza manualmente o nome da conta ou clique no botão **Selecionar**.

3. Se já introduziu manualmente o nome de uma conta de utilizador do Microsoft Windows, clique no botão **Permitir** para determinar o identificador de segurança (SID) da conta de utilizador.

   Se optar por não determinar o identificador de segurança (SID), clicando no botão **Permitir**, este será determinado quando a tarefa for executada no computador.

   A determinação do SID da conta de utilizador do Microsoft Windows ao adicionar um comando para edição da conta do Agente de Autenticação é uma forma conveniente de garantir que o nome de conta de utilizador do Microsoft Windows introduzido manualmente está correto. Se a conta de utilizador do Microsoft Windows não existir ou pertencer a um domínio não confiável, a tarefa de grupo para gestão de contas de Agente de Autenticação é concluída com erro.

4. 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.

5. Selecione a caixa de verificação **Modificar definições de autenticação baseada em password** para tornar editáveis as definições de autenticação baseada em password.

6. 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.

7. Se selecionou a caixa de verificação **Permitir autenticação baseada em password** durante o passo anterior:

   a. No campo **Password**, introduza a nova password da conta do Agente de Autenticação.

   b. No campo **Confirmar password**, confirme a password introduzida no passo anterior.

8. 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.

9. Especifique o valor da definição de alteração de password ao efetuar a autenticação no Agente de Autenticação.

10. 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.

11. 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.

12. Se selecionou a caixa de verificação **Permitir autenticação baseada em certificado** durante o passo anterior, clique no botão **Procurar** e selecione o ficheiro certificado eletrónico do token ou smart-card na janela **Selecionar ficheiro de certificado**.

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. Na janela **Editar conta de utilizador**, clique em **OK**.

Adicionar um comando para a eliminação de uma conta do Agente de Autenticação

Para adicionar um comando para eliminação de uma conta do Agente de Autenticação:

1. Na secção **Configuração** da janela **Propriedades: <nome da tarefa de gestão de contas do Agente de Autenticação>**, abra o menu de contexto do botão **Adicionar** e selecione **Comando de eliminação de conta**.

   É aberta a janela **Eliminar conta de utilizador**.

2. No campo **Conta do Windows** da janela **Eliminar conta de utilizador**, especifique o nome da conta de utilizador do Microsoft Windows utilizada para criar a conta do Agente de Autenticação que pretende editar. Para tal, introduza manualmente o nome da conta ou clique no botão **Selecionar**.

3. Se já introduziu manualmente o nome de uma conta de utilizador do Microsoft Windows, clique no botão **Permitir** para determinar o identificador de segurança (SID) da conta de utilizador.

   Se optar por não determinar o identificador de segurança (SID), clicando no botão **Permitir**, este será determinado quando a tarefa for executada no computador.

   A determinação do SID da conta de utilizador do Microsoft Windows ao adicionar um comando para eliminação da conta do Agente de Autenticação é uma forma conveniente de garantir que o nome de conta de utilizador do Microsoft Windows introduzido manualmente está correto. Se a conta de utilizador do Microsoft Windows não existir ou pertencer a um domínio não confiável, a tarefa de grupo para gestão de contas de Agente de Autenticação é concluída com erro.

4. Na janela **Eliminar conta de utilizador**, clique em **OK**.

Restaurar as credenciais da conta do Agente de Autenticação

Estas instruções destinam-se a utilizadores de computadores cliente com o Kaspersky Endpoint Security instalado.

Para restaurar o nome de utilizador e a password da conta do Agente de Autenticação:

1. O Agente de Autenticação é carregado num computador com unidades de disco rígido encriptadas antes de o sistema operativo ser carregado. Na interface do Agente de Autenticação, clique no botão **Esquecer Password** para iniciar o processo de restauro do nome de utilizador e da password de uma conta do Agente de Autenticação.

2. Siga as instruções do Agente de Autenticação para obter as unidades de pedidos para repor o nome de utilizador e a password da conta do Agente de Autenticação.

3. Comunique os conteúdos dos bloqueios de pedidos ao administrador da rede local da sua empresa, juntamente com o nome do computador.

4. Introduza as secções da resposta ao pedido de restauro do nome de utilizador e password do Agente de Autenticação que foram criados e fornecidos pelo administrador da rede local.

5. Introduza uma nova password para a conta do Agente de Autenticação e confirme-a.

   O nome de utilizador da conta do Agente de Autenticação é definido utilizando as secções da resposta a pedidos de restauro do nome de utilizador e password da conta do Agente de Autenticação.

Após a introdução e confirmação da nova password da conta do Agente de Autenticação, a password será guardada e ser-lhe-á concedido acesso a unidades de disco rígido encriptadas.

Responder a um pedido de utilizador para restaurar credenciais da conta do Agente de Autenticação

Para criar e enviar as secções do utilizador da resposta ao pedido do utilizador para restauro do nome de utilizador e password de uma conta do Agente de Autenticação:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração que inclui o computador do utilizador que solicitou o restauro do nome de utilizador e da password de uma conta do Agente de Autenticação.
3. Na área de trabalho, selecione o separador **Dispositivos**.
4. No separador **Dispositivos**, selecione o computador do utilizador que solicitou o restauro do nome de utilizador e da password de uma conta do Agente de Autenticação e clique nele com o botão direito do rato para abrir o menu de contexto.
5. No menu de contexto, selecione a opção **Conceder acesso a dispositivos e dados em modo offline**.

   É aberta a janela **Conceder acesso a dispositivos e dados em modo offline**.
6. Na janela **Conceder acesso a dispositivos e dados em modo offline**, selecione o separador **Agente de Autenticação**.
7. Na secção **Algoritmo de encriptação em utilização**, selecione o tipo de algoritmo de encriptação.
8. 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.
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.

    Os conteúdos das secções da resposta ao pedido do utilizador para recuperação do nome de utilizador e password de início de uma conta do Agente de Autenticação serão apresentados no campo **Chave de acesso**.
11. Enumere o conteúdo dos bloqueios de resposta ao utilizador.

Ver detalhes da encriptação de dados

Esta secção descreve como visualizar os detalhes da encriptação de dados.

Sobre o estado de encriptação

Enquanto as tarefas de encriptação e desencriptação decorrem, o Kaspersky Endpoint Security transmite informação sobre o estado dos parâmetros de encriptação aplicados a computadores cliente para o Kaspersky Security Center.

Os seguintes valores de estado de encriptação são possíveis:

- *Política indefinida*. Não foi definida uma política do Kaspersky Security Center para o computador.
- *Encriptação / desencriptação decorrer*. 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 e / ou desencriptação de dados no computador foi concluída utilizando as configurações 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.
- *Não suportado*. A funcionalidade de encriptação de dados não está disponível no computador.

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 **Dispositivo geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração ao qual o computador em questão pertence.
3. Na área de trabalho, selecione o separador **Dispositivos**.

   O separador **Dispositivos** na área de trabalho apresenta as propriedades de computadores no grupo de administração selecionado.
4. No separador **Dispositivos** da área de trabalho, faça deslizar a barra de deslocamento totalmente para a direita.

   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, encriptação de unidades de disco rígido e encriptação de unidades amovíveis ligadas ao computador.

Visualizar as estatísticas de encriptação em painel de detalhes do Kaspersky Security Center

Para visualizar o estado de encriptação em painel de detalhes do Kaspersky Security Center:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da consola, selecione o **Servidor de Administração — Nó <Nome do computador>**.
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 **Estatísticas**, clique no botão **Personalizar vista**.

      É aberta a janela **Propriedades: Estatísticas**.

b. Na janela **Propriedades: Estatísticas**, clique em **Adicionar**.

É aberta a janela **Propriedades: Nova página**.

c. Na secção **Geral** da janela **Propriedades: Nova página**, introduza o nome da página.

d. Na secção **Painéis de detalhes**, clique no botão **Adicionar**.

É aberta a janela **Novo painel de detalhes**.

e. Na janela **Novo painel de detalhes** no grupo **Estado de proteção**, selecione o item **Encriptação de dispositivo**.

f. Clique em **OK**.

É aberta a janela **Propriedades: Controlo de Encriptação**.

g. Se for necessário, edite os detalhes do painel de detalhes. Para tal, utilize as secções **Ver** e **Dispositivos** da janela **Propriedades: Encriptação do dispositivo**.

h. Clique em **OK**.

i. Repita os passos d – h das instruções, selecionando o item **Encriptação de unidades amovíveis** na secção **Estado da proteção** da janela **Novo painel de detalhes**.

Os painéis de detalhes adicionados são apresentados na lista **Painéis de detalhes** da janela **Propriedades: Nova página**.

j. Na janela **Propriedades: Nova página**, clique em **OK**.

O nome da página com painéis de detalhes criada nos passos anteriores é apresentado na lista **Páginas** da janela **Propriedades: Estatísticas**.

k. Na janela **Propriedades: Estatísticas**, clique em **Fechar**.

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 **Computadores geridos**, da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração que inclui o computador cliente cuja lista de erros de encriptação pretende visualizar.

3. Na área de trabalho, selecione o separador **Dispositivos**.

4. No separador **Dispositivos**, selecione o nome do computador na lista e clique com o botão direito do rato para abrir o menu de contexto.

5. Execute uma das seguintes ações:

- No menu de contexto do computador, selecione **Proteção**.

- No menu de contexto do computador, selecione o item **Propriedades**. Na janela **Propriedades: <nome do computador>**, selecione a secção **Proteção**.

6. Na secção **Proteção** da janela **Propriedades: <nome do computador>**, clique na ligação **Ver lista de 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 **Erros de encriptação de dados**.

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 **Servidor de Administração** da árvore da Consola de Administração, selecione o separador **Relatórios**.
3. Clique no botão **Criar modelo de relatório**.

   O Assistente de Modelos de Relatório é iniciado.
4. Siga as instruções do Assistente de Modelos de Relatório. Na janela **Selecionar tipo de modelo de relatório** na secção **Outra**, selecione um dos seguintes itens:

   - **Relatório de estado de encriptação de dispositivos geridos**.
   - **Relatório de encriptação de dados de dispositivos armazenados**.
   - **Relatório de erros de encriptação**.
   - **Relatório sobre o acesso bloqueado a ficheiros encriptados**.

   Depois de concluir o Novo Assistente de Modelos de Relatório, o novo modelo de relatório é apresentado na tabela no separador **Relatórios**.
5. Selecione o modelo de relatório que foi criado nos passos prévios das instruções.

O processo de criação do relatório é iniciado. O relatório é apresentado numa nova janela.

Gerir ficheiros encriptados com funcionalidade de encriptação de ficheiros limitada

Quando a política do Kaspersky Security Center é aplicada e os ficheiros são posteriormente encriptados, o Kaspersky Endpoint Security recebe uma chave de encriptação necessária para aceder diretamente aos 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 podem não ser 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.

Aceder a ficheiros encriptados sem ligação ao Kaspersky Security Center

Estas instruções destinam-se a utilizadores de computadores cliente com o Kaspersky Endpoint Security instalado.

Para aceder a ficheiros encriptados sem ligação ao Kaspersky Security Center:

1. Tente aceder ao ficheiro encriptado de que necessita.

   Se não existir ligação ao Kaspersky Security Center quando tentar aceder a um ficheiro armazenado numa unidade local do computador, o Kaspersky Endpoint Security gera um ficheiro com um pedido de acesso a todos os ficheiros encriptados que estão armazenados em unidades locais. Se tentar aceder a um ficheiro armazenado numa unidade amovível, o Kaspersky Endpoint Security gera um ficheiro que solicita o acesso a todos os ficheiros encriptados que estão armazenados na unidade amovível. É aberta a janela **Acesso ao ficheiro bloqueado**.

2. Enviar o ficheiro que contém um pedido de acesso a ficheiros encriptados ao administrador de rede local. Para o fazer, execute uma das seguintes ações:

   - Para enviar por e-mail o ficheiro que solicita acesso a ficheiros encriptados ao administrador de rede local, clique no botão **Enviar por e-mail**.
   - Para guardar o ficheiro que solicita acesso aos ficheiros encriptados e enviá-lo ao administrador de rede local através de um método diferente, clique no botão **Guardar**.

3. Obtenha o ficheiro-chave para aceder a ficheiros encriptados que lhe tenham sido criados e fornecidos pelo administrador de rede local.

4. Ative a chave de acesso a ficheiros encriptados através de uma das seguintes formas:

   - Em qualquer gestor de ficheiros, selecione o ficheiro ou a chave de acesso a ficheiros encriptados. Abra-o com um duplo clique.

- Execute as seguintes ações:

  a. Abra a janela principal do Kaspersky Endpoint Security.

  b. Clique no botão .

  Esta ação abre a janela **Eventos**.

  c. Selecione o separador **Estado do acesso aos ficheiros e dispositivos**.

  O separador apresenta uma lista de todos os pedidos de acesso a ficheiros encriptados.

  d. Selecione o pedido para o qual recebeu o ficheiro-chave para acesso a ficheiros encriptados.

  e. Para carregar o ficheiro-chave fornecido para acesso aos ficheiros encriptados, clique em **Procurar**.

  É aberta a caixa de diálogo padrão **Selecionar ficheiro-chave de acesso** do Microsoft Windows.

  f. Na janela **Selecionar ficheiro-chave de acesso** do Microsoft Windows, selecione o ficheiro fornecido pelo administrador com a extensão .kesdr e o nome correspondente ao nome do ficheiro de pedido de acesso.

  g. Clique no botão **Abrir**.

  h. Na janela **Eventos**, clique em **OK**.

Se um ficheiro com um pedido de acesso a ficheiros encriptados for gerado durante uma tentativa de acesso a um ficheiro armazenado numa unidade local do computador, o Kaspersky Endpoint Security concede acesso a todos os ficheiros encriptados que estão armazenados em unidades locais. Se for gerado um ficheiro de acesso de pedido para ficheiros encriptados durante uma tentativa de acesso a um ficheiro armazenado numa unidade amovível, o Kaspersky Endpoint Security concede acesso a todos os ficheiros encriptados que estão armazenados na unidade amovível. Para aceder a ficheiros encriptados que estão armazenados noutras unidades amovíveis, tem de obter um ficheiro-chave de acesso individual para cada unidade amovível.

Fornecer acesso de utilizador a ficheiros encriptados sem ligação ao Kaspersky Security Center

Para fornecer acesso de utilizador a ficheiros encriptados sem ligação ao Kaspersky Security Center:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração que inclui o computador do utilizador que requer acesso aos ficheiros encriptados.
3. Na área de trabalho, selecione o separador **Dispositivos**.
4. No separador **Dispositivos**, selecione o computador do utilizador que solicitou acesso a ficheiros encriptados, e clique com o botão direito do rato para abrir o menu de contexto.
5. No menu de contexto, selecione a opção **Conceder acesso a dispositivos e dados em modo offline**.

   É aberta a janela **Conceder acesso a dispositivos e dados em modo offline**.
6. Na janela **Conceder acesso a dispositivos e dados em modo offline**, selecione o separador **Encriptação**.
7. No separador **Encriptação**, clique no botão **Procurar**.

   É apresentada a caixa de diálogo padrão **Selecionar ficheiro de acesso de pedido** do Microsoft Windows.

8. Na janela **Selecionar ficheiro de acesso de pedido**, especifique o caminho para o ficheiro de pedido enviado pelo utilizador e clique em **Abrir**.

   O Kaspersky Security Center gera um ficheiro-chave de acesso a ficheiros encriptados. Os detalhes do pedido do utilizador estão disponíveis no separador **Encriptação**.

9. Execute uma das seguintes ações:

   - Para enviar por e-mail o ficheiro-chave de acesso gerado para o utilizador, clique no botão **Enviar por e-mail**.
   - Para guardar o ficheiro-chave de acesso para os ficheiros encriptados e enviá-lo ao utilizador através de um método diferente, clique no botão **Guardar**.

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 **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração para o qual pretende editar os modelos de mensagens de pedido de acesso a ficheiros encriptados.
3. Na área de trabalho, selecione o separador **Políticas**.
4. Selecione a política pretendida.
5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:

   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.

6. Na secção **Encriptação de dados**, selecione a subsecção **Definições de encriptação comuns**.
7. Na secção **Modelos**, clique no botão **Modelos**.

   É aberta a janela **Modelos**.

8. Execute as seguintes ações:

   - Se pretender editar o modelo de mensagem de utilizador, selecione o separador **Mensagem do utilizador**. A janela **Acesso ao ficheiro recusado** é aberta quando o utilizador tenta aceder a um ficheiro encriptado enquanto não existe uma chave disponível no computador para aceder aos ficheiros encriptados. Ao clicar no botão **Enviar por e-mail** na janela **Acesso ao ficheiro recusado**, é criada automaticamente uma mensagem do utilizador. Esta mensagem é enviada ao administrador da rede da empresa local com conjunto com o ficheiro a solicitar acesso a ficheiros encriptados.
   - Se pretender editar o modelo de mensagem de administrador, selecione o separador **Mensagem do administrador**. Esta mensagem é criada automaticamente quando clica no botão **Enviar por e-mail** na janela **Conceder acesso a ficheiros encriptados** e é enviada ao utilizador depois de acesso a ficheiros encriptados ter sido concedido ao utilizador.

9. Editar os modelos da mensagem.

Pode utilizar o botão **Predefinição** e a lista pendente **Variável**.

10. Clique em **OK**.

11. Para guardar as alterações, na janela **Propriedades: <Nome da política>** clique em **OK**.

Trabalhar com dispositivos encriptados quando não existe acesso aos mesmos

Obter acesso a dispositivos encriptados

Um utilizador pode ser obrigado a solicitar o acesso a dispositivos encriptados nos seguintes casos:

- o disco rígido foi encriptado num computador diferente.
- a chave de encriptação de um dispositivo não está no computador (por exemplo, depois da primeira tentativa de aceder à unidade amovível encriptada no computador) e o computador não está ligado ao Kaspersky Security Center.

  depois de o utilizador ter aplicado a chave de acesso ao dispositivo encriptado, o Kaspersky Endpoint Security guarda a chave de encriptação no computador do utilizador e permite o acesso a este dispositivo depois de tentativas de acesso subsequentes, mesmo que não exista ligação ao Kaspersky Security Center.

O acesso a dispositivos encriptados pode ser obtido da seguinte forma:

1. O utilizador utiliza a interface da aplicação do Kaspersky Endpoint Security para criar um ficheiro de acesso de pedido com a extensão kesdc e envia-a ao administrador da rede local empresarial.
2. O administrador utiliza a Consola de Administração do Kaspersky Security Center para criar um ficheiro-chave de acesso com a extensão kesdr e envia-a ao utilizador.
3. O utilizador aplica a chave de acesso.

Restaurar dados em dispositivos encriptados

Um utilizador pode utilizar a Ferramenta de Restauro de Dispositivo Encriptado (doravante designada Ferramenta de Restauro) para trabalhar com dispositivos encriptados. Tal pode ser necessário nos seguintes casos:

- O procedimento para utilizar uma chave de acesso para obter acesso foi malsucedido.
- Os componentes de encriptação não foram instalados no computador com o dispositivo encriptado.

Os dados necessários para restaurar o acesso a dispositivos encriptados ao utilizar a Ferramenta de Restauro estão na memória do computador do utilizador na forma desencriptada durante algum tempo. Para reduzir o risco de acesso não autorizado a esses dados, recomendamos que restaure o acesso aos dispositivos encriptados em computadores fidedignos.

Os dados em dispositivos encriptados podem ser restaurados da seguinte forma:

1. O utilizador utiliza a Ferramenta de Restauro para criar um ficheiro de acesso de pedido com a extensão fdertc e envia-a ao administrador da rede local empresarial.

2. O administrador utiliza a Consola de Administração do Kaspersky Security Center para criar um ficheiro-chave de acesso com a extensão fdertr e envia-a ao utilizador.

3. O utilizador aplica a chave de acesso.

Para restaurar dados em discos rígidos de sistema encriptados, o utilizador também pode especificar as credenciais da conta de Agente de Autenticação na Ferramenta de Restauro. Se os metadados da conta do Agente de Autenticação tiverem sido corrompidos, o utilizador deve concluir o procedimento de restauro ao utilizar um ficheiro de acesso de pedido.

Antes de restaurar dados em dispositivos encriptados, recomenda-se o cancelamento da política de encriptação do Kaspersky Security Center no computador onde esta operação vai ser realizada. Este procedimento impede que a unidade seja encriptada novamente.

Obter acesso a dispositivos encriptados através da interface da aplicação

Estas instruções destinam-se a utilizadores de computadores cliente com o Kaspersky Endpoint Security instalado.

Para obter acesso a dispositivos encriptados através da interface da aplicação:

1. Tente aceder ao dispositivo encriptado de que necessita.

   É aberta a janela **Acesso aos dados está bloqueado**.

2. Envie ao administrador da rede local empresarial o ficheiro de acesso de pedido com a extensão kesdc do dispositivo encriptado. Para o fazer, execute uma das seguintes ações:

   - Para enviar por e-mail ao administrador da rede local empresarial o ficheiro de acesso de pedido gerado para o dispositivo encriptado, clique no botão **Enviar por e-mail**.

   - Para guardar o ficheiro de acesso de pedido para o dispositivo encriptado e enviá-lo ao administrador de rede local empresarial através de um método diferente, clique no botão **Guardar**.

   Se tiver fechado a janela **Acesso aos dados está bloqueado** sem guardar o ficheiro de acesso de pedido ou sem enviá-lo ao administrador da rede local empresarial, pode fazê-lo em qualquer momento na janela **Eventos** no separador **Estado do acesso aos ficheiros e dispositivos**. Para abrir esta janela, clique no botão na janela principal da aplicação.

3. Obtenha e guarde o ficheiro-chave de acesso do dispositivo encriptado que foi criado e fornecido pelo administrador da rede local empresarial.

4. Utilize um dos seguintes métodos para aplicar a chave de acesso para aceder ao dispositivo encriptado:

   - Em qualquer gestor de ficheiros, encontre o ficheiro-chave de acesso ao dispositivo encriptado e clique duas vezes no mesmo para o abrir.

- Execute as seguintes ações:

  a. Abra a janela principal do Kaspersky Endpoint Security.

  b. Clique no botão para abrir a janela **Eventos**.

  c. Selecione o separador **Estado do acesso aos ficheiros e dispositivos**.

  O separador apresenta uma lista de todos os pedidos de acesso a ficheiros encriptados e dispositivos.

  d. Selecione o pedido para o qual recebeu o ficheiro-chave de acesso para aceder ao dispositivo encriptado.

  e. Para carregar o ficheiro-chave de acesso recebido para aceder ao dispositivo encriptado, clique em **Procurar**.

  É aberta a caixa de diálogo padrão **Selecionar ficheiro-chave de acesso** do Microsoft Windows.

  f. Na janela padrão **Selecionar ficheiro-chave de acesso** do Microsoft Windows, selecione o ficheiro fornecido pelo administrador com a extensão kesdr e o nome correspondente ao nome de ficheiro do ficheiro de acesso de pedido correspondente para o dispositivo encriptado.

  g. Clique no botão **Abrir**.

  h. Na janela **Estado do acesso aos ficheiros e dispositivos**, clique em **OK**.

Consequentemente, o Kaspersky Endpoint Security concede o acesso ao dispositivo encriptado.

Conceder acesso de utilizador a dispositivos encriptados

Para conceder acesso de utilizador a um dispositivo encriptado:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração que inclui o computador do utilizador que requer acesso ao dispositivo encriptado.
3. Na área de trabalho, selecione o separador **Dispositivos**.
4. No separador **Dispositivos**, selecione o computador do utilizador que solicitou acesso ao dispositivo encriptado e clique com o botão direito do rato para abrir o menu de contexto.
5. No menu de contexto, selecione a opção **Conceder acesso a dispositivos e dados em modo offline**.

   É aberta a janela **Conceder acesso a dispositivos e dados em modo offline**.
6. Na janela **Conceder acesso a dispositivos e dados em modo offline**, selecione o separador **Encriptação**.
7. No separador **Encriptação**, clique no botão **Procurar**.

   É apresentada a caixa de diálogo padrão **Selecionar ficheiro de acesso de pedido** do Microsoft Windows.
8. Na janela **Selecionar ficheiro de acesso de pedido**, especifique o caminho até ao ficheiro de pedido com a extensão kesdc que recebeu do utilizador.
9. Clique no botão **Abrir**.

O Kaspersky Security Center gera um ficheiro-chave de acesso a dispositivo encriptado com a extensão kesdr. Os detalhes do pedido do utilizador estão disponíveis no separador **Encriptação**.

10. Execute uma das seguintes ações:

    - Para enviar por e-mail o ficheiro-chave de acesso gerado para o utilizador, clique no botão **Enviar por e-mail**.
    - Para guardar o ficheiro-chave de acesso para o dispositivo encriptado e fornecê-lo ao utilizador através de outro método, clique no botão **Guardar**.

Fornecer a um utilizador uma chave de recuperação para unidades de disco rígido encriptadas com o BitLocker

Para enviar a um utilizador uma chave de recuperação para uma unidade de disco rígido de sistema que foi encriptada utilizando o BitLocker:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração que inclui o computador do utilizador que requer acesso à unidade encriptada.
3. Na área de trabalho, selecione o separador **Dispositivos**.
4. No separador **Dispositivos**, selecione o computador pertencente ao utilizador que requer acesso à unidade encriptada.
5. Clique com o botão direito para abrir o menu de contexto e selecione **Conceder acesso a dispositivos e dados em modo offline**.

   É aberta a janela **Conceder acesso a dispositivos e dados em modo offline**.
6. Na janela **Conceder acesso a dispositivos e dados em modo offline**, 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.

8. Envie ao utilizador a chave que está indicada no campo **Chave de recuperação**.

Para enviar a um utilizador uma chave de recuperação para uma unidade de disco rígido não pertencente ao sistema que foi encriptada utilizando o BitLocker:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na árvore da Consola de Administração, selecione a pasta **Adicional** → **Encriptação e proteção de dados** → **Dispositivos encriptados**.

   A área de trabalho apresenta uma lista dos dispositivos encriptados.

3. Na área de trabalho, selecione o dispositivo encriptado de que necessita para restaurar o acesso.

4. Clique com o botão direito do rato para visualizar o menu de contexto e selecione **Obter a chave de acesso ao dispositivo encriptado especificado**.

   Esta ação abre a janela **Restaurar acesso a uma unidade encriptada com o BitLocker**.

5. Solicitar ao utilizador o ID da chave de recuperação indicado na janela de introdução da password do BitLocker e compará-lo com o ID no campo **ID da chave de recuperação**.

   Se os IDs não forem correspondentes, esta chave não é válida para restaurar o acesso à unidade especificada. Certifique-se de que o nome do computador selecionado corresponde ao nome do computador do utilizador.

6. Envie ao utilizador a chave que está indicada no campo **Chave de recuperação**.

Criação do ficheiro executável do Ferramenta de Restauro

Estas instruções destinam-se a utilizadores de computadores cliente com o Kaspersky Endpoint Security instalado.

Para criar o ficheiro executável da Ferramenta de Restauro:

1. Abra a janela principal da aplicação.

2. Clique no botão no canto inferior esquerdo da janela principal da aplicação para abrir a janela **Suporte**.

3. Na janela **Suporte**, clique no botão **Restaurar dispositivo encriptado**.

   O Ferramenta de Restauro de dispositivo encriptado é iniciado.

4. Clique no botão **Criar Ferramenta de Restauro autónoma** na janela do Ferramenta de Restauro.

   É apresentada a janela **Criar Ferramenta de Restauro autónoma**.

5. Na janela **Guardar em**, introduza manualmente o caminho para a pasta, para guardar o ficheiro executável do Ferramenta de Restauro ou clique no botão **Procurar**.

6. Clique em **OK** na janela **Criar Ferramenta de Restauro autónoma**.

   O ficheiro executável do Ferramenta de Restauro (fdert.exe) é guardado na pasta selecionada.

Restaurar dados em dispositivos encriptados utilizando a Ferramenta de Restauro

Estas instruções destinam-se a utilizadores de computadores cliente com o Kaspersky Endpoint Security instalado.

Para restaurar o acesso um dispositivo encriptado utilizando o Ferramenta de Restauro:

1. Execute a Ferramenta de Restauro de uma das seguintes formas:

   - Clique no botão na janela principal do Kaspersky Endpoint Security para abrir a janela **Suporte** e clique em **Restaurar dispositivo encriptado**.

   - Execute o ficheiro executável fdert.exe da Ferramenta de Restauro. Este ficheiro é criado pelo Kaspersky Endpoint Security.

2. Na janela do Ferramenta de Restauro, na lista suspensa **Selecionar dispositivo**, selecione um dispositivo encriptado para o qual pretende restaurar o acesso.

3. Clique no botão **Verificar** para permitir que o utilitário defina as ações que devem ser executadas no dispositivo: se deve ser desbloqueado ou desencriptado.

   Se o computador tiver acesso à funcionalidade de encriptação do Kaspersky Endpoint Security, a Ferramenta de Restauro solicita que desbloqueie o dispositivo. Uma vez que o desbloqueio do dispositivo não o desencripta, o dispositivo fica diretamente acessível em consequência de estar desbloqueado. Se o computador não tiver acesso à funcionalidade de encriptação do Kaspersky Endpoint Security, a Ferramenta de Restauro solicita que desencripte o dispositivo.

4. 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.

5. Clique no botão **Desbloquear** ou **Desencriptar**, dependendo dos resultados do diagnóstico.

   É apresentada a janela **Definições de desbloqueio do dispositivo** ou **Definições de desencriptação do dispositivo**.

6. Se pretende restaurar dados ao utilizar uma conta de Agente de Autenticação:

   a. selecione a opção **Utilizar parâmetros da conta do Agente de Autenticação**.

   b. Nos campos **Nome** e **Password**, especifique as credenciais da conta 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.

7. Se pretende utilizar uma chave de acesso para restaurar dados:

   a. selecione a opção **Especificar chave de acesso ao dispositivo manualmente**.

   b. Clique no botão **Receber chave de acesso**.

   c. É aberta a janela **Receber chave de acesso ao dispositivo**.

   d. Clique no botão **Guardar** e selecione a pasta na qual vai guardar o ficheiro de acesso de pedido com a extensão fdertc.

   e. 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.

f. Obtenha e guarde o ficheiro-chave de acesso que foi criado e fornecido pelo administrador da rede local empresarial.

g. Clique no botão **Carregar** e selecione o ficheiro-chave de acesso com a extensão fdertr na janela que se abre.

8. Se estiver a desencriptar um dispositivo, também terá de especificar as outras definições de desencriptação na janela **Definições de desencriptação do dispositivo**. Para tal:

   - Especificar a área para desencriptar:
     - Se pretender desencriptar o dispositivo completo, selecione a opção **Desencriptar todo o dispositivo**.
     - Se quiser desencriptar uma porção dos dados num dispositivo, selecione a opção **Desencriptar áreas individuais do dispositivo** e utilize os campos **Início** e **Fim** para especificar os limites da área de desencriptação.
   - Selecione o local de escrita dos dados desencriptados:
     - Se pretender que os dados no dispositivo original sejam reescritos com os dados desencriptados, desmarque a caixa de verificação **Guardar dados em ficheiro após desencriptação**.
     - Se pretender guardar os dados desencriptados separadamente dos dados encriptados originais, selecione a caixa de verificação **Guardar dados em ficheiro após desencriptação** e utilize o botão **Procurar** para especificar o caminho no qual vai guardar os dados.

9. Clique em **OK**.

O processo de desbloqueio/desencriptação do dispositivo é iniciado.

Responder ao pedido de um utilizador para restaurar dados em dispositivos encriptados

Para criar um ficheiro-chave para aceder a um dispositivo encriptados e fornecê-lo a um utilizador:

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

2. Na árvore da Consola de Administração, selecione a pasta **Adicional** → **Encriptação e proteção de dados** → **Dispositivos encriptados**.

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 a chave de acesso do dispositivo encriptado especificado**.

   Se não estiver seguro para que computador o ficheiro de acesso de pedido foi gerado, na árvore da Consola de Administração selecione a pasta **Adicional** → **Encriptação e proteção de dados** e, na área de trabalho, clique na ligação **Obter a chave de encriptação do dispositivo**.

   É apresentada a janela **Permitir acesso ao dispositivo**.

4. Selecione o algoritmo de encriptação em utilização. Para tal, selecione uma das seguintes opções:

- **AES256**, se o Kaspersky Endpoint Security foi instalado a partir de um pacote de distribuição localizado na pasta aes256 no computador em que o dispositivo foi encriptado;
- **AES56**, se o Kaspersky Endpoint Security foi instalado a partir de um pacote de distribuição localizado na pasta aes56 no computador em que o dispositivo foi encriptado;

5. Clique no botão **Procurar**.

   É apresentada a caixa de diálogo padrão **Selecionar ficheiro de acesso de pedido** do Microsoft Windows.

6. Na janela **Selecionar ficheiro de acesso de pedido**, especifique o caminho até ao ficheiro de pedido com a extensão fdertc que recebeu do utilizador.

7. Clique no botão **Abrir**.

   O Kaspersky Security Center gera um ficheiro-chave de acesso com a extensão fdertr para aceder ao dispositivo encriptado.

8. Execute uma das seguintes ações:
   - Para enviar por e-mail o ficheiro-chave de acesso gerado para o utilizador, clique no botão **Enviar por e-mail**.
   - Para guardar o ficheiro-chave de acesso para o dispositivo encriptado e fornecê-lo ao utilizador através de outro método, clique no botão **Guardar**.

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 controlava o computador durante a encriptação dos dados.

O acesso aos dados encriptados será concedido com as mesmas condições aplicadas antes da falha do sistema operativo.

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).

Proteção de Rede

Esta secção contém informações sobre a monitorização do tráfego de rede e instruções sobre o modo de configuração das definições das portas de rede monitorizadas.

Sobre a Proteção de Rede

Durante o funcionamento do Kaspersky Endpoint Security, os componentes como Antivírus de E-mail, Antivírus de Internet e Antivírus de MI monitorizam os fluxos de dados transmitidos através de protocolos específicos e que passam por determinadas portas TCP e UDP abertas no seu computador. Por exemplo, o Antivírus de E-mail verifica dados transmitidos através de SMTP, enquanto o Antivírus de Internet verifica dados transmitidos através de HTTP e FTP.

O Kaspersky Endpoint Security divide as portas TCP e UDP do sistema operativo em vários grupos, conforme a probabilidade de a sua segurança vir a ser comprometida. Algumas portas de rede estão reservadas para serviços que podem ser vulneráveis. É aconselhável monitorizar estas portas de forma mais minuciosa, uma vez que a probabilidade de serem atacadas é maior. 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 Antivírus de E-mail, Antivírus de Internet e Antivírus de MI ao monitorizarem o tráfego de rede.

Configurar as definições da monitorização do tráfego de rede

Pode efetuar as ações seguintes para configurar as definições da monitorização de tráfego 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.

Ativar a monitorização de todas as portas de rede

Para ativar a monitorização de todas as portas de rede:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, selecione a secção **Proteção de Antivírus**.
   As definições da Proteção de Antivírus são apresentadas na parte direita da janela.
3. Na secção **Portas monitorizadas**, selecione **Monitorizar todas as portas de rede**.
4. Para guardar as alterações, clique no botão **Guardar**.

Criar uma lista de portas de rede monitorizadas

Para criar uma lista de portas de rede monitorizadas:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, selecione a secção **Proteção de Antivírus**.

   As definições da Proteção de Antivírus são apresentadas na parte direita da janela.
3. Na secção **Portas monitorizadas**, selecione **Monitorizar apenas portas selecionadas**.
4. Clique no botão **Configuração**.

   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.
5. Na lista de portas de rede, execute as seguintes ações:

   - Selecione as caixas de verificação junto às portas de rede que pretende incluir na lista de portas de rede monitorizadas.

     Por defeito, as caixas de verificação são selecionadas junto a todas as portas de rede listadas na janela **Portas de rede**.
   - Desmarque as caixas de verificação junto às portas de rede que pretende excluir da lista de portas de rede monitorizadas.
6. Se uma porta de rede não for apresentada na lista de portas de rede, adicione a mesma do seguinte modo:

   a. Na lista de portas de rede, clique na ligação **Adicionar** para abrir a janela **Porta de rede**.

   b. Introduza o número da porta de rede no campo **Porta**.

   c. Introduza o nome da porta de rede no campo **Descrição**.

   d. Clique em **OK**.

      A janela **Porta de rede** é fechada. A nova porta adicionada é apresentada no fim da lista de portas de rede.
7. Na janela **Portas de rede**, clique em **OK**.
8. Para guardar as alterações, clique no botão **Guardar**.

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, selecione a caixa de verificação **Monitorizar todas as portas de rede** na secção **Portas monitorizadas** ou configure a monitorização de todas as portas para aplicações que estabelecem ligação ao 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. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, selecione a secção **Proteção de Antivírus**.

   As definições da Proteção de Antivírus são apresentadas na parte direita da janela.
3. Na secção **Portas monitorizadas**, selecione **Monitorizar apenas portas selecionadas**.
4. Clique no botão **Configuração**.

   É aberta a janela **Portas de rede**.
5. Selecione a caixa de verificação **Monitorizar todas as portas das aplicações especificadas**.
6. Na lista de aplicações na caixa de verificação **Monitorizar todas as portas das aplicações especificadas** execute as seguintes ações:

   - Selecione as caixas de verificação junto aos nomes das aplicações para as quais pretende monitorizar todas as portas de rede.

     Por defeito, as caixas de verificação são selecionadas junto a todas as aplicações listadas na janela **Portas de rede**.

   - Desmarque as caixas de verificação junto aos nomes das aplicações para as quais não pretende monitorizar todas as portas de rede.
7. Se uma aplicação não estiver incluída na lista de aplicações, adicione-a da seguinte forma:

   a. Clique na ligação **Adicionar** na lista de aplicações e abra o menu de contexto.

   b. No menu de contexto, selecione o modo como a aplicação deverá ser adicionada à lista de aplicações:

      - Para selecionar uma aplicação da lista de aplicações instaladas no computador, selecione o comando **Aplicações**. É aberta a janela **Selecionar aplicação**, que permite especificar o nome da aplicação.

      - Para especificar a localização do ficheiro executável da aplicação, selecione o comando **Procurar**. É aberta a janela padrão **Abrir** no Microsoft Windows, que permite especificar o nome do ficheiro executável da aplicação.

     A janela **Aplicação** é aberta após selecionar a aplicação.

   c. No campo **Nome**, introduza um nome para a aplicação selecionada.

   d. Clique em **OK**.

A janela **Aplicação** é fechada. A aplicação adicionada é apresentada no fim da lista de aplicações.

8. Na janela **Portas de rede**, clique em **OK**.

9. Para guardar as alterações, clique no botão **Guardar**.

Atualização bases de dados e módulos de software de aplicação

Esta secção contém informações sobre Atualizações de bases de dados e módulos da aplicação (também denominadas "atualizações") e instruções sobre como configurar as definições de atualização.

Sobre as atualizações de bases de dados e módulos da 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 sucesso o pacote de atualização dos servidores de atualização da Kaspersky. Por predefinição, as definições da ligação à Internet são automaticamente determinadas. Se utilizar um servidor de proxy, terá de ajustar as definições da ligação.

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).

A informação sobre o estado atual das bases de dados do Kaspersky Endpoint Security é apresentada em **Atualizar**, na secção **Tarefas** no separador **Proteção e Controlo** da janela principal da aplicação.

A informação sobre os resultados de atualização que ocorrem durante o desempenho da tarefa de atualização está registada no relatório do Kaspersky Endpoint Security.

Sobre as origens 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.

Configuração das definições de atualização

Pode executar as seguintes ações para configurar as definições de atualização:

- Adicionar novas origens de atualização.

  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.

  Se forem selecionados vários recursos como origens de atualização, o Kaspersky Endpoint Security tentar estabelecer ligação aos mesmos, um após o outro, começando pelo topo da lista, e executa a tarefa de atualização recolhendo o pacote de atualização na primeira origem disponível.

  > Se selecionar um recurso localizado fora da rede local como origem de atualização, será necessária uma ligação à Internet para efetuar a atualização.

- Selecionar a região do servidor de atualização da Kaspersky.

  Se utilizar servidores de atualização da Kaspersky como origem de atualização, pode selecionar a localização do servidor de atualização da Kaspersky utilizado para transferir o pacote de atualização. Os servidores de atualização da Kaspersky estão localizados em vários países. A utilização dos servidores de atualização da Kaspersky mais próximos ajuda a reduzir o tempo despendido na recolha de um pacote de atualização.

  Por predefinição, a aplicação utiliza a informação sobre a região atual do registo do sistema operativo.

- Configurar a atualização do Kaspersky Endpoint Security a partir de uma pasta partilhada.

  Para poupar no tráfego de Internet, pode configurar as atualizações do Kaspersky Endpoint Security de modo a que os computadores da rede local recebam atualizações a partir de uma pasta partilhada. Para este fim, um dos computadores na rede local recebe um pacote de atualização do servidor do Kaspersky Security Center ou dos servidores de atualização da Kaspersky e copia-o para uma pasta partilhada. Após esta ação, os restantes computadores da rede local podem receber o pacote de atualização a partir desta pasta partilhada.

- 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 **Planificadas** 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.

- Configurar a tarefa de atualização para execução com os direitos de uma conta de utilizador diferente.

Adicionar uma origem de atualização

Para adicionar uma origem de atualização:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione **Atualizar**.
   Na parte direita da janela, são apresentadas as Definições de atualização da aplicação.
3. Na secção **Modo de execução e origem da atualização**, clique no botão **Origem da atualização**.
   Esta ação abre o separador **Origem** da janela **Atualizar**.
4. No separador **Origem**, clique no botão **Adicionar**.
   A janela **Selecionar Origem de atualização** é aberta.
5. Na janela **Selecionar Origem de atualização**, selecione uma pasta com o pacote de atualização ou introduza o caminho completo para a pasta no campo **Origem**.
6. Clique em **OK**.
7. Na janela **Atualização**, clique em **OK**.
8. Para guardar as alterações, clique no botão **Guardar**.

Selecionar a região do servidor de atualização

Para selecionar a região do servidor de atualização:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione **Atualizar**.
   Na parte direita da janela, são apresentadas as Definições de atualização da aplicação.
3. Na secção **Modo de execução e origem da atualização**, clique no botão **Origem da atualização**.
   Esta ação abre o separador **Origem** da janela **Atualizar**.
4. No separador **Origem**, na secção **Configurações regionais**, escolha **Selecione a partir da lista**.
5. Na lista suspensa, selecione o país mais próximo da sua localização atual.
6. Clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

Configurar atualizações a partir de uma pasta partilhada

Pode configurar as atualizações do Kaspersky Endpoint Security a partir de uma pasta partilhada executando os passos seguintes:

1. Ative a cópia de um pacote de atualização para uma pasta partilhada em um dos computadores na rede local.
2. Configure as atualizações do Kaspersky Endpoint Security a partir da pasta partilhada especificada para os restantes computadores na rede local.

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

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione **Atualizar**.

   Na parte direita da janela, são apresentadas as Definições de atualização da aplicação.
3. Na secção **Adicional**, selecione a caixa de verificação **Copiar atualizações para a pasta**.
4. Especifique o caminho para a pasta partilhada em que pretende colocar o pacote de atualização. Pode especificar o caminho através de uma das seguintes duas formas:
   - Introduza o caminho para a pasta partilhada no campo junto à caixa de verificação **Copiar atualizações para a pasta**.
   - Clique no botão **Procurar**. Em seguida, na janela **Selecionar pasta** apresentada, selecione a pasta pretendida e clique em **OK**.
5. Para guardar as alterações, clique no botão **Guardar**.

Para configurar a atualização do Kaspersky Endpoint Security a partir de uma pasta partilhada:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione **Atualizar**.

   Na parte direita da janela, são apresentadas as Definições de atualização da aplicação.
3. Na secção **Modo de execução e origem da atualização**, clique no botão **Origem da atualização**.

   Esta ação abre o separador **Origem** da janela **Atualizar**.
4. No separador **Origem**, clique no botão **Adicionar**.

   A janela **Selecionar Origem de atualização** é aberta.
5. Na janela **Selecionar Origem de atualização**, selecione a pasta partilhada que contém o pacote de atualização ou introduza o caminho completo para a pasta partilhada no campo **Origem**.
6. Clique em **OK**.
7. No separador **Origem**, desmarque as caixas de verificação junto aos nomes das origens de atualização que não foram especificadas como a pasta partilhada.
8. Clique em **OK**.

9. Para guardar as alterações, clique no botão **Guardar**.

Selecionar o modo de execução da tarefa de atualização

Para selecionar o modo de execução da tarefa de atualização:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione **Atualizar**.

   Na parte direita da janela, são apresentadas as Definições de atualização da aplicação.
3. Clique no botão **Modo de execução**.

   O separador **Modo de execução** é apresentado na janela **Atualizar**.
4. Na secção **Modo de execução**, selecione uma das opções seguintes para iniciar uma 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 **Planificadas**.
5. Execute uma das seguintes ações:

   - Se selecionou a opção **Automaticamente** ou **Manualmente**, consulte o passo 6 das instruções.
   - Se selecionou a opção **Planificadas**, especifique as Configuração do agendamento de execução da tarefa de atualização. Para tal:

     a. Na lista suspensa **Frequência**, especifique o início da tarefa de atualização. Selecione uma das seguintes opções: **Minutos**, **Horas**, **Dias**, **Todas as semanas**, **A uma hora especificada**, **Todos os meses** ou **Após o início da aplicação**.

     b. Dependendo da opção selecionada na lista suspensa **Frequência**, especifique valores para as configurações que definem a hora de início da tarefa de atualização.

     c. No campo **Adiar execução, após o início da aplicação, durante**, especifique o intervalo de tempo em que início da tarefa de atualização é adiado, após o início do Kaspersky Endpoint Security.

     > Se o item **Após o início da aplicação** estiver selecionado na lista suspensa **Frequência**, o campo **Adiar execução, após o início da aplicação, durante** não está disponível.

     d. Se pretender que o Kaspersky Endpoint Security execute as tarefas de atualização ignoradas assim que possível, selecione a caixa de verificação **Executar tarefas ignoradas**.

     > Se as opções **Horas**, **Minutos** ou **Após o início da aplicação** estiverem selecionadas na lista suspensa **Frequência**, a caixa de verificação **Executar tarefas ignoradas** não está disponível.

6. Clique em **OK**.

7. Para guardar as alterações, clique no botão **Guardar**.

Iniciar uma tarefa de atualização com os direitos de outra conta de utilizador

Por defeito, 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 por não ter os direitos de um utilizador de servidor de proxy autorizado. 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. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione **Atualizar**.

   Na parte direita da janela, são apresentadas as Definições de atualização da aplicação.

3. Na secção **Modo de execução e origem da atualização**, clique no botão **Modo de execução**.

   O separador **Modo de execução** é apresentado na janela **Atualizar**.

4. No separador **Modo de execução**, na secção **Utilizador**, selecione a caixa de verificação **Executar tarefa como**.

5. No campo **Nome**, introduza o nome da conta de utilizador cujos direitos são necessários para aceder à origem de atualização.

6. No campo **Password**, introduza a password do utilizador cujos direitos são necessários para aceder à origem de atualização.

7. Clique em **OK**.

8. Para guardar as alterações, clique no botão **Guardar**.

Configurar as atualizações de atualização dos módulos da aplicação

Para configurar as atualizações de atualização dos módulos da aplicação:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione **Atualizar**.

   Na parte direita da janela, são apresentadas as Definições de atualização da aplicação.

3. Na secção **Adicional**, execute uma das seguintes ações:

- Selecione a caixa de verificação **Transferir atualizações dos módulos da aplicação** se pretender que a aplicação inclua as atualizações dos módulos da aplicação nos pacotes de atualização.

- Caso contrário, desmarque a caixa de verificação **Transferir atualizações dos módulos da aplicação**.

4. Se a caixa de verificação **Transferir atualizações dos módulos da aplicação** estiver selecionada no passo anterior, especifique as condições através das quais a aplicação instalará as atualizações do módulo da aplicação:

   - Selecione a opção **Instalar atualizações críticas e aprovadas** se pretender que a aplicação instale atualizações críticas dos módulos da aplicação automaticamente e outras atualizações após a sua instalação ser aprovada, localmente através da interface da aplicação ou utilizando o Kaspersky Security Center.

   - Selecione a opção **Instalar apenas atualizações aprovadas** se pretender que a aplicação instale atualizações dos módulos da aplicação após a sua instalação ser aprovada, localmente através da interface da aplicação ou utilizando o Kaspersky Security Center.

5. Para guardar as alterações, clique no botão **Guardar**.

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 transferir um pacote de atualização dos servidores da Kaspersky, é necessária uma ligação à Internet.

Para iniciar ou parar uma tarefa de atualização:

1. Abra a janela principal da aplicação.

2. Selecione o separador **Proteção e Controlo**.

3. Clique na secção **Tarefas**.

   A secção **Tarefas** é aberta.

4. Clique com o botão direito do rato para visualizar o menu de contexto da linha que inclui o nome da tarefa de atualização.

   Ao clicar na linha, é aberto um menu de ações a executar na tarefa de atualização.

5. Execute uma das seguintes ações:

   - Se pretender iniciar a tarefa de atualização, selecione **Iniciar atualização** no menu.

     O estado de evolução da tarefa de atualização, que é apresentado à direita do botão **Atualizar**, é alterado para *Em execução*.

   - Se pretender parar a tarefa de atualização, selecione **Parar atualização** no menu.

     O estado de evolução da tarefa de atualização, que é apresentado à direita do botão **Atualizar**, é alterado para *parado*.

Reverter a 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 não válida que leva o Kaspersky Endpoint Security a bloquear uma aplicação segura.

Para reverter a última atualização:

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Tarefas**.
   A secção **Tarefas** é aberta.
4. Clique com o botão direito do rato para visualizar o menu de contexto da tarefa **Atualização**.
5. Selecione **Reverter atualização**.

Configurar o servidor de proxy

Para configurar as definições do servidor proxy:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione **Atualizar**.
   Na parte direita da janela, são apresentadas as Definições de atualização da aplicação.
3. Na secção **Servidor de proxy**, clique no botão **Configuração**.
   Abre-se a janela **Configuração do servidor de proxy**.
4. Na janela **Configuração do servidor de proxy**, selecione a caixa de verificação **Utilizar servidor de proxy**.
5. Especifique as definições do servidor de proxy.
6. Clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

Também pode configurar as definições do servidor de proxy na janela principal da aplicação, no separador **Configuração**, na secção **Configurações avançadas**.

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.

Esta secção descreve as especificidades e a configuração de tarefas de verificação, níveis de segurança, métodos e tecnologias de verificação e instruções sobre o processamento de ficheiros que não tenham sido processados pelo Kaspersky Endpoint Security durante um scan de vírus.

Sobre as tarefas de verificação

Para localizar vírus e outros tipos de software malicioso e verificar a integridade de módulos de aplicação, o Kaspersky Endpoint Security inclui as seguintes tarefas:

- **Verificação completa**. Uma verificação minuciosa de todo o computador. Por defeito, o Kaspersky Endpoint Security verifica os seguintes objetos:
  - Memória Kernel
  - Objetos carregados ao iniciar o sistema operativo
  - Setores de inicialização
  - Cópia de segurança do sistema operativo
  - Todas as unidades de disco rígido e amovíveis
- **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.
- **Verificação personalizada**. O Kaspersky Endpoint Security verifica os objetos selecionados pelo utilizador. Pode verificar qualquer objeto da seguinte lista:
  - Memória Kernel
  - Objetos carregados ao iniciar o sistema operativo
  - Cópia de segurança do sistema operativo
  - Caixa de correio do Outlook
  - Todas as unidades de disco rígido, amovíveis e de rede
  - Qualquer ficheiro selecionado
- **Verificação de integridade**. O Kaspersky Endpoint Security verifica se os módulos de aplicação foram corrompidos ou modificados.

As tarefas Verificação Completa e Verificação de Áreas Críticas são ligeiramente diferentes das outras. Para estas tarefas, não é recomendado editar o âmbito de verificação.

Depois do início das tarefas de verificação, o seu progresso é apresentado no campo junto do nome da tarefa de verificação em execução, na secção **Tarefas** no separador **Proteção e Controlo** da janela principal do Kaspersky Endpoint Security.

A informação sobre os resultados da verificação e eventos, que ocorreram durante a execução das tarefas de verificação, é registada num relatório do Kaspersky Endpoint Security.

Iniciar ou parar uma tarefa de verificação

Independentemente do modo de execução da tarefa de verificação selecionado, pode iniciar ou parar uma tarefa de verificação em qualquer altura.

Para iniciar ou parar uma tarefa de verificação:

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Tarefas**.

   A secção **Tarefas** é aberta.
4. Clique com o botão direito do rato para visualizar o menu de contexto da linha que inclui o nome da tarefa de verificação.

   É apresentado um menu com as ações da tarefa de verificação.
5. Execute uma das seguintes ações:

   - Se pretender iniciar a tarefa de verificação, selecione **Iniciar verificação** no menu.

     O estado do progresso da tarefa apresentado à direita do botão com o nome desta tarefa de verificação é alterado para *Em execução*.

   - Se pretender parar a tarefa de verificação, selecione **Parar verificação** no menu.

     O estado do progresso da tarefa apresentado à direita do botão com o nome desta tarefa de verificação é alterado para *Parado*.

Configurar definições das tarefas de verificação

Para configurar as definições das tarefas de verificação, pode executar as seguintes ações:

- Alterar o nível de segurança.

  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.

- Alterar a ação que o Kaspersky Endpoint Security executa se detetar um ficheiro infetado.

- Editar o âmbito de verificação.

  Pode alargar ou restringir o âmbito de verificação, adicionando ou removendo objetos de verificação ou alterando o tipo de ficheiros a verificar.

- Otimizar a 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).

  Também pode ativar a utilização das tecnologias iChecker e iSwift. Estas tecnologias otimizam a velocidade da verificação de ficheiros, excluindo os ficheiros que não foram modificados desde a verificação mais recente.

- Configurar a verificação de ficheiros compostos.

- Configurar a utilização de métodos de verificação.

  Quando ativo, o Kaspersky Endpoint Security utiliza a análise de assinaturas. Durante a análise de assinaturas, o Kaspersky Endpoint Security faz corresponder o objeto detetado a registos na respetiva base de dados. De acordo com as recomendações dos especialistas da Kaspersky, a análise de assinaturas está sempre ativada.

  Para aumentar a eficácia da proteção, pode utilizar a análise heurística. Durante a análise heurística, o Kaspersky Endpoint Security analisa a atividade de objetos no sistema operativo. A análise heurística pode detetar objetos maliciosos dos quais não existem atualmente registos na base de dados do Kaspersky Endpoint Security.

- Selecionar o modo de execução da tarefa de verificação.

  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.

  Pode adiar o início da tarefa de verificação após a inicialização da aplicação, caso tenha selecionado o modo de execução da tarefa de atualização **Planificadas** e a hora de inicialização do Kaspersky Endpoint Security corresponda ao agendamento de execução da tarefa de verificação. A tarefa de verificação só pode ser executada depois de decorrido o intervalo de tempo especificado após a inicialização do Kaspersky Endpoint Security.

- Configurar a tarefa de verificação para ser executada com outra conta de utilizador.

- Especificar as definições para a verificação de unidades amovíveis quando forem ligados.

Alterar o nível de segurança

Para executar tarefas de verificação, o Kaspersky Endpoint Security utiliza várias combinações de configurações. Estas combinações de definições guardadas na aplicação são designadas *níveis de segurança*. Existem três níveis de segurança predefinidos: **Elevado**, **Recomendado** e **Baixo**. As definições do nível de segurança **Recomendado** são consideradas ideais. São recomendadas pelos peritos da Kaspersky.

Para alterar um nível de segurança:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione a subsecção que contém o nome da tarefa de verificação pretendida (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).

   Na parte direita da janela, são apresentadas as configurações da tarefa de verificação selecionada.

3. Na secção **Nível de segurança**, execute uma das seguintes ações:

- Se quiser aplicar um dos níveis de segurança predefinidos (**Elevado**, **Recomendado** ou **Baixo**), selecione-o com o controlo de deslize.
- Se pretender configurar um nível de segurança personalizado, clique no botão **Configuração** e especifique as configurações na janela que aparece com o nome da tarefa de verificação.

  Depois de configurar um nível de segurança personalizado, o nome do nível de segurança de e-mail na secção **Nível de segurança** é alterado para **Configurações Personalizadas**.
- Se pretender alterar o nível de segurança para **Recomendado**, clique no botão **Predefinições**.

4. Para guardar as alterações, clique no botão **Guardar**.

Alterar a ação a executar em ficheiros infetados

Para alterar a ação a executar em ficheiros infetados:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione a subsecção que contém o nome da tarefa de verificação pretendida (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).

   Na parte direita da janela, são apresentadas as configurações da tarefa de verificação selecionada.
3. Na secção **Ação após deteção de ameaças**, selecione a opção desejada:
   - **Selecionar ação automaticamente**.
   - **Realização ação**.
4. Se selecionou a opção **Realização ação** durante o passo anterior, selecione as seguintes caixas de verificação:
   - Selecione a caixa de verificação **Desinfetar** se pretender que o Kaspersky Endpoint Security desinfete objetos nos quais as ameaças foram detetadas.

     Mesmo que esta opção esteja selecionada, o Kaspersky Endpoint Security aplica a ação **Remover** aos ficheiros que pertencem à aplicação Windows Store.
   - Selecione a caixa de verificação **Eliminar** se pretender que o Kaspersky Endpoint Security elimine objetos nos quais foram detetadas ameaças.
   - Selecione as caixas de verificação **Desinfetar** e **Eliminar** se pretender que o Kaspersky Endpoint Security tente desinfetar objetos nos quais as ameaças foram detetadas e eliminar objetos que não seja possível desinfetar.
   - Desmarque as caixas de verificação **Desinfetar** e **Eliminar** se pretender que o Kaspersky Endpoint Security não execute qualquer ação relativamente a objetos nos quais são detetadas ameaças e, em alternativa, apenas notifique o utilizador quanto aos resultados da verificação destes objetos.
5. Para guardar as alterações, clique no botão **Guardar**.

Criação de uma lista de objetos a verificar

Para gerar uma lista de objetos a verificar, pode utilizar um dos dois seguintes métodos:

- No separador **Proteção e Controlo** na janela principal da aplicação
- Na janela de definições da aplicação

> Este método está disponível apenas para as tarefas de **Verificação Completa** e de **Verificação de Áreas Críticas**. A lista de objetos a verificar para a tarefa **Verificação Personalizada** só pode ser criada no separador **Proteção e Controlo**.

Para criar uma lista de objetos a verificar no separador Proteção e Controlo da janela principal da aplicação:

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Tarefas**.

   A secção **Tarefas** é aberta.
4. Clique com o botão direito do rato para abrir o menu de contexto da linha que contém o nome da tarefa e selecione **Âmbito de verificação**.

   É aberta a janela **Âmbito de verificação**.
5. Se pretender adicionar um novo objeto ao âmbito de verificação:
   a. Clique no botão **Adicionar**.

      É apresentada a janela **Selecionar âmbito de verificação**.
   b. Selecione o objeto e clique em **Adicionar**.

      Todos os objetos que são selecionados na janela **Selecionar âmbito de verificação** são apresentados na lista **Âmbito de verificação**.
   c. Clique em **OK**.
6. Se pretender alterar o caminho para um objeto no âmbito de verificação:
   a. Selecione o objeto no âmbito de verificação.
   b. Clique no botão **Editar**.

      É apresentada a janela **Selecionar âmbito de verificação**.
   c. Introduza o novo caminho para o objeto no âmbito de verificação.
   d. Clique em **OK**.
7. Se pretender remover um novo objeto do âmbito de verificação:
   a. Selecione o objeto que pretende remover do âmbito de verificação.

Para selecionar vários objetos, selecione-os mantendo premida a tecla **CTRL**.

b. Clique no botão **Remover**.

É aberta uma janela para confirmar a eliminação.

c. Clique em **Sim** na janela para confirmar a remoção.

Não é possível remover ou editar objetos que estejam incluídos no âmbito de verificação predefinido.

8. Para excluir um objeto do âmbito de verificação, desmarque a caixa de verificação junto ao objeto na janela **Âmbito de verificação**.

O objeto permanece na lista do âmbito de verificação, mas não é verificado quando a tarefa de verificação for executada.

9. Clique em **OK**.

10. Para guardar as alterações, clique no botão **Guardar**.

Para criar uma lista de objetos a verificar a partir da janela de definições da aplicação:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione a subsecção com o nome da tarefa de verificação pretendida: **Verificação Completa** ou **Verificação de Áreas Críticas**.

Na parte direita da janela, são apresentadas as configurações da tarefa de verificação selecionada.

3. Clique no botão **Âmbito de verificação**.

É aberta a janela **Âmbito de verificação**.

4. Crie uma lista de objetos a verificar segundo os passos 5-10 das instruções anteriores.

Selecionar o tipo de ficheiros a verificar

Pode utilizar os dois seguintes métodos para selecionar o tipo de ficheiros a verificar:

- No separador **Proteção e Controlo** na janela principal da aplicação
- Na janela de definições da aplicação

Este método está disponível apenas para as tarefas de **Verificação Completa** e de **Verificação de Áreas Críticas**. O tipo de ficheiros a verificar para a tarefa de **Verificação Personalizada** só pode ser selecionado no separador **Proteção e Controlo**.

Para selecionar o tipo de ficheiros a verificar no separador Proteção e Controlo da janela principal da aplicação:

1. Abra a janela principal da aplicação.

2. Selecione o separador **Proteção e Controlo**.

3. Clique na secção **Tarefas**.

   A secção **Tarefas** é aberta.

4. Clique com o botão direito do rato para abrir o menu de contexto da linha que contém o nome da tarefa e selecione **Configuração**.

   É apresentada uma janela com o nome da tarefa de verificação selecionada.

5. Na janela com o nome da tarefa de verificação selecionada, selecione o separador **Âmbito**.

6. Na secção **Tipos de ficheiros**, especifique o tipo de ficheiros que pretende verificar durante a execução da tarefa de verificação selecionada:

   - Se pretender verificar todos os ficheiros, selecione **Todos os ficheiros**.
   - Se pretender verificar os ficheiros com os formatos mais vulneráveis a infeção, selecione **Ficheiros verificados por formato**.
   - Se pretender verificar os ficheiros com as extensões tipicamente mais vulneráveis a infeção, selecione **Ficheiros verificados por extensão**.

   Ao selecionar o tipo de ficheiros a verificar, tenha em atenção o seguinte:

   - Existem alguns formatos de ficheiro (tais como TXT) nos quais existe uma baixa probabilidade de intrusão de código malicioso e subsequente ativação. Por outro lado, existem formatos de ficheiro que contêm ou podem conter código executável (tais como .exe, .dll e .doc). O risco de intrusão e ativação de código malicioso nesses ficheiros é elevado.
   - Um intruso pode enviar um vírus ou outro programa malicioso 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 Antivírus de Ficheiros analisa o cabeçalho do ficheiro, independentemente da extensão. Se esta análise revelar que o ficheiro tem o formato EXE, a aplicação verifica-o.

7. Na janela que contém o nome de uma tarefa de verificação, clique em **OK**.

8. Para guardar as alterações, clique no botão **Guardar**.

Para selecionar o tipo de ficheiros a verificar a partir da janela de definições da aplicação:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione a subsecção com o nome da tarefa de verificação pretendida: **Verificação Completa** ou **Verificação de Áreas Críticas**.

   Na parte direita da janela, são apresentadas as configurações da tarefa de verificação selecionada.

3. Na secção **Nível de segurança**, clique no botão **Configuração**.

   É apresentada uma janela com o nome da tarefa de verificação selecionada.

4. Na janela com o nome da tarefa de verificação selecionada, selecione o separador **Âmbito**.

5. Conclua os passos 5-7 das instruções anteriores.

Otimizar a verificação de ficheiros

Para otimizar a verificação de ficheiros:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione a subsecção que contém o nome da tarefa de verificação pretendida (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).

   Na parte direita da janela, são apresentadas as configurações da tarefa de verificação selecionada.
3. Na secção **Nível de segurança**, clique no botão **Configuração**.

   É apresentada uma janela com o nome da tarefa de verificação selecionada.
4. Na janela apresentada, selecione o separador **Âmbito**.
5. Na secção **Otimização da verificação**, execute as seguintes ações:

   - Selecione a caixa de verificação **Verificar apenas os ficheiros novos e modificados**.
   - Selecione a caixa de verificação **Ignorar ficheiros verificados durante mais de** e especifique a duração da verificação de um ficheiro individual (em segundos).
6. Clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

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.

Para configurar a verificação de ficheiros compostos:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione a subsecção que contém o nome da tarefa de verificação pretendida (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).

   Na parte direita da janela, são apresentadas as configurações da tarefa de verificação selecionada.
3. Na secção **Nível de segurança**, clique no botão **Configuração**.

   É apresentada uma janela com o nome da tarefa de verificação selecionada.
4. Na janela apresentada, selecione o separador **Âmbito**.
5. Na secção **Verificação de ficheiros compostos**, especifique os ficheiros compostos que pretende verificar: arquivos, pacotes de instalação, ficheiros em formato do office, ficheiros em formato de e-mail e arquivos protegidos por password.
6. Se a caixa de verificação **Verificar apenas os ficheiros novos e modificados** estiver desmarcada na secção **Otimização da verificação**, clique na ligação **todos/novos** junto ao nome do tipo de ficheiro composto se

pretender especificar para cada tipo de ficheiro composto se deve verificar todos os ficheiros desse tipo ou apenas os ficheiros novos.

Esta ligação altera o respetivo valor quando clica na mesma.

Se a caixa de verificação **Verificar apenas os ficheiros novos e modificados** estiver selecionada, apenas são verificados os ficheiros novos.

7. Clique no botão **Adicional**.

   É aberta a janela **Ficheiros compostos**.

8. Na secção **Limite de tamanho**, execute uma das seguintes ações:

   - Se não pretender descompactar ficheiros compostos extensos, selecione a caixa de verificação **Não descompactar ficheiros compostos extensos** e especifique o valor desejado no campo **Tamanho máximo dos ficheiros**.
   - Se pretender descompactar ficheiros compostos extensos, independentemente do seu tamanho, desmarque a caixa de verificação **Não descompactar ficheiros compostos extensos**.

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

9. Clique em **OK**.
10. Na janela com o nome de uma tarefa de verificação, clique em **OK**.
11. Para guardar as alterações, clique no botão **Guardar**.

Utilizar métodos de verificação

Para utilizar métodos de verificação:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione a subsecção que contém o nome da tarefa de verificação pretendida (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).

   Na parte direita da janela, são apresentadas as configurações da tarefa de verificação selecionada.

3. Na secção **Nível de segurança**, clique no botão **Configuração**.

   É apresentada uma janela com o nome da tarefa de verificação selecionada.

4. Na janela que é aberta, selecione o separador **Adicional**.
5. Se pretender que a aplicação utilize a análise heurística ao executar a tarefa de verificação na secção **Métodos de verificação**, selecione a caixa de verificação Análise heurística. Em seguida utilize a barra indicadora para definir o nível de análise heurística: **Nível superficial**, **Nível médio** ou **Nível aprofundado**.
6. Clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

Utilizar tecnologias de verificação

Para utilizar tecnologias de verificação:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione a subsecção que contém o nome da tarefa de verificação pretendida (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).

   Na parte direita da janela, são apresentadas as configurações da tarefa de verificação selecionada.
3. Na secção **Nível de segurança**, clique no botão **Configuração**.

   É apresentada uma janela com o nome da tarefa de verificação selecionada.
4. Na janela que é aberta, selecione o separador **Adicional**.
5. Na secção **Tecnologias de verificação**, selecione as caixas de verificação junto aos nomes das tecnologias que pretende utilizar durante a verificação.
6. Clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

Selecionar o modo de execução para a tarefa de verificação

Para selecionar o modo de execução da tarefa de verificação:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione a subsecção que contém o nome da tarefa pretendida (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).

   Na parte direita da janela, são apresentadas as configurações da tarefa de verificação selecionada.
3. Clique no botão **Modo de execução**.

   Uma janela com as propriedades da tarefa selecionada é apresentada no separador **Modo de execução**.
4. Na secção **Modo de execução**, selecione o modo de execução da tarefa: **Manualmente** ou **Planificadas**.
5. Se selecionou a opção **Planificadas**, especifique as definições do agendamento. Para tal:

   a. Na lista pendente **Frequência**, selecione a frequência de execução da tarefa (**Minutos**, **Horas**, **Dias**, **Todas as semanas**, **A uma hora especificada**, **Todos os meses** ou **Após o início da aplicação**, **Executar após cada atualização**).

   b. Dependendo da frequência selecionada, configure as configurações avançadas que especificam o agendamento de execução da tarefa.

   c. Se pretender que o Kaspersky Endpoint Security inicie as tarefas de verificação ignoradas assim que for possível, selecione a caixa de verificação **Executar tarefas ignoradas**.

Se o item **Minutos**, **Horas**, **Após o início da aplicação** ou **Executar após cada atualização** for selecionado na lista pendente **Frequência**, a caixa de verificação **Executar tarefas ignoradas** fica indisponível.

a. Se pretender que o Kaspersky Endpoint Security suspenda as tarefas quando os recursos do computador são limitados, selecione a caixa de verificação **Executar apenas quando o computador está inativo**.

   Esta opção de agendamento ajuda a conservar os recursos do computador.

6. Clique em **OK**.

7. Para guardar as alterações, clique no botão **Guardar**.

Iniciar uma tarefa de verificação com a conta de outro utilizador

Por defeito, uma tarefa de verificação é executada com as autorizações da conta através da qual o utilizador iniciou sessão no sistema operativo. Contudo, poderá ser necessário executar uma tarefa de verificação com outra conta de utilizador. Pode especificar um utilizador que possua os direitos adequados nas definições da tarefa de verificação e executar a tarefa de verificação com a conta deste utilizador.

Para configurar o início de uma tarefa de verificação com outra conta de utilizador:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione a subsecção que contém o nome da tarefa pretendida (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).

   Na parte direita da janela, são apresentadas as configurações da tarefa de verificação selecionada.

3. Clique no botão **Modo de execução**.

   É apresentada janela com as propriedades da tarefa selecionada no separador **Modo de execução**.

4. No separador **Modo de execução**, na secção **Utilizador**, selecione a caixa de verificação **Executar tarefa como**.

5. No campo **Nome**, introduza o nome da conta de utilizador cujos direitos de acesso são necessários para iniciar a tarefa de verificação.

6. No campo **Password**, introduza a password do utilizador cujos direitos de acesso são necessários para iniciar a tarefa de verificação.

7. Clique em **OK**.

8. Para guardar as alterações, clique no botão **Guardar**.

Verificar unidades amovíveis quando forem ligadas ao computador

Alguns programas maliciosos exploram as vulnerabilidades do sistema operativo para se replicarem através de redes locais e unidades amovíveis. O Kaspersky Endpoint Security permite verificar a existência de vírus e outro software malicioso em unidades amovíveis quando forem ligadas ao computador.

Para configurar a verificação de unidades amovíveis quando forem ligadas:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, selecione a secção **Tarefas agendadas**.

   As definições de tarefas são apresentadas na parte direita da janela.
3. Na secção **Verificar unidades amovíveis quando forem ligados**, na lista suspensa **Ação ao ligar unidade amovível**, selecione a ação pretendida:

   - **Não verificar**
   - **Verificação detalhada**

     Neste modo, o Kaspersky Endpoint Security verifica todos os ficheiros localizados na unidade amovível, incluindo ficheiros dentro de objetos compostos.
   - **Verificação Rápida**

     Neste modo, o Kaspersky Endpoint Security verifica apenas ficheiros potencialmente infetáveis e não descompacta objetos compostos.
4. Se pretender que o Kaspersky Endpoint Security verifique apenas unidades amovíveis cujo tamanho não ultrapasse o valor especificado, selecione a caixa de verificação **Tamanho máximo da unidade amovível** e especifique um valor em megabytes no campo junto à mesma.
5. Para guardar as alterações, clique no botão **Guardar**.

Processar ficheiros não processados

Esta secção contém instruções sobre como processar ficheiros infetados e provavelmente infetados que o Kaspersky Endpoint Security não tenha processado ao verificar a existência de vírus e outras ameaças no computador.

Sobre ficheiros não processados

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 ficheiros não processados.

Um ficheiro infetado é considerado como *processado* se o Kaspersky Endpoint Security executar uma das seguintes ações nesse ficheiro, de acordo com as configurações da aplicação especificadas, ao verificar a existência de vírus e outras ameaças no computador:

- Desinfetar.
- Remover.
- Eliminar se a desinfeção falhar.

Um ficheiro infetado é considerado *não processado* se, por algum motivo, o Kaspersky Endpoint Security não executar uma ação neste ficheiro, de acordo com as configurações da aplicação especificadas, ao verificar 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).
- A ação selecionada na secção **Ação após deteção de ameaças** para tarefas de verificação é **Informar**. O utilizador deve selecionar a ação **Ignorar** quando for apresentada uma notificação sobre o ficheiro infetado.

Pode iniciar manualmente uma tarefa de Verificação Personalizada para os ficheiros na lista de ficheiros não processados, depois de atualizar bases de dados e módulos da aplicação. O estado do ficheiro pode alterar-se depois da verificação. Pode executar as ações necessárias no ficheiro, dependendo do estado.

Por exemplo, pode executar as seguintes ações:

- Eliminar ficheiros com o estado *Infetado*.
- Restaurar ficheiros infetados que contenham informações importantes e *restaurar ficheiros assinalados como Desinfetados* ou Não infetados.
- Ficheiros de Quarentena com estado *Provavelmente infetado*.

Gerir a lista de ficheiros não processados

A lista de ficheiros não processados é apresentada sob a forma de uma tabela.

Pode realizar as operações seguintes com ficheiros não processados:

- Ver a lista de ficheiros não processados.
- Verificar ficheiros não processados utilizando a versão atual das bases de dados e módulos do Kaspersky Endpoint Security.
- Restaurar ficheiros da lista de ficheiros não processados para as respetivas pastas originais ou para outra pasta, selecionada por si (quando não for possível escrever na pasta original).
- Remover ficheiros da lista de ficheiros não processados.
- Abra a pasta em que o ficheiro não processado estava originalmente localizado.

Pode também executar as seguintes ações ao gerir dados na tabela:

- Filtrar os eventos de ficheiros não processados pelo valor da coluna ou por condições de filtro personalizadas.
- Utilizar a função de procura de eventos de ficheiros não processados.
- Ordenar os eventos de ficheiros não processados.
- Alterar a ordem e definir as colunas apresentadas na lista de ficheiros não processados.
- Agrupar eventos de ficheiros não processados.

Pode copiar eventos de ficheiros não processados selecionados para a área de transferência, se necessário.

Iniciar uma tarefa de Verificação Personalizada para ficheiros não processados

Pode iniciar manualmente uma tarefa de Verificação Personalizada para ficheiros não processados. Pode iniciar a verificação se, por exemplo, a última verificação foi interrompida por alguma razão ou se pretende voltar a verificar os ficheiros não processados depois da última atualização de bases de dados e módulos de aplicação.

Para iniciar uma Verificação Personalizada de ficheiros não processados:

1. Abra a janela principal da aplicação.
2. Na parte superior da janela principal da aplicação, clique na ligação **Quarentena** para abrir a janela **Armazenamento**.
3. Na janela **Armazenamento**, selecione o separador **Ficheiros não processados**.
4. Na tabela do separador **Ficheiros não processados**, selecione um ou vários eventos associados a ficheiros que pretenda verificar.

   Para selecionar vários eventos, selecione-os mantendo premida a tecla **CTRL**.
5. Pode iniciar a tarefa de Verificação Personalizada através de uma das seguintes duas formas:
   - Clique no botão **Verificar novamente**.
   - Clique com o botão direito do rato para visualizar o menu de contexto e selecione **Verificar novamente**.

Apagar ficheiros da lista de ficheiros não processados

Para apagar ficheiros da lista de ficheiros não processados:

1. Abra a janela principal da aplicação.
2. Na parte superior da janela principal da aplicação, clique na ligação **Quarentena** para abrir a janela **Armazenamento**.
3. Na janela **Armazenamento**, selecione o separador **Ficheiros não processados**.
4. Na tabela do separador **Ficheiros não processados**, selecione um ou vários eventos associados a ficheiros que pretenda eliminar.

   Para selecionar vários eventos, selecione-os mantendo premida a tecla **CTRL**.
5. Para apagar os ficheiros, execute uma das seguintes ações:
   - Clique no botão **Remover**.
   - Clique com o botão direito do rato para visualizar o menu de contexto e selecione **Eliminar**.

Verificação de Vulnerabilidade

Esta secção contém informações sobre as especificidades e as definições da tarefa Verificação de Vulnerabilidade, bem como instruções para gerir a lista de vulnerabilidades detetadas pelo Kaspersky Endpoint Security ao executar a tarefa Verificação de Vulnerabilidade.

Ver informações sobre vulnerabilidades das aplicações em execução

A informação relativa a vulnerabilidades de execução de aplicações está disponível se o Kaspersky Endpoint Security estiver instalado num computador que tenha o Microsoft Windows para estações de trabalho em execução. Esta informação não está disponível se o Kaspersky Endpoint Security estiver instalado num computador que utiliza o Microsoft Windows para servidores de ficheiros.

Para ver informações sobre vulnerabilidades das aplicações em execução:

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Abra a secção **Controlo de terminal**.
4. Clique no botão **Monitor de Atividade das Aplicações**.

A janela **Controlo de Privilégios das Aplicações** é aberta no separador **Monitor de Atividade das Aplicações**. A tabela **Monitor de Atividade das Aplicações** apresenta informação resumida sobre a atividade das aplicações que estão em execução no sistema operativo. A gravidade da vulnerabilidade das aplicações em execução conforme determinado pelo componente Monitor de Vulnerabilidades é apresentada na coluna **Gravidade da vulnerabilidade**.

Sobre a tarefa Verificação de Vulnerabilidade

As vulnerabilidades no sistema operativo podem ser causadas, por exemplo, por erros de programação ou engenharia, passwords falíveis e atividades de software malicioso. Ao verificar a existência de vulnerabilidades, a aplicação analisa o sistema operativo e procura anomalias e danos nas configurações das aplicações da Microsoft e de outros fornecedores.

Uma Verificação de Vulnerabilidade executa diagnósticos de segurança do sistema operativo e deteta características de software que podem ser usadas por intrusos para espalhar objetos maliciosos e obter acesso às informações pessoais.

Após o início da tarefa de verificação de vulnerabilidade, o seu progresso é apresentado no campo junto do nome da tarefa **Verificação de vulnerabilidade** na secção **Tarefas**, no separador **Proteção e Controlo** da janela principal do Kaspersky Endpoint Security.

Os resultados da tarefa Verificação de Vulnerabilidade são registados nos relatórios.

Iniciar ou parar a tarefa Verificação de Vulnerabilidade

Independentemente do modo de execução selecionado para a tarefa Verificação de Vulnerabilidade, pode iniciar ou parar a mesma em qualquer altura.

Para iniciar ou parar a tarefa Verificação de vulnerabilidade:

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Clique na secção **Tarefas**.

   A secção **Tarefas** é aberta.
4. Clique com o botão direito do rato para aceder ao menu de contexto da linha com o nome da tarefa Verificação de Vulnerabilidade.

   É apresentado um menu das operações da tarefa Verificação de Vulnerabilidade.
5. Execute uma das seguintes ações:

   - Para iniciar a tarefa Verificação de Vulnerabilidade, selecione **Iniciar verificação** do menu.

     O estado do progresso da tarefa apresentado à direita do botão com o nome da tarefa Verificação de Vulnerabilidade é alterado para *Em execução*.

   - Para parar a tarefa Verificação de Vulnerabilidade, selecione **Parar verificação** do menu.

     O estado do progresso da tarefa apresentado à direita do botão com o nome da tarefa Verificação de Vulnerabilidade é alterado para *Parado*.

Configuração das definições da Verificação de Vulnerabilidades

Para configurar as definições da Verificação de Vulnerabilidades, pode executar as seguintes ações:

- Crie o âmbito da Verificação de Vulnerabilidades.

  Pode expandir ou reduzir o âmbito de verificação adicionando ou removendo aplicações a verificar quanto a vulnerabilidades.

- Selecione o modo de execução para a tarefa de Verificação de Vulnerabilidade.

  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 possível.

- Configurar a tarefa para execução com os direitos de uma conta de utilizador diferente.

  Por defeito, uma tarefa de verificação é executada com as autorizações da conta através da qual o utilizador iniciou sessão no sistema operativo. Contudo, poderá ser necessário executar uma tarefa de verificação com outra conta de utilizador. Pode especificar um utilizador que possua os direitos adequados nas definições da tarefa e executar a tarefa com a conta deste utilizador.

Criar o Âmbito de verificação de vulnerabilidades

Um âmbito de verificação de vulnerabilidade consiste num fornecedor de software e num caminho para a pasta na qual o software foi instalado (por exemplo, todas as aplicações da Microsoft instaladas na pasta Programas).

Para criar um âmbito de verificação de vulnerabilidade:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione **Verificação de Vulnerabilidade**.

   Na parte direita da janela, são apresentadas as definições da tarefa Verificação de Vulnerabilidade.
3. Na secção **Âmbito de verificação**:

   a. Para utilizar o Kaspersky Endpoint Security para procurar vulnerabilidades em aplicações da Microsoft instaladas no computador, selecione a caixa de verificação **Microsoft**.

   b. Para utilizar o Kaspersky Endpoint Security para procurar vulnerabilidades em todas as aplicações instaladas no computador, que não as da Microsoft, selecione a caixa de verificação **Outros fornecedores**.

   c. Na janela **Área adicional de verificação de vulnerabilidades**, clique em **OK**.

   É aberta a janela **Âmbito de verificação de vulnerabilidades**.

   d. Crie o âmbito de verificação de vulnerabilidades. Para tal, utilize os botões **Adicionar** e **Remover**.

   e. Na janela **Âmbito de verificação de vulnerabilidades**, clique em **OK**.
4. Para guardar as alterações, clique no botão **Guardar**.

Selecionar o modo de execução para a tarefa de Verificação de Vulnerabilidades

Para selecionar o modo de execução da tarefa Verificação de Vulnerabilidade:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione **Verificação de Vulnerabilidade**.

   Na parte direita da janela, são apresentadas as definições da tarefa Verificação de Vulnerabilidade.
3. Clique no botão **Modo de execução**.

   Esta ação abre o separador **Modo de execução** da janela **Verificação de Vulnerabilidade**.
4. Na secção **Modo de execução**, selecione uma das seguintes opções de execução para iniciar a tarefa Verificação de vulnerabilidade:

   - Se pretender iniciar a tarefa Verificação de Vulnerabilidade manualmente, selecione **Manualmente**.
   - Se pretender configurar um agendamento de execução para a tarefa Verificação de Vulnerabilidade, selecione **Planificadas**.
5. Execute uma das seguintes ações:

   - Se selecionou a opção **Manualmente**, avance para o passo 6 destas instruções.
   - Se selecionou a opção **Planificadas**, especifique as definições do agendamento de execução da tarefa Verificação de Vulnerabilidade. Para tal:

a. Na lista suspensa **Frequência**, especifique quando iniciar a tarefa Verificação de Vulnerabilidade. Selecione uma das seguintes opções: **Dias**, **Todas as semanas**, **A uma hora especificada**, **Todos os meses**, **Após o início da aplicação** ou **Executar após cada atualização**.

b. Dependendo do item selecionado na lista suspensa **Frequência**, especifique valores para as configurações que definem a hora de início da tarefa Verificação de Vulnerabilidade.

c. Se pretender que o Kaspersky Endpoint Security inicie as tarefas de Verificação de Vulnerabilidade ignoradas assim que for possível, selecione a caixa de verificação **Executar tarefas ignoradas**

> Se a opção **Após o início da aplicação** ou **Executar após cada atualização** estiver selecionada na lista suspensa **Frequência**, a caixa de verificação **Executar tarefas ignoradas** não estará disponível.

6. Clique em **OK**.

7. Para guardar as alterações, clique no botão **Guardar**.

Iniciar a tarefa de Verificação de Vulnerabilidades utilizando os direitos de uma conta de utilizador diferente

Por defeito, a tarefa Verificação de Vulnerabilidade é iniciada com a conta com a qual o utilizador iniciou sessão no sistema operativo. Contudo, poderá ser necessário iniciar a tarefa Verificação de Vulnerabilidade com outra conta de utilizador. Pode especificar um utilizador com estes direitos nas definições da tarefa Verificação de vulnerabilidade e iniciar a tarefa Verificação de vulnerabilidade com esta conta de utilizador.

Para configurar o início da tarefa Verificação de Vulnerabilidade com outra conta de utilizador:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione **Verificação de Vulnerabilidade**.

   Na parte direita da janela, são apresentadas as definições da tarefa Verificação de Vulnerabilidade.

3. Clique no botão **Modo de execução**.

   Esta ação abre o separador **Modo de execução** da janela **Verificação de Vulnerabilidade**.

4. No separador **Modo de execução**, na secção **Utilizador**, selecione a caixa de verificação **Executar tarefa como**.

5. No campo **Nome**, introduza o nome da conta do utilizador cujos direitos são necessários para iniciar a tarefa Verificação de vulnerabilidade.

6. No campo **Password**, introduza a password do utilizador cujos direitos são necessários para iniciar a tarefa Verificação de vulnerabilidade.

7. Clique em **OK**.

8. Para guardar as alterações, clique no botão **Guardar**.

Gerir a lista de vulnerabilidades

Ao gerir a lista de vulnerabilidades, pode executar as seguintes ações:

- Ver a lista de vulnerabilidades.
- Reiniciar a tarefa Verificação de Vulnerabilidade depois de atualizar as bases de dados e módulos da aplicação.
- Ver informações detalhadas sobre a vulnerabilidade e recomendações sobre como reparar a mesma, numa secção em separado.
- Ocultar entradas selecionadas na lista de vulnerabilidades.
- Filtrar a lista de vulnerabilidades por nível de importância.
- Filtrar a lista de vulnerabilidades pelos valores dos estados *Corrigidos* e *Oculto*.

Pode também executar as seguintes ações ao gerir dados na tabela:

- Filtrar a lista de vulnerabilidades pelos valores da coluna ou por condições de filtragem personalizadas.
- Utilizar a função de procura de vulnerabilidades.
- Ordenar entradas na lista de vulnerabilidades.
- Alterar a ordem e disposição das colunas apresentadas na lista de vulnerabilidades.
- Agrupar entradas na lista de vulnerabilidades.

Sobre a lista de vulnerabilidades

O Kaspersky Endpoint Security regista os resultados da tarefa Verificação de Vulnerabilidade na lista de vulnerabilidades.

Depois de o utilizador rever as vulnerabilidades específicas e executar as ações recomendadas para as corrigir, o Kaspersky Endpoint Security altera o estado das vulnerabilidades para *Corrigidos*.

Se o utilizador não pretender apresentar entradas sobre vulnerabilidades específicas na lista de vulnerabilidades, poderá optar por ocultá-las. O Kaspersky Endpoint Security atribui o estado *Oculto* a tais vulnerabilidades.

A lista de vulnerabilidades é apresentada sob a forma de uma tabela. Cada linha da tabela contém as seguintes informações:

- Um ícone que significa o nível de gravidade da vulnerabilidade. Os níveis de importância de vulnerabilidades são os seguintes:
  - Ícone . **Crítica**. Este nível de gravidade aplica-se a vulnerabilidades altamente perigosas, que têm de ser corrigidas de imediato. Os intrusos exploram ativamente vulnerabilidades deste nível para infetar o sistema operativo do computador ou aceder aos dados pessoais do utilizador. A Kaspersky recomenda que prontamente tome todas as medidas necessárias para reparar quaisquer vulnerabilidades do nível de gravidade "Crítico".
  - Ícone . **Importante**. Este nível de gravidade aplica-se a vulnerabilidades importantes, que é necessário corrigir logo que possível. Os intrusos podem explorar ativamente as vulnerabilidades deste nível. Atualmente, os intrusos não exploram ativamente vulnerabilidades do nível de gravidade "Importante". A

Kaspersky recomenda que prontamente tome todas as medidas necessárias para reparar quaisquer vulnerabilidades do nível de gravidade "Importante".

- Ícone . **Aviso**. Este nível de gravidade aplica-se a vulnerabilidades cuja correção pode ser adiada. Contudo, tais vulnerabilidades podem ameaçar a segurança do computador no futuro.

- ID de vulnerabilidade.
- Nome da aplicação na qual a vulnerabilidade foi detetada.
- Breve descrição da vulnerabilidade.
- Informações sobre o publicador do software, conforme indicado na assinatura digital.
- Resultado de ações empreendidas para corrigir a vulnerabilidade.

Reiniciar a tarefa Verificação de Vulnerabilidade

Para atualizar as informações sobre vulnerabilidades anteriormente detetadas, pode reiniciar a tarefa Verificação de Vulnerabilidade. Pode ser necessário reiniciar a tarefa de verificação se a verificação de vulnerabilidade for, por algum motivo, interrompida ou se pretender verificar a existência de vulnerabilidades no computador após a última atualização de bases de dados e módulos da aplicação.

Para reiniciar a tarefa Verificação de Vulnerabilidade:

1. Abra a janela principal da aplicação.
2. Na parte superior da janela principal da aplicação, clique na ligação **Quarentena** para abrir a janela **Armazenamento**.
3. Na janela **Armazenamento**, selecione o separador **Vulnerabilidades**.

   O separador **Vulnerabilidades** contém uma lista das vulnerabilidades que o Kaspersky Endpoint Security detetou durante a tarefa Verificação de Vulnerabilidade.
4. No canto inferior direito da janela **Armazenamento**, clique no botão **Verificar novamente**.

O Kaspersky Endpoint Security atualiza a informação detalhada sobre as vulnerabilidades na lista de vulnerabilidades.

O estado de uma vulnerabilidade corrigida pela instalação da correção proposta não altera outra verificação de vulnerabilidade.

Corrigir uma vulnerabilidade

Pode corrigir uma vulnerabilidade instalando uma atualização de sistema operativo, alterando a configuração da aplicação ou instalando uma correção de aplicação.

As vulnerabilidades detetadas podem aplicar-se não às aplicações instaladas mas a cópias das mesmas. Uma correção pode corrigir uma vulnerabilidade apenas se a aplicação estiver instalada.

Para corrigir uma vulnerabilidade:

1. Abra a janela principal da aplicação.
2. Na parte superior da janela principal da aplicação, clique na ligação **Quarentena** para abrir a janela **Armazenamento**.
3. Na janela **Armazenamento**, selecione o separador **Vulnerabilidades**.

   O separador **Vulnerabilidades** contém uma lista das vulnerabilidades que o Kaspersky Endpoint Security detetou durante a tarefa Verificação de Vulnerabilidade.
4. Na lista de vulnerabilidades, selecione a entrada que corresponde à vulnerabilidade em questão.

   Uma secção com informações sobre esta vulnerabilidade e recomendações sobre como repará-la abre-se no fundo da lista de vulnerabilidades.

   As informações que se seguem estão disponíveis para cada vulnerabilidade selecionada:

   - Nome da aplicação na qual a vulnerabilidade foi detetada.
   - Versão da aplicação na qual a vulnerabilidade foi detetada.
   - Nível de gravidade de uma vulnerabilidade.
   - ID de vulnerabilidade.
   - Data e hora da última deteção de vulnerabilidades.
   - Recomendações para corrigir a vulnerabilidade (por exemplo, uma ligação para um site com uma atualização de sistema operativo ou uma correção de aplicação).
   - Ligação para um site com uma descrição da vulnerabilidade.
5. Para ver uma descrição detalhada da vulnerabilidade, clique na ligação **Informação adicional** para abrir uma página de Internet que contém uma descrição da ameaça associada à vulnerabilidade selecionada. O site www.secunia.com permite-lhe transferir a atualização necessária para a versão atual da aplicação e instalá-la.
6. Para corrigir uma vulnerabilidade, selecione um dos seguintes métodos:

   - Se uma ou mais correções estiverem disponíveis para a aplicação, instale a correção necessária seguindo as instruções fornecidas junto do nome da correção.
   - Se estiver disponível uma atualização de sistema operativo, instale a atualização necessária seguindo as instruções fornecidas junto do nome da atualização.

   A vulnerabilidade é corrigida depois de instalar a correção ou atualização. O Kaspersky Endpoint Security atribui a esta vulnerabilidade um estado que significa que a vulnerabilidade foi corrigida. A entrada sobre a vulnerabilidade corrigida é apresentada a cinzento na lista de vulnerabilidades.
7. Se não forem fornecidas quaisquer informações sobre como corrigir uma vulnerabilidade na parte inferior da janela, experimente reiniciar a tarefa Verificação de Vulnerabilidade depois de atualizar as bases de dados e módulos do Kaspersky Endpoint Security. Uma vez que o Kaspersky Endpoint Security verifica a existência de

vulnerabilidades no sistema a partir de uma base de dados de vulnerabilidades, uma entrada sobre uma vulnerabilidade corrigida poderá ser apresentada após a atualização da aplicação.

Ocultar entradas da lista de vulnerabilidades

Pode ocultar uma entrada de vulnerabilidade selecionada. O Kaspersky Endpoint Security atribui o estado *Oculto* às entradas selecionadas na lista de vulnerabilidades e marcadas como ocultas. Em seguida, pode filtrar a lista de vulnerabilidades pelo valor do estado *Oculto*.

Para ocultar uma entrada na lista de vulnerabilidades:

1. Abra a janela principal da aplicação.
2. Na parte superior da janela principal da aplicação, clique na ligação **Quarentena** para abrir a janela **Armazenamento**.
3. Na janela **Armazenamento**, selecione o separador **Vulnerabilidades**.

   O separador **Vulnerabilidades** contém uma lista das vulnerabilidades que o Kaspersky Endpoint Security detetou durante a tarefa Verificação de Vulnerabilidade.
4. Na lista de vulnerabilidades, selecione a entrada sobre a vulnerabilidade que quer ocultar.

   Uma secção com informações sobre esta vulnerabilidade e recomendações sobre como repará-la abre-se no fundo da lista de vulnerabilidades.
5. Clique no botão **Ocultar**.

   O Kaspersky Endpoint Security atribui o estado *Oculto* à vulnerabilidade selecionada. As entradas sobre vulnerabilidades com o estado *Oculto* são movidas para o fim da lista de vulnerabilidades e desativadas.
6. Para ocultar uma entrada referente a uma vulnerabilidade na lista de vulnerabilidades, selecione a caixa de verificação **Oculto** no cimo da lista.

Filtrar a lista de vulnerabilidades por nível de gravidade

Para filtrar a lista de vulnerabilidades por nível de gravidade:

1. Abra a janela principal da aplicação.
2. Na parte superior da janela principal da aplicação, clique na ligação **Quarentena** para abrir a janela **Armazenamento**.
3. Na janela **Armazenamento**, selecione o separador **Vulnerabilidades**.

   O separador **Vulnerabilidades** contém uma lista das vulnerabilidades que o Kaspersky Endpoint Security detetou durante a tarefa Verificação de Vulnerabilidade. Três ícones do nível de gravidade de vulnerabilidade (Aviso, Importante, Crítico) aparecem na parte superior da lista de vulnerabilidades, na linha **Mostrar gravidade**. Ao clicar nestes ícones, pode filtrar a lista de vulnerabilidades pelo nível de gravidade.
4. Clique em um, dois, ou três ícones do nível de gravidade da vulnerabilidade. As vulnerabilidades que correspondem aos níveis de gravidade selecionados são apresentadas na lista. Para deixar de mostrar as vulnerabilidades que correspondem a um nível de gravidade específico na lista, clique novamente no ícone do

nível de gravidade relevante. Se nenhum nível de gravidade foi selecionado, isso significa que a lista de vulnerabilidades está vazia.

As condições de filtragem da entrada de vulnerabilidade especificada são guardadas depois de fechar a janela **Armazenamento**.

Filtrar a lista de vulnerabilidades pelos valores dos estados Corrigidos e Oculto

Para filtrar a lista de vulnerabilidades pelos valores dos estados Corrigidos e Oculto:

1. Abra a janela principal da aplicação.
2. Na parte superior da janela principal da aplicação, clique na ligação **Quarentena** para abrir a janela **Armazenamento**.
3. Na janela **Armazenamento**, selecione o separador **Vulnerabilidades**.

   O separador **Vulnerabilidades** contém uma lista das vulnerabilidades que o Kaspersky Endpoint Security detetou durante a tarefa Verificação de Vulnerabilidade.
4. As caixas de verificação que representam o estado das vulnerabilidades são apresentadas junto da definição **Mostrar vulnerabilidades**. Para filtrar a lista de vulnerabilidades pelo estado *Corrigidos*, execute uma das seguintes ações:

   - Para apresentar entradas sobre vulnerabilidades corrigidas na lista de vulnerabilidades, selecione a caixa de verificação **Corrigidos**. As entradas de vulnerabilidades corrigidas são apresentadas a cinzento na lista de vulnerabilidades.
   - Para ocultar entradas sobre vulnerabilidades corrigidas na lista de vulnerabilidades, desmarque a caixa de verificação **Corrigidos**.
5. Para filtrar a lista de vulnerabilidades pelo estado *Oculto*, execute uma das seguintes ações:

   - Para apresentar entradas sobre vulnerabilidades ocultas na lista de vulnerabilidades, selecione a caixa de verificação **Oculto**. As entradas de vulnerabilidades ocultas são apresentadas a cinzento na lista de vulnerabilidades.
   - Para ocultar entradas sobre vulnerabilidades ocultas na lista de vulnerabilidades, desmarque a caixa de verificação **Oculto**.

As condições de filtragem da entrada de vulnerabilidade especificada não são guardadas depois de fechar a janela **Armazenamento**.

Verificar a integridade dos módulos da aplicação

Esta secção contém informações sobre as especificidades e as definições da tarefa verificação de integridade.

Sobre a tarefa de 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.

Após o início da tarefa de verificação de integridade, o seu progresso é apresentado no campo junto do nome da tarefa na secção **Tarefas**, no separador **Proteção e Controlo** da janela principal do Kaspersky Endpoint Security.

Os resultados da tarefa de verificação de integridade são registados nos relatórios.

Iniciar ou parar uma tarefa de verificação de integridade

Independentemente do modo de execução selecionado, pode iniciar ou parar uma tarefa de verificação de integridade em qualquer altura.

Para iniciar ou parar uma tarefa de verificação de integridade:

1. Abra a janela principal da aplicação.
2. Selecione o separador **Proteção e Controlo**.
3. Abra a secção **Tarefas**.
4. Clique com o botão direito do rato para visualizar o menu de contexto da linha que inclui o nome da tarefa de verificação de integridade.
5. Execute uma das seguintes ações:
   - Para iniciar a tarefa de verificação de integridade, selecione **Iniciar verificação** no menu de contexto.

     O estado do progresso da tarefa apresentado à direita do botão com o nome desta tarefa é alterado para *Em execução*.
   - Se pretender parar a tarefa de verificação de integridade, selecione **Parar verificação** no menu de contexto.

     O estado do progresso da tarefa apresentado à direita do botão com o nome desta tarefa é alterado para *Parado*.

Selecionar o modo de execução da tarefa de verificação de integridade

Para selecionar o modo de execução da tarefa de verificação de integridade:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Tarefas agendadas**, selecione **Verificação de integridade**.

   Na parte direita da janela, são apresentadas as definições da tarefa de verificação de integridade.

3. Na secção **Modo de execução**, selecione uma das seguintes opções:

   - Se pretender iniciar manualmente a tarefa de verificação de integridade, selecione **Manualmente**.
   - Se pretender configurar um agendamento de execução para a tarefa de verificação de integridade, selecione **Planificadas**.

4. Se selecionou a opção **Planificadas** durante o passo anterior, especifique as definições do agendamento de execução da tarefa. Para tal:

   a. Na lista pendente **Frequência**, especifique quando a tarefa de verificação de integridade deve ser iniciada. Selecione uma das seguintes opções: **Minutos**, **Horas**, **Dias**, **Todas as semanas**, **A uma hora especificada**, **Todos os meses** ou **Após o início da aplicação**.

   b. Dependendo da opção selecionada na lista pendente **Frequência**, especifique o valor para as definições que definem a hora de início da tarefa.

   c. Se pretender que o Kaspersky Endpoint Security inicie as tarefas de verificação de integridade ignoradas assim que for possível, selecione a caixa de verificação **Executar tarefas ignoradas**.

   > Se o item **Após o início da aplicação**, **Minutos** ou **Horas** estiver selecionado na lista pendente **Frequência**, a caixa de verificação **Executar tarefas ignoradas** não está disponível.

   d. Se pretender que o Kaspersky Endpoint Security suspenda as tarefas quando os recursos do computador são limitados, selecione a caixa de verificação **Executar apenas quando o computador está inativo**.

   Esta opção de agendamento ajuda a conservar os recursos do computador.

5. Clique em **OK**.

6. Para guardar as alterações, clique no botão **Guardar**.

Gerir relatórios

Esta secção descreve como configurar as definições de relatório e gerir relatórios.

Princípios da gestão de relatórios

Nos relatórios são registadas informações sobre o funcionamento de cada componente do Kaspersky Endpoint Security, do desempenho de cada tarefa de verificação, tarefa de atualização, tarefa de controlo de integridade e tarefa de verificação de vulnerabilidades, bem como sobre o funcionamento geral da aplicação registado nos relatórios.

Os dados do relatório são apresentados sob a forma de uma tabela que contém uma lista de eventos. Cada 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, tem de premir o botão ⊞ junto ao nome do gráfico. Os eventos registados durante o funcionamento de vários componentes ou 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.
- Relatório **Todos os componentes de proteção**. Contém informações sobre eventos registados durante o funcionamento dos seguintes componentes do Kaspersky Endpoint Security:
  - Antivírus de Ficheiros
  - Antivírus de E-mail.
  - Antivírus de Internet.
  - Antivírus de MI.
  - Monitorização do Sistema.
  - Firewall.
  - Bloqueio de Ataques de Rede.
  - Prevenção de ataques BadUSB.
- Relatório sobre o funcionamento de um componente ou sobre a execução de uma tarefa do Kaspersky Endpoint Security.
- Relatório **Encriptação**. 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:

- **Eventos Informativos**. Ícone. Eventos formais que normalmente não contêm informações importantes.

- **Eventos Importantes**. Ícone. Eventos que necessitam da sua atenção, dado que refletem situações importantes no funcionamento do Kaspersky Endpoint Security.
- **Eventos Críticos**. Ícone. 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.
- 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. Neste caso, o Kaspersky Endpoint Security elimina todas as entradas dos relatórios selecionados, desde a entrada mais antiga até à data atual.

Configurar as definições de relatórios

Pode configurar as definições de relatórios das seguintes formas:

- 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. Pode cancelar a restrição de tempo ou alterar a duração máxima do armazenamento de relatórios.

- Configurar o tamanho máximo do ficheiro de relatório.

  Pode especificar o tamanho máximo do ficheiro que contém o relatório. Por defeito, 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. Pode cancelar a restrição de tamanho do ficheiro de relatório ou definir um valor diferente.

Configurar o prazo máximo de armazenamento de relatórios

Para modificar o prazo máximo do armazenamento de relatórios:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Configurações avançadas**, selecione **Relatórios e Armazenamento**.

3. Na parte direita da janela, na secção **Parâmetros do relatório**, execute um dos passos seguintes:

   - Para limitar o prazo de armazenamento de relatórios, selecione a caixa de verificação **Guardar relatórios até**. No campo junto à caixa de verificação **Guardar relatórios até**, especifique o prazo máximo do armazenamento de relatórios.

     O prazo máximo predefinido do armazenamento para relatórios é de 30 dias.

   - Para cancelar o limite do prazo de armazenamento de relatórios, desmarque o botão **Guardar relatórios até**.

   O limite do prazo de armazenamento de relatórios está ativado por defeito.

4. Para guardar as alterações, clique no botão **Guardar**.

Configurar o tamanho máximo do ficheiro de relatório

Para configurar o tamanho máximo do ficheiro de relatórios:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Configurações avançadas**, selecione **Relatórios e Armazenamento**.

3. Na parte à direita da secção **Parâmetros do relatório**, execute uma das ações seguintes:

   - Para limitar o tamanho do ficheiro de relatórios, selecione a caixa de verificação **Tamanho máximo dos ficheiros**. No campo à direita da caixa de verificação **Tamanho máximo dos ficheiros**, especifique o tamanho máximo do ficheiro de relatório.

     Por defeito, o tamanho do ficheiro de relatório é de 1024 MB.

   - Para remover a restrição do tamanho do ficheiro de relatórios, desmarque a caixa de verificação **Tamanho máximo dos ficheiros**.

   O limite do tamanho do ficheiro de relatório está ativo por defeito.

4. Para guardar as alterações, clique no botão **Guardar**.

Visualização de relatórios

Para visualizar os relatórios:

1. Abra a janela principal da aplicação.

2. Na parte superior da janela principal da aplicação, clique na ligação **Relatórios** para abrir a janela **Relatórios**.

3. Para gerar o relatório Todos os componentes de proteção, na secção esquerda da janela **Relatórios**, selecione o item **Todos os componentes de proteção** na lista de componentes e tarefas.

   O relatório Todos os componentes de proteção é apresentado à direita da janela, que contém uma lista de eventos no funcionamento de todos os componentes de proteção do Kaspersky Endpoint Security.

4. Para gerar um relatório sobre o funcionamento de um componente ou tarefa, na lista de componentes e tarefas, na parte esquerda da janela **Relatórios**, selecione um componente ou 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.

Por defeito, os eventos de relatório são ordenados pela ordem ascendente dos valores da coluna **Data do evento**.

Ver informações de evento num relatório

Pode ver um resumo detalhado de cada evento no relatório.

Para visualizar um resumo detalhado de um evento no relatório:

1. Abra a janela principal da aplicação.
2. Na parte superior da janela principal da aplicação, clique na ligação **Relatórios** para abrir a janela **Relatórios**.
3. Na parte esquerda da janela, selecione o relatório relevante sobre o componente ou tarefa.

   Os eventos incluídos no âmbito de relatório são apresentados na tabela, na parte direita da janela. Para encontrar eventos específicos no relatório, use as funções de filtro, procura e ordenação.
4. Selecione o evento relevante no relatório.

É apresentada uma secção com o resumo de evento na parte de baixo da janela.

Guardar um relatório em ficheiro

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. Abra a janela principal da aplicação.
2. Na parte superior da janela principal da aplicação, clique na ligação **Relatórios** para abrir a janela **Relatórios**.
3. Execute uma das seguintes ações:

   - Para gerar o relatório "Todos os componentes de proteção", selecione **Todos os componentes de proteção** na lista de componentes e tarefas.

     O relatório "Todos os componentes de proteção" é apresentado na parte direita da janela, contendo uma lista de eventos no funcionamento de todos os componentes de proteção.

   - Para criar um relatório do funcionamento de uma tarefa ou componente específico, selecione este componente ou tarefa na lista de componentes e tarefas.

     É apresentado um relatório na parte direita da janela, que contém uma lista dos eventos do funcionamento da tarefa ou componente selecionado.
4. Se necessário, pode modificar a apresentação dos dados no relatório:

- Filtro de eventos
- Procura de eventos
- Reordenação de colunas
- Ordenação de eventos

5. Clique no botão **Guardar relatório** na parte superior direita da janela.
   É apresentado um menu de contexto.
6. No menu de contexto, selecione a codificação para guardar o ficheiro do relatório: **Guardar como ANSI** ou **Guardar como Unicode**.
   É aberta a janela padrão **Guardar como** do Microsoft Windows.
7. Na janela **Guardar como**, especifique a pasta de destino do ficheiro de relatório.
8. No campo **Nome do ficheiro**, introduza o nome do ficheiro de relatório.
9. No campo **Tipo de ficheiro**, selecione o formato do relatório pretendido: TXT ou CSV.
10. Clique no botão **Guardar**.

Limpar relatórios

Para remover informações dos relatórios:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Configurações avançadas**, selecione **Relatórios e Armazenamento**.
3. Na parte direita da janela, na secção **Parâmetros do relatório**, clique no botão **Eliminar relatórios**.
   É aberta a janela **Limpar relatórios**.
4. Selecione as caixas de verificação junto aos relatórios nos quais pretende apagar as informações:
   - **Todos os relatórios**.
   - **Relatório de proteção geral**. Contém informações sobre o funcionamento dos seguintes componentes do Kaspersky Endpoint Security:
     - Antivírus de Ficheiros
     - Antivírus de E-mail.
     - Antivírus de Internet.
     - Antivírus de MI.
     - Monitorização do Sistema.
     - Firewall.

- Bloqueio de Ataques de Rede.
- Prevenção de ataques BadUSB.

- **Relatório de tarefas de verificação**. Contém informações sobre as tarefas de verificação concluídas:
  - Verificação Completa
  - Verificação de Áreas Críticas
  - Verificação Personalizada
  - Verificação de integridade.
- **Relatório de tarefa de atualização**. Contém informações sobre as tarefas de atualização concluídas:
- **Relatório da Firewall**. Contém informações sobre o funcionamento da Firewall.
- **Relatório de componentes de controlo**. Contém informações sobre o funcionamento dos seguintes componentes do Kaspersky Endpoint Security:
  - Controlo de Arranque das Aplicações.
  - Controlo de Privilégios das Aplicações.
  - Monitor de Vulnerabilidades.
  - Controlo de dispositivos.
  - Controlo de Internet.
- **Relatório de encriptação de dados**.

5. Clique em **OK**.

Serviço de notificação

Esta secção contém informações sobre o serviço de notificações que alerta o utilizador de eventos no funcionamento do Kaspersky Endpoint Security e contém ainda instruções sobre como configurar parâmetros de notificação.

Sobre as notificações do Kaspersky Endpoint Security

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 módulo 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.

Configurar o serviço de notificação

Pode executar as seguintes ações de modo a configurar o serviço de notificação:

- Configurar as definições dos registos de eventos em que o Kaspersky Endpoint Security regista os eventos.
- Configure a forma como as notificações no ecrã são apresentadas.
- Configurar o envio de notificações de e-mail.

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. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Configurações avançadas**, selecione **Relatórios e Armazenamento**.

   A parte direita da janela apresenta as definições de relatórios e armazenamento.
3. Na secção **Notificações**, clique no botão **Configuração**.

   Esta ação abre a janela **Notificações**.

   Os componentes e as tarefas do Kaspersky Endpoint Security são apresentados na parte esquerda da janela. Na parte direita da janela são apresentados os eventos gerados para a tarefa ou componente selecionado.
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 registo local** e **Guardar no Registo de Eventos do Windows**.

   Os eventos cujas caixas de verificação estão selecionadas na coluna **Guardar no registo local** são apresentados em **Registos de aplicações e serviços** na secção **Registo de Eventos Kaspersky**. Os eventos cujas caixas de verificação estão selecionadas na coluna **Guardar no Registo de Eventos do Windows** são apresentados em **Registos do Windows** na secção **Aplicação**. Para abrir os registos de eventos, clique **em Iniciar → Painel de comando → Administração → Visualizador de Eventos**.
6. Clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

Configurar a apresentação e o envio de notificações

Para configurar a apresentação e o envio de notificações:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Configurações avançadas**, selecione **Relatórios e Armazenamento**.

   A parte direita da janela apresenta as definições de relatórios e armazenamento.
3. Na secção **Notificações**, clique no botão **Configuração**.

   Esta ação abre a janela **Notificações**.

   Os componentes e as tarefas do Kaspersky Endpoint Security são apresentados na parte esquerda da janela. Na parte direita da janela são apresentados os eventos gerados para o componente ou tarefa selecionados.
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 requeridos.

   As informações sobre os eventos selecionados são apresentadas no ecrã como mensagens de pop-up na área de notificação da barra de tarefas do Microsoft Windows.
6. Na coluna **Notificar por e-mail**, selecione as caixas de verificação junto aos eventos pretendidos.

   As informações sobre os eventos selecionados são enviadas por e-mail se as definições de envio de notificações por e-mail estiverem configuradas.

7. Clique no botão **Configuração de notificações por e-mail**.

   É apresentada a janela **Configuração de notificações por e-mail**.

8. Selecione a caixa de verificação **Enviar notificações de eventos** para ativar a entrega de informações sobre os eventos do Kaspersky Endpoint Security selecionados na coluna **Notificar por e-mail**.

9. Especifique as definições de entrega de notificações por e-mail.

10. Clique em **OK**.

11. Na janela **Configuração de notificações por e-mail**, clique em **OK**.

12. Para guardar as alterações, clique no botão **Guardar**.

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. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, na secção **Configurações Avançadas**, selecione **Interface**.

   As definições da interface do Kaspersky Endpoint Security são apresentadas na parte direita da janela.

3. Na secção **Avisos**, selecione as caixas de verificação à frente das categorias de eventos sobre os quais pretende visualizar as notificações na área de notificação do Microsoft Windows.

4. Para guardar as alterações, clique no botão **Guardar**.

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.

Gerir a Quarentena e Cópia de Segurança

Esta secção descreve como pode configurar e gerir a Quarentena e Cópia de segurança.

Sobre a Quarentena e Cópia de Segurança

A *Quarentena* é uma lista de ficheiros provavelmente infetados. Os *ficheiros provavelmente infetados* são ficheiros que podem conter vírus e outras ameaças ou respetivas variantes.

Quando o Kaspersky Endpoint Security coloca em quarentena um ficheiro provavelmente infetado, não copia o ficheiro, mas move o mesmo: a aplicação apaga o ficheiro do disco rígido ou da mensagem de e-mail e guarda o ficheiro num armazenamento de dados especial. Os ficheiros em Quarentena são guardados num formato especial e não constituem uma ameaça.

O Kaspersky Endpoint Security pode detetar e colocar em quarentena um ficheiro provavelmente infetado durante um scan de vírus e também durante o funcionamento dos componentes Antivírus de Ficheiros, Antivírus de E-mail e Monitorização do Sistema.

O Kaspersky Endpoint Security coloca os ficheiros em Quarentena nas situações seguintes:

- O código do ficheiro é semelhante a um programa conhecido, mas parcialmente modificado, ou possui uma estrutura idêntica a software malicioso, e não está registado na base de dados do Kaspersky Endpoint Security. Neste caso, o ficheiro é colocado em Quarentena após a análise heurística pelo Antivírus de Ficheiros e pelo Antivírus de E-mail ou durante o scan de vírus. A análise heurística raramente gera falsos diagnósticos positivos.

- A sequência de operações que o ficheiro executa é perigosa. Neste caso, o ficheiro é colocado em Quarentena após o componente Monitorização do Sistema ter analisado o seu comportamento.

O *Cópia de segurança* é uma lista de cópias de segurança de ficheiros que foram apagados ou modificados durante o processo de desinfeção. A *Cópia de segurança* é um ficheiro criado durante a primeira tentativa de desinfetar ou eliminar este ficheiro. As cópias de segurança dos ficheiros são armazenadas num formato especial e não constituem uma ameaça.

Por vezes, não é possível manter a integridade dos ficheiros durante a desinfeção. Se perder acesso, parcial ou totalmente, a informações importantes num ficheiro desinfetado, após a desinfeção, pode tentar recuperar a cópia desinfetada do ficheiro para a respetiva pasta original.

É possível que, após nova atualização da base de dados ou dos módulos de software da aplicação, o Kaspersky Endpoint Security consiga identificar definitivamente as ameaças e neutralizá-las. É por isso recomendado verificar os ficheiros em quarentena Executar após cada atualização da base de dados e do módulo de software da aplicação.

Configurar as definições de Quarentena e Cópia de segurança

O armazenamento de dados é constituído por Quarentena e Cópia de segurança. Pode configurar as definições de Quarentena e Cópia de segurança do seguinte modo:

- Configurar o prazo de armazenamento máximo para os ficheiros em Quarentena e para as cópias de ficheiros em Cópia de segurança.

O prazo de armazenamento máximo predefinido para os ficheiros em Quarentena e para as cópias de ficheiros em Cópia de segurança é de 30 dias. Quando o prazo de armazenamento máximo termina, o Kaspersky Endpoint Security apaga os ficheiros mais antigos do armazenamento de dados. Pode cancelar a restrição de tempo ou alterar o prazo máximo de armazenamento de ficheiros.

- Pode configurar o tamanho máximo da Quarentena e Cópia de segurança.

  Por defeito, o tamanho máximo de Quarentena e Cópia de Segurança é 100 MB. Quando o armazenamento de dados atinge o limite, o Kaspersky Endpoint Security apaga automaticamente os ficheiros mais antigos da Quarentena e Cópia de Segurança para que o tamanho máximo do armazenamento de dados não seja excedido. Pode cancelar o limite de tamanho da Quarentena e Cópia de Segurança ou alterar o tamanho máximo.

Configurar o prazo de armazenamento máximo para os ficheiros em Quarentena e para as cópias de ficheiros em Cópia de segurança

Para configurar o prazo de armazenamento máximo para os ficheiros em Quarentena e para as cópias de ficheiros em Cópia de segurança:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Configurações avançadas**, selecione **Relatórios e Armazenamento**.
3. Execute uma das seguintes ações:
   - Para limitar o prazo de armazenamento de ficheiros da Quarentena e Cópia de Segurança, na secção **Definições de Quarentena e Cópia de segurança** na parte à direita da janela, selecione a caixa de verificação **Armazenar objetos no máximo durante**. No campo à direita da caixa de verificação **Guardar objetos até**, especifique o prazo máximo de armazenamento de ficheiros na Quarentena e para as cópias de ficheiro em Cópia de segurança. O prazo de armazenamento para os ficheiros em Quarentena e para as cópias de ficheiros em Cópia de segurança está limitado a 30 dias, por defeito.
   - Para cancelar o limite do prazo de armazenamento de ficheiros da Quarentena e Cópia de Segurança, na secção **Definições de Quarentena e Cópia de segurança**, selecione a caixa de verificação **Armazenar objetos no máximo durante**.
4. Para guardar as alterações, clique no botão **Guardar**.

Configurar o tamanho máximo da Quarentena e Cópia de segurança

Para configurar o tamanho máximo da Quarentena e Cópia de Segurança:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Configurações avançadas**, selecione **Relatórios e Armazenamento**.
3. Execute uma das seguintes ações:
   - Se pretender limitar o tamanho total da Quarentena e Cópia de Segurança, selecione a caixa de verificação **Tamanho de armazenamento máximo** à direita da janela na secção **Definições de Quarentena e Cópia de**

segurança e especifique o tamanho máximo da Quarentena e da Cópia de segurança no campo à direita da caixa de verificação **Tamanho de armazenamento máximo**.

Por defeito, o tamanho de armazenamento máximo para dados que englobem o diretório Quarentena e as cópias de segurança dos ficheiros é de 100 MB.

- Se quiser remover o limite do tamanho da Quarentena e Cópia de segurança, desmarque a caixa de verificação **Tamanho de armazenamento máximo** na parte direita da janela na secção **Definições de Quarentena e Cópia de segurança**.

O tamanho da Quarentena e Cópia de segurança é ilimitado por defeito.

4. Para guardar as alterações, clique no botão **Guardar**.

Gerir a Quarentena

O Kaspersky Endpoint Security elimina ficheiros automaticamente com qualquer estado da Quarentena após o prazo de armazenamento definido nas definições avançadas ter terminado.

Estão disponíveis as seguintes operações de ficheiros ao gerir a Quarentena:

- Ver os ficheiros colocados em quarentena pelo Kaspersky Endpoint Security.
- Verificar ficheiros provavelmente infetados utilizando a versão atual das bases de dados e módulos do Kaspersky Endpoint Security.
- Restaurar ficheiros da Quarentena para as pastas originais.
- Restaurar ficheiros da Quarentena.
- Abra as pastas nas quais os ficheiros estavam originalmente localizados.

O conjunto dos ficheiros colocados em quarentena é apresentado como uma tabela.

Pode também executar as seguintes ações ao gerir dados na tabela:

- Filtrar ficheiros em quarentena por colunas e por condições de filtragem personalizadas.
- Utilizar a função de procura de ficheiros em quarentena.
- Ordenar ficheiros em quarentena.
- Alterar a ordem e o conjunto das colunas apresentadas na tabela de ficheiros em quarentena.

Pode copiar os eventos de Quarentena selecionados para a área de transferência. Para selecionar vários ficheiros em quarentena, clique com o botão direito para abrir o menu de contexto de qualquer ficheiro e selecione **Selecionar todos**. Para remover a seleção de ficheiros que não pretende verificar, clique neles enquanto mantém premida a tecla **CTRL**.

Ativar e desativar a verificação de ficheiros em Quarentena após uma atualização

Se o Kaspersky Endpoint Security detetar sinais de infeção ao verificar um ficheiro mas não conseguir determinar que programas maliciosos foram responsáveis pela infeção, o Kaspersky Endpoint Security move este ficheiro para a Quarentena. O Kaspersky Endpoint Security pode identificar claramente as ameaças e neutralizá-las, depois de as bases de dados e os módulos da aplicação serem atualizados. Pode ativar a verificação automática dos ficheiros em Quarentena após cada atualização das bases de dados e módulos da aplicação.

Recomendamos verificar regularmente os ficheiros na Quarentena. A verificação pode alterar o estado dos ficheiros. Alguns ficheiros poderão ser desinfetados e restaurados para a respetiva localização original para que possa continuar a utilizar os mesmos.

Para ativar a verificação dos ficheiros em quarentena depois das atualizações:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Configurações avançadas**, selecione **Relatórios e Armazenamento**.

   Na parte direita da janela, são apresentadas as configurações de gestão de relatórios e armazenamento.
3. Na secção **Definições de Quarentena e Cópia de segurança**, execute uma das ações seguintes:
   - Para ativar a verificação dos ficheiros em quarentena após cada atualização do Kaspersky Endpoint Security, selecione a caixa de verificação **Verificar novamente a Quarentena após a atualização**.
   - Para desativar a verificação dos ficheiros em quarentena após cada atualização do Kaspersky Endpoint Security, desmarque a caixa de verificação **Verificar novamente a Quarentena após a atualização**.
4. Para guardar as alterações, clique no botão **Guardar**.

Iniciar uma tarefa de Verificação Personalizada para os ficheiros em Quarentena

Após uma atualização das bases de dados e dos módulos de software da aplicação, o Kaspersky Endpoint Security pode identificar as ameaças em ficheiros na quarentena e neutralizar os mesmos. Se a aplicação não estiver configurada para verificar automaticamente ficheiros em quarentena depois de cada atualização de bases de dados e módulos de aplicação, pode iniciar manualmente uma tarefa de Verificação Personalizada para ficheiros em quarentena.

Para iniciar uma tarefa de Verificação Personalizada para os ficheiros em quarentena, execute as seguintes ações:

1. Abra a janela principal da aplicação.
2. Na parte superior da janela principal da aplicação, clique na ligação **Quarentena** para abrir a janela **Armazenamento**.

   O separador **Quarentena** da janela **Armazenamento** é apresentado.
3. No separador **Quarentena**, selecione um ou mais ficheiros provavelmente infetados que pretenda verificar.

   Para selecionar vários ficheiros em quarentena, clique com o botão direito para abrir o menu de contexto de qualquer ficheiro e selecione **Selecionar todos**. Para remover a seleção de ficheiros que não pretende verificar, clique neles enquanto mantém premida a tecla **CTRL**.
4. Pode iniciar a tarefa de Verificação Personalizada através de uma das seguintes duas formas:
   - Clique no botão **Verificar novamente**.

- Clique com o botão direito do rato para visualizar o menu de contexto e selecione **Verificar novamente**.

Quando a verificação estiver concluída, é apresentada uma notificação com o número de ficheiros verificados e o número de ameaças detetadas.

Recuperar ficheiros da Quarentena

Para restaurar ficheiros da Quarentena:

1. Abra a janela principal da aplicação.
2. Na parte superior da janela principal da aplicação, clique na ligação **Quarentena** para abrir a janela **Armazenamento**.

   O separador **Quarentena** da janela **Armazenamento** é apresentado.
3. Se quiser restaurar todos os ficheiros da Quarentena, selecione **Restaurar tudo** a partir do menu de contexto de qualquer ficheiro.

   O Kaspersky Endpoint Security restaura todos os ficheiros da Quarentena para as respetivas pastas originais.
4. Para restaurar um ou mais ficheiros em quarentena:

   a. No separador **Quarentena**, selecione um ou mais ficheiros que pretenda restaurar a partir da Quarentena.

   Para selecionar vários ficheiros em quarentena, clique com o botão direito para abrir o menu de contexto de qualquer ficheiro e selecione **Selecionar todos**. Para remover a seleção de ficheiros que não pretende verificar, clique neles enquanto mantém premida a tecla **CTRL**.

   b. Para restaurar os ficheiros, execute uma das seguintes ações:

   - Clique no botão **Restaurar**.
   - Clique com o botão direito do rato para abrir o menu de contexto e selecione **Restaurar**.

O Kaspersky Endpoint Security restaura os ficheiros selecionados para as respetivas pastas originais.

Apagar ficheiros da Quarentena

Para apagar ficheiros da Quarentena:

1. Abra a janela principal da aplicação.
2. Na parte superior da janela principal da aplicação, clique na ligação **Quarentena** para abrir a janela **Armazenamento**.

   O separador **Quarentena** da janela **Armazenamento** é apresentado.
3. Se quiser eliminar todos os ficheiros da Quarentena, selecione **Eliminar tudo** a partir do menu de contexto de qualquer ficheiro.

   O Kaspersky Endpoint Security elimina todos os ficheiros da Quarentena.
4. Para eliminar um ou mais ficheiros em quarentena:

a. No separador **Quarentena**, selecione um ou mais ficheiros provavelmente infetados que pretenda eliminar da Quarentena.

Para selecionar vários ficheiros em quarentena, clique com o botão direito para abrir o menu de contexto de qualquer ficheiro e selecione **Selecionar todos**. Para remover a seleção de ficheiros que não pretende verificar, clique neles enquanto mantém premida a tecla **CTRL**.

b. Para apagar os ficheiros, execute uma das seguintes ações:

- Clique no botão **Remover**.
- Clique com o botão direito do rato para visualizar o menu de contexto e selecione **Eliminar**.

O Kaspersky Endpoint Security apaga os ficheiros selecionados da Quarentena.

Gerir Cópias de segurança

Se for detetado código malicioso no ficheiro, o Kaspersky Endpoint Security bloqueia o ficheiro, coloca uma cópia em Cópia de segurança e tenta desinfetá-la. Se a desinfeção do ficheiro for bem-sucedida, o estado da cópia de segurança do ficheiro é alterado para *Desinfetados*. O ficheiro fica disponível na sua pasta original. Se não for possível desinfetar um ficheiro, o Kaspersky Endpoint Security elimina-o da sua pasta original. Pode restaurar o ficheiro da cópia de segurança para a respetiva pasta original.

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 Kaspersky Endpoint Security elimina automaticamente as cópias de segurança dos ficheiros com qualquer estado da Cópia de segurança, após o prazo de armazenamento nas definições da aplicação ter terminado.

Também pode eliminar manualmente qualquer cópia de um ficheiro da Cópia de segurança.

O conjunto de cópias de segurança de ficheiros é apresentado como uma tabela.

Ao gerir a Cópia de segurança, pode executar as seguintes ações com cópias de segurança de ficheiros:

- Ver o conjunto de cópias de segurança de ficheiros.
- Restaurar as cópias de segurança dos ficheiros para as pastas originais.
- Apagar cópias de segurança de ficheiros da Cópia de segurança.

Pode também executar as seguintes ações ao gerir dados na tabela:

- Filtrar cópias de segurança por colunas, incluindo por condições de filtros personalizadas.
- Utilizar a função de procura de cópias de segurança.
- Ordenar as cópias de segurança.
- Alterar a ordem e o conjunto de colunas apresentadas na tabela de cópias de segurança.

Pode copiar os eventos de Cópia de segurança selecionados para a área de transferência. Para selecionar vários ficheiros de Cópia de Segurança, clique com o botão direito para abrir o menu de contexto de qualquer ficheiro e selecione **Selecionar todos**. Para remover a seleção de ficheiros que não pretende verificar, clique neles enquanto mantém premida a tecla **CTRL**.

Restaurar ficheiros a partir da Cópia de segurança

Para restaurar ficheiros a partir da Cópia de segurança:

1. Abra a janela principal da aplicação.
2. Na parte superior da janela principal da aplicação, clique na ligação **Quarentena** para abrir a janela **Armazenamento**.
3. Na janela **Armazenamento**, selecione o separador **Cópia de segurança**.
4. Se quiser restaurar todos os ficheiros da Cópia de segurança, selecione **Restaurar tudo** a partir do menu de contexto de qualquer ficheiro.

   O Kaspersky Endpoint Security restaura todos os ficheiros a partir das cópias de segurança para as respetivas pastas originais.
5. Para restaurar um ou mais ficheiros a partir da Cópia de segurança:

   a. Na tabela, no separador **Cópia de segurança**, selecione um ou mais ficheiros da Cópia de segurança.

      Para selecionar vários ficheiros em quarentena, clique com o botão direito para abrir o menu de contexto de qualquer ficheiro e selecione **Selecionar todos**. Para remover a seleção de ficheiros que não pretende verificar, clique neles enquanto mantém premida a tecla **CTRL**.

   b. Para restaurar os ficheiros, execute uma das seguintes ações:

      - Clique no botão **Restaurar**.
      - Clique com o botão direito do rato para abrir o menu de contexto e selecione **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

Para apagar cópias de segurança de ficheiros da Cópia de segurança:

1. Abra a janela principal da aplicação.
2. Na parte superior da janela principal da aplicação, clique na ligação **Quarentena** para abrir a janela **Armazenamento**.
3. Na janela **Armazenamento**, selecione o separador **Cópia de segurança**.
4. Se pretende eliminar todos os ficheiros da Cópia de segurança, execute uma das seguintes ações:

- No menu de contexto de qualquer ficheiro, selecione **Eliminar tudo**.
- Clique no botão **Limpar armazenamento**.

O Kaspersky Endpoint Security elimina todas as cópias de segurança dos ficheiros da Cópia de segurança.

5. Se quiser eliminar um ou mais ficheiros da Cópia de segurança:

   a. Na tabela, no separador **Cópia de segurança**, selecione um ou mais ficheiros da Cópia de segurança.

   Para selecionar vários ficheiros de Cópia de Segurança, clique com o botão direito para abrir o menu de contexto de qualquer ficheiro e selecione **Selecionar todos**. Para remover a seleção de ficheiros que não pretende verificar, clique neles enquanto mantém premida a tecla **CTRL**.

   b. Para apagar os ficheiros, execute uma das seguintes ações:

   - Clique no botão **Remover**.
   - Clique com o botão direito do rato para visualizar o menu de contexto e selecione **Eliminar**.

O Kaspersky Endpoint Security elimina as cópias de segurança selecionadas dos ficheiros da Cópia de segurança.

Configurações avançadas da aplicação

Esta secção descreve as configurações avançadas do Kaspersky Endpoint Security e como podem ser configuradas.

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 linha de comandos com as configurações predefinidas.

  Para tal, deve guardar o ficheiro de configuração na mesma pasta onde está localizado o kit 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. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, selecione a secção **Configurações avançadas**.

   As configurações avançadas da aplicação são apresentadas na parte direita da janela.
3. Na secção **Gerir definições**, clique no botão **Guardar**.

   Esta ação abre a janela padrão **Selecione um ficheiro de configuração** do Microsoft Windows.
4. Especifique o caminho no qual pretende guardar o ficheiro de configuração e introduza o seu nome.

   Para utilizar o ficheiro de configuração para a instalação local ou remota do Kaspersky Endpoint Security, deve denominá-lo install.cfg.
5. Clique no botão **Guardar**.

Para importar as definições do Kaspersky Endpoint Security de um ficheiro de configuração:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, selecione a secção **Configurações avançadas**.

   As configurações avançadas da aplicação são apresentadas na parte direita da janela.
3. Na secção **Gerir definições**, clique no botão **Carregar**.

   Esta ação abre a janela padrão **Selecione um ficheiro de configuração** do Microsoft Windows.
4. Especifique o caminho para o ficheiro de configuração.
5. Clique no botão **Abrir**.

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

Zona confiável

Esta secção contém informações sobre a zona confiável e instruções sobre como configurar a exclusão de verificação e criar uma lista de aplicações confiáveis.

Sobre a zona confiável

Uma *zona confiável* consiste numa lista de objetos e aplicações, configurada pelo administrador do sistema, que o Kaspersky Endpoint Security não monitoriza quando está ativo. Ou seja, trata-se de um conjunto de exclusões de scan.

O administrador cria a zona confiável 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 confiável 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.

Pode excluir da verificação os tipos de objetos seguintes:

- Ficheiros de determinados formatos
- Ficheiros selecionados por uma máscara
- Ficheiros selecionados
- Pastas
- Processos de aplicação

Exclusões de scan

Uma *exclusão de verificação* consiste num conjunto de condições sob as quais o Kaspersky Endpoint Security não verifica a existência de vírus e outras ameaças num objeto.

As exclusões de scan 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 utilizadas como um componente auxiliar em software malicioso. Alguns exemplos destas aplicações incluem ferramentas de administração remota, clientes de IRC, servidores FTP, vários utilitários para suspensão ou ocultação de processos, keyloggers (registadores de teclas digitadas), decifradores de passwords e auto-dialers (ligações telefónicas automáticas). Tais aplicações não são classificadas como vírus. Pode obter detalhes sobre software legal que pode ser utilizado por criminosos para danificar o computador ou os dados pessoais na Enciclopédia de Vírus da Kaspersky em www.securelist.com/ru/threats/detect.

Essas aplicações podem ser bloqueadas pelo Kaspersky Endpoint Security. Para impedir que sejam bloqueadas, pode configurar exclusões de scan para as aplicações em utilização. Para tal, adicione o nome ou a máscara do nome indicada na Enciclopédia de Vírus da Kaspersky à zona confiável. Por exemplo, pode usar, frequentemente, um programa de Administrador Remoto. Trata-se de uma aplicação de acesso remoto que concede ao utilizador controlo sobre um computador remoto. 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 Enciclopédia de Vírus da Kaspersky.

Se for instalada no seu computador uma aplicação que recolhe informação e a envia para ser processada, é possível que o Kaspersky Endpoint Security a classifique como software malicioso. Para evitar esta situação, pode excluir a aplicação das verificações configurando o Kaspersky Endpoint Security como descrito neste documento.

As exclusões de scan podem ser utilizadas pelos seguintes componentes e tarefas da aplicação, que são configurados pelo administrador do sistema:

- Antivírus de Ficheiros
- Antivírus de E-mail.
- Antivírus de Internet.
- Controlo de Privilégios das Aplicações.
- Tarefas de verificação
- Monitorização do Sistema.

A lista de aplicações confiáveis

A *lista de aplicações confiáveis* 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 defeito, o Kaspersky Endpoint Security verifica objetos que sejam abertos, executados ou guardados por qualquer outro processo de programa e controla a atividade de todas as aplicações e tráfego de rede gerado pelos mesmos. O Kaspersky Endpoint Security exclui da verificação as aplicações na lista de aplicações confiáveis.

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 confiáveis. 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 confiáveis.

A exclusão de aplicações confiáveis 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 confiável. Uma aplicação pode ser totalmente excluída da verificação do Kaspersky Endpoint Security com exclusões de scan.

Criar uma exclusão 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.

Para criar uma exclusão de verificação:

1. Abra a janela de definições da aplicação.
2. Selecione a secção **Proteção de Antivírus** à esquerda.

   As definições da Proteção de Antivírus são apresentadas na parte direita da janela.
3. Na secção **Exclusões de scan e aplicações confiáveis**, clique no botão **Configuração**.

   A janela **Zona confiável** é aberta no separador **Exclusões de scan**.
4. Clique no botão **Adicionar**.

   É aberta a janela **Exclusão de verificação**. Nesta janela, pode criar uma exclusão de scan utilizando um ou ambos os critérios da secção **Propriedades**.
5. Para excluir um ficheiro ou pasta da verificação:

   a. Na secção **Propriedades**, selecione a caixa de verificação **Ficheiro ou pasta**.

   b. Clique na ligação **Selec. ficheiro ou pasta** na secção **Descrição da exclusão de verificação** 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**.

   Num ficheiro ou máscara de nome da pasta, pode usar o carácter asterisco (*) para ocupar o lugar de qualquer conjunto de caracteres no nome do ficheiro.

   Por exemplo, pode usar máscaras para adicionar os seguintes caminhos:

   - Caminhos para ficheiros localizados em qualquer pasta:
     - A máscara "*.exe" incluirá todos os caminhos para ficheiros com a extensão EXE.
     - A máscara "teste" incluirá todos os caminhos para ficheiros denominados "teste".
   - Caminhos para ficheiros localizados numa pasta especificada:
     - A máscara "C:\dir*.*" incluirá todos os caminhos para ficheiros localizados na pasta C:\dir\, mas não nas subpastas de C:\dir\.
     - A máscara "C:\dir*" incluirá 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\test" incluirá todos os caminhos para ficheiros denominados "teste" localizados na pasta C:\dir\, mas não nas subpastas de C:\dir\.
     - A máscara "C:\dir*\test" incluirá todos os caminhos para 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*.*" incluirá todos os caminhos para ficheiros em pastas denominadas "dir", mas não nas subpastas dessas pastas.
- A máscara "dir*" incluirá todos os caminhos para ficheiros em pastas denominadas "dir", mas não nas subpastas dessas pastas.
- A máscara "dir\" inclui todos os caminhos para ficheiros em pastas denominadas "dir", mas não nas subpastas dessas pastas.
- A máscara "dir*.exe" inclui todos os caminhos para ficheiros com a extensão EXE em pastas denominadas "dir", mas não nas subpastas dessas pastas.
- A máscara "dir\test" incluirá todos os caminhos para ficheiros denominados "teste" em pastas denominadas "dir", mas não nas subpastas dessas pastas.

d. Na janela **Nome do ficheiro ou pasta**, clique em **OK**.

É apresentada uma ligação para a pasta ou ficheiro adicionado na secção **Descrição da exclusão de verificação**, da janela **Exclusão de verificação**.

6. 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** para abrir a janela **Nome do objeto**.

c. Introduza o nome do objeto ou o nome da máscara de acordo com a classificação da Enciclopédia de Vírus da Kaspersky:

d. Clique em **OK** na janela **Nome do objeto**.

É apresentada uma ligação para o nome do objeto adicionado na secção **Descrição da exclusão de verificação** da janela **Exclusão de verificação**.

7. Se necessário, no campo **Comentário**, introduza um breve comentário na exclusão de verificação que está a criar.

8. 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** 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. Na janela **Componentes de proteção**, clique em **OK**.

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.

9. Na janela **Exclusão de verificação**, clique em **OK**.

A exclusão de verificação adicionada é apresentada na tabela no separador **Exclusões de scan** da janela **Zona confiável**. As definições configuradas desta exclusão de verificação são apresentadas na secção **Descrição da exclusão de verificação**.

10. Na janela **Zona confiável**, clique em **OK**.

11. Para guardar as alterações, clique no botão **Guardar**.

Modificar uma exclusão de verificação

Para modificar uma exclusão de verificação:

1. Abra a janela de definições da aplicação.

2. Selecione a secção **Proteção de Antivírus** à esquerda.

   As definições da Proteção de Antivírus são apresentadas na parte direita da janela.

3. Na secção **Exclusões de scan e aplicações confiáveis**, clique no botão **Configuração**.

   A janela **Zona confiável** é aberta no separador **Exclusões de scan**.

4. Selecione a exclusão de verificação que pretende modificar na lista.

5. Alterar as definições de exclusão de verificação utilizando um dos seguintes métodos:

   - Clique no botão **Editar**.

     É apresentada a janela **Exclusões de scan**.

   - Abra a janela para editar a definição necessária clicando na ligação do campo **Descrição da exclusão de verificação**.

6. Se clicou no botão **Editar** durante o passo anterior, clique em **OK** na janela **Exclusão de verificação**.

   As definições modificadas desta exclusão de verificação são apresentadas na secção **Descrição da exclusão de verificação**.

7. Na janela **Zona confiável**, clique em **OK**.

8. Para guardar as alterações, clique no botão **Guardar**.

Eliminar uma exclusão de verificação

Para eliminar uma exclusão de verificação:

1. Abra a janela de definições da aplicação.

2. Selecione a secção **Proteção de Antivírus** à esquerda.

   As definições da Proteção de Antivírus são apresentadas na parte direita da janela.

3. Na secção **Exclusões de scan e aplicações confiáveis**, clique no botão **Configuração**.

   A janela **Zona confiável** é aberta no separador **Exclusões de scan**.

4. Selecione a exclusão de verificação necessária na lista de exclusões de scan.
5. Clique no botão **Remover**.

   A exclusão de verificação eliminada deixa de ser apresentada na lista.
6. Na janela **Zona confiável**, clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

Ativar e desativar a exclusão de verificação

Para ativar ou desativar uma exclusão de verificação:

1. Abra a janela de definições da aplicação.
2. Selecione a secção **Proteção de Antivírus** à esquerda.

   As definições da Proteção de Antivírus são apresentadas na parte direita da janela.
3. Na secção **Exclusões de scan e aplicações confiáveis**, clique no botão **Configuração**.

   A janela **Zona confiável** é aberta no separador **Exclusões de scan**.
4. Selecione a exclusão necessária na lista de exclusões de scan.
5. Execute uma das seguintes ações:

   - Para ativar uma exclusão de verificação, selecione a caixa de verificação junto do nome desta exclusão de verificação.
   - Para desativar uma exclusão de verificação, desmarque a caixa de verificação junto do nome desta exclusão de verificação.
6. Clique em **OK**.
7. Para guardar as alterações, clique no botão **Guardar**.

Editar a lista de aplicações confiáveis

Para editar a lista de aplicações confiáveis:

1. Abra a janela de definições da aplicação.
2. Selecione a secção **Proteção de Antivírus** à esquerda.

   As definições da Proteção de Antivírus são apresentadas na parte direita da janela.
3. Na secção **Exclusões de scan e aplicações confiáveis**, clique no botão **Configuração**.

   É aberta a janela **Zona confiável**.
4. Na janela **Zona confiável**, selecione o separador **Aplicações confiáveis**.

5. Para adicionar uma aplicação à lista de aplicações confiáveis:

   a. Clique no botão **Adicionar**.

   b. No menu de contexto que é aberto, execute uma das seguintes ações:

   - Se pretende localizar a aplicação na lista de aplicações instaladas no computador, selecione o item **Aplicações** no menu.

     É aberta a janela **Selecionar aplicação**.

   - Se pretende especificar o caminho para o ficheiro executável da aplicação pretendida, selecione **Procurar**.

     É aberta a janela padrão **Abrir ficheiro** no Microsoft Windows.

   c. Selecione a aplicação através de uma das seguintes formas:

   - Se selecionou **Aplicações** no passo anterior, selecione a aplicação na lista de aplicações instaladas no computador e clique em **OK** na janela **Selecionar aplicação**.

   - Se selecionou **Procurar** no passo anterior, especifique o caminho para o ficheiro executável da aplicação relevante e clique no botão **Abrir** na janela padrão **Abrir** do Microsoft Windows.

   Estas ações fazem com que a janela **Exclusões de scan para a aplicação** seja aberta.

   a. Selecione as caixas de verificação à frente das regras da zona confiável relevante para a aplicação selecionada:

   - **Não verificar ficheiros abertos**.
   - **Não monitorizar a atividade das aplicações**.
   - **Não herdar restrições do processo-pai (aplicação)**.
   - **Não monitorizar atividades de subaplicações**.
   - **Não bloquear interação com a interface da aplicação**.
   - **Não verificar tráfego de rede**.

   b. Na janela **Exclusões de scan para a aplicação**, clique em **OK**.

   A aplicação confiável que adicionou é apresentada na lista de aplicações confiáveis.

6. Para editar as definições de uma aplicação confiável:

   a. Selecione uma aplicação confiável na lista de aplicações confiáveis.

   b. Clique no botão **Editar**.

   c. É apresentada a janela **Exclusões de scan para a aplicação**.

   d. Selecione ou desmarque as caixas de verificação à frente das regras da zona confiável relevante para a aplicação selecionada:

Se não estiver selecionada nenhuma das regras da zona confiável na janela **Exclusões de scan para a aplicação**, a aplicação confiável é incluída na verificação. Neste caso, a aplicação confiável não é removida da lista de aplicações confiáveis, mas a respetiva caixa de verificação fica desmarcada.

e. Na janela **Exclusões de scan para a aplicação**, clique em **OK**.

7. Para remover uma aplicação confiável da lista de aplicações confiáveis:

   a. Selecione uma aplicação confiável na lista de aplicações confiáveis.

   b. Clique no botão **Remover**.

8. Na janela **Zona confiável**, clique em **OK**.

9. Para guardar as alterações, clique no botão **Guardar**.

Ativar e desativar as regras da zona confiável para uma aplicação da lista de aplicações confiáveis

Ativar ou desativar a ação de regras da zona confiável para uma aplicação da lista de aplicações confiáveis:

1. Abra a janela de definições da aplicação.

2. Selecione a secção **Proteção de Antivírus** à esquerda.
   As definições da Proteção de Antivírus são apresentadas na parte direita da janela.

3. Na secção **Exclusões de scan e aplicações confiáveis**, clique no botão **Configuração**.
   É aberta a janela **Zona confiável**.

4. Na janela **Zona confiável**, selecione o separador **Aplicações confiáveis**.

5. Na lista de aplicações confiáveis, selecione a aplicação confiável pretendida.

6. Execute uma das seguintes ações:

   - Para excluir uma aplicação confiável da verificação do Kaspersky Endpoint Security, selecione a caixa de verificação junto ao nome da mesma.

   - Para incluir uma aplicação confiável na verificação do Kaspersky Endpoint Security, desmarque a caixa de verificação junto ao nome da mesma.

7. Clique em **OK**.

8. Para guardar as alterações, clique no botão **Guardar**.

Utilizar o armazenamento de certificados de sistema confiáveis

A utilização do armazenamento de certificados de sistema permite-lhe excluir aplicações assinadas por uma assinatura digital confiável de verificações de vírus. O Kaspersky Endpoint Security atribui automaticamente essas aplicações ao grupo *Fidedignas*.

Para começar a utilizar o armazenamento de certificados de sistema confiáveis:

1. Abra a janela de definições da aplicação.
2. Selecione a secção **Proteção de Antivírus** à esquerda.

   As definições da Proteção de Antivírus são apresentadas na parte direita da janela.
3. Na secção **Exclusões de scan e aplicações confiáveis**, clique no botão **Configuração**.

   É aberta a janela **Zona confiável**.
4. Na janela **Zona confiável**, selecione o separador **Arquivo de certificados do sistema confiável**.
5. Selecione a caixa de verificação **Utilizar arquivo de certificados do sistema confiável**.
6. Na lista pendente **Arquivo de certificados do sistema confiável**, selecione o armazenamento de sistema do Kaspersky Endpoint Security que deve ser considerado como confiável.
7. Na janela **Zona confiável**, clique em **OK**.
8. Para guardar as alterações, clique no botão **Guardar**.

Autodefesa do Kaspersky Endpoint Security

Esta secção descreve os mecanismos de autodefesa e defesa por controlo remoto do Kaspersky Endpoint Security e fornece instruções para configurar as definições destes mecanismos.

Sobre a Autodefesa do Kaspersky Endpoint Security

O Kaspersky Endpoint Security protege o computador de programas maliciosos, incluindo software malicioso que tenta bloquear o funcionamento do Kaspersky Endpoint Security ou mesmo apagá-lo do computador.

A estabilidade do sistema de segurança do computador é assegurada pelos mecanismos de autodefesa e defesa por controlo remoto no Kaspersky Endpoint Security.

O mecanismo de *Autodefesa* impede a alteração ou a eliminação dos ficheiros de aplicação do disco rígido, dos processos da memória e no registo do sistema.

A *Defesa por Controlo Remoto* bloqueia todas as tentativas de um computador remoto de controlar os serviços da aplicação.

Nos computadores com sistemas operativos de 64 bits, apenas a Autodefesa do Kaspersky Endpoint Security está disponível para impedir a alteração e a eliminação de ficheiros de aplicações no disco rígido e nas entradas do registo do sistema.

Ativar ou desativar a Autodefesa

O mecanismo de Autodefesa do Kaspersky Endpoint Security está ativado por defeito. Se necessário, pode desativar a autodefesa.

Para ativar ou desativar a Autodefesa:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, selecione a secção **Configurações avançadas**.

   As configurações avançadas da aplicação são apresentadas na parte direita da janela.
3. Execute uma das seguintes ações:
   - Para ativar o mecanismo de Autodefesa, selecione a caixa de verificação **Ativar Autodefesa**.
   - Para desativar o mecanismo de Autodefesa, desmarque a caixa de verificação **Ativar Autodefesa**.
4. Para guardar as alterações, clique no botão **Guardar**.

Ativar ou desativar a Defesa por Controlo Remoto

O mecanismo de defesa por controlo remoto está ativado por defeito. Pode desativar o mecanismo de defesa por controlo remoto, se necessário.

Para ativar ou desativar o mecanismo de defesa por controlo remoto:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, selecione a secção **Configurações avançadas**.

   As configurações avançadas da aplicação são apresentadas na parte direita da janela.
3. Execute uma das seguintes ações:
   - Para ativar o mecanismo de defesa por controlo remoto, selecione **Desativar a gestão externa do serviço do sistema**.
   - Para desativar o mecanismo de defesa por controlo remoto, desmarque **Desativar a gestão externa do serviço do sistema**.
4. Para guardar as alterações, clique no botão **Guardar**.

Disponibilizar apoio para aplicações de administração remota

Ocasionalmente, poderá ser necessária a utilização de uma aplicação de administração remota quando a proteção de controlo externa está ativada.

Para ativar o funcionamento de aplicações de administração remota:

1. Abra a janela de definições da aplicação.
2. Selecione a secção **Proteção de Antivírus** à esquerda.

   As definições da Proteção de Antivírus são apresentadas na parte direita da janela.
3. Na secção **Exclusões de scan e aplicações confiáveis**, clique no botão **Configuração**.

   É aberta a janela **Zona confiável**.
4. Na janela **Zona confiável**, selecione o separador **Aplicações confiáveis**.
5. Clique no botão **Adicionar**.
6. No menu de contexto que é aberto, execute uma das seguintes ações:

   - Para localizar a aplicação de administração remota na lista de aplicações instaladas no computador, selecione o item **Aplicações** no menu.

     É aberta a janela **Selecionar aplicação**.
   - Para especificar o caminho para o ficheiro executável da aplicação de administração remota, selecione **Procurar**.

     É aberta a janela padrão **Abrir ficheiro** no Microsoft Windows.
7. Selecione a aplicação através de uma das seguintes formas:

   - Se selecionou **Aplicações** no passo anterior, selecione a aplicação na lista de aplicações instaladas no computador e clique em **OK** na janela **Selecionar aplicação**.
   - Se selecionou **Procurar** no passo anterior, especifique o caminho para o ficheiro executável da aplicação relevante e clique no botão **Abrir** na janela padrão **Abrir** do Microsoft Windows.

   Estas ações fazem com que a janela **Exclusões de scan para a aplicação** seja aberta.
8. Selecione a caixa de verificação **Não monitorizar a atividade das aplicações**.
9. Na janela **Exclusões de scan para a aplicação**, clique em **OK**.

   A aplicação confiável que adicionou é apresentada na lista de aplicações confiáveis.
10. Para guardar as alterações, clique no botão **Guardar**.

Desempenho do Kaspersky Endpoint Security e compatibilidade com outras aplicações

Esta secção contém informações sobre o desempenho do Kaspersky Endpoint Security e compatibilidade com outras aplicações, bem como orientações para a seleção de tipos de objetos detetáveis e o modo de funcionamento do Kaspersky Endpoint Security.

Sobre o desempenho do Kaspersky Endpoint Security e compatibilidade com outras aplicações

Desempenho do Kaspersky Endpoint Security

O desempenho do Kaspersky Endpoint Security refere-se ao número de tipos de objetos que podem danificar o computador e que são detetáveis, bem como ao consumo de energia e à utilização de recursos do computador.

Selecionar tipos de objetos detetáveis

O Kaspersky Endpoint Security permite-lhe ajustar a proteção do seu computador e selecionar os tipos de objetos que a aplicação deteta em funcionamento. O Kaspersky Endpoint Security verifica sempre o sistema operativo quanto à presença de vírus, worms e programas Trojan. Não é possível desativar a verificação destes tipos de objetos. Tal software malicioso pode causar danos significativos no computador. Para uma maior segurança do computador, pode expandir o intervalo de tipos de objetos detetáveis, ativando a monitorização de software legal que pode ser utilizado por criminosos para danificar o seu computador ou dados pessoais.

Utilizar o modo de poupança de energia

O consume de energia das aplicações é um aspeto chave nos computadores portáteis. As tarefas agendadas do Kaspersky Endpoint Security normalmente consomem recursos consideráveis. Quando o computador está a funcionar com bateria, pode utilizar o modo de poupança de energia para otimizar a carga da bateria.

No modo de poupança de energia, as seguintes tarefas agendadas são adiadas automaticamente:

- Tarefa de atualização
- Tarefa de Verificação Completa
- Tarefa de Verificação de Áreas Críticas
- Tarefa de Verificação Personalizada
- Tarefa de Verificação de Vulnerabilidade
- 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, os programas maliciosos conseguem penetrar nos níveis mais baixos de um sistema operativo, o que os torna, praticamente, impossíveis de apagar. 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 os programas maliciosos, cujos processos já tenham iniciado na memória RAM e que impedem que o Kaspersky Endpoint Security remova os mesmos utilizando outros métodos. Deste modo, a ameaça é neutralizada. Enquanto a Desinfeção Avançada decorre, é recomendado não iniciar novos processos nem editar o registo do sistema operativo. A tecnologia de desinfeção avançada utiliza recursos consideráveis do sistema operativo, o que poderá tornar outras aplicações mais lentas.

Após o processo de Desinfeção Avançada concluir num computador com o Microsoft Windows para estações de trabalho, o Kaspersky Endpoint Security solicita ao utilizador permissão para reiniciar o computador. Após o reinicio do sistema, o Kaspersky Endpoint Security elimina os ficheiros de software malicioso e inicia uma verificação completa mais rápida do computador.

Não é possível apresentar um pedido de reinício num computador com o Microsoft Windows para servidores de ficheiros, devido às especificidades do Kaspersky Endpoint Security para servidores de ficheiros. 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 de ficheiros e inicie uma tarefa de grupo de *Scan de vírus* numa altura conveniente para os utilizadores do servidor de ficheiros.

Selecionar tipos de objetos detetáveis

Para selecionar tipos de objetos detetáveis:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, selecione a secção **Proteção de Antivírus**.

   As definições da Proteção de Antivírus são apresentadas na parte direita da janela.
3. Na secção **Objetos**, clique no botão **Configuração**.

   A janela **Objetos para deteção** abre.
4. Selecione as caixas de verificação em frente aos tipos de objetos que pretende que o Kaspersky Endpoint Security detete:

   - **Ferramentas maliciosas**
   - **Adware**
   - **Auto-dialers**

- **Outra**
- **Ficheiros comprimidos que podem provocar danos**
- **Ficheiros multicomprimidos**

5. Clique em **OK**.

   A janela **Objetos para deteção** fecha-se. Na secção **Objetos**, os tipos selecionados de objetos são apresentados por baixo da lista **Está ativada a deteção dos tipos de objeto seguintes**.

6. Para guardar as alterações, clique no botão **Guardar**.

Ativar ou desativar a Tecnologia de Desinfeção Avançada para estações de trabalho

Para ativar ou desativar a Tecnologia de Desinfeção Avançada para estações de trabalho:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, selecione a secção **Proteção de Antivírus**.

   As definições da Proteção de Antivírus são apresentadas na parte direita da janela.

3. Na parte direita da janela, execute uma das seguintes ações:
   - Selecione **Ativar Tecnologia de Desinfeção Avançada** para ativar a tecnologia de desinfeção avançada.
   - Desmarque **Ativar Tecnologia de Desinfeção Avançada** para desativar a tecnologia de desinfeção avançada.
4. Para guardar as alterações, clique no botão **Guardar**.

Quando a tarefa de Desinfeção avançada é iniciada pelo Kaspersky Security Center, a maioria das funções do sistema operativo não estão disponíveis para o utilizador. A estação de trabalho é reiniciada após a tarefa ter sido concluída.

Ativar ou desativar a Tecnologia de Desinfeção Avançada para servidores de ficheiros

Para ativar a tecnologia de Desinfeção Avançada para servidores de ficheiros, execute uma das seguintes ações:

- Ative a Tecnologia de Desinfeção Avançada nas propriedades da política ativa do Kaspersky Security Center. Para tal:
  a. Abra a secção **Configurações Gerais de Proteção** na janela de propriedades da política.
  b. Selecione a caixa de verificação **Ativar Tecnologia de Desinfeção Avançada**.
  c. Para guardar as alterações, clique em **OK** na janela de propriedades da política.

- Nas propriedades da tarefa de grupo Scan de vírus do Kaspersky Security Center, selecione a caixa de verificação **Executar a Desinfeção Avançada imediatamente**.

Para desativar a Tecnologia de Desinfeção Avançada para servidores de ficheiros, execute um dos procedimentos seguintes:

- Ative a Tecnologia de Desinfeção Avançada nas propriedades da política do Kaspersky Security Center. Para tal:

  a. Abra a secção **Configurações Gerais de Proteção** na janela de propriedades da política.

  b. Desmarque a caixa de verificação **Ativar Tecnologia de Desinfeção Avançada**.

  c. Para guardar as alterações, clique em **OK** na janela de propriedades da política.

- Nas propriedades da tarefa de grupo Scan de vírus do Kaspersky Security Center, desmarque a caixa de verificação **Executar a Desinfeção Avançada imediatamente**.

Ativar ou desativar o modo de poupança de energia

Para ativar ou desativar o modo de poupança de energia:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, selecione a secção **Configurações avançadas**.

   As configurações avançadas da aplicação são apresentadas na parte direita da janela.
3. Na secção **Modo de funcionamento**, clique no botão **Configuração**.

   É apresentada a janela **Modo operativo** abre-se.
4. Execute as seguintes ações na janela **Modo operativo**:

   - Para ativar o modo de poupança de energia, selecione a caixa de verificação **Adiar as tarefas agendadas quando o computador estiver ligado com bateria**.

     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 Vulnerabilidade
     - Tarefa de Verificação de Integridade

   - Se pretende desativar o modo de poupança de energia, desmarque a caixa de verificação **Adiar as tarefas agendadas quando o computador estiver ligado com bateria**. Neste caso, o Kaspersky Endpoint Security executa as tarefas agendadas, independentemente da fonte de alimentação do computador.

5. Para guardar as alterações, clique no botão **Guardar**.

Ativar ou desativar a concessão de recursos para outras aplicações

Para ativar ou desativar a concessão de recursos para outras aplicações:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, selecione a secção **Configurações avançadas**.

   As configurações avançadas da aplicação são apresentadas na parte direita da janela.
3. Na secção **Modo de funcionamento**, clique no botão **Configuração**.

   É apresentada a janela **Modo operativo** abre-se.
4. Execute as seguintes ações na janela **Modo operativo**:

   - Se pretender ativar o modo no qual os recursos são concedidos para outras aplicações, selecione a caixa de verificação **Conceder 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 Vulnerabilidade
     - Tarefa de Verificação de Integridade
   - Se pretender desativar o modo no qual os recursos são concedidos para outras aplicações, desmarque a caixa de verificação **Conceder recursos para outras aplicações**. Neste caso, o Kaspersky Endpoint Security executa as tarefas agendadas, independentemente do funcionamento de outras aplicações.

   Por defeito, a aplicação está configurada para conceder recursos para outras aplicações.
5. Para guardar as alterações, clique no botão **Guardar**.

Proteção por password

Esta secção contém informações sobre a restrição de acesso ao Kaspersky Endpoint Security através de uma password.

Sobre a restrição de acesso ao Kaspersky Endpoint Security

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.

Pode restringir o acesso ao Kaspersky Endpoint Security definindo um nome de utilizador e uma password e especificando operações para as quais a aplicação solicita essas credenciais ao utilizador:

Quando uma versão anterior da aplicação é atualizada para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows, a password é guardada (caso tenha sido definida). Para editar as definições de proteção por password pela primeira vez, utilize o nome de utilizador predefinido KLAdmin.

Ativar e desativar a proteção por password

Recomendamos cuidado na utilização de uma password para restringir o acesso à aplicação. Caso se esqueça da password, contacte o Suporte Técnico da Kaspersky Technical para obter instruções de desativação da proteção por password.

Para ativar a proteção por password:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, selecione a secção **Configurações avançadas**.

   As definições da aplicação são apresentadas na parte direita da janela.
3. Na secção **Proteção por password**, clique no botão **Configuração**.

   É aberta a janela **Proteção por Password**.
4. Selecione a caixa de verificação **Ativar proteção por password**.
5. No campo **Nome de utilizador**, introduza o nome de utilizador que deve ser especificado na janela **Verificação de password** quando as operações protegidas por password subsequentes são executadas.
6. No campo **Nova password**, introduza uma password para aceder à aplicação.
7. Confirme a password no campo **Confirmar password**.
8. Se pretender restringir o acesso a todas as operações com a aplicação, na secção **Âmbito da password**, clique no botão **Selecionar todos**.
9. Se pretender restringir seletivamente o acesso de utilizador, na secção **Âmbito da password**, selecione as caixas de verificação junto dos nomes das operações relevantes:
   - **Configurar definições da aplicação**.
   - **Sair da aplicação**.
   - **Desativar componentes de proteção**.
   - **Desativar componentes de controlo**.

- **Remover chave**.
- **Remover/modificar/restaurar a aplicação**.
- **Repor o acesso aos dados em ficheiros encriptados**.
- **Ver relatórios**.

10. Clique no botão **OK**.

    A aplicação verifica as passwords introduzidas. Se as passwords corresponderem, a aplicação aplica a password. Se as passwords não forem correspondentes, a aplicação solicita que confirme a password novamente no campo **Confirmar password**.

Depois de a proteção por password ser ativada, a aplicação solicita uma password sempre que uma operação incluída no âmbito da password é executada. Se não pretender que a aplicação solicite novamente a password sempre que tenta executar uma operação protegida por password durante a sessão atual, pode selecionar a caixa de verificação **Guardar password para a atual sessão** na janela **Verificação de password**.

Quando a caixa de verificação **Guardar password para a atual sessão** está desmarcada, a aplicação solicita a password ao utilizador sempre que tentar executar uma operação protegida por password.

Para desativar a proteção por password:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, selecione a secção **Configurações avançadas**.

   As definições da aplicação são apresentadas na parte direita da janela.
3. Na secção **Proteção por password**, clique no botão **Configuração**.

   É aberta a janela **Proteção por Password**.
4. Desmarque a caixa de verificação **Ativar proteção por password**.

   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.
5. Clique no botão **OK**.

Depois de a proteção por password ser desativada, o acesso restrito à aplicação será cancelado no próximo arranque do Kaspersky Endpoint Security.

Modificar a password de acesso ao Kaspersky Endpoint Security

Para alterar a password de acesso para o Kaspersky Endpoint Security:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, selecione a secção **Configurações avançadas**.
3. Na secção **Proteção por password**, clique no botão **Configuração**.

É aberta a janela **Proteção por Password**.

4. Introduza o nome de utilizador no campo **Nome de utilizador**.
5. No campo **Nova password**, introduza uma nova password para aceder à aplicação.
6. No campo **Confirmar password**, introduza novamente a nova password.
7. Clique em **OK**.

   A aplicação verifica as passwords introduzidas. Se as passwords forem correspondentes, a aplicação aplica a nova password e fecha a janela **Proteção por password**. Se as passwords não forem correspondentes, a aplicação solicita que confirme a password novamente no campo **Confirmar password**.

8. Para guardar as alterações, na janela de definições da aplicação, clique no botão **Guardar**.

Sobre a utilização de uma password temporária

Ao trabalhar em computadores cliente geridos por uma política do Kaspersky Security Center, os utilizadores podem necessitar de executar operações com o Kaspersky Endpoint Security que estejam protegidas por password ao nível da política. Quando a proteção por password está ativada, apenas o administrador do Kaspersky Security Center pode executar as operações especificadas no âmbito da password. Contudo, se a ligação ao Kaspersky Security Center tiver sido perdida (como quando o utilizador está fora da rede empresarial), as funções de trabalho com a interface local do Kaspersky Security Center são limitadas.

Para fornecer a um utilizador a capacidade de executar operações necessárias sem dar ao utilizador a password estabelecida nas definições de política, o administrador do Kaspersky Security Center pode criar uma password temporária. Uma password temporária tem um período de validade limitado e um âmbito de ação limitado. Depois de o utilizador introduzir a password temporária na interface local da aplicação, as operações permitidas pelo administrador do Kaspersky Security Center ficam disponíveis.

Quando a password temporária expira, o Kaspersky Endpoint Security continua a funcionar conforme as definições da política do Kaspersky Security Center. As operações protegidas por password ao nível de política ficam indisponíveis para o utilizador.

Criar uma password temporária utilizando a Consola de Administração do Kaspersky Security Center

Para criar uma password temporária e enviá-la a um utilizador:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração que inclui o computador do utilizador que está a solicitar a password temporária.
3. Na área de trabalho, selecione o separador **Dispositivos**.
4. No menu de contexto do computador que pertence ao utilizador que está a solicitar a password temporária, selecione **Propriedades**.

   É apresentada a janela **Propriedades: <Nome do computador>**.

5. Na janela **Propriedades: <Nome do computador>**, selecione a secção **Aplicações**.

6. Selecione o Kaspersky Endpoint Security Service Pack 2 for Windows e abra a janela de propriedades da aplicação utilizando um dos seguintes métodos:

   - Clique no botão **Propriedades** na parte inferior do ecrã.
   - No menu de contexto da aplicação, selecione **Propriedades**.

   Esta ação abre a janela **Definições da aplicação" <Nome da aplicação>"**.

7. Na janela **Definições da aplicação "<Nome da aplicação>"**, na secção **Configurações Avançadas**, selecione a subsecção **Definições da aplicação**.

8. Na secção **Proteção por password**, clique no botão **Configuração**.

   É aberta a janela **Proteção por Password**.

9. Na janela de **Proteção por password**, na secção de **Palavra-passe temporária**, clique no botão **Configuração**.

   Este botão está disponível se a proteção por password estiver ativa para o Kaspersky Security Center na política do Kaspersky Security Center em execução no computador.

   É apresentada a janela **Criar password temporária**.

10. No campo de **Data de validade**, especifique a data na qual o utilizador deixará de poder utilizar a password temporária.

    Nesta data, a password temporária deixará de estar válida. Será necessário criar uma nova password temporário para fornecer acesso para executar operações na interface local do Kaspersky Endpoint Security.

11. Na tabela **de 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 no botão **Criar**.

    Esta ação abre a janela **Palavra-passe temporária** que contém uma password encriptada.

13. Copie a password e as instruções sobre a aplicação da mesma e envie-as ao utilizador.

Aplicar uma password temporária na interface do Kaspersky Endpoint Security

Estas instruções destinam-se a utilizadores de computadores cliente com o Kaspersky Endpoint Security instalado.

Para aplicar uma password temporária:

1. Abra a janela de definições da aplicação.

2. Na parte esquerda da janela, selecione a secção **Configurações avançadas**.

   As definições da aplicação são apresentadas na parte direita da janela.

3. Na secção **Proteção por password**, clique no botão **Palavra-passe temporária**.

É apresentada a janela **Palavra-passe temporária**.

4. Selecione a caixa de verificação **Ativar password temporária**.

5. No campo de entrada, especifique a password fornecida pelo administrador do Kaspersky Security Center.

6. Clique em **OK** para guardar as alterações.

Depois de a password temporária ser aplicada, ficam disponíveis as operações especificadas pelo administrador do Kaspersky Security Center. A janela **Palavra-passe temporária** apresenta a data de validade da password temporária e as operações permitidas.

Administração remota da aplicação através do Kaspersky Security Center

Esta secção descreve a administração do Kaspersky Endpoint Security através do Kaspersky Security Center.

Sobre a gestão da aplicação através 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, tudo isto remotamente.

Para obter informações adicionais sobre a gestão da aplicação através do Kaspersky Security Center não fornecidas neste documento, consulte o *Manual do Administrador do Kaspersky Security Center*.

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

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

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

Pode utilizar um administration plug-in para alterar os seguintes itens:

- Políticas
- Perfis de política
- Tarefas de grupo
- Tarefas locais
- Definições locais do Kaspersky Endpoint Security

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

Se um componente for aberto, o administration plug-in verifica a sua informação de compatibilidade. Se a versão do administration plug-in for igual ou posterior à versão especificada na informação de compatibilidade, pode alterar as definições deste componente. Caso contrário, não pode utilizar o administration plug-in para alterar as definições do componente selecionado. É recomendada a atualização do administration plug-in.

Alterar configurações definidas anteriormente utilizando uma versão posterior do administration plug-in

Pode utilizar uma versão posterior do administration plug-in para alterar todas as configurações definidas anteriormente e configurar novas definições que não estiveram presentes na sua versão do administration plug-in utilizada anteriormente.

Para novas definições, uma versão posterior do administration plug-in atribui os valores predefinidos quando uma política, perfil de política ou tarefa são guardados pela primeira vez.

Após a alteração das definições de uma política, do perfil de política ou de uma tarefa de grupo utilizando uma versão posterior do administration plug-in, estes componentes ficam indisponíveis para versões anteriores do administration plug-in. As definições locais do Kaspersky Endpoint Security e as definições das tarefas locais ainda estão disponíveis para o administration plug-in das versões anteriores.

Iniciar e parar o Kaspersky Endpoint Security num computador cliente

Para iniciar ou parar a aplicação num computador cliente:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivo geridos** 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 **Dispositivos**.
4. Selecione 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 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 10 for Windows.
8. Execute as seguintes ações:

   - Para iniciar a aplicação, clique no botão à direita da lista de aplicações da Kaspersky ou execute as seguintes ações:

     a. Selecione **Propriedades** no menu de contexto do Kaspersky Endpoint Security ou clique no botão **Propriedades** localizado na lista de aplicações da Kaspersky.

     É aberta a janela de **configurações da aplicação do Kaspersky Endpoint Security 10 for Windows**.

     b. Na secção **Geral**, clique no botão **Executar** na parte direita da janela.

   - Para parar a aplicação, clique no botão à direita da lista de aplicações da Kaspersky ou execute as seguintes ações:

     a. Selecione **Propriedades** no menu de contexto do Kaspersky Endpoint Security ou clique no botão **Propriedades** localizado na lista de aplicações da Kaspersky.

É aberta a janela de **configurações da aplicação do Kaspersky Endpoint Security 10 for Windows**.

b. Na secção **Geral**, clique no botão **Parar** na parte direita da janela.

Configurar as definições do Kaspersky Endpoint Security

Para configurar as definições do Kaspersky Endpoint Security:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivo geridos** 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 **Dispositivos**.
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 a aplicação Kaspersky Endpoint Security 10 for Windows.
8. Execute uma das seguintes ações:

   - Selecione **Propriedades** no menu de contexto do Kaspersky Endpoint Security 10 for Windows.
   - Clique no botão **Propriedades** na lista de aplicações da Kaspersky.

   É aberta a janela de **configurações da aplicação do Kaspersky Endpoint Security 10 for Windows**.
9. Na secção **Configurações avançadas**, configure as definições do Kaspersky Endpoint Security juntamente com as definições de relatórios e armazenamento.

   As restantes secções da janela de **definições da aplicação do Kaspersky Endpoint Security 10 for Windows** são as mesmas das secções da aplicação padrão do Kaspersky Security Center. É fornecida uma descrição destas secções no *Manual do Administrador do Kaspersky Security Center*.

   > Se uma aplicação estiver sujeita a uma política que proíbe alterações a definições específicas, não poderá editar as mesmas ao configurar as definições da aplicação na secção **Configurações avançadas**.
10. Para guardar as alterações, na janela de **definições da aplicação do Kaspersky Endpoint Security 10 for Windows**, clique em **OK**.

Gerir tarefas

Esta secção descreve como gerir tarefas no Kaspersky Endpoint Security. Pode consultar o *Manual do Administrador do Kaspersky Security Center* para obter mais detalhes sobre a gestão de tarefas através do Kaspersky Security Center.

Sobre as tarefas para o Kaspersky Endpoint Security

O Kaspersky Security Center controla a atividade das aplicações da Kaspersky em computadores cliente através de tarefas. As tarefas implementam as funções administrativas principais como, por exemplo, instalação da chave, verificação do computador e atualizações de bases de dados e de módulos de software da aplicação.

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 um conjunto de computadores que não pertencem a grupos de administração.

  As tarefas para conjuntos de computadores fora dos grupos de administração apenas se aplicam aos computadores cliente especificados nas definições das tarefas. Se forem adicionados novos computadores cliente a um conjunto de computadores para o qual esteja configurada uma tarefa, esta tarefa não se aplica aos novos computadores. Para aplicar a tarefa a estes computadores, crie uma nova tarefa ou edite as definições da tarefa existente.

Para gerir remotamente o Kaspersky Endpoint Security, pode utilizar as seguintes tarefas de qualquer um dos tipos apresentados:

- **Adicionar chave**. O Kaspersky Endpoint Security adiciona uma chave para a ativação da aplicação, incluindo uma chave adicional.
- **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.
- **Inventário**. O Kaspersky Endpoint Security recolhe informações sobre todos os ficheiros executáveis da aplicação armazenados no computador.

  Pode ativar o inventário de módulos DLL e de ficheiros de script. Neste caso, o Kaspersky Security Center receberá informações sobre os módulos DLL carregados num computador com o Kaspersky Endpoint Security instalado e sobre ficheiros que contêm scripts.

  Ativar o inventário de módulos DLL e de ficheiros de script aumenta significativamente a duração de tarefas de inventário e o tamanho da base de dados.
- **Atualização**. O Kaspersky Endpoint Security atualiza bases de dados e módulos da aplicação de acordo com as definições de atualização configuradas.
- **Reverter**. O Kaspersky Endpoint Security reverte a última atualização de bases de dados e módulos.
- **Scan de vírus**. O Kaspersky Endpoint Security verifica a existência de vírus e outras ameaças nas áreas do computador especificadas nas definições da tarefa.

- **A verificar ligação com KSN**. O Kaspersky Endpoint Security envia uma consulta sobre a disponibilidade dos servidores de KSN e atualiza o estado da ligação de KSN.
- **Verificação de integridade**. O Kaspersky Endpoint Security recebe dados sobre o jogo de módulos da aplicação instalados no computador cliente e verifica a assinatura digital de cada módulo.
- **Gestão das contas de Agente de Autenticação**. Enquanto executa esta tarefa, o Kaspersky Endpoint Security gera comandos de remoção, adição ou alteração das contas do Agente de Autenticação.

Pode executar as seguintes ações com tarefas:

- Iniciar, parar, suspender e retomar tarefas.
- Criar novas tarefas.
- Editar definições de tarefas.

Os direitos de acesso às definições das 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.

Configurar o modo de gestão de tarefas

Para configurar o modo para trabalhar com tarefas na interface local do Kaspersky Endpoint Security:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração para o qual pretende configurar o modo para trabalhar com tarefas na interface local do Kaspersky Endpoint Security.
3. Na área de trabalho, selecione o separador **Políticas**.
4. Selecione a política pretendida.
5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.
6. Na secção de **Configurações avançadas**, selecione a subsecção **Definições da aplicação**.
7. Na secção **Modo operativo**:
   - Se pretende permitir que os utilizadores trabalhem com tarefas locais na interface e na linha de comandos do Kaspersky Endpoint Security, selecione a caixa de verificação **Permitir utilização de tarefas locais**.

Se a caixa de verificação estiver desmarcada, as funções das tarefas locais são paradas. Neste modo, as tarefas locais não são executadas de acordo com o agendamento. As tarefas locais também estão indisponíveis para iniciar e editar a interface local do Kaspersky Endpoint Security e quando estão a trabalhar com a linha de comandos.

- Se pretender permitir que os utilizadores visualizem a lista de tarefas de grupo, selecione a caixa de verificação **Permitir que as tarefas sejam apresentadas**.
- Se pretender permitir que os utilizadores alterem as definições das tarefas de grupo, selecione a caixa de verificação **Permitir a gestão de tarefas de grupo**.

8. Clique em **OK** para guardar as alterações.
9. Aplicar a política.

   Consulte o *Manual do Administrador do Kaspersky Security Center* para obter mais informações sobre a aplicação da política do Kaspersky Security Center.

Criar uma tarefa local

Para criar uma tarefa local:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivo geridos** 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 **Dispositivos**.
4. Selecione um computador para o qual pretende criar uma tarefa local.
5. Execute uma das seguintes ações:
   - No menu de contexto do computador cliente, selecione a opção **Todas as tarefas** Criar tarefa.
   - No menu de contexto do computador cliente, selecione **Propriedades**, e na janela **Propriedades:<Nome do computador>** que aparece, no separador **Tarefas**, clique no botão**Adicionar**.
   - Na lista pendente **Realização ação**, selecione **Criar tarefa**.

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

Criar uma tarefa de grupo

Para criar uma tarefa de grupo:

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

2. Execute uma das seguintes ações:

   - Selecione a pasta **Dispositivos geridos** na árvore da Consola de Administração para criar uma tarefa de grupo para todos os computadores geridos pelo Kaspersky Security Center.
   - Na pasta **Dispositivo geridos** 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. Selecione o separador **Tarefas** na área de trabalho.
4. Clique no botão **Criar tarefa**.

   O Assistente de Tarefas é iniciado.

5. Siga as instruções do Assistente de Tarefas.

Criar uma tarefa para uma seleção de dispositivos

Para criar uma tarefa da seleção de dispositivos, realize as operações seguintes:

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 **Criar tarefa**.

   O Assistente de Tarefas é iniciado.

4. Siga as instruções do Assistente de Tarefas.
5. Na janela **Selecionar dispositivos aos quais será atribuída a tarefa** do Assistente, clique no botão **Atribuir tarefa a uma seleção de dispositivos**.
6. Na janela seguinte do Assistente, clique no botão **Selecionar**.

   É apresentada a janela **Seleção de dispositivos**.

7. Selecione os dispositivos necessários.
8. Clique em **OK** na janela **Seleção de dispositivos**.
9. Siga as instruções do Assistente de Tarefas.

Iniciar, parar, suspender e retomar uma tarefa

Se a aplicação Kaspersky Endpoint Security estiver em execução num computador cliente, é possível, iniciar, parar, suspender e retomar uma tarefa neste computador cliente através do Kaspersky Security Center. Quando o Kaspersky Endpoint Security é suspenso, as tarefas em execução são suspensas e não é possível iniciar, parar, suspender ou retomar uma tarefa com o Kaspersky Security Center.

Para iniciar, parar, suspender ou retomar uma tarefa local:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivo geridos** 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 **Dispositivos**.
4. Selecione o computador no qual pretende iniciar, parar, pausar ou retomar uma tarefa local.
5. Clique com o botão direito do rato para visualizar o menu de contexto do computador cliente e selecione **Propriedades**.

   É aberta uma janela de propriedades do computador cliente.
6. Selecione a secção **Tarefas**.

   É apresentada uma lista das tarefas locais na parte direita da janela.
7. Selecione a tarefa local que pretende iniciar, parar, suspender ou retomar.
8. Executar a ação necessária na tarefa utilizando um dos seguintes métodos:

   - Clique com o botão direito do rato para abrir o menu de contexto da tarefa local e selecionar **Executar/Parar/Pausar/Retomar**.
   - Para iniciar ou parar uma tarefa local, clique no botão / à direita da lista de tarefas locais.
   - Execute as seguintes ações:

     a. Clique no botão **Propriedades** abaixo da lista de tarefas local ou selecione **Propriedades** no menu de contexto da tarefa.

     É apresentada a janela **Propriedades: <Nome da tarefa>**.

     b. No separador **Geral**, clique no botão **Executar/Parar/Pausar/Retomar**.

Para iniciar, parar, pausar ou retomar uma tarefa de grupo:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com o nome do grupo de administração para o qual pretende iniciar, parar, pausar ou retomar uma tarefa de grupo.
3. Selecione o separador **Tarefas** na área de trabalho.

   As tarefas de grupo são apresentadas na parte direita da janela.
4. Selecione uma tarefa de grupo que pretende iniciar, parar, pausar ou retomar.
5. Executar a ação necessária na tarefa utilizando um dos seguintes métodos:

   - No menu de contexto da tarefa de grupo, selecione **Executar/Parar/Pausar/Retomar**.
   - Clique no botão / na parte direita da janela para iniciar ou parar uma tarefa de grupo.
   - Execute as seguintes ações:

     a. Clique na ligação **Definições da Tarefa** na parte direita da área de trabalho da Consola de Administração ou selecione **Propriedades** no menu de contexto da tarefa.

É apresentada a janela **Propriedades: <Nome da tarefa>**.

b. No separador **Geral**, clique no botão **Executar/Parar/Pausar/Retomar**.

Para iniciar, parar, pausar ou retomar uma tarefa para uma seleção de computadores:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Tarefas** da árvore da Consola de Administração, selecione a tarefa para o conjunto de computadores que pretende iniciar, parar, pausar ou retomar.
3. Execute uma das seguintes ações:
   - No menu de contexto da tarefa, selecione **Executar/Parar/Pausar/Retomar**.
   - Clique no botão / na parte direita da janela para iniciar ou parar a tarefa para computadores específicos.
   - Execute as seguintes ações:
     a. Clique na ligação **Definições da Tarefa** na parte direita da área de trabalho da Consola de Administração ou selecione **Propriedades** no menu de contexto da tarefa.
     É apresentada a janela **Propriedades: <Nome da tarefa>**.
     b. No separador **Geral**, clique no botão **Executar/Parar/Pausar/Retomar**.

Editar definições de tarefas

Para editar as definições de uma tarefa local:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivo geridos** 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 **Dispositivos**.
4. Selecione um computador para o qual quer configurar definições da aplicação.
5. Clique com o botão direito do rato para visualizar o menu de contexto do computador cliente e selecione **Propriedades**.
   É aberta uma janela de propriedades do computador cliente.
6. Selecione a secção **Tarefas**.
   É apresentada uma lista das tarefas locais na parte direita da janela.
7. Selecione a tarefa local pretendida na lista de tarefas locais.
8. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.

9. Na janela **Propriedades:<Nome da tarefa local>**, selecione a secção **Configuração**.
10. Edite as definições da tarefa local.
11. Para guardar as alterações, na janela **Propriedades: <Nome da tarefa local>**, clique em **OK**.
12. Para guardar as alterações, na janela **Propriedades: <Nome do computador>**, clique em **OK**.

Para editar as definições de uma tarefa de grupo:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos**, abra a pasta com o nome do grupo de administração relevante.
3. Selecione o separador **Tarefas** na área de trabalho.
   As tarefas de grupo são apresentadas na área de trabalho da Consola de Administração.
4. Selecione a tarefa de grupo necessária.
5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.
6. Na janela **Propriedades: <Nome da tarefa de grupo>**, selecione a secção **Configuração**.
7. Edite as definições da tarefa de grupo.
8. Para guardar as alterações, na janela **Propriedades: <Nome da tarefa de grupo>**, clique em **OK**.

Para editar as definições de uma tarefa para uma seleção de computadores:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Tarefas** da árvore da Consola de Administração, selecione a tarefa para a seleção de computadores cujas definições pretende editar.
3. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.
4. Na janela **Propriedades: <Nome da tarefa para a seleção de computadores>**, selecione a secção **Configuração**.
5. Editar as definições de tarefas para a seleção de computadores.
6. Para guardar as alterações, na janela **Propriedades: <Nome da tarefa para a seleção de computadores>**, clique em **OK**.

Exceto a secção **Configuração**, todas as secções na janela de propriedades da tarefa são idênticas às usadas no Kaspersky Security Center. Para obter uma descrição detalhada, consulte o *Manual do Administrador do Kaspersky Security Center*. A secção **Definições** contém as definições específicas do Kaspersky Endpoint Security 10 for Windows. Os seus conteúdos dependem da tarefa selecionada ou do tipo de tarefa.

Gerir políticas

Esta secção descreve a criação e configuração de políticas para o Kaspersky Endpoint Security. Para obter informações mais detalhadas sobre a gestão do Kaspersky Endpoint Security utilizando as políticas do Kaspersky Security Center, consulte o *Manual do Administrador do Kaspersky Security Center*.

Sobre políticas

Pode utilizar políticas para aplicar definições idênticas do Kaspersky Endpoint Security em todos os computadores cliente de um grupo de administração.

Pode alterar localmente os valores das definições especificadas por uma política para computadores individuais num grupo de administração que utilize o Kaspersky Endpoint Security. Apenas pode alterar localmente as definições cuja alteração não esteja proibida pela política.

A possibilidade de editar uma definição da aplicação num computador cliente é determinada pelo estado "bloquear" da definição na política:

- Se uma definição estiver "bloqueada" (), não pode editar localmente o valor desta definição. O valor de configuração especificado pela política é utilizado para todos os computadores de cliente dentro do grupo de administração.
- Quando uma definição está "desbloqueada" (), pode editar a definição localmente. Uma definição configurada localmente é aplicada a todos os computadores cliente no grupo de administração. A definição configurada pela política não é aplicada.

Depois de a política ser aplicada pela primeira vez, as definições locais da aplicação são modificadas em função das definições de políticas.

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.

Os âmbitos funcionais seguintes do Kaspersky Endpoint Security são destacados:

- Proteção de Antivírus. O âmbito funcional inclui Antivírus de Ficheiros, Antivírus de E-mail, Antivírus de Internet, Antivírus de MI, Verificação de Vulnerabilidade e tarefas de verificação.
- Controlo de Arranque das Aplicações. O âmbito funcional inclui o componente Controlo do Arranque das Aplicações.
- Controlo de dispositivos. O âmbito funcional inclui o componente Controlo de Dispositivos.
- Encriptação. O âmbito funcional inclui componentes de encriptação de unidade de disco rígido, ficheiros e pastas.

- Zona confiável. O âmbito funcional inclui a Zona confiável.
- Controlo de Internet. O âmbito funcional inclui o componente Controlo de Internet.
- Prevenção de Intrusões. Este âmbito funcional inclui Monitor de Atividade das Aplicações, Monitor de Vulnerabilidades, Firewall, Bloqueio de Ataques de Rede e Controlo de Privilégios das Aplicações.
- Funcionalidade básica. Este âmbito funcional inclui definições gerais da aplicação que não estão especificadas para outros âmbitos funcionais, incluindo: licenciamento, definições da KSN, tarefas de inventário, tarefas de atualização dos módulos e bases de dados da aplicação, Autodefesa, definições avançadas da aplicação, relatórios e armazenamentos, definições de proteção de password e definições da interface da aplicação.

Pode realizar as operações seguintes com a política:

- Criar uma política.
- Editar definições de políticas.

  Se a conta de utilizador com a qual acedeu ao Servidor de Administração não tem permissões para editar as definições de determinados âmbitos funcionais, as definições destes âmbitos funcionais não estão disponíveis para edição.

- Apagar uma política.
- Alterar o estado da política.

Para obter informações sobre a utilização de políticas que não estão relacionadas com a interação com o Kaspersky Endpoint Security, consulte o *Manual do Administrador do Kaspersky Security Center*.

Criar uma política

Para criar uma política:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Execute uma das seguintes ações:
   - Selecione a pasta **Dispositivos geridos** na árvore da Consola de Administração se pretender criar uma política para todos os computadores geridos pelo Kaspersky Security Center.
   - Na pasta **Dispositivo geridos** 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 **Políticas**.
4. Execute uma das seguintes ações:
   - Clique no botão **Criar políticas**.
   - Clique com o botão direito do rato para abrir o menu de contexto e selecione **Criar** Política.

   O Assistente de Política é iniciado.

5. Siga as instruções do Assistente de Política.

Editar definições de políticas

Para editar definições de políticas:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. Na pasta **Dispositivos geridos** da árvore da Consola de Administração, abra a pasta com nome do grupo de administração relevante para o qual pretende editar as definições de políticas.
3. Na área de trabalho, selecione o separador **Políticas**.
4. Selecione a política pretendida.
5. Abra a janela **Propriedades:<Nome da política>** utilizando um dos seguintes métodos:
   - No menu de contexto da política, selecione **Propriedades**.
   - Clique na ligação **Configurar política** localizada na parte direita da área de trabalho da Consola de Administração.

   As definições de política do Kaspersky Endpoint Security 10 for Windows incluem as definições de componentes e as definições da aplicação. As secções **Proteção de Antivírus** e **Controlo de terminal** da janela **Propriedades: <Nome de política>** apresenta as definições dos componentes de proteção e controlo, a secção **Encriptação de Dados** apresenta as definições de encriptação de ficheiros e pastas, e a secção de **Configurações avançadas** apresenta as definições da aplicação.

   Para ativar a apresentação das definições de encriptação de dados e das definições do componente de controlo nas definições de política, tem de selecionar as caixas de verificação correspondentes na janela **Definições de Interface** do Kaspersky Security Center.
6. Editar as definições de políticas.
7. Para guardar as alterações, na janela **Propriedades: <Nome da política>** clique em **OK**.

Selecionar as definições a apresentar na política do Kaspersky Security Center

Para selecionar as definições a apresentar na política do Kaspersky Security Center:

1. Abra a Consola de Administração do Kaspersky Security Center.
2. No menu de contexto do nó do **Servidor de Administração – <Nome do computador>** da árvore da Consola de Administração, selecione Ver Configurações da Interface de Utilizador.

   A janela **Configurações da Interface de Utilizador** é apresentada.
3. Na janela **Configurações da Interface de Utilizador**, selecione as caixas de verificação à frente das definições que em frente das definições que pretende que sejam apresentadas nas definições de criação da política do Kaspersky Security Center e nas propriedades da política:

- Selecione a caixa de verificação **Apresentar componentes de controlo de terminal** para permitir a apresentação das definições dos componentes de controlo na janela do Assistente de Nova Política do Kaspersky Security Center e nas propriedades de política.

- Selecione a caixa de verificação **Apresentar encriptação e proteção de dados** para permitir a apresentação das definições de encriptação de dados na janela do Assistente de Nova Política do Kaspersky Security Center e nas propriedades de política.

4. Clique em **OK**.

Enviar mensagens de utilizador para o servidor do Kaspersky Security Center

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 de Arranque 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 de Arranque 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 utilizado para enviar mensagens e o modelo utilizado depende da existência de uma política do Kaspersky Security Center ativa em execução no computador com o Kaspersky Endpoint Security instalado e da existência de uma ligação ao 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 Security Center 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 Security Center instalado, é enviada a mensagem padrão para o Servidor de Administração do Kaspersky Security Center.

  Neste caso, as mensagens de utilizador estão disponíveis para visualização no armazenamento de eventos do Kaspersky Security Center. Os campos de mensagem estão preenchidos com os valores dos campos do modelo definidos na política do Kaspersky Security Center.

- Se uma política de fora do escritório do Kaspersky Security Center estiver em execução no computador com o Kaspersky Endpoint Security instalado, o método utilizado para enviar 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.

Ver as mensagens dos utilizadores no armazenamento de eventos do Kaspersky Security Center

Os dispositivos de Controlo de Arranque das Aplicações, Controlo de Dispositivos e Controlo de Internet permitem aos utilizadores da rede local que tenham o Kaspersky Endpoint Security instalado enviar mensagens ao administrador.

Um utilizador pode enviar mensagens ao administrador utilizando dois métodos:

- Como um evento no armazenamento de eventos do Kaspersky Security Center.

  O evento de utilizador é enviado para o armazenamento de eventos do Kaspersky Security Center se a aplicação do Kaspersky Endpoint Security instalada no computador do utilizador estiver a funcionar sob uma política ativa.

- Uma mensagem de e-mail.

  A informação do utilizador é enviada por e-mail se a aplicação do Kaspersky Endpoint Security que está instalada no computador do utilizador não estiver a executar uma política ou estiver a executar uma política de fora do escritório.

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 **Servidor de Administração** da árvore da Consola de Administração, selecione o separador **Eventos**.

   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 **de Eventos de seleção**, selecione **Pedidos do utilizador**.
4. Selecione a mensagem a enviar ao administrador.
5. Abra a janela **Definições do evento** de uma das seguintes formas:

   - Clique com o botão direito do rato no evento. No menu de contexto que é aberto, selecione **Propriedades**.
   - Clicar no botão **Abrir a janela de propriedades do evento** na parte direita da área de trabalho da Consola de Administração.

Participar na Kaspersky Security Network

Esta secção contém informações sobre a participação na Kaspersky Security Network, bem como instruções sobre como ativar ou desativar a utilização da Kaspersky Security Network.

Sobre a participação na Kaspersky Security Network

Para proteger o seu computador de forma mais eficaz, o Kaspersky Endpoint Security utiliza dados recolhidos de utilizadores em todo o mundo. A *Kaspersky Security Network* foi concebida para recolher 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.

Conforme a localização da infraestrutura, existe um serviço global da KSN (a infraestrutura é alojada pelos servidores da Kaspersky) e um serviço privado da KSN (a infraestrutura é alojada por servidores de terceiros, por exemplo na rede do fornecedor de serviços da Internet).

Após alterar a licença, envie os detalhes da nova chave ao fornecedor de serviços para que possa utilizar o KSN Privado. Caso contrário, a troca de dados com a KSN não será possível.

Graças aos utilizadores que participam na KSN, a Kaspersky consegue recolher rapidamente informações sobre o tipo e a origem das ameaças, desenvolver soluções para as neutralizar e minimizar o número de falsos diagnósticos positivos apresentados pelos componentes da aplicação.

Durante a participação na KSN, a aplicação envia automaticamente a estatística gerada durante a operação da aplicação para a KSN. A aplicação também pode enviar determinados ficheiros (ou partes de ficheiros) que os intrusos possam utilizar para danificar o computador ou os dados de verificação adicional da Kaspersky.

Não são recolhidos, processados ou armazenados quaisquer dados pessoais. 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 que contém 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, a Kaspersky pode publicar bases de dados de antivírus da aplicação que desativam temporariamente ou restringem em parte os pedidos à Kaspersky Security Network. Neste caso, o estado da ligação à KSN aparece como *Ativado com restrições*.

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 KSN Proxy armazena dados processados, reduzindo a carga na ligação de rede externa e tornando mais rápida a receção de informação solicitada pelo computador do utilizador.

Pode obter mais detalhes sobre o serviço KSN Proxy no *Manual do Administrador do Kaspersky Security Center*.

As definições do KSN Proxy podem ser configuradas nas propriedades da política do *Kaspersky Security Center*.

A participação na Kaspersky Security Network é voluntária. A aplicação convida o utilizador a participar na KSN durante a configuração inicial da aplicação. Os utilizadores podem começar ou interromper a participação na KSN em qualquer momento.

Ativar e desativar a utilização da Kaspersky Security Network

Para ativar ou desativar a utilização da Kaspersky Security Network:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, na secção **Configurações Avançadas**, selecione a subsecção **Configurações da KSN**.

   As definições da Kaspersky Security Network são apresentadas na parte direita na janela.
3. Execute uma das seguintes ações:
   - Se pretender ativar a utilização do Kaspersky Security Network, selecione a caixa de verificação **Aceito a Declaração da KSN e os termos da participação**.
   - Se pretender desativar a utilização do Kaspersky Security Network, desmarque a caixa de verificação **Aceito a Declaração da KSN e os termos da participação**.
4. Para guardar as alterações, clique no botão **Guardar**.

Verificar a ligação à Kaspersky Security Network

Para testar a ligação à Kaspersky Security Network:

1. Abra a janela principal da aplicação.
2. Na parte superior da janela, clique no botão **Kaspersky Security Network**.

   É aberta a janela **Kaspersky Security Network**.

   A parte esquerda da janela **Kaspersky Security Network** indica o modo de ligação à Kaspersky Security Network, sob a forma de um botão **KSN** redondo:
   - Se o Kaspersky Endpoint Security não estiver ligado à Kaspersky Security Network, o botão **KSN** é apresentado a cinzento. O estado apresentado por baixo do botão **KSN** indica *Desativado*.
   - Se o Kaspersky Endpoint Security estiver ligado à Kaspersky Security Network e os servidores da KSN estiverem disponíveis, o botão **KSN** é apresentado a verde. A seguinte informação é apresentada sob o botão **KSN**: estado *Ativado*, tipo de KSN em utilização – **KSN privado** ou **KSN Global** e a hora da última

sincronização com os servidores da KSN. A parte direita da janela apresenta as estatísticas da reputação dos ficheiros, recursos da Internet e software.

O Kaspersky Endpoint Security recolhe dados estatísticos sobre a utilização da KSN quando abre a janela **Kaspersky Security Network**. As estatísticas não são atualizadas em tempo real.

- Se o Kaspersky Endpoint Security estiver ligado à Kaspersky Security Network e os servidores da KSN não estiverem disponíveis, o botão **KSN** é apresentado a vermelho. O estado apresentado por baixo do botão **KSN** indica *Ativado*.

  Se a hora da última sincronização com os servidores da KSN exceder 15 minutos ou apresentar o estado *Desconhecido*, isso significa que os servidores da KSN não estão disponíveis. Nesta situação, é recomendado que contacte o Suporte Técnico ou o seu fornecedor de serviços.

  A ligação aos servidores da Kaspersky Security Network pode perder-se pelas seguintes razões:

  - O computador não está ligado à Internet.
  - A aplicação não foi ativada ou a licença expirou.
  - Foram detetados problemas relacionados com a chave (por exemplo, a chave foi adicionada à lista negra).

Verificar a reputação de um ficheiro na Kaspersky Security Network

O serviço da KSN permite-lhe recuperar a informação sobre aplicações que estão incluídas nas bases de dados de reputação da Kaspersky. Tal permite uma gestão flexível das políticas de inicialização de aplicações ao nível da empresa, impedindo a inicialização de adware e programas que podem ser utilizados por criminosos para danificar o seu computador ou dados pessoais.

Para verificar a reputação de um ficheiro na Kaspersky Security Network:

1. Clique com o botão direito para abrir o menu de contexto do ficheiro cuja reputação pretende verificar.
2. Selecione a opção **Verificar reputação na KSN**.

Esta opção está disponível caso tenha aceite os termos da Declaração de Recolha de Dados da KSN.

Esta ação abre a janela **<Nome de ficheiro> - Reputação na KSN**. A janela **<Nome de ficheiro> - a Reputação na KSN** apresenta a seguinte informação sobre o ficheiro que está a ser verificado:

- **Caminho**. Caminho no qual o ficheiro é guardado para o disco.
- **Versão**. Versão da aplicação (informação apresentada apenas para ficheiros executáveis).
- **Assinatura digital**. Presença de uma assinatura digital no ficheiro.
- **Assinado**. Data na qual o certificado foi assinado com uma assinatura digital.

- **Criado**. Data de criação do ficheiro.
- **Modificado**. Data da última modificação do ficheiro.
- **Tamanho**. Espaço em disco ocupado pelo ficheiro.
- Informação sobre quantos utilizadores confiam no ficheiro ou o bloqueiam.

Proteção melhorada com a Kaspersky Security Network

A Kaspersky oferece aos utilizadores um nível adicional de proteção através da Kaspersky Security Network. Este método de proteção foi concebido para combater ameaças avançadas persistentes e ataques a vulnerabilidades conhecidas. Tecnologias de nuvem integrada e os conhecimentos dos analistas de vírus da Kaspersky tornam o Kaspersky Endpoint Security na seleção superior para proteção contra as mais sofisticadas ameaças de rede.

Os detalhes sobre a proteção avançada no Kaspersky Endpoint Security estão disponíveis no site da Kaspersky.

Fontes de informação sobre a aplicação

Página do Kaspersky Endpoint Security no website da 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.

Página do Kaspersky Endpoint Security na Base de Conhecimento

A Base de conhecimento é uma secção do site de Suporte Técnico.

Na página do Kaspersky Endpoint Security na Base de Conhecimento pode ler artigos que fornecem informação útil, recomendações e respostas às perguntas frequentes sobre como comprar, instalar, e utilizar a aplicação.

Os artigos da Base de Conhecimento podem responder a questões relacionadas não só com o Kaspersky Endpoint Security, mas também com outras aplicações da Kaspersky. Os artigos da Base de Conhecimentos podem conter também notícias do Suporte Técnico.

Discutir as aplicações da Kaspersky no Fórum

Se a sua questão não requer uma resposta urgente, pode discuti-la com os especialistas da Kaspersky e outros utilizadores no nosso Fórum.

Neste fórum, pode visualizar os tópicos existentes, deixar os seus comentários e criar novos tópicos de discussão.

Contactar o Suporte Técnico

Esta secção descreve a forma como obter suporte técnico e os termos de acordo com os quais é disponibilizado.

Como obter suporte técnico

Se não conseguir encontrar uma solução para o seu problema na documentação da aplicação ou numa das fontes de informação sobre a aplicação, é recomendado contactar o Suporte Técnico. Os especialistas do Suporte Técnico irão responder às suas questões sobre a instalação e utilização da aplicação.

O suporte técnico está disponível apenas para utilizadores que adquiriram uma licença comercial. Os utilizadores que receberam uma licença de avaliação não têm direito ao suporte técnico.

Antes de contactar o Suporte Técnico, leia as regras relativas ao suporte técnico.

Pode contactar o Suporte Técnico através de uma das seguintes formas:

- Contactando o Suporte Técnico por telefone
- Enviando um pedido ao Suporte Técnico da Kaspersky através do portal Kaspersky CompanyAccount

Suporte Técnico por telefone

Pode contactar os representantes do Suporte Técnico a partir da maior parte das regiões em todo o mundo. Pode encontrar informações sobre como receber suporte técnico na sua região e sobre os contactos do Suporte Técnico no site de Suporte técnico da Kaspersky.

Antes de contactar o Suporte Técnico, leia as regras relativas ao suporte técnico.

Suporte Técnico através de Kaspersky CompanyAccount

Kaspersky CompanyAccount é um portal para empresas que utilizam aplicações da Kaspersky. O portal Kaspersky CompanyAccount é concebido para facilitar a interação entre utilizadores e especialistas da Kaspersky através de pedidos por via eletrónica. Pode utilizar o portal Kaspersky CompanyAccount para monitorizar o estado dos seus pedidos eletrónicos guardar um histórico desses pedidos.

Pode registar todos os funcionários da sua organização numa conta única em Kaspersky CompanyAccount. Uma conta única permite-lhe gerir de forma central os pedidos eletrónicos dos funcionários registados na Kaspersky e também gerir os privilégios desses funcionários através do Kaspersky CompanyAccount.

O portal Kaspersky CompanyAccount está disponível nos seguintes idiomas:

- Inglês
- Espanhol

- Italiano
- Alemão
- Polaco
- Português
- Russo
- Francês
- Japonês

Para saber mais sobre o Kaspersky CompanyAccount, visite o site do Suporte Técnico.

Recolher informação para o Suporte Técnico

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 e descargas de falhas da aplicação.

Pode recolher as informações necessárias com a ajuda do Kaspersky Endpoint Security. As informações recolhidas podem ser guardadas na unidade de disco rígido e carregadas mais tarde, quando lhe for conveniente.

Enquanto efetuam o diagnóstico, os especialistas do Suporte Técnico podem pedir-lhe para alterar definições da aplicação por:

- Ativar a funcionalidade que recolhe 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 e transmissão das informações de diagnóstico recolhidas.
- 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 linha de comando adicionais, módulos de depuração, utilitários específicos, etc.) e irão informá-lo sobre o âmbito dos dados reunidos para depuração. As informações de diagnóstico expandido reunidas são guardadas no computador do utilizador. Os dados reunidos não são transmitidos automaticamente para a Kaspersky.

As definições utilizadas para determinar o endereço do servidor descarga para envio de ficheiros de descarga para a Kaspersky são guardadas no computador do utilizador. Se necessário, os valores destas definições podem ser editados na chave do registo do sistema operativo `"DumpServerConfigUrl"="https://dmpcfg.kaspersky-labs.com/dumpserver/config.xml"`.

As operações indicadas acima devem ser executadas apenas sob a supervisão dos especialistas de Suporte Técnico, seguindo as suas instruções. Alterações não supervisionadas às definições da aplicação executadas de formas diferentes das descritas no Manual do Administrador ou das instruções dos especialistas de Suporte Técnico podem tornar o sistema operativo mais lento ou interromper o seu funcionamento, afetar a segurança do computador ou comprometer a disponibilidade e a integridade dos dados processados.

Criar um ficheiro de rastreio

Para criar um ficheiro de rastreio:

1. Abra a janela principal da aplicação.
2. Na janela da aplicação principal, clique no botão .
   É aberta a janela **Suporte**.
3. Na janela **Suporte**, clique no botão **Rastreio do sistema**.
   É aberta a janela **Informação para o Suporte Técnico**.
4. Para iniciar o processo de rastreio, selecione a caixa de verificação **Ativar rastreio**.
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. Reproduza a situação em que o problema ocorreu.
7. Para parar o processo de rastreio, regresse à janela **Informação para o Suporte Técnico** e desmarque a caixa de verificação **Ativar rastreio**.

Depois de criar o ficheiro de rastreio, pode carregar os resultados do rastreio para o servidor da Kaspersky.

Conteúdos e armazenamento dos ficheiros de rastreio

O utilizador é responsável por garantir a segurança dos dados recolhidos, em particular, por monitorizar e restringir o acesso aos dados recolhidos armazenados no computador, até que os mesmos sejam enviados à Kaspersky.

Os ficheiros de rastreio são armazenados no seu computador de forma modificada que não pode ser lida desde que a aplicação esteja a ser utilizada, sendo permanentemente apagados quando a aplicação é removida.

Os ficheiros de rastreio são armazenados na pasta ProgramData\Kaspersky Lab.

O ficheiro de rastreio tem o seguinte formato de nome: `KES<version number_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log.enc1`.

O ficheiro de rastreio do Agente de Autenticação é guardado na pasta de informação de volume de sistema com o nome seguinte: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Pode ver os dados guardados nos ficheiros de rastreio. Contacte o Suporte técnico da Kaspersky para obter informações sobre como ver os dados.

Todos os ficheiros de rastreio contêm os dados comuns seguintes:

- Hora do evento.
- Número da linha de execução.

  O ficheiro de rastreio do Agente de Autenticação não contém esta informação.

- O componente da aplicação que causou o evento.
- O nível de gravidade do evento (evento informativo, de aviso, crítico, erro).
- Uma descrição do evento que envolve a execução do comando por um componente da aplicação e o resultado da execução deste comando.

Conteúdos dos ficheiros de rastreio SRV.log, GUI.log e ALL.log

Os ficheiros de rastreio SRV.log, GUI.log e ALL.log podem armazenar a informação seguinte além 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.
- 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 tráfego é registado em ficheiros de rastreio apenas de trafmon2.ppl.
- 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.

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.

Conteúdos dos ficheiros de rastreio dos plug-ins da aplicação

Os ficheiros de rastreio dos plug-ins da aplicação contêm as informações seguintes além dos dados gerais:

- O ficheiro de rastreio shellex.dll.log do plug-in que inicia a tarefa de verificação a partir do menu de contexto contém informação sobre a execução da tarefa de verificação e dados necessários para depurar o plug-in.
- O ficheiro de rastreio mcou.OUTLOOK.EXE do Antivírus de E-mail pode conter partes de mensagens de e-mail, incluindo endereços de e-mail.

Conteúdos do ficheiro de rastreio do Agente de Autenticação

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.

Ativar ou desativar a transmissão de ficheiros de descarga e rastreio para a Kaspersky

Para ativar ou desativar a transmissão de ficheiros de descarga e rastreio para a Kaspersky:

1. Abra a janela de definições da aplicação.
2. Na parte esquerda da janela, selecione a secção **Configurações avançadas**.

   As configurações avançadas da aplicação são apresentadas na parte direita da janela.
3. Na secção **Modo de funcionamento**, clique no botão **Configuração**.

   É apresentada a janela **Modo operativo** abre-se.
4. Na janela de **Modo operativo**, selecione a caixa de verificação **Ativar gravação de descarga** para permitir que a registe informações nos ficheiros de descarga da aplicação.
5. Execute uma das seguintes ações:

   - Selecione a caixa de verificação **Enviar ficheiros de descarga e de rastreio para a Kaspersky** se pretender que a aplicação apresente uma confirmação na janela **Carregar informações para Suporte Técnico para o servidor** para enviar ficheiros de descarga de memória e de rastreio para a Kaspersky para análise das causas da falha da aplicação no próximo arranque da aplicação.

- Caso contrário, desmarque a caixa de verificação **Enviar ficheiros de descarga e de rastreio para a Kaspersky**.

6. Clique em **OK** na janela **Modo de funcionamento**.

7. Para guardar as alterações clique no botão **Guardar** na janela principal da aplicação.

Enviar ficheiros para o servidor de Suporte Técnico

Os ficheiros que contenham informação sobre o sistema operativo, ficheiros de rastreio e ficheiros de descarga devem ser enviados aos especialista do Suporte técnico da Kaspersky.

Para enviar ficheiros para o servidor de Suporte Técnico:

1. Reinicie o Kaspersky Endpoint Security após qualquer falha durante o seu funcionamento.

   Esta ação abre a janela **Falha da inicialização anterior da aplicação**.

   > A janela **Falha da inicialização anterior da aplicação** será apresentada sempre que o Kaspersky Endpoint Security for iniciado (inclusive depois de reiniciar o computador) até que envie os ficheiros de descarga ou de rastreio para o Suporte Técnico ou até clicar no botão **Não enviar**.

2. Na janela **Falha da inicialização anterior da aplicação**, abra a lista de ficheiros gerados clicando em **aqui**.

3. Selecione as caixas de verificação junto aos ficheiros que pretende enviar para o Suporte Técnico.

4. Clique no botão **Mostrar texto da declaração**.

   É apresentada a janela **Declaração de Fornecimento de Dados**.

5. Leia o texto da Declaração de Fornecimento de Dados e clique no botão **Fechar**.

6. Na janela **Falha da inicialização anterior da aplicação**, selecione a caixa de verificação **Aceito a Declaração de Fornecimento de Dados**.

7. Clique no botão **Enviar**.

   Esta ação abre a janela **Número de pedido**.

8. Na janela **Número de pedido**, especifique o número que foi atribuído ao seu pedido quando contactou com o Suporte Técnico através do Kaspersky CompanyAccount.

9. Clique em **OK**.

Os ficheiros de dados selecionados são colocados em pacotes e enviados para o servidor de Suporte Técnico.

Ativar e desativar a proteção de ficheiros de descarga e de rastreio

Os ficheiros de descarga e de rastreio contêm informações sobre o sistema operativo, bem como sobre dados confidenciais do utilizador. Para evitar o acesso não autorizado a estes dados, pode ativar a proteção de ficheiros de descarga e de rastreio.

Se a proteção de ficheiros de descarga e de rastreio estiver ativada, os ficheiros podem ser acedidos pelos seguintes utilizadores:

- Os ficheiros de rastreio podem ser acedidos pelo administrador do sistema e pelo administrador local, bem como pelo utilizador que ativou o registo de ficheiros de descarga e de rastreio.
- Os ficheiros de rastreio podem ser acedidos apenas pelo administrador do sistema e pelo administrador local.

Para ativar ou desativar a proteção de ficheiros de descarga e de rastreio:

1. Abra a janela de definições da aplicação.
2. Selecione a secção **Configurações Avançadas** à esquerda.

   As definições da aplicação são apresentadas na parte direita da janela.
3. Na secção **Modo de funcionamento**, clique no botão **Configuração**.

   É apresentada a janela **Modo operativo** abre-se.
4. Execute uma das seguintes ações:

   - Selecione a caixa de verificação **Ativar proteção de ficheiros de descarga e de rastreio** se pretender ativar a proteção.
   - Desmarque a caixa de verificação **Ativar proteção de ficheiros de descarga e de rastreio** se pretender desativar a proteção.
5. Clique em **OK** na janela **Modo de funcionamento**.
6. Para guardar as alterações clique no botão **Guardar** na janela principal da aplicação.

Os ficheiros de descarga e de rastreio que foram editados enquanto a proteção estava ativa permanecem protegidos mesmo depois de esta ser desativada.

Glossário

Agente de Autenticação

Interface para passar pelo 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 do sistema.

Agente de Rede Connector

A funcionalidade da aplicação que liga a aplicação ao Network Agent. O Network Agent permite a administração remota da aplicação através do Kaspersky Security Center.

Âmbito de proteção

Objetos que estão a ser constantemente verificados pela proteção de antivírus 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.

Análise de assinaturas

Uma tecnologia de deteção de ameaças que utiliza as bases de dados do Kaspersky Endpoint Security, que contêm descrições das ameaças conhecidas e dos métodos para apagar as mesmas. A proteção que utiliza a análise de assinaturas fornece um nível de segurança minimamente aceitável. De acordo com as recomendações dos especialistas da Kaspersky, este método está sempre ativado.

Análise heurística

A tecnologia foi desenvolvida para detetar ameaças que não é possível detetar utilizando a versão atual das bases de dados da aplicação da Kaspersky. Permite detetar ficheiros que podem estar infetados com um vírus desconhecido ou com uma variante de um vírus conhecido.

Arquivo

Um ou vários ficheiros compactados num único ficheiro comprimido. Uma aplicação especializada, denominada arquivador, é necessária para compactar e descompactar dados.

Atualização

O procedimento de substituição ou adição de novos ficheiros (bases de dados ou módulos da aplicação) obtidos a partir dos servidores de atualização da Kaspersky.

Base de dados de endereços da Web maliciosos

Uma lista de endereços de Internet 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.

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.

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

Documento eletrónico que contém a chave privada e informações sobre o proprietário da chave e o âmbito desta, e que confirma que a chave pública pertence ao proprietário. O certificado tem de ser assinado pelo centro de certificação que o emitiu.

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.

Cópia de segurança

É tentado um armazenamento especial de cópias de segurança de ficheiros que são criados antes da desinfeção ou eliminação.

Correção

Uma pequena adição à aplicação que corrige erros de programação descobertos durante a operação da aplicação ou instala atualizações.

Definições da aplicação

As definições da aplicação comuns a todos os tipos de tarefas e que regem o funcionamento geral da aplicação, tais como as definições de desempenho da aplicação, as definições de relatórios e as definições de cópia de segurança.

Definições de tarefas

Definições da aplicação específicas para cada tipo de tarefas.

Desinfeção

Um método de processamento de objetos infetados que resulta numa recuperação total ou parcial dos dados. Nem todos os objetos infetados podem ser desinfetados.

Emissor do certificado

O centro de certificação que emitiu o certificado.

Explorações

Programe código que utilize algum tipo de vulnerabilidade no sistema ou no software. As explorações de vulnerabilidades são utilizadas frequentemente para instalar software malicioso no computador sem o conhecimento do utilizador.

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 provavelmente infetado

Um ficheiro que contém código modificado de um vírus conhecido ou código semelhante ao de um vírus, mas que ainda não é conhecido pela Kaspersky. Os ficheiros provavelmente infetados são detetados pelo Analisador Heurístico.

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, password e porta de ligação HTTP 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 contexto da Proteção de 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.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 nenhuma funcionalidade de encriptação 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.

Lista negra de endereços

Uma lista de endereços de e-mail para os quais todas as mensagens de entrada são bloqueadas pela aplicação da Kaspersky, independentemente do conteúdo das mensagens.

Máscara de ficheiro

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:

- ***** — substitui qualquer zero ou mais caracteres.
- **?** — substitui qualquer carácter.

Tenha em atenção que o nome e a extensão estão sempre separados por um ponto final.

Módulos da aplicação

Os ficheiros incluídos no ficheiro de configuração da aplicação, que implementam as funcionalidades principais da aplicação. Um módulo executável em separado corresponde a cada tipo de tarefa executada pela aplicação (Proteção em tempo real, Verificação a pedido e Atualização). Ao iniciar uma verificação completa do computador a partir da janela principal da aplicação, é iniciado o módulo desta tarefa.

Mover ficheiros para a Quarentena

Um método de processamento do ficheiro provavelmente infetado em que o acesso ao ficheiro é bloqueado e o ficheiro movido da sua localização original para a pasta de quarentena, onde é mantido encriptado para excluir a ameaça de infeção.

Network Agent

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.

Objeto OLE

Um ficheiro anexado ou um ficheiro incorporado noutro ficheiro. As aplicações da Kaspersky permitem a verificação da existência de vírus em objetos OLE. Por exemplo, se inserir uma tabela do Microsoft Office Excel® num documento do Microsoft Office Word, a tabela é verificada como um objeto OLE.

Quarentena

O Kaspersky Endpoint Security coloca os ficheiros provavelmente infetados nesta pasta. Os ficheiros em quarentena são armazenados de forma encriptada.

Requerente do Certificado

Titular de uma chave privada ligada a um certificado. Pode ser um utilizador, aplicação, qualquer objeto virtual, computador ou serviço.

Serviço de rede

Conjunto de parâmetros que define a atividade de rede. Para esta atividade de rede, pode criar uma regra de rede que regula o funcionamento da Firewall.

Servidor de Administração

Um componente do Kaspersky Security Center que armazena centralmente informações sobre todas as aplicações da Kaspersky instaladas na rede da empresa. Também pode ser utilizado para gerir estas aplicações.

Sites de phishing

Um tipo de fraude da Internet em que as mensagens de e-mail são enviadas com o objetivo de roubar dados confidenciais, que são mais frequentemente dados financeiros.

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.

Thumbprint do Certificado

Informação utilizada para identificar uma chave de certificado. Uma thumbprint é criada através da aplicação de uma aplicando uma função de hash criptográfica ao valor da chave.

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.

Informação sobre código de terceiros

A informação sobre código de terceiros está incluída no ficheiro legal_notices.txt, na pasta de instalação da aplicação.

Avisos de marca comercial

As marcas comerciais registadas e marcas de serviços são propriedade dos respetivos detentores.

Adobe, Acrobat e Shockwave são marcas comerciais ou marcas comerciais registadas da Adobe Systems Incorporated nos Estados Unidos e/ou em todo o mundo.

Mac e FireWire são marcas comerciais da Apple, Inc. registadas nos Estados Unidos e em todo o mundo.

AutoCAD é uma marca comercial ou marca comercial registada da Autodesk, Inc. e/ou das suas subsidiárias/filiais nos Estados Unidos e em todo o mundo.

A marca nominativa Bluetooth e o respetivo logótipo são propriedade da Bluetooth SIG, Inc.

Borland é uma marca comercial ou marca comercial registada da Borland Software Corporation nos Estados Unidos e em todo o mundo.

Citrix e Citrix Provisioning Services são marcas comerciais da Citrix Systems, Inc. e/ou as suas filiais registadas no instituto de patentes dos Estados Unidos e outros países.

o dBase é uma marca comercial da dataBased Intelligence, Inc.

EMC e SecurID são marcas comerciais da EMC Corporation ou marcas comerciais registadas da EMC Corporation nos EUA ou em todo o mundo.

ICQ é uma marca comercial e/ou marca de serviço da ICQ LLC.

Intel e Pentium são marcas comerciais da Intel Corporation registadas nos Estados Unidos e em todo o mundo.

Logitech é uma marca comercial ou marca comercial registada da Logitech Company nos EUA e em todo o mundo.

Mail.ru é uma marca comercial registada da Mail.Ru LLC.

Microsoft, Windows, Internet Explorer, Access, Excel, PowerPoint, Outlook, Outlook Express, Windows Server, Visual Basic, Visual FoxPro, BitLocker, LifeCam Cinema, PowerShell e Surface são marcas comerciais da Microsoft Corporation registadas nos Estados Unidos e em todo o mundo.

Mozilla e Thunderbird são as marcas comerciais da Mozilla Foundation.

Novell é uma marca comercial da Novell Inc. registada nos E.U.A e em todo o mundo.

Java e JavaScript são marcas comerciais registadas da Oracle Corporation e/ou das suas filiais.

SafeNet é a marca comercial registada da SafeNet, Inc.

UNIX é uma marca comercial registada nos Estados Unidos e em todo o mundo e é utilizada com a licença da X/Open Company Limited.