System Center

Endpoint Protection para o Mac

Manual de Instalação e Guia do Utilizador

Microsoft

Índice

System Center Endpoint Protection

Dado que a popularidade dos sistemas operativos baseados em Unix está a aumentar, os autores de malware estão a desenvolver mais ameaças que visam os utilizadores do Mac. O System Center Endpoint Protection oferece proteção poderosa e eficaz contra estas ameaças emergentes. O System Center Endpoint Protection também inclui a capacidade de desviar ameaças do Windows, protegendo os utilizadores do Mac à medida que interagem com utilizadores do Windows e vice-versa. Apesar de o malware do Windows não representar uma ameaça direta ao Mac, a desativação do malware que infectou uma máquina do Mac impedirá a sua propagação para computadores baseados em Windows, através de uma rede local ou da Internet.

Requisitos do sistema

Para um desempenho ideal do System Center Endpoint Protection, o sistema deve satisfazer os seguintes requisitos de hardware e de software:

System Center Endpoint Protection:

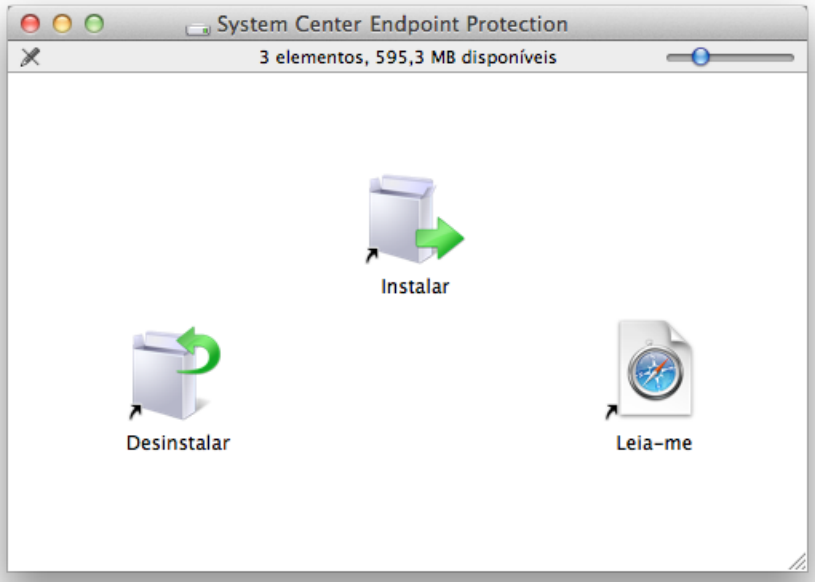
	Requisitos do sistema
Arquitetura do processador	32 bits, 64 bits Intel®
Sistema operativo	Mac OS X 10.6 e posterior
Memória	512 MB
Espaço livre em disco	100 MB

Instalação

Antes de iniciar o processo de instalação, feche todos os programas abertos no computador. O System Center Endpoint Protection contém componentes que podem entrar em conflito com outros programas antivírus que já podem estar instalados no computador. Recomenda-se vivamente que remova todos os outros programas antivírus para evitar possíveis problemas. Pode instalar o System Center Endpoint Protection a partir de um CD/DVD de instalação ou de um ficheiro transferido a partir do nosso Web site.

Para iniciar o assistente de instalação, execute uma das seguintes ações:

- Se instalar a partir do CD/DVD de instalação, insira-o no computador, abra-o a partir do ambiente de trabalho ou da janela Finder e clique duas vezes no ícone **Instalar**.
- Se instalar a partir de um ficheiro transferido, abra o ficheiro que transferiu e clique duas vezes no ícone **Instalar**.



Inicie o instalador e o assistente de instalação orientá-lo-á ao longo do processo de configuração básica. Após concordar com o Contrato de Licença de Software e ler a Declaração de Privacidade, poderá escolher um dos seguintes tipos de instalação:

- Típica 4
- Personalizada 4

Instalação típica

O modo de instalação típica inclui opções de configuração apropriadas para a maioria dos utilizadores. Estas definições proporcionam segurança máxima em combinação com um excelente desempenho do sistema. A instalação típica é a opção predefinida e é recomendada caso não possua requisitos particulares para definições específicas.

Depois de selecionar o modo de instalação **Típica**, configure a **Deteção de aplicações potencialmente não desejadas**. As aplicações potencialmente não desejadas não são necessariamente maliciosas, mas podem afetar negativamente o comportamento do sistema operativo. Estas aplicações estão frequentemente integradas noutros programas e podem ser difíceis de notar durante o processo de instalação. Apesar de estas aplicações apresentarem geralmente uma notificação durante a instalação, podem ser instaladas facilmente sem o seu consentimento.

Depois de instalar o System Center Endpoint Protection, deve executar uma análise do computador para verificar a existência de código malicioso. Na janela principal do programa, clique em **Análise do computador** e, em seguida, em **Análise inteligente**. Para obter mais informações sobre a análise do computador a pedido, consulte a secção Análise do computador a pedido 10.

Instalação personalizada

O modo de instalação personalizada destina-se a utilizadores experientes que pretendem modificar as definições avançadas durante o processo de instalação.

Depois de selecionar o modo de instalação **Personalizada**, ser-lhe-á solicitado para configurar as definições do **Servidor proxy**. Se estiver a utilizar um servidor proxy, poderá definir os parâmetros agora, selecionando a opção **Utilizo um servidor proxy**. Introduza o endereço IP ou o URL do servidor proxy no campo **Endereço**. No campo Porta, especifique a porta em que o servidor proxy aceita as ligações (3128 por predefinição). Caso o servidor proxy requeira autenticação, introduza um **Nome de utilizador** e uma **Palavra-**

passe válidos para obter acesso ao servidor proxy. Se tiver a certeza de que nenhum servidor proxy está a ser utilizado, escolha a opção **Não utilizo um servidor proxy**. Se não tiver a certeza, poderá utilizar as definições atuais do sistema, selecionando **Utilizar as definições do sistema (Recomendado)**.

No próximo passo, poderá **Definir utilizadores privilegiados** que poderão editar a configuração do programa. Na lista de utilizadores, no lado esquerdo, selecione os utilizadores e selecione **Adicionar** para incluí-los na lista **Utilizadores privilegiados**. Para visualizar todos os utilizadores do sistema, selecione a opção **Mostrar todos os utilizadores**.

O próximo passo do processo de instalação é configurar a **Deteção de aplicações potencialmente não desejadas**. As aplicações potencialmente não desejadas não são necessariamente maliciosas, mas podem afetar negativamente o comportamento do sistema operativo. Estas aplicações estão frequentemente integradas noutros programas e podem ser difíceis de notar durante o processo de instalação. Apesar de estas aplicações apresentarem geralmente uma notificação durante a instalação, podem ser instaladas facilmente sem o seu consentimento.

Depois de instalar o System Center Endpoint Protection, deve executar uma análise do computador para verificar a existência de código malicioso. Na janela principal do programa, clique em **Análise do computador** e, em seguida, em **Análise inteligente**. Para obter mais informações sobre as análises do computador a pedido, consulte a secção Análise do computador a pedido 10.

Desinstalação

Se pretender desinstalar o System Center Endpoint Protection do computador, execute uma das seguintes ações:

- insira o CD/DVD de instalação do System Center Endpoint Protection no computador, abra-o a partir do ambiente de trabalho ou da janela Finder e clique duas vezes no ícone **Desinstalar**,
- abra o ficheiro de instalação do System Center Endpoint Protection (*.dmg*) e clique duas vezes no ícone **Desinstalar** ou
- inicie o **Finder**, abra a pasta **Aplicações** no disco rígido, prima ctrl e clique no ícone System Center Endpoint Protection e selecione a opção **Mostrar conteúdo do pacote**. Abra a pasta **Contents > Helpers** e clique duas vezes no ícone **Uninstaller**.

Guia para iniciantes

Este capítulo fornece uma visão geral inicial do System Center Endpoint Protection e respetivas definições básicas.

Interface do utilizador

A janela principal do System Center Endpoint Protection está dividida em duas secções principais. A janela principal à direita apresenta informações correspondentes à opção selecionada no menu principal à esquerda.

Segue-se uma descrição das opções existentes no menu principal:

- **Estado da proteção** - Fornece informações sobre o estado da proteção do System Center Endpoint Protection. Se o **Modo avançado** estiver ativado, o submenu **Estatísticas** será apresentado.
- **Análise do computador** - Esta opção permite configurar e iniciar a Análise do computador a pedido.
- **Atualizar** - Apresenta informações sobre as atualizações da base de dados de assinatura de vírus.
- **Configurar** - Selecione esta opção para ajustar o nível de segurança do computador. Se o **Modo avançado** estiver ativado, o submenu **Antivírus e antispyware** será apresentado.
- **Ferramentas** - Fornece acesso a **Relatórios**, **Quarentena** e **Agenda**. Esta opção é apresentada apenas no **Modo avançado**.
- **Ajuda** - Fornece informações sobre o programa e acesso a ficheiros de ajuda.

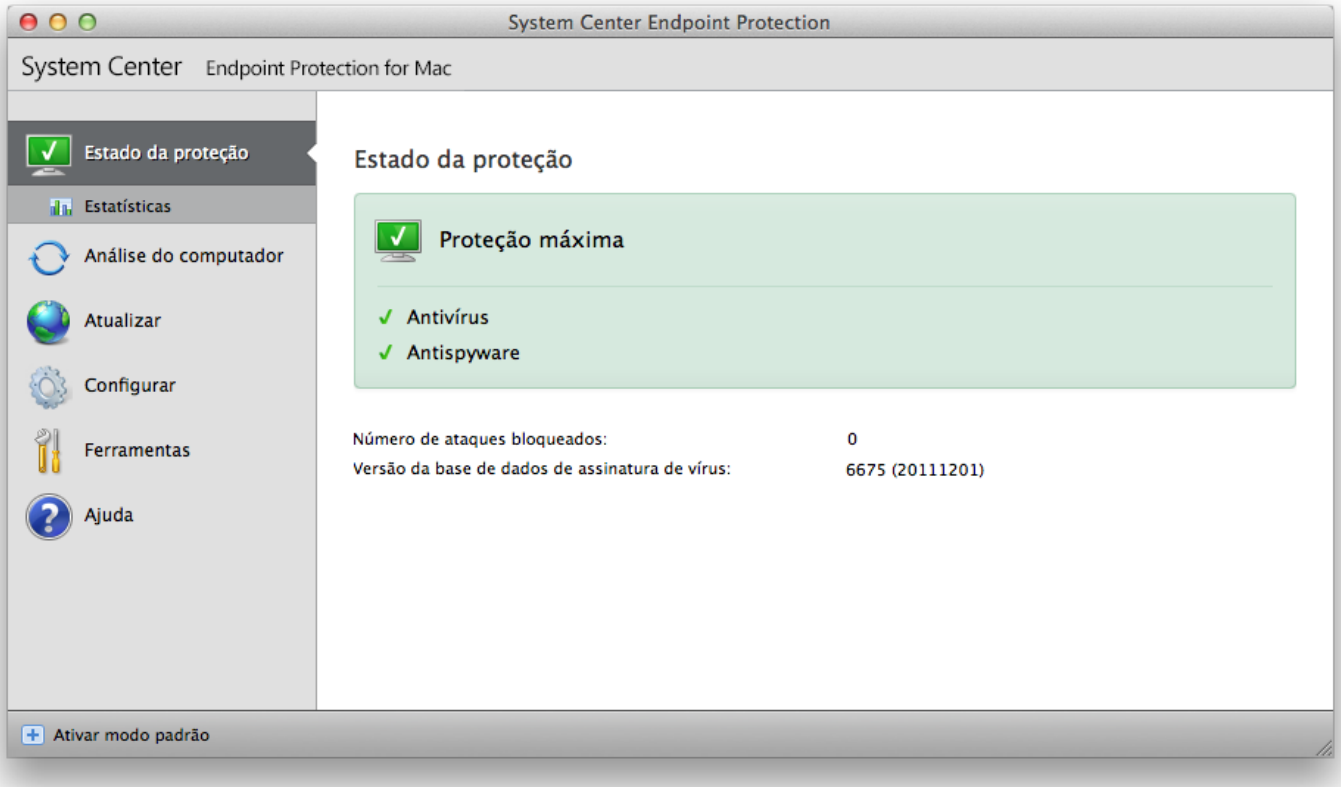
A interface do utilizador do System Center Endpoint Protection permite aos utilizadores alternarem entre o Modo padrão e avançado. O modo padrão fornece acesso aos recursos necessários para operações comuns. Este não apresenta opções avançadas. Para alternar entre os modos, clique no ícone de adição (**+**), junto a **Ativar modo avançado/Ativar modo padrão**, no canto inferior esquerdo da janela principal do programa ou prima cmd+M.

A alternância para o modo Avançado adiciona a opção **Ferramentas** ao menu principal. A opção **Ferramentas** permite-lhe aceder aos submenus de **Relatórios**, **Quarentena** e **Agenda**.

NOTA: Todas as instruções restantes deste guia ocorrem no **Modo avançado**.

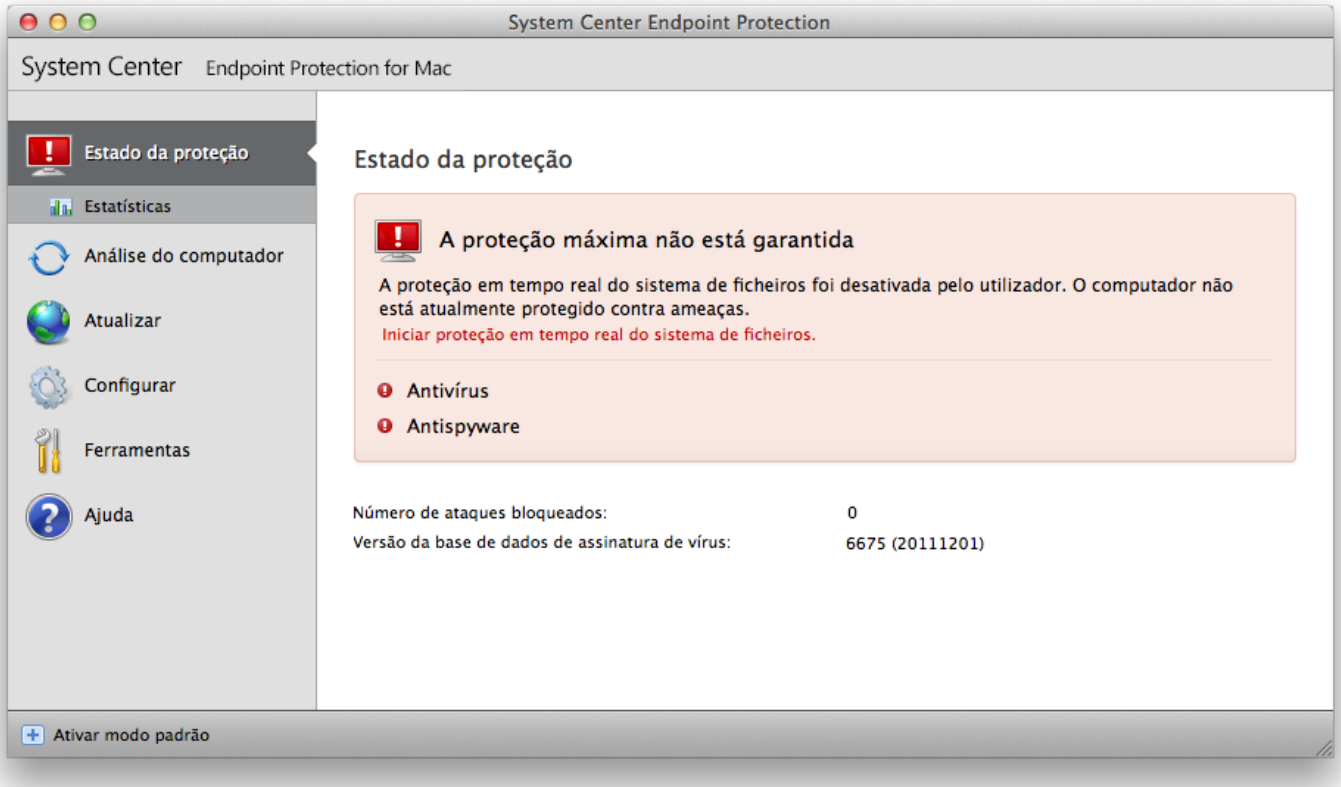
Verificação do funcionamento do sistema

Para ver o **Estado da proteção**, clique na opção superior do menu principal. Um resumo de estado sobre o funcionamento do System Center Endpoint Protection será apresentado na janela principal, bem como submenu com **Estatísticas**. Selecione-o para ver informações mais detalhadas e estatísticas sobre as análises do computador que foram realizadas no sistema. A janela Estatísticas está disponível apenas no modo avançado.



O que fazer se o programa não funcionar corretamente

Se os módulos ativados estiverem a funcionar corretamente, é-lhes atribuído um ícone de visto verde. Caso contrário, será apresentado um ponto de exclamação vermelho ou um ícone de notificação laranja e serão apresentadas informações adicionais sobre o módulo na parte superior da janela. É igualmente apresentada uma solução sugerida para corrigir o módulo. Para alterar o estado dos módulos individuais, clique em **Configurar** no menu principal e clique no módulo pretendido.



Trabalhar com o System Center Endpoint Protection

Proteção antivírus e antispyware

A proteção antivírus protege contra ataques de sistemas maliciosos, modificando ficheiros que representam ameaças internas. Se uma ameaça com código malicioso for detectada, o módulo antivírus poderá eliminá-la, bloqueando-a e, em seguida, limpando, eliminando ou movendo-a para a quarentena.

Proteção em tempo real do sistema de ficheiros

A Proteção em tempo real do sistema de ficheiros controla todos os eventos relativos a antivírus no sistema. Todos os ficheiros são analisados em termos de código malicioso quando são abertos, criados ou executados no computador. A Proteção em tempo real do sistema de ficheiros é ativada na inicialização do sistema.

Configuração da proteção em tempo real

A Proteção em tempo real do sistema de ficheiros verifica todos os tipos de suporte e aciona uma análise com base em vários eventos. A Proteção em tempo real do sistema de ficheiros pode variar para ficheiros recém-criados e existentes. No caso de ficheiros recém-criados, é possível aplicar um nível mais profundo de controlo.

Por predefinição, a Proteção em tempo real é ativada no momento da inicialização do sistema, proporcionando análise ininterrupta. Em casos especiais (por exemplo, se houver um conflito com outra Análise em tempo real), é possível terminar a Proteção em tempo real, clicando no ícone do System Center Endpoint Protection localizado na barra de menu (parte superior do ecrã) e selecionando a opção **Desativar Proteção em Tempo Real do Sistema de Ficheiros**. Também é possível terminar a proteção em tempo real na janela principal do programa (**Configurar** > **Antivírus e antispyware** > **Desativar**).

Para modificar as definições avançadas da Proteção em tempo real, aceda a **Configurar** > **Introduzir preferências da aplicação ...** > **Proteção** > **Proteção em tempo real** e clique no botão **Configurar...**, junto das **Opções avançadas** (descritas na secção denominada Opções de análise avançadas 8).

Análise ativada (Análise acionada por evento)

Por predefinição, todos os ficheiros são analisados na **Abertura de ficheiro**, **Criação de ficheiro** ou **Execução de ficheiro**. Recomendamos que mantenha as predefinições, uma vez que fornecem o nível máximo de Proteção em tempo real ao seu computador.

Opções de análise avançadas

Nesta janela, é possível definir os tipos de objeto que serão analisados pelo mecanismo de análise e ativar/desativar a **Heurística avançada** , bem como modificar as definições de arquivos compactados e cache de ficheiro.

Não recomendamos que altere os valores predefinidos na secção **Predefinições de ficheiros compactados**, a menos que seja necessário resolver um problema específico, uma vez que valores superiores de compactação de arquivos compactados podem impedir o desempenho do sistema.

Pode alternar a análise da Heurística avançada para ficheiros executados, criados e modificados separadamente, clicando na caixa de verificação **Heurística avançada** em cada uma das respetivas secções de parâmetros do mecanismo.

Para proporcionar o impacto mínimo no sistema ao utilizar a Proteção em tempo real, pode definir o tamanho da cache de otimização. Este comportamento fica ativo durante a utilização da opção **Ativar cache de ficheiro limpo**. Se este recurso for desativado, todos os ficheiros serão analisados sempre que forem acedidos. Os ficheiros não serão analisados repetidamente depois de serem colocados em cache (a não ser que sejam modificados), até o tamanho definido da cache. Os ficheiros são novamente analisados logo após cada atualização da base de dados de assinatura de vírus.

Clique em **Ativar cache de ficheiro limpo** para ativar/desativar esta função. Para definir a quantidade de ficheiros a colocar em cache, basta introduzir o valor pretendido no campo de entrada junto a **Tamanho da cache**.

Os parâmetros de análise adicionais podem ser definidos na janela **Configuração do mecanismo**. Pode definir os tipos de **Objetos** que devem ser analisados, utilizando o nível **Opções** e **Limpeza**, bem como definindo **Extensões** e **Limites** de tamanho de ficheiros para a Proteção em tempo real do sistema de ficheiros. Pode aceder à janela de configuração do mecanismo clicando no botão **Configurar...** junto a **Mecanismo** na janela Configuração avançada. Para obter informações mais detalhadas sobre os parâmetros do mecanismo, consulte Configuração de parâmetros do mecanismo 13.

Exclusões da análise

Esta secção permite-lhe excluir determinados ficheiros e pastas da análise.

- **Caminho** - caminho para ficheiros e pastas excluídos
- **Ameaça** - se houver um nome de uma ameaça junto a um ficheiro excluído, significa que o ficheiro só foi excluído para a ameaça em questão e não completamente. Por conseguinte, se o ficheiro for infetado posteriormente com outro malware, será detetado pelo módulo antivírus.
- **Adicionar...** - exclui objetos da deteção. Introduza o caminho para um objeto (também podem utilizar caracteres universais * e ?) ou selecionar a pasta ou ficheiro na estrutura em árvore.
- **Editar...** - permite-lhe editar as entradas selecionadas.
- **Eliminar** - remove as entradas selecionadas.
- **Padrão** - cancela todas as exclusões.

Quando modificar a configuração da proteção em tempo real

A Proteção em tempo real é o componente mais essencial para a manutenção de um sistema seguro. Tenha cuidado ao modificar os parâmetros da Proteção em tempo real. Recomendamos que modifique estes parâmetros apenas em casos específicos. Por exemplo, se houver uma situação de conflito com uma determinada aplicação ou Análise em tempo real de outro programa antivírus.

Após instalar o System Center Endpoint Protection, todas as definições serão otimizadas para proporcionar o nível máximo de segurança do sistema aos utilizadores. Para restaurar as predefinições, clique no botão **Padrão** localizado na parte inferior esquerda da janela **Proteção em tempo real** (**Configurar** > **Introduzir preferências da aplicação ...** > **Proteção** > **Proteção em tempo real**).

Verificação da proteção em tempo real

Para verificar se a Proteção em tempo real está a funcionar e a detetar vírus, utilize o ficheiro de teste eicar.com. Este ficheiro de teste é especial, inofensivo e detetável por todos os programas antivírus. O ficheiro foi criado pelo instituto EICAR (European Institute for Computer Antivirus Research) para testar a funcionalidade de programas antivírus.

Para verificar o estado da Proteção em tempo real remotamente, estabeleça ligação ao computador cliente através do **Terminal** e emita o seguinte comando:
`/Applications/.scep/Contents/MacOS/scep_daemon --status`

O estado da Análise em tempo real será apresentada como `RTPStatus=Enabled` ou `RTPStatus=Disabled`.

A saída do bash do Terminal inclui ainda os seguintes estados:

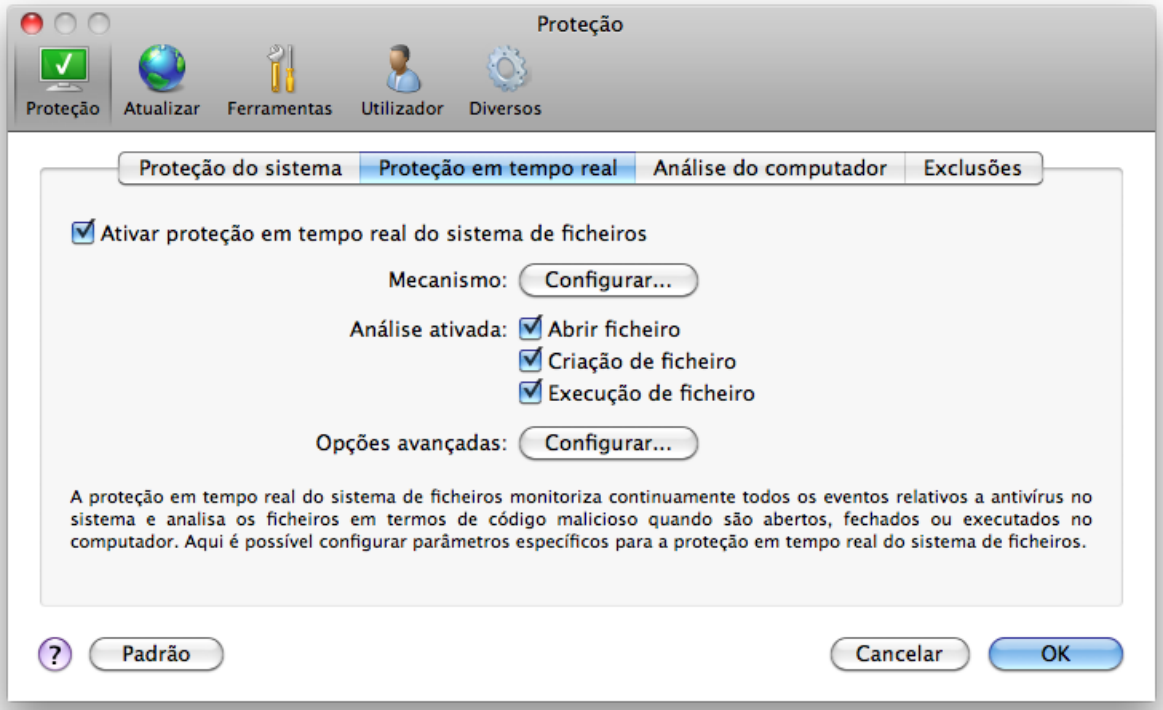
- versão do System Center Endpoint Protection instalada no computador cliente
- data e versão da base de dados de assinatura de vírus
- caminho para o servidor de atualização

NOTA: A utilização do Terminal é recomendada apenas para utilizadores avançados.

O que fazer se a proteção em tempo real não funcionar

Neste capítulo, descrevemos situações problemáticas que podem surgir quando usamos a Proteção em tempo real e como resolvê-las.

A Proteção em tempo real está desativada
Se a Proteção em tempo real foi inadvertidamente desativada por um utilizador, será necessário reativá-la. Para reativar a Proteção em tempo real, navegue até **Configurar** > **Antivírus e antispyware** e clique na hiperligação **Ativar proteção em tempo real do sistema de ficheiros** (à direita) na janela principal do programa. Em alternativa, pode ativar a proteção em tempo real do sistema de ficheiros na janela Configuração avançada, em **Proteção** > **Proteção em tempo real**, selecionando a opção **Ativar proteção em tempo real do sistema de ficheiros**.



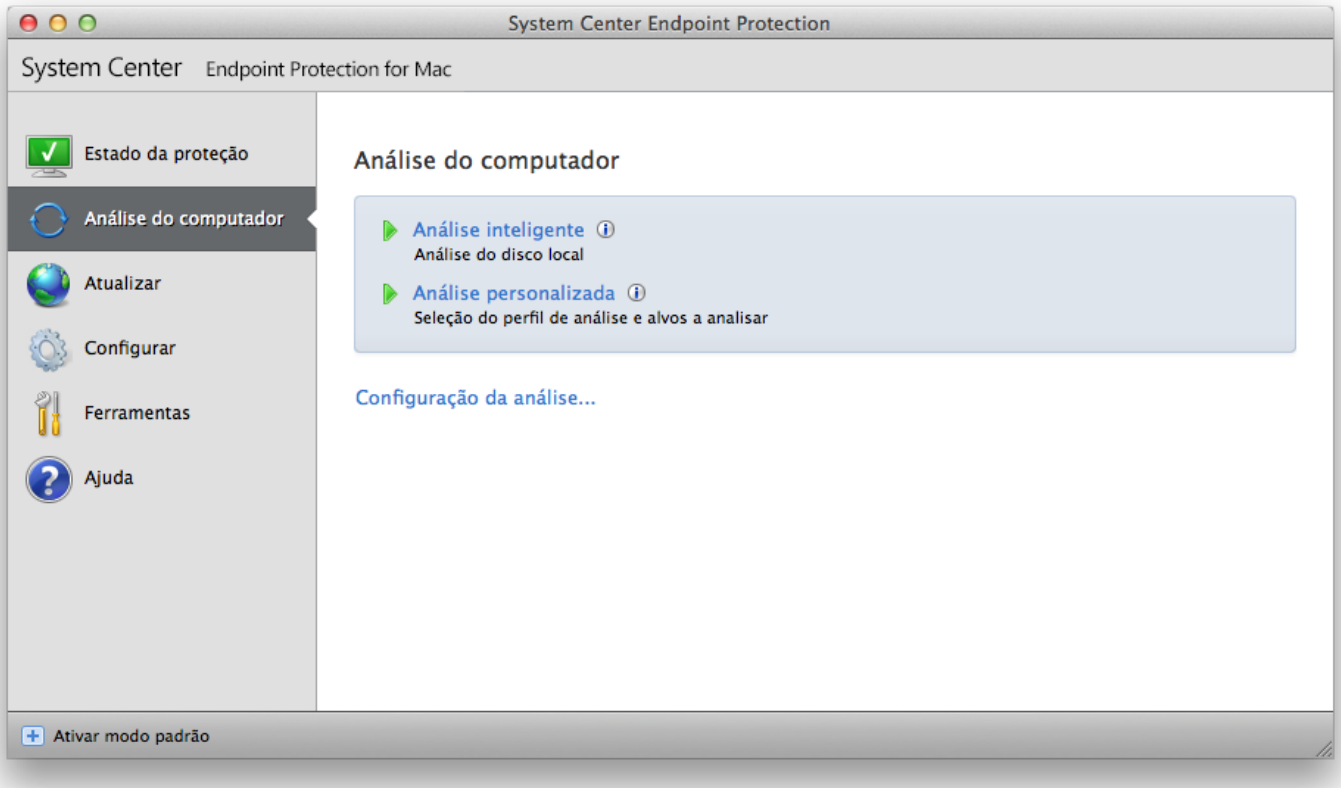
A Proteção em tempo real não deteta nem limpa infiltrações
Verifique se não existe outro programa antivírus instalado no computador. Se forem ativadas duas proteções em tempo real ao mesmo tempo, as mesmas poderão entrar em conflito. Recomendamos que desinstale todos os programas antivírus que possam estar instalados no sistema.

A Proteção em tempo real não é iniciada
Se a Proteção em tempo real não for ativada na inicialização do sistema, talvez existam conflitos com outros programas. Se for este o caso, consulte os especialistas do Suporte ao cliente.

Análise do computador a pedido

Se suspeitar que o computador está infetado (se se comportar de modo anormal), execute a **Análise do computador** > **Análise inteligente** para examinar se existem infiltrações no computador. Para obter proteção máxima, as análises do computador devem ser executadas regularmente como parte das medidas usuais de segurança; não faça análises apenas quando suspeitar de uma infeção. A análise normal pode detetar infiltrações que não foram detetadas pela Análise em tempo real quando foram guardadas no disco. Isto pode acontecer caso a Análise em tempo real esteja desativada no momento da infeção ou se a base de dados de assinatura de vírus não estiver atualizada.

Recomendamos que execute uma Análise do computador a pedido pelo menos uma vez por mês. A análise pode ser configurada como uma tarefa agendada em **Ferramentas** > **Agenda**.



Também pode arrastar e soltar pastas e ficheiros selecionados do ambiente de trabalho ou da janela Finderpara o ecrã principal do System Center Endpoint Protection, para o ícone de âncora, ícone da barra de menu (parte superior do ecrã) ou para o ícone da aplicação (localizado na pasta */Aplicações*).

Tipos de análise

Existem dois tipos disponíveis de análise do computador a pedido. A **Análise inteligente** analisa rapidamente o sistema sem necessidade de mais configurações dos parâmetros de análise. A **Análise personalizada** permite selecionar qualquer perfil de análise predefinido, bem como escolher alvos de análise específicos.

Análise inteligente

A análise inteligente permite-lhe iniciar rapidamente uma análise do computador e limpar ficheiros infetados, sem a necessidade de intervenção do utilizador. A sua principal vantagem é a operação fácil, sem configurações de análise detalhadas. A Análise inteligente verifica todos os ficheiros em todas as pastas e limpa ou elimina automaticamente as infiltrações detetadas. O nível de limpeza é automaticamente definido para o valor predefinido. Para obter informações mais detalhadas sobre os tipos de limpeza, consulte a secção sobre Limpeza 14.

Análise personalizada

A **Análise personalizada** é ideal caso pretenda especificar parâmetros de análise, como alvos de análise e métodos de análise. A vantagem de executar a Análise personalizada é o facto de possibilitar a configuração dos parâmetros detalhadamente. Podem ser guardadas configurações diferentes nos perfis de análise definidos pelo utilizador, o que poderá ser útil se a análise for executada repetidas vezes com os mesmos parâmetros.

Para selecionar os alvos de análise, selecione **Análise do computador** > **Análise personalizada** e selecione **Alvos de análise** na estrutura em árvore. Um alvo de análise pode ser também especificado com mais exatidão através da introdução do caminho para a pasta ou ficheiro(s) que pretende incluir. Se estiver interessado apenas na análise do sistema, sem ações de limpeza adicionais, selecione a opção **Analisar sem limpar**. Além disso, pode selecionar entre três níveis de limpeza clicando em **Configurar...** > **Limpeza**.

A realização de análises de computador com a Análise personalizada é recomendada para utilizadores avançados com experiência anterior na utilização de programas antivírus.

Alvos de análise

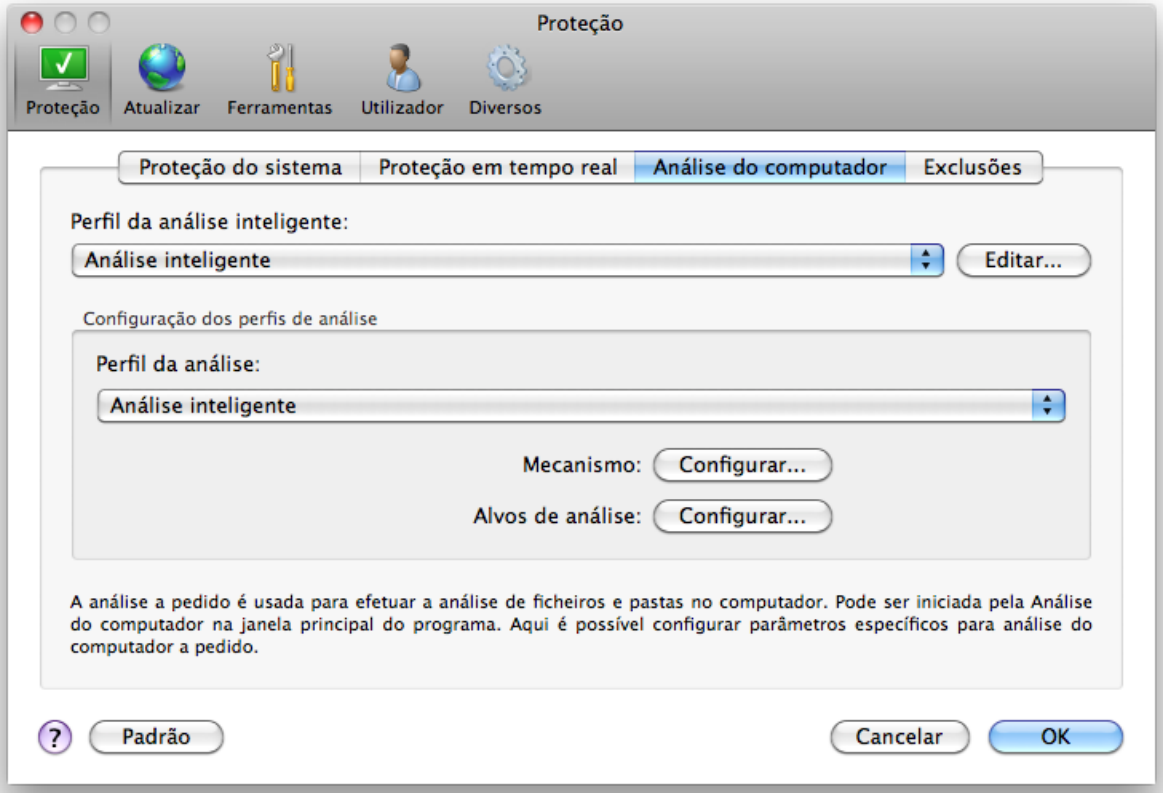
A estrutura em árvore de Alvos de análise permite-lhe selecionar ficheiros e pastas que serão analisados quanto a vírus. As pastas também podem ser selecionadas de acordo com as definições de um perfil.

Um alvo de análise pode ser definido com mais exatidão através da introdução do caminho para a pasta ou ficheiro(s) que pretende incluir na análise. Selecione os alvos na estrutura em árvore que lista todas as pastas disponíveis no computador.

Perfis de análise

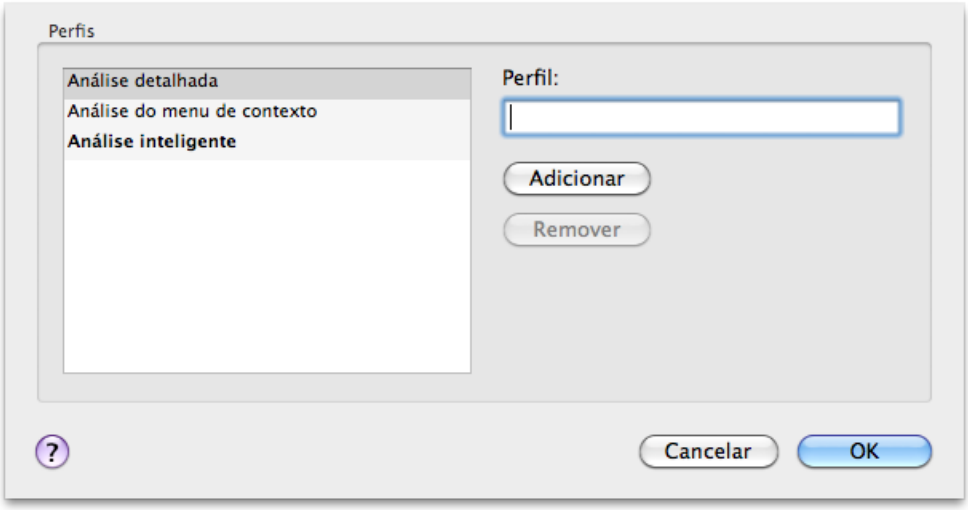
As suas definições de análise favoritas podem ser guardadas para análise futura. Recomendamos a criação de um perfil diferente (com diversos alvos de análise, métodos de análise e outros parâmetros) para cada análise utilizada regularmente.

Para criar um novo perfil, aceda a **Configurar** > **Introduzir preferências da aplicação ...** > **Proteção** > **Análise do computador** e clique em **Editar...** junto à lista de perfis atuais.



Para ajudar a criar um perfil de análise de acordo com as suas necessidades, consulte a secção Configuração de parâmetros do mecanismo 13 para obter uma descrição de cada parâmetro da configuração de análise.

Exemplo: Suponhamos que pretende criar o seu próprio perfil de análise e que a configuração de Análise inteligente é parcialmente adequada. Porém, não pretende analisar empacotadores em tempo real nem aplicações potencialmente inseguras e que pretende também aplicar a Limpeza rigorosa. Na janela **Lista de perfis da análise a pedido**, introduza o nome do perfil, clique no botão **Adicionar** e confirme clicando em **OK**. Ajuste os parâmetros de acordo com os seus requisitos, configurando o **Mecanismo** e os **Alvos de análise**.



Configuração de parâmetros do mecanismo

A tecnologia de análise utilizada no System Center Endpoint Protection é proativa, o que significa que também fornece proteção durante as primeiras horas da propagação de uma nova ameaça. Utiliza uma combinação de diversos métodos (análise de código, emulação de código, assinaturas genéricas e assinaturas de vírus) que funcionam em conjunto para otimizar significativamente a segurança do sistema. O mecanismo de análise é capaz de controlar diversos fluxos de dados simultaneamente, maximizando a eficiência e a taxa de deteção. Esta tecnologia também evita com êxito os rootkits.

As opções de configuração da tecnologia do mecanismo permitem-lhe especificar diversos parâmetros de análise:

- Tipos e extensões de ficheiros que serão analisados
- A combinação de diversos métodos de deteção
- Níveis de limpeza, etc.

Para aceder à janela de configuração, clique em **Configurar** > **Antivírus e antispyware** > **Configuração avançada da proteção antivírus e antispyware** e clique no botão **Configurar...** , localizado nos caracteres universais **Proteção do sistema**, **Proteção em tempo real** e **Análise do computador**. Cenários de segurança diferentes podem exigir configurações diferentes. Como tal, os parâmetros do mecanismo são configurados individualmente para os seguintes módulos de proteção:

- **Proteção do sistema** > Análise automática de ficheiros na inicialização
- **Proteção em tempo real** > Proteção em tempo real do sistema de ficheiros
- **Análise do computador** > Análise do computador a pedido

Os parâmetros do mecanismo são especificamente otimizados para cada módulo e a respetiva modificação pode influenciar significativamente o funcionamento do sistema. Por exemplo, a alteração das definições para analisar sempre empacotadores em tempo real ou a ativação da heurística avançada no módulo de Proteção em tempo real do sistema de ficheiros pode resultar num sistema mais lento. Por conseguinte, recomendamos que mantenha os parâmetros predefinidos do mecanismo inalterados para todos os módulos, à exceção da Análise do computador.

Objetos

A seção **Objetos** permite definir os ficheiros do computador a analisar quanto a infiltrações.

- **Ficheiros** - fornece a análise de todos os tipos de ficheiros comuns (programas, imagens, áudio, ficheiros de vídeo, ficheiros de base de dados, etc.)
- **Hiperligações simbólicas** - (apenas Análise a pedido) analisa determinados tipos especiais de ficheiros que contenham uma cadeia de caracteres de texto que seja interpretada e seguida pelo sistema operativo como um caminho para outro ficheiro ou diretório.
- **Ficheiros de email** - (não disponível na Proteção em tempo real) analisa ficheiros especiais que contenham mensagens de email.
- **Caixas de correio** - (não disponível na Proteção em tempo real) analisa as caixas de correio do utilizador no sistema. A utilização incorreta desta opção pode resultar num conflito com o seu cliente de email.
- **Arquivos compactados** - (não disponível na Proteção em tempo real) fornece a análise de ficheiros em arquivos compactados (. rar, .zip, .arj, .tar ,etc.).
- **Arquivos compactados de auto-extração** - (não disponível na Proteção em tempo real) analisa ficheiros incluídos em arquivos compactados de auto-extração.
- **Empacotadores em tempo real** - ao contrário dos tipos de arquivos compactados padrão, os empacotadores em tempo real são descompactados na memória, além de empacotadores estáticos padrão (UPX, yoda, ASPack, FGS, etc.).

Opções

Na seção **Opções**, pode selecionar os métodos utilizados durante uma análise do sistema para verificar infiltrações. As opções disponíveis são:

- **Heurística** - A heurística utiliza um algoritmo que analisa a atividade (maliciosa) de programas. A principal vantagem da deteção heurística é a capacidade de detetar novos softwares maliciosos, que não existiam antes ou não estavam incluídos na lista de vírus conhecidos (base de dados de assinatura de vírus).
- **Heurística avançada** - A heurística avançada é constituída por um algoritmo heurístico exclusivo, otimizado para a deteção de worms e cavalos de troia informáticos escritos em linguagens de programação de elevado nível. A capacidade de deteção do programa é significativamente superior devido à heurística avançada.
- **Aplicações potencialmente não desejadas** - Estas aplicações não são necessariamente maliciosas, mas podem afetar negativamente o desempenho do computador. Tais aplicações exigem geralmente o consentimento para a instalação. Se estas aplicações estiverem presentes no computador, o sistema irá comportar-se de modo diferente (em comparação ao modo anterior à instalação destas aplicações). As alterações mais significativas incluem janelas pop-up não desejadas, ativação e execução de processos ocultos, aumento da utilização de recursos do sistema, alterações nos resultados de pesquisa e aplicações em comunicação com servidores remotos.
- **Aplicações potencialmente inseguras** - estas aplicações referem-se a softwares comerciais e legítimos que podem sofrer abusos por parte de atacantes, caso tenham sido instaladas sem o conhecimento do utilizador. A classificação inclui programas como ferramentas de acesso remoto, motivo pelo qual esta opção está, por predefinição, desativada.

Limpeza

As definições de limpeza determinam o modo como a análise limpa os ficheiros infetados. Existem 3 níveis de limpeza:

- **Sem limpeza** - Os ficheiros infetados não são limpos automaticamente. O programa irá apresentar uma janela de aviso e permitir-lhe escolher uma ação.
- **Limpeza padrão** - O programa tentará limpar ou eliminar automaticamente um ficheiro infetado. Se não for possível selecionar a ação correta automaticamente, o programa irá possibilitar-lhe escolher as ações a seguir. A possibilidade de escolher as ações a seguir também será apresentada se não for possível concluir uma ação predefinida.
- **Limpeza rigorosa** - O programa irá limpar ou eliminar todos os ficheiros infetados (incluindo os arquivos compactados). As únicas exceções são os ficheiros do sistema. Se não for possível limpá-los, ser-lhe-á disponibilizada uma ação a tomar na janela de aviso.

Aviso: No modo de limpeza Padrão, o arquivo compactado será eliminado na íntegra apenas se todos os ficheiros do arquivo compactado estiverem infetados. Se no arquivo compactado existirem ficheiros legítimos, o mesmo não será eliminado. Se, no modo de Limpeza rigorosa, for detetado um ficheiro do arquivo compactado infetado, o arquivo compactado será eliminado na íntegra, mesmo se existirem ficheiros limpos.

Extensões

Uma extensão é a parte do nome de ficheiro delimitada por um ponto final. A extensão define o tipo e o conteúdo do ficheiro. Esta secção de configuração de parâmetros do mecanismo permite definir os tipos de ficheiros a excluir da análise.

Por predefinição, todos os ficheiros são analisados, independentemente das respetivas extensões. Qualquer extensão pode ser adicionada à lista de ficheiros excluídos da análise. Com os botões **Adicionar** e **Remover**, pode ativar ou desativar a análise das extensões pretendidas.

A exclusão de ficheiros da análise é por vezes necessária caso a análise de determinados tipos de ficheiros impedir o funcionamento correto do programa. Por exemplo, pode ser aconselhável excluir as extensões *.log*, *.cfg* e *.tmp*.

Limites

A secção **Limites** permite especificar o tamanho máximo de objetos e os níveis de arquivos compactados aninhados a analisar:

- **Tamanho máximo:** Define o tamanho máximo dos objetos a analisar. O módulo antivírus irá analisar apenas objetos mais pequenos que o tamanho especificado. Não recomendamos que altere o valor predefinido, pois geralmente não há motivo para modificá-lo. Esta opção deverá ser alterada apenas por utilizadores avançados que tenham motivos específicos para excluir objetos maiores da análise.
- **Tempo máximo da análise:** Define o tempo máximo designado para a análise de um objeto. Se um valor definido pelo utilizador for introduzido aqui, o módulo antivírus interromperá a análise de um objeto depois de decorrido o período especificado, independentemente de a análise ter ou não terminado.
- **Nível de compactação de ficheiros:** Especifica a profundidade máxima da análise de arquivos compactados. Não recomendamos que altere o valor predefinido de 10; em circunstâncias normais, não haverá motivo para modificá-lo. Se a análise for encerrada prematuramente devido ao número de arquivos compactados aninhados, o arquivo compactado permanecerá sem verificação.
- **Tamanho máximo do ficheiro:** Esta opção permite especificar o tamanho máximo de ficheiro dos arquivos incluídos em arquivos compactados (quando são extraídos) a analisar. Se a análise for encerrada prematuramente devido a este limite, o arquivo compactado permanecerá sem verificação.

Outros

Com a Otimização inteligente ativada, as definições ideais são utilizadas para garantir o nível mais eficiente de análise, mantendo simultaneamente a velocidade de análise mais elevada. Os diversos módulos de proteção efetuam a análise de maneira inteligente, utilizando diferentes métodos de análise e aplicando-os a tipos específicos de ficheiros. A Otimização inteligente não é definida de modo rígido no produto. A nossa equipa de desenvolvimento está a implementar continuamente novas alterações que vão sendo integradas no System Center Endpoint Protection através de atualizações regulares. Se a Otimização inteligente estiver desativada, apenas as definições configuradas pelo utilizador no núcleo do mecanismo do módulo em questão serão aplicadas durante a realização de uma análise.

Analisar fluxos de dados alternativos (apenas a análise a pedido)
Os fluxos de dados alternativos (bifurcações de recursos/dados) utilizados pelo sistema de ficheiros são associações de ficheiros e pastas invisíveis às técnicas comuns de análise. Muitas infiltrações tentam evitar a deteção, disfarçando-se de fluxos de dados alternativos.

Foi detetada uma infiltração

As infiltrações podem atingir o sistema a partir de vários pontos de entrada: páginas Web, pastas compartilhadas, email ou dispositivos de computador amovíveis (USB, discos externos, CDs, DVDs, disquetes, etc.).

Se o computador estiver a apresentar sinais de infecção por malware, por exemplo, estiver mais lento, bloquear com frequência, etc., recomendamos que efetue os seguintes passos:

1. Abra o System Center Endpoint Protection e clique em **Análise do computador**.
2. Clique em **Análise inteligente** (para obter mais informações, consulte a secção Análise inteligente 11).
3. Após a análise ter terminado, reveja o relatório para verificar o número de ficheiros verificados, infetados e limpos.

Se pretende analisar apenas uma determinada parte do disco, clique em **Análise personalizada** e selecione os alvos a analisar quanto a vírus.

Como exemplo geral de como as infiltrações são tratadas no System Center Endpoint Protection, suponha que uma infiltração é detetada pelo monitor do sistema de ficheiros em tempo real, que utiliza o nível de limpeza padrão. O mesmo tentará limpar ou eliminar o ficheiro. Se não houver uma ação predefinida disponível para o módulo de proteção em tempo real, ser-lhe-á pedido que selecione uma opção numa janela de alertas. Geralmente as opções **Limpar**, **Eliminar** e **Nenhuma ação** estão disponíveis. A seleção da opção **Nenhuma ação** não é recomendada, visto que os ficheiros infetados se manteriam intocados. Uma exceção a esta situação é quando tiver a certeza de que o ficheiro é inofensivo e foi detetado por engano.

Limpeza e eliminação – Aplique a limpeza se um ficheiro tiver sido atacado por um vírus que anexou a esse ficheiro um código malicioso. Se esse for o caso, tente primeiro limpar o ficheiro infetado para restaurá-lo para o respetivo estado original. Se o ficheiro for constituído exclusivamente por código malicioso, o mesmo será eliminado.

Eliminação de ficheiros em arquivos compactados - No modo de limpeza padrão, os arquivos compactados serão eliminados apenas se contiverem ficheiros infetados e nenhum ficheiro limpo. Por outras palavras, os arquivos compactados não serão eliminados se contiverem também ficheiros limpos inofensivos. No entanto, tenha cuidado quando realizar uma análise de **Limpeza rigorosa**. Com este tipo de limpeza, o arquivo será eliminado se contiver, pelo menos, um ficheiro infetado, independentemente do estado dos restantes ficheiros incluídos no arquivo compactado.

Atualização do programa

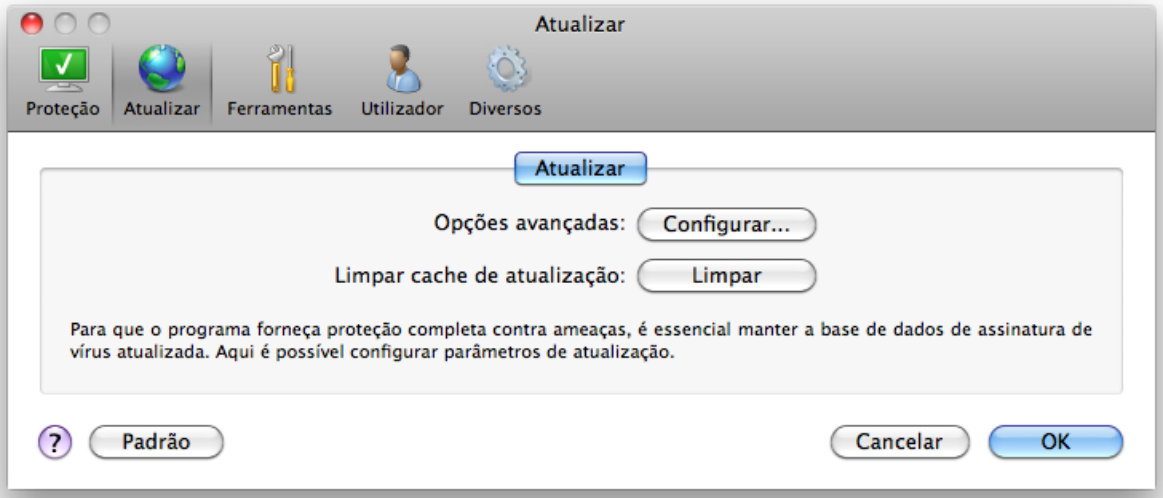
É necessário atualizar o System Center Endpoint Protection com regularidade para manter o nível máximo de segurança. O módulo de atualização garante que o programa está sempre atualizado através da transferência da base de dados de assinatura de vírus mais recente.

No menu principal, ao clicar em **Atualizar**, poderá saber o estado atual da atualização, incluindo o dia e a hora da última atualização bem sucedida, e se será necessário efetuar uma atualização. Para iniciar o processo de atualização manualmente, clique em **Atualizar base de dados de assinatura de vírus**.

Em circunstâncias normais, quando as atualizações são transferidas corretamente, é apresentada a mensagem *Atualização não necessária – a base de dados de assinaturas de vírus instalada é atual* na janela Atualizar.

A janela Atualizar também contém informações sobre a versão da base de dados de assinatura de vírus. Este indicador numérico é uma hiperligação ativa para o Web site que lista todas as assinaturas adicionadas durante a atualização em causa.

Configuração da atualização



Para ativar a utilização do modo de teste (modo de teste de transferências), clique no botão **Configurar...** junto a **Opções avançadas** e selecione a caixa de verificação **Ativar modo de teste**. Para desativar as notificações da bandeja do sistema que são apresentadas após cada atualização bem sucedida, selecione a caixa de verificação **Não mostrar notificação sobre atualização bem sucedida**.

Para eliminar todos os dados de atualização armazenados temporariamente, clique no botão **Limpar** junto a **Limpar cache de atualização**. Utilize esta opção se estiver com dificuldades durante a atualização.

Como criar tarefas de atualização

As atualizações podem ser acionadas manualmente clicando em **Atualizar base de dados de assinatura de vírus** na janela principal, apresentada depois de clicar em **Atualizar** no menu principal.

As atualizações também podem ser executadas como tarefas agendadas. Para configurar uma tarefa agendada, clique em **Ferramentas** > **Agenda**. Por predefinição, as seguintes tarefas estão ativadas no System Center Endpoint Protection:

- **Atualização automática de rotina**
- **Atualizar automaticamente após início de sessão do utilizador**

Cada uma das tarefas de atualização pode ser modificada para satifazer as suas necessidades. Além das tarefas de atualização predefinidas, pode criar novas tarefas de atualização com uma configuração definida pelo utilizador. Para obter mais detalhes sobre a criação e a configuração de tarefas de atualização, consulte a secção Agenda 17.

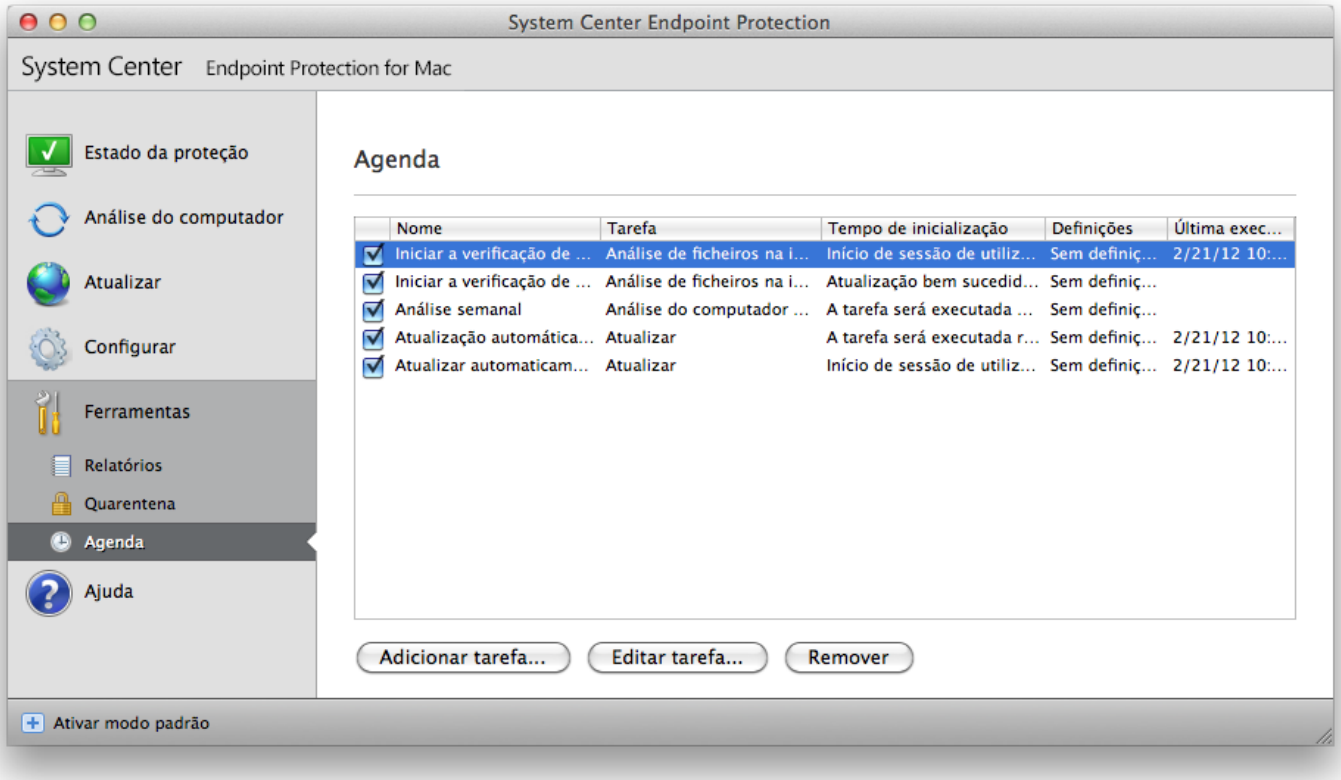
Atualização para uma nova compilação

Para obter a máxima proteção, é importante utilizar a compilação mais recente do System Center Endpoint Protection. Para verificar se existe uma nova versão, clique em **Atualizar** no menu principal à esquerda. Se estiver disponível uma nova compilação, será apresentada uma mensagem a indicar *Está disponível uma nova versão do produto!* na parte inferior da janela. Clique em **Saber mais...** para apresentar uma nova janela com o número da versão da nova compilação e o registo de alterações.

Clique em **Transferir** para transferir a compilação mais recente. Clique em **Fechar** para fechar a janela e transferir a atualização mais tarde.

Agenda

A **Agenda** ficará disponível se o Modo avançado no System Center Endpoint Protection estiver ativado. Pode encontrar a Agenda no menu principal do System Center Endpoint Protection em **Ferramentas**. A **Agenda** contém uma lista de todas as tarefas agendadas e propriedades de configuração, como a data e a hora predefinidas e o perfil de análise utilizado.



Por predefinição, as seguintes tarefas agendadas são apresentadas na Agenda:

- Atualização automática de rotina
- Atualizar automaticamente após início de sessão do utilizador
- Análise de ficheiros na inicialização após início de sessão do utilizador
- Análise de ficheiros na inicialização após atualização bem sucedida da base de dados de assinatura de vírus
- Manutenção de relatórios (após a ativação da opção **Mostrar tarefas do sistema** na configuração da agenda)
- Análise semanal

Para editar a configuração de uma tarefa agendada existente (tanto predefinida como definida pelo utilizador), prima ctrl, clique na tarefa que pretende modificar e selecione **Editar...** ou selecione a tarefa e clique no botão **Editar tarefa...**.

Finalidade do agendamento de tarefas

A Agenda gere e inicia tarefas agendadas com as configurações e propriedades predefinidas. A configuração e as propriedades contêm informações, como a data e a hora, bem como os perfis especificados a utilizar durante a execução da tarefa.

Criação de novas tarefas

Para criar uma nova tarefa na Agenda, clique no botão **Adicionar tarefa...** ou prima ctrl, clique no campo em branco e selecione **Adicionar...** no menu de contexto. Estão disponíveis cinco tipos de tarefas agendadas :

- **Executar aplicação**
- **Atualizar**
- **Manutenção de relatórios**
- **Análise do computador a pedido**
- **Análise de ficheiros na inicialização do sistema**

Como a tarefa Atualizar é uma das tarefas agendadas usadas com frequência, iremos explicar como adicionar uma nova tarefa de atualização.

No menu pendente **Tarefa agendada**, selecione **Atualizar**. Introduza o nome da tarefa no campo **Nome da tarefa**. Selecione a frequência da tarefa no menu pendente **Executar tarefa**. As opções disponíveis são: **Definida pelo utilizador**, **Uma vez**, **Repetidamente**, **Diariamente**, **Semanalmente** e **Evento acionado**. Com base na frequência selecionada, serão apresentados diferentes parâmetros de atualização.

Se selecionar **Definida pelo utilizador**, ser-lhe-á pedido que especifique a data/hora no formato cron (consulte a secção Criação de tarefa definida pelo utilizador 18 para obter mais detalhes).

Em seguida, defina a ação a tomar se não for possível executar ou concluir a tarefa na hora agendada. Estão disponíveis as três opções seguintes:

- **Aguardar até a próxima hora agendada**
- **Executar a tarefa logo que possível**
- **Executar a tarefa imediatamente se a hora desde a última execução exceder o intervalo especificado** (o intervalo pode ser definido utilizando a opção **Intervalo mínimo da tarefa**)

No próximo passo, é apresentada uma janela de resumo com as informações sobre a tarefa agendada atual. Clique no botão **Concluir**.

A nova tarefa agendada será adicionada à lista de tarefas agendadas no momento.

O sistema, por predefinição, contém tarefas agendadas fundamentais para garantir a funcionalidade correta do produto. Estas tarefas não devem ser alteradas e, por predefinição, estão ocultas. Para alterar esta opção e tornar estas tarefas visíveis, aceda a **Configurar** > **Introduzir preferências da aplicação ...** > **Ferramentas** > **Agenda** e selecione a opção **Mostrar tarefas do sistema**.

Criação de tarefa definida pelo utilizador

A data e a hora da tarefa **Definida pelo utilizador** têm de ser introduzidas no formato cron estendido por ano (uma cadeia composta por 6 campos separados por um espaço em branco):

```
minuto(0-59) hora(0-23) dia do mês(1-31) mês(1-12) ano(1970-2099) dia da semana(0-7)(Domingo = 0 ou 7)
```

Exemplo:

```
30 6 22 3 2012 4
```

Caracteres especiais suportados nas expressões cron:

- asterisco (`*`) - a expressão corresponderá a todos os valores do campo; por exemplo, asterisco no 3.º campo (dia do mês) significa todos os dias
- hífen (`-`) - define intervalos; por exemplo, `3-9`
- vírgula (`,`) - separa itens de uma lista; por exemplo, `1,3,7,8`
- barra (`/`) - define incrementos de intervalos; por exemplo, `3-28/5` no 3.º campo (dia do mês) significa 3.º dia do mês e depois de 5 em 5 dias.

Os nomes dos dias (segunda a domingo) e os nomes dos meses (janeiro a dezembro) não são suportados.

NOTA: Se definir o dia do mês e o dia da semana, o comando será executado apenas quando ambos os campos corresponderem.

Quarentena

A principal tarefa da quarentena é armazenar os ficheiros infetados em segurança. Os ficheiros devem ser colocados em quarentena se não for possível limpá-los, se não for seguro nem aconselhável eliminá-los ou se estiverem a ser falsamente detetados pelo System Center Endpoint Protection.

Pode optar por colocar qualquer ficheiro em quarentena. Recomenda-se a colocação de um ficheiro em quarentena se se comportar de modo suspeito, mas não for detetado pela análise antivírus.

Os ficheiros armazenados na pasta de quarentena podem ser visualizados numa tabela que apresenta a data e a hora da quarentena, o caminho da localização original do ficheiro infetado, o tamanho do ficheiro em bytes, o motivo (por exemplo, adicionado pelo utilizador...) e o número de ameaças (por exemplo, se for um arquivo compactado que contém diversas infiltrações). A pasta de quarentena com os ficheiros colocados em quarentena (*/Library/Application Support/Microsoft/scep/cache/quarantine*) permanece no sistema mesmo depois da desinstalação do System Center Endpoint Protection. Os ficheiros em quarentena são armazenados num formato encriptado e podem ser restaurados novamente após a instalação do System Center Endpoint Protection.

Colocação de ficheiros em quarentena

O System Center Endpoint Protection coloca automaticamente os ficheiros eliminados em quarentena (caso não tenha cancelado esta opção na janela de alertas). Se pretender, é possível colocar manualmente em quarentena qualquer ficheiro suspeito clicando no botão **Quarentena...**. O menu de contexto pode ser utilizado também para esta finalidade - prima ctrl, clique no campo em branco, selecione **Quarentena...**, escolha o ficheiro que pretende colocar em quarentena e clique no botão **Abrir**.

Restauro da Quarentena

Os ficheiros colocados em quarentena podem também ser restaurados para o local original. Para tal, utilize o botão **Restaurar**. A opção Restaurar também está disponível no menu de contexto premindo ctrl, clicando no ficheiro em questão na janela **Quarentena** e, em seguida, clicando em **Restaurar**. O menu de contexto oferece também a opção **Restaurar para...**, que permite restaurar um ficheiro para uma localização diferente da localização original da qual foi eliminado.

Relatórios

Os relatórios contêm informações sobre todos os eventos importantes do programa que ocorreram e fornecem uma visão geral das ameaças detetadas. O registo em relatório atua como uma ferramenta essencial na análise do sistema, na deteção de ameaças e na resolução de problemas. O registo em relatório é realizado ativamente em segundo plano, sem interação do utilizador. As informações são registadas com base nas definições atuais de detalhe do relatório. É possível ver mensagens de texto e relatórios diretamente do ambiente do System Center Endpoint Protection, bem como arquivar relatórios.

Os relatórios podem ser acedidos a partir do menu principal do System Center Endpoint Protection, clicando em **Ferramentas** > **Relatórios**. Selecione o tipo de relatório pretendido, utilizando o menu pendente **Relatório** na parte superior da janela. Estão disponíveis os seguintes relatórios:

1. **Ameaças detetadas** – Utilize esta opção para ver todas as informações sobre eventos relacionados com a deteção de infiltrações.
2. **Eventos** - Esta opção destina-se à resolução de problemas de administradores do sistema e utilizadores. Todas as ações importantes executadas pelo System Center Endpoint Protection são registadas nos relatórios de eventos.
3. **Análise do computador** - Os resultados de todas as análises concluídas são apresentadas nesta janela. Clique duas vezes em qualquer entrada para ver os detalhes da respetiva Análise do computador a pedido.

Em cada secção, as informações apresentadas podem ser copiadas diretamente para a área de transferência, selecionando a entrada e clicando no botão **Copiar**.

Manutenção de relatórios

A configuração de relatórios do System Center Endpoint Protection pode ser acedida a partir da janela principal do programa. Clique em **Configurar** > **Introduzir preferências da aplicação ...** > **Ferramentas** > **Relatórios**. Pode especificar as seguintes opções para os relatórios:

- **Eliminar relatórios antigos automaticamente** - as entradas de relatórios anteriores ao número de dias especificado são automaticamente eliminadas.
- **Otimizar automaticamente relatórios** - ativa a desfragmentação automática de relatórios se a percentagem especificada de registos não utilizados foi ultrapassada.

É possível armazenar todas as informações relevantes apresentadas na interface gráfica do utilizador e mensagens de ameaça ou eventos em formatos de texto legíveis por humanos, tais como texto simples ou CSV (valores separados por vírgulas). Se pretender disponibilizar estes ficheiros para processamento com ferramentas de terceiros, marque a caixa de verificação junto de **Ativar relatórios de ficheiros de texto**.

Para definir a pasta alvo em que os relatórios serão guardados, clique em **Configurar...** junto de **Configuração avançada**.

Com base nas opções selecionadas em **Relatórios de Texto: Editar**, pode guardar relatórios com as seguintes informações:

- As ameaças detetadas pela Análise de inicialização, Proteção em tempo real ou Análise do computador são armazenadas no ficheiro com o nome threatslog.txt.
- Eventos como *Nome de utilizador e palavra-passe inválidos*, *Não é possível atualizar a base de dados de assinatura de vírus*, etc. são guardados no ficheiro eventslog.txt.
- Os resultados de todas as análises concluídas são guardadas no formato scanlog.NÚMERO.txt.

Para configurar os filtros do **Padrão de registos de relatórios de análise do computador**, clique no botão **Editar...** junto desta opção e marque/desmarque os tipos de relatórios conforme necessário. Mais explicações sobre estes tipos de relatórios neste capítulo 20.

Filtragem de relatórios

Regista em relatórios as informações de armazenamento sobre eventos importantes do sistema. A funcionalidade de filtragem de relatórios permite visualizar registos sobre um tipo específico de evento.

Os tipos de relatórios usados com frequência são listados a seguir:

- **Avisos críticos** - erros críticos do sistema (por exemplo, falha ao iniciar a proteção antivírus)
- **Erros** - mensagens de erro, como "*Erro ao transferir ficheiro*" e erros críticos
- **Avisos** - mensagens de aviso
- **Registos informativos** - mensagens informativas, incluindo atualizações bem sucedidas, alertas, etc.
- **Registos de diagnóstico** - informações necessárias para ajustar o programa e também todos os registos descritos acima.

Interface do utilizador

As opções de configuração da interface do utilizador no System Center Endpoint Protection permitem-lhe ajustar o ambiente de trabalho de acordo com as suas necessidades. Estas opções de configuração podem ser acedidas em **Configurar** > **Introduzir preferências da aplicação ...** > **Utilizador** > **Interface**.

Nesta seção, a opção Modo avançado permite aos utilizadores alternar para o Modo avançado. O Modo avançado apresenta as definições mais detalhadas e os controles adicionais do System Center Endpoint Protection.

Para ativar a funcionalidade do ecrã inicial na inicialização, selecione a opção **Mostrar ecrã inicial na inicialização**.

Na secção **Usar menu padrão**, pode selecionar as opções **No modo padrão**/**No modo avançado** para ativar a utilização do menu padrão na janela principal do programa nos respetivos modos de apresentação.

Para ativar as sugestões de ferramentas, selecione a opção **Mostrar sugestões**. A opção **Mostrar ficheiros ocultos** permite-lhe visualizar e selecionar ficheiros ocultos na configuração **Alvos de análise** de uma **Análise do computador**.

Alertas e notificações

A secção **Alertas e notificações** permite-lhe configurar o modo como os alertas de ameaças e as notificações do sistema são tratados no System Center Endpoint Protection.

A desativação da opção **Mostrar alertas** irá cancelar todas as janelas de alertas e será adequada apenas em situações específicas. Para a maioria dos utilizadores, recomendamos que a predefinição desta opção seja mantida (ativada).

A seleção da opção **Mostrar notificações no ambiente de trabalho** irá ativar as janelas de alertas que não requeiram a interação do utilizador para serem apresentadas no ambiente de trabalho (por predefinição, no canto superior direito do ecrã). Pode definir o período durante o qual a notificação será apresentada, ajustando o valor **Fechar notificações automaticamente depois de** X **segundos**.

Configuração avançada de alertas e notificações

Mostrar apenas notificações que requerem interação do utilizador
Com esta opção, pode alternar a apresentação das mensagens que requeiram a interação do utilizador.

Mostrar apenas notificações que requerem interação do utilizador ao executar aplicações em modo de ecrã inteiro
Esta opção é útil durante apresentações ou outras atividades que requeiram o modo de ecrã inteiro.

Privilégios

As definições do System Center Endpoint Protection podem ser muito importantes para a política de segurança da organização. As modificações não autorizadas podem pôr em risco a estabilidade e a proteção do seu sistema. Por conseguinte, pode escolher os utilizadores que terão permissão para editar a configuração do programa.

Para especificar os utilizadores privilegiados, aceda a **Configurar** > **Introduzir preferências da aplicação ...** > **Utilizador** > **Privilégios**.

Para fornecer segurança máxima ao seu sistema, é fundamental que o programa seja configurado corretamente. As modificações não autorizadas podem resultar na perda de dados importantes. Para definir uma lista de utilizadores privilegiados, basta selecioná-los na lista **Utilizadores** do lado esquerdo e clicar no botão **Adicionar**. Para remover um utilizador, basta selecionar o respetivo nome na lista **Utilizadores privilegiados** do lado direito e clicar em **Remover**.

NOTA: Se a lista de utilizadores privilegiados estiver vazia, todos os utilizadores do sistema terão permissão para editar as definições do programa.

Menu de contexto

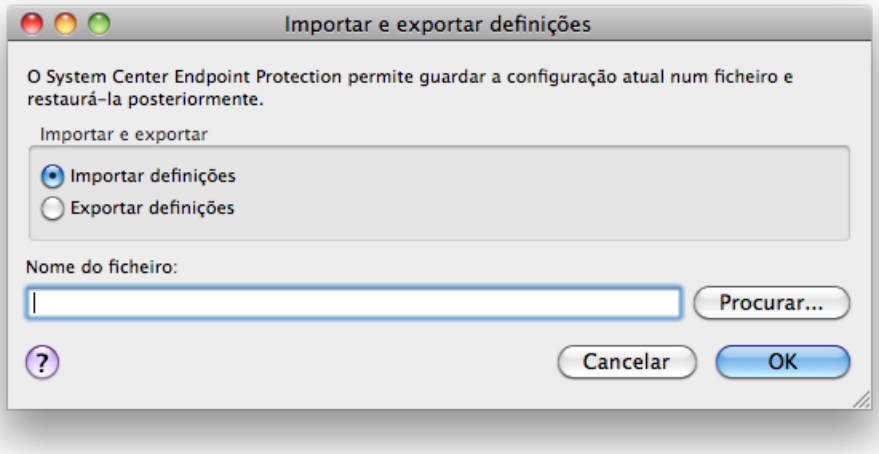
A integração do menu de contexto pode ser ativada na secção **Configurar** > **Introduzir preferências da aplicação ...** > **Utilizador** > **Menu de contexto**, selecionando a caixa de verificação **Integrar ao menu de contexto**.

Utilizador avançado

Importar e exportar definições

A importação e a exportação das definições do System Center Endpoint Protection estão disponíveis no modo Avançado, em **Configurar**.

A Importação e a Exportação utilizam arquivos compactados para armazenar a configuração. A importação e a exportação são úteis caso seja necessário fazer uma cópia de segurança da configuração do System Center Endpoint Protection para que a mesma possa ser utilizada posteriormente. A opção de exportação de definições também é conveniente para os utilizadores que pretendam utilizar as suas configurações preferenciais do System Center Endpoint Protection em diversos sistemas. Os utilizadores também podem importar o ficheiro de configuração para transferir as definições pretendidas.



Importar definições

Importar uma configuração é muito fácil. No menu principal, clique em **Configurar** > **Importar e exportar definições ...** e selecione a opção **Importar definições**. Introduza o nome do ficheiro de configuração ou clique no botão **Procurar...** para procurar o ficheiro de configuração que pretende importar.

Exportar definições

Os passos para exportar uma configuração são muito semelhantes. No menu principal, clique em **Configurar** > **Importar e exportar definições ...** Selecione a opção **Exportar definições** e introduza o nome do ficheiro de configuração. Utilize o navegador para selecionar uma localização no computador onde pretende guardar o ficheiro de configuração.

Configuração do servidor proxy

As definições do servidor proxy podem ser configuradas em **Diversos** > **Servidor proxy**. A especificação do servidor proxy neste nível define as definições globais do servidor proxy para todas as funções do System Center Endpoint Protection. Aqui os parâmetros serão utilizados por todos os módulos que exigem ligação à Internet.

Para especificar as definições do servidor proxy para este nível, selecione a caixa de verificação **Usar servidor proxy** e, em seguida, o endereço IP ou o URL do servidor proxy no campo **Servidor proxy**. No campo Porta, especifique a porta em que o servidor proxy aceita as ligações (3128 por predefinição). Se a comunicação com o servidor proxy requerer autenticação, selecione a caixa de verificação **O servidor proxy requer autenticação** e introduza um **Nome de utilizador** e uma **Palavra-passe** válidos nos respetivos campos.

Bloqueio de suporte amovível

Os suportes amovíveis (por exemplo, CD ou chaves USB) podem conter código malicioso e colocar o computador em risco. Para bloquear o suporte amovível, marque a caixa de verificação junto de **Ativar bloqueio de suporte amovível**. Para permitir o acesso a determinados tipos de suporte, desmarque as caixas de verificação junto dos tipos de suporte que pretende disponibilizar.

Marque a caixa de verificação junto de **Outros** se pretender aplicar estas definições a tipos de suporte que não CD, DVD, FireWire ou USB. Esta definição aplica-se, principalmente, a periféricos ligados ao seu computador através da interface Thunderbolt.

Glossário

Tipos de infiltrações

Uma infiltração é uma parte do software malicioso que tenta aceder e/ou danificar o computador de um utilizador.

Vírus

Um vírus informático é uma infiltração que corrompe os ficheiros existentes no computador. O nome vírus é proveniente dos vírus biológicos, uma vez que utilizam técnicas semelhantes para se propagarem de um computador para outro.

Os vírus informáticos atacam principalmente ficheiros executáveis, scripts e documentos. Para se replicar, um vírus anexa o seu "corpo" ao fim de um ficheiro de destino. Em resumo, um vírus informático funciona da seguinte maneira: após a execução do ficheiro infetado, o vírus ativa-se a si próprio (antes da aplicação original) e realiza a sua tarefa predefinida. Só depois disso, a aplicação original pode ser executada. Um vírus só pode infetar um computador se um utilizador (acidental ou deliberadamente) executar ou abrir o programa malicioso.

Os vírus informáticos podem variar em termos de finalidade e gravidade. Alguns deles são extremamente perigosos devido à sua capacidade de eliminar propositadamente ficheiros de um disco rígido. Por outro lado, alguns vírus não causam quaisquer danos; apenas servem para aborrecer o utilizador e demonstrar as capacidades técnicas dos respetivos autores.

É importante salientar que os vírus (quando comparados com os cavalos de troia ou spyware) estão a tornar-se cada vez mais raros, uma vez que não são comercialmente atrativos para os autores de software malicioso. Além disso, o termo "vírus" é frequentemente utilizado de modo incorreto para abranger todos os tipos de infiltrações. Esta utilização está gradualmente a ser ultrapassada e substituída pelo novo e mais preciso termo "malware" (software malicioso).

Se o seu computador for infetado por um vírus, será necessário restaurar os ficheiros infetados para o estado original, ou seja, limpá-los utilizando um programa antivírus.

Exemplos de vírus são: *OneHalf*, *Tenga* e *Yankee Doodle*.

Worms

Um worm informático é um programa que contém código malicioso que ataca os computadores host e se propaga através de uma rede. A diferença básica entre um vírus e um worm é que os worms têm a capacidade de se replicar e viajar por conta própria; estes não dependem dos ficheiros host (ou dos setores de inicialização). Os worms são propagados através dos endereços de email da sua lista de contatos ou aproveitam-se das vulnerabilidades da segurança das aplicações de rede.

Os worms são, por conseguinte, muito mais viáveis que os vírus informáticos. Devido à ampla disponibilidade da Internet, os worms podem propagar-se por todo o globo em horas após a sua libertação – em alguns casos, até em minutos. Esta capacidade de se replicarem de forma autónoma e rápida torna-os mais perigosos que outros tipos de malware.

Um worm ativado num sistema pode causar muitos transtornos: Pode eliminar ficheiros, prejudicar o desempenho do sistema ou até mesmo desativar programas. A natureza de um worm informático qualifica-o como um "meio de transporte" para outros tipos de infiltrações.

Se o seu computador for infectado por um worm, recomendamos que elimine os ficheiros infetados porque provavelmente contêm código malicioso.

Exemplos de worms conhecidos são: *Lovsan/Blaster*, *Stration/Warezov*, *Bagle* e *Netsky*.

Cavalos de troia (Trojans)

Historicamente, os cavalos de troia informáticos foram definidos como uma classe de infiltrações que tenta apresentar-se como programas úteis, enganando assim os utilizadores que permitem a respetiva execução. Atualmente, deixou de ser necessário disfarçar os cavalos de troia. O seu único propósito é infiltrar-se o mais facilmente possível e atingir os seus objetivos maliciosos. O "cavalo de troia" tornou-se um termo muito genérico para descrever qualquer infiltração que não pertença a nenhuma classe específica de infiltração.

Uma vez que esta é uma categoria muito abrangente, é frequentemente dividida em muitas subcategorias:

- Downloader – Um programa malicioso com a capacidade de fazer a transferência de outras infiltrações da Internet.
- Dropper – Um tipo de cavalo de troia criado para instalar outros tipos de malware em computadores comprometidos.
- Backdoor – Uma aplicação que se comunica com atacantes remotos e que permite que obtenham acesso a um sistema e assumam o controlo do mesmo.
- Keylogger – (keystroke logger) – Um programa que regista cada toque de tecla do utilizador e envia as informações para os atacantes remotos.

- Dialer – Dialers são programas criados para estabelecerem ligação com os números premium-rate. É quase impossível para um utilizador notar que foi criada uma nova ligação. Os dialers apenas podem causar danos aos utilizadores com modems de ligação telefónica, que deixaram de ser utilizados com tanta frequência.
- Os cavalos de troia geralmente tomam a forma de ficheiros executáveis. Se um ficheiro no computador for detetado como um cavalo de troia, recomenda-se que o elimine, uma vez que é muito provável que contenha código malicioso.

Exemplos de cavalos de troia conhecidos são: *NetBus*, *Trojandownloader.Small.ZL*, *Slapper*.

Adware

Adware é a abreviatura de "advertising-supported software" (software suportado por publicidade). Os programas que apresentam material publicitário pertencem a esta categoria. Geralmente, as aplicações adware abrem automaticamente uma nova janela pop-up com publicidade num navegador da Internet, ou mudam a home page do mesmo. O adware está frequentemente integrado em programas freeware, permitindo que os criadores de programas freeware cubram os custos de programação das suas aplicações (normalmente úteis).

O adware por si só não é perigoso; os utilizadores serão apenas incomodados pela publicidade. O perigo está no facto de o adware também poder realizar funções de análise (à semelhança do spyware).

Se decidir utilizar um produto freeware, preste especial atenção ao programa de instalação. É muito provável que o instalador o notifique sobre a instalação de um programa adware extra. Normalmente, poderá cancelá-lo e instalar o programa sem o adware.

Alguns programas não serão instalados sem o adware, caso contrário as respetivas funcionalidades ficarão limitadas. Isto significa que o adware irá aceder com frequência ao sistema "legalmente", uma vez que os utilizadores assim o concordaram. Neste caso, é melhor prevenir do que remediar. Se um ficheiro for detetado como adware no computador, recomenda-se que o elimine, uma vez que há uma grande probabilidade de conter código malicioso.

Spyware

Esta categoria abrange todas as aplicações que enviam informações privadas sem o consentimento/conhecimento do utilizador. Os spywares utilizam as funções de análise para enviar diversos dados estatísticos, como listas dos Web sites visitados, endereços de email da lista de contatos do utilizador ou uma lista das teclas registadas.

Os autores de spyware alegam que estas técnicas têm por objetivo saber mais sobre as necessidades e os interesses dos utilizadores e permitir um melhor direcionamento da publicidade. O problema é que não existe uma distinção clara entre as aplicações maliciosos e as úteis, e ninguém pode assegurar que as informações recebidas não serão utilizadas indevidamente. Os dados obtidos pelas aplicações spyware podem conter códigos de segurança, PINs, números de contas bancárias, etc. O spyware é frequentemente integrado em versões gratuitas de um programa pelo seu autor com a finalidade de gerar receitas ou incentivar à aquisição do software. Geralmente, os utilizadores são informados da presença do spyware durante a instalação do programa no sentido de os incentivar a atualizar para uma versão paga sem o mesmo.

Exemplos de produtos freeware bem conhecidos que vêm integrados com spyware são as aplicações cliente das redes P2P (peer-to-peer). O Spyfalcon ou Spy Sheriff (e muitos mais) pertencem a uma subcategoria de spyware específica; parecem ser programas antispyware, mas são, na verdade programas spyware.

Se um ficheiro for detectado como spyware no computador, recomenda-se que o elimine, uma vez que há uma grande probabilidade de conter código malicioso.

Aplicações potencialmente inseguras

Existem muitos programas legítimos cuja função é a de simplificar a administração dos computadores ligados em rede. No entanto, nas mãos erradas, estes podem ser utilizados indevidamente para fins maliciosos. O System Center Endpoint Protection fornece a opção de detetar tais ameaças.

"Aplicações potencialmente inseguras" é a classificação utilizada para software comercial legítimo. Esta classificação inclui programas como ferramentas de acesso remoto, aplicações para desbloquear palavras-passe e keyloggers (um programa que regista cada toque de tecla do utilizador).

Se pensa haver uma aplicação potencialmente insegura e em execução no computador (e que não instalou), consulte o administrador de rede ou remova a aplicação.

Aplicações potencialmente não desejadas

As aplicações potencialmente não desejadas não são necessariamente maliciosas, mas podem afetar negativamente o desempenho do computador. Tais aplicações exigem geralmente o consentimento para a instalação. Se estas aplicações estiverem presentes no computador, o sistema irá comportar-se de modo diferente (em comparação ao modo como se comportava antes da instalação destas aplicações). As alterações mais significativas são:

- são abertas novas janelas que não visualizava anteriormente
- ativação e execução de processos ocultos
- aumento da utilização de recursos do sistema
- alterações nos resultados de pesquisa
- a aplicação comunica com servidores remotos.