SOPHOS

Cybersecurity made simple.

Sophos Central Device Encryption

Manual do administrador

Índice

1 Sobre a Sophos Central Device Encryption

O Sophos Central Device Encryption permite gerenciar a Encriptação da Unidade de Disco do BitLocker em endpoints do Windows e a encriptação FileVault em endpoints do Mac através do Sophos Central.

A encriptação de discos rígidos mantém os dados em segurança, mesmo quando um dispositivo é perdido ou roubado.

Este manual descreve como configurar e usar o Device Encryption. Ele trata também sobre como acessar seu código de recuperação usando o Portal de Autoatendimento. Para obter detalhes sobre as configurações de política, alertas e recuperação por meio do Sophos Central, consulte Sophos Central ajuda.

Informações relacionadas

Ajuda do Sophos Central

2 Gerenciar encriptação da unidade do BitLocker

Esta seção descreve os pré-requisitos para usar Encriptação da Unidade de Disco do BitLocker em endpoints do Windows na sua rede, os vários modos de autenticação disponíveis e como eles interagem com as configurações da política de grupo de propriedade.

2.1 Migrar para o Sophos Central Device Encryption

Se você já estiver usando o SafeGuard Enterprise com Encriptação da Unidade de Disco do BitLocker ou Sophos Full Disk Encryption, esta sessão descreve como migrar para o Sophos Central Device Encryption.

Falaremos sobre:

- SafeGuard Enterprise e BitLocker
- SafeGuard Enterprise e Sophos Full Disk Encryption
- Para obter informações sobre como migrar endpoints do Mac, consulte Migrar para o Sophos Central Device Encryption (Mac).

Tarefas relacionadas

Migrar para o Sophos Central Device Encryption (Mac) (página 14)
Se quiser usar o Sophos Central para gerenciar endpoints do Mac que já estão encriptados com FileVault, você precisa aplicar uma política Sophos Central Device Encryption para esses endpoints, ou pontos finais.

2.1.1 Migrar do SafeGuard Enterprise BitLocker

Siga estas etapas para migrar.

Nota
Se estiver usando o BitLocker with SafeGuard Enterprise versão 6.x ou 7.x, recomendamos que você faça o upgrade para a mais nova versão do SafeGuard Enterprise primeiro.

Se estiver usando o SafeGuard Enterprise versão 6.x ou 7.x, você deverá decodificar o disco do sistema seguindo os passos na Ajuda do administrador no SafeGuard Enterprise antes de poder migrar para o Sophos Central Device Encryption.

Para migrar de um SafeGuard Enterprise BitLocker Client (versão 8.0 ou posterior) para o Sophos Central Device Encryption:

1. Vá para **Painel de controle > Desinstalar um programa** e clique com o botão direto em **Sophos SafeGuard Client**.
2. Selecione **Alterar** no menu exibido.
   É aberto o assistente para instalação do Sophos SafeGuard Client.

3. Desinstale o componente BitLocker.

   Nota
   Remover o componente BitLocker não decodifica seus volumes ou arquivos.

4. Instale o software Sophos Central Device Encryption.
5. Certifique-se de que a política Sophos Central Device Encryption esteja atribuída ao endpoint e ativada.

Agora você pode gerenciar o BitLocker usando o Sophos Central. Não é necessário encriptar novamente. Assim que você aplica a política Sophos Central Device Encryption ao endpoint, o código de recuperação é renovado e enviado ao Sophos Central. A funcionalidade de encriptação de arquivo permanece inalterada.

Informações relacionadas
Ajuda do administrador no SafeGuard Enterprise

2.1.2 Migrar do SafeGuard Enterprise Full Disk Encryption

Siga estas etapas para migrar.

Para migrar do SafeGuard Enterprise Full Disk Encryption:

1. Desinstale o software Sophos SafeGuard Client.
   Volumes encriptados são decodificados automaticamente. Arquivos encriptados permanecem encriptados.
2. Instale o software Sophos Central Device Encryption.
3. Certifique-se de que a política Sophos Central Device Encryption esteja atribuída ao endpoint e habilitada.
4. Reinstale o módulo SafeGuard Enterprise Full Disk Encryption (encriptação sincronizada ou encriptação de arquivo baseada em local).

Agora você pode gerenciar o BitLocker usando o Sophos Central. Assim que a política Sophos Central Device Encryption tenha sido aplicada ao endpoint, a encriptação começa em segundo plano e o código de recuperação é renovado e enviado ao Sophos Central.

2.2 Preparar o Device Encryption

Por default, a maioria das unidades de sistemas está preparada para o BitLocker. Caso contrário, o Sophos Central Device Encryption automaticamente executará a ferramenta de linha de comando da Microsoft `BdeHdCfg.exe` requerida para preparar a unidade de disco.

Isso significa que uma partição separada do BitLocker é criada na unidade de disco do sistema.

Durante a configuração do Sophos Central Device Encryption, uma mensagem informará ao usuário que é necessária uma reinicialização para preparar a unidade de disco do sistema. O usuário pode optar por fazer a reinicialização imediatamente ou adiar a operação. A Encriptação de Dispositivo só pode ter início quando o computador for reinicializado e a preparação da unidade de disco do sistema tiver sido bem-sucedida.

A versão do .NET Framework exigida pelo Device Encryption é instalada nos endpoints automaticamente.

2.3 Encriptação de dispositivo, passo a passo

Siga estas etapas para encriptar dispositivos.

Antes que os usuários possam começar:

- O software agente do Sophos Central deve ser instalado nos endpoints.
- Uma política de Encriptação de Dispositivo deve ser configurada e habilitada no Sophos Central.
- Os usuários devem iniciar uma sessão interativa em seus endpoints para que eles sejam conectados e sincronizados com o Sophos Central. Observe que o logon remoto não é suportado.
- O sistema operacional deve ser compatível com a Encriptação de Unidade de Disco BitLocker. Para obter mais informações, consulte Preparar encriptação de dispositivo e Compatibilidade do sistema de encriptação do dispositivo.

Estas instruções lhe informam o que os usuários verão e o que precisarão fazer:

1. Se o hardware de segurança TPM ainda não estiver habilitado, uma ação BIOS é desencadeada para habilitá-lo. Será necessária uma reinicialização. O usuário pode fazer a reinicialização imediatamente ou adiá-la.
   Durante a reinicialização, o usuário será solicitado a habilitar o TPM. Caso o TPM não puder ser habilitado ou o usuário não responder, será exibida uma mensagem.
2. Caso o TPM esteja ativo e habilitado, porém sem proprietário, o software agente do Sophos Central automaticamente gerará e definirá as informações de proprietário do TPM. Um alerta será enviado ao Sophos Central caso isso não aconteça.
3. Caso as chaves de endosso do TPM estejam ausentes, o software agente do Sophos Central automaticamente as criará. Um alerta será enviado ao Sophos Central caso isso não aconteça.
4. Se a política Device Encryption não especificar que ela **Requer autenticação na inicialização**, a encriptação do disco rígido inicia automaticamente. Nesse caso, o usuário não precisará fazer nada. Você pode ir direto para o passo 8.
5. Se a política Device Encryption especificar que ela **Requer autenticação na inicialização**, o usuário verá o diálogo **Sophos Device Encryption**.
   - Caso a política Device Encryption requeira um PIN ou senha para autenticação, siga as instruções na tela para definir o PIN ou senha. Se TPM+PIN for usado, a chave de encriptação para o disco do sistema será armazenada no TPM.

     Nota
     Os usuários devem ter cuidado ao criarem uma senha. O ambiente de pré-inicialização é compatível apenas com teclados com layout em Inglês dos EUA. Caso definam um PIN ou senha com caracteres especiais, pode ser que tenham que usar teclas diferentes ao digitá-los para iniciar posteriormente uma sessão.

   - Caso a política Device Encryption requeira um pen drive para autenticação, será necessário conectar uma unidade de memória flash USB ao computador. A unidade de memória flash USB deve ser formatada com NTFS, FAT ou FAT32.
6. Quando o usuário clica em **Reiniciar e Encriptar**, o computador é reinicializado e verifica se a Device Encryption funciona.
   O usuário pode selecionar **Deixar para mais tarde** para fechar o diálogo. No entanto, ele aparecerá novamente na próxima vez em que o usuário iniciar uma sessão ou quando você alterar a política Device Encryption.

7. Se o usuário não puder inserir o PIN/senha correta, ele pode pressionar a tecla `Esc`. O sistema é inicializado normalmente, pois a encriptação ainda não foi aplicada. O usuário é solicitado a inserir novamente o PIN/senha após iniciar a sessão.
8. É possível ver quais usuários ainda não possuem a encriptação habilitada. Isso significa que eles ainda não reiniciaram seus computadores ou ainda não completaram as instruções na tela. Procure em **Relatórios** no Sophos Central.
9. Se o teste de pré-inicialização for bem-sucedido, o software agente do Sophos Central iniciará a encriptação dos discos rígidos. A encriptação ocorre em segundo plano, permitindo aos usuários trabalharem normalmente com os seus computadores.
   Caso o teste de hardware apresente erro, o sistema será reinicializado e a encriptação não será imposta. Será enviado um evento ao Sophos Central para que você seja notificado.
10. Após o agente do Sophos Central ter encriptado o volume do sistema, será iniciada a encriptação dos volumes de dados (se especificado na política). A proteção desses volumes é armazenada no volume do sistema, para que os volumes de dados estejam automaticamente disponíveis após a inicialização. Isso significa que quando um usuário inicia uma sessão em seu computador, os volumes de dados podem ser acessados sem qualquer outra interação por parte do usuário. Os volumes de dados removíveis, como unidades flash USB, não são encriptados.

Você pode encontrar dois arquivos - `CDE.log` e `CDE_trace.xml` em `%ProgramData%\Sophos\Sophos Data Protection\Logs` no endpoint.

Conceitos relacionados

Preparar o Device Encryption (página 3)
Por default, a maioria das unidades de sistemas está preparada para o BitLocker. Caso contrário, o Sophos Central Device Encryption automaticamente executará a ferramenta de linha de comando da Microsoft `BdeHdCfg.exe` requerida para preparar a unidade de disco.

Compatibilidade do sistema de Encriptação de Dispositivo (página 5)
A tabela abaixo faz um resumo dos tipos de proteção que são compatíveis com qual plataforma. O tipo de proteção aplicada depende da versão utilizada do Windows e se há um hardware de segurança TPM disponível.

TPM+PIN (página 7)
O modo TPM+PIN utiliza o hardware de segurança TPM do computador e um PIN como forma de autenticação.

2.4 Compatibilidade do sistema de Encriptação de Dispositivo

A tabela abaixo faz um resumo dos tipos de proteção que são compatíveis com qual plataforma. O tipo de proteção aplicada depende da versão utilizada do Windows e se há um hardware de segurança TPM disponível.

O número entre parênteses descreve a prioridade do tipo de proteção específica.

(*) Quando a função **Requer autenticação na inicialização** encontra-se habilitada, a instalação da proteção 'apenas TPM' não é possível e, portanto, o TPM+PIN é a primeira prioridade.

	Win 7 sem TPM	Win 7 com TPM	Win 8.1 sem TPM	Win 8.1 com TPM	Win 10 sem TPM	Win 10 com TPM
Apenas TPM	-	ok (1*)	-	ok (1*)	-	ok (1*)

	Win 7 sem TPM	Win 7 com TPM	Win 8.1 sem TPM	Win 8.1 com TPM	Win 10 sem TPM	Win 10 com TPM
TPM+PIN	-	ok (2)	-	ok (2)	-	ok (2)
Frase de segurança	-	-	ok (1)	ok (3)	ok (1)	ok (3)
Pen drive	ok (1)	ok (3)	-	-	-	-

Poderá ser necessário configurar o TPM no computador de endpoint quando estiver utilizando o Central Device Encryption.

Se estiver utilizando o TPM 2.0 ou posterior, você tem de formatar o disco rígido como GPT e o BIOS tem de estar no modo UEFI.

Se estiver utilizando o TPM 1.2, tem de ativar o TPM no BIOS/UEFI e este tem de estar pronto para ser utilizado. Você pode verificar isso usando `TPM.MSC`.

Recomendamos que atualize os seus computadores de endpoint para a versão mais recente do BIOS/UEFI antes de instalar o Central Device Encryption.

Quando o modo Windows FIPS está habilitado, a encriptação BitLocker é compatível apenas em sistemas que possuam o Windows 8.1 ou Windows 10. Para obter informações detalhadas sobre o BitLocker no modo FIPS no Windows 7, consulte Uma senha de recuperação compatível com FIPS não pode ser salva no AD DS para BitLocker no Windows 7 ou no Windows Server 2008 R2.

Você pode usar discos rígidos encriptados com a Sophos Central Device Encryption. Para obter mais informações, consulte Unidade de disco rígido encriptada.

Central Device Encryption é compatível com BitLocker pré-provisionado.

Informações relacionadas

Uma senha de recuperação compatível com FIPS não pode ser salva no AD DS para BitLocker no Windows 7 ou no Windows Server 2008 R2

Unidade de disco rígido encriptada

2.5 Modos de autenticação da Encriptação de Dispositivo

Você pode usar o botão **Requer autenticação na inicialização** nas configurações de Encriptação de Dispositivo para definir se os usuários precisam se autenticar ao iniciarem uma sessão em seus computadores.

O modo de autenticação instalado nos computadores depende do sistema, das configurações da política de grupo do BitLocker e da política de Encriptação de Dispositivo. Dependendo da compatibilidade do sistema de Encriptação de Dispositivo, um dos seguintes modos de autenticação será instalado nos endpoints:

- TPM+PIN
- Frase de segurança
- Apenas TPM
- Pen drive

Em endpoints que já estão encriptados com o BitLocker, uma mensagem informará os usuários sobre as etapas necessárias.

Quando você ativa **Requer autenticação na inicialização**, os usuários são solicitados a definir um PIN / frase de segurança / pen drive e clicar em **Aplicar**. Após isso, eles precisarão usar esse PIN / frase de segurança / pen drive toda vez que iniciarem o computador. Quando você desativa **Requer autenticação na inicialização**, o modo Apenas TPM é aplicado automaticamente e nenhuma outra autenticação adicional será necessária. Os usuários são informados que seu computador desbloqueará automaticamente o dispositivo quando ele for iniciado.

A Sophos Device Encryption pode configurar automaticamente o objeto da política de grupo (GPO) para que todos os modos de autenticação sejam permitidos, contanto que o ajuste correspondente seja definido em **não configurado**. Quando você configura manualmente o ajuste, o software não apaga estas definições. Para mais informações, consulte Configurações das políticas de grupo do BitLocker.

Os usuários podem decidir adiar a instalação dos modos de autenticação. Neste caso, não haverá nenhuma encriptação. Sempre que um usuário reinicia uma sessão no Windows ou quando você implanta uma nova política de encriptação, o sistema solicita ao usuário reiniciar o computador. Após a reinicialização, o modo de autenticação é instalado e tem início a Encriptação de Dispositivo. Após isso, os usuários não poderão desencriptar seus dispositivos.

Conceitos relacionados

Compatibilidade do sistema de Encriptação de Dispositivo (página 5)
A tabela abaixo faz um resumo dos tipos de proteção que são compatíveis com qual plataforma. O tipo de proteção aplicada depende da versão utilizada do Windows e se há um hardware de segurança TPM disponível.

Configurações das políticas de grupo do BitLocker (página 9)
O Sophos Central define automaticamente algumas políticas de grupo, para que os administradores não precisem preparar os computadores para encriptação de dispositivo.

2.5.1 TPM+PIN

O modo TPM+PIN utiliza o hardware de segurança TPM do computador e um PIN como forma de autenticação.

Os usuários precisarão inserir esse PIN no ambiente de pré-inicialização do Windows sempre que o computador for iniciado.

O TPM+PIN requer um TPM preparado e as configurações de GPO do sistema devem permitir o modo TPM+PIN.

Se todas as condições forem atendidas, o diálogo de configuração do TPM+PIN será exibido e o usuário solicitado a definir um PIN. O usuário pode clicar em **Reiniciar e Encriptar** para imediatamente reinicializar o computador e começar a encriptação.

Caso a configuração de GPO **Permitir PINs avançados para a inicialização** esteja habilitada, o PIN pode incluir números, letras e caracteres especiais. Do contrário, somente números serão permitidos.

Os PINs para o BitLocker devem possuir de 4 a 20 caracteres. Você pode definir um tamanho mínimo maior através de uma política de grupo. O software agente do Sophos Central configurará a política de grupo para permitir PINs avançados. A caixa de diálogo informa o usuário sobre quais caracteres podem ser inseridos e quais os tamanhos mínimos e máximos permitidos.

Nota
Todos os usuários de um computador Windows específico precisam usar o mesmo PIN para desbloquear o disco do sistema. Posteriormente, eles se conectam ao sistema operacional com suas credenciais individuais. O single sign-on não é compatível em computadores Windows.

2.5.2 Frase de segurança

Para autenticação em endpoints sem o hardware de segurança TPM, é possível utilizar uma frase de segurança.

Os usuários precisarão inserir esta frase de segurança no ambiente de pré-inicialização do Windows sempre que o computador for iniciado.

A proteção por frase de segurança requer o Windows 8.0 ou versão mais recente e as configurações de GPO do sistema devem permitir o modo de frase de segurança.

Se todas as condições forem atendidas, o diálogo de configuração da frase de segurança será exibido e o usuário solicitado a definir uma frase de segurança com comprimento de 8 a 100 caracteres. O usuário pode clicar em **Reiniciar e Encriptar** para imediatamente reinicializar o computador e começar a encriptação.

2.5.3 Apenas TPM

O modo 'Apenas TPM' utiliza o hardware de segurança TPM do computador sem qualquer autenticação de PIN.

Isso significa que o usuário pode ligar o computador sem ser solicitado a informar um PIN no ambiente de pré-inicialização do Windows.

O modo 'Apenas TPM' requer um TPM preparado e a configuração da política de Encriptação de Dispositivo **Requer autenticação na inicialização** deve ser desabilitada. Além disso, as configurações de GPO do sistema devem permitir a proteção 'Apenas TPM'.

Se todas as condições forem atendidas, será exibida a caixa de diálogo da instalação da proteção 'Apenas TPM'. O usuário pode clicar em **Reiniciar e Encriptar** para imediatamente reiniciar o computador e começar a encriptação.

2.5.4 Pen drive

O modo Pen Drive utiliza um código armazenado em uma unidade de memória flash USB como forma de autenticação.

Para cada inicialização, a unidade de memória flash USB deve estar conectada ao computador.

A proteção de pen drive é utilizada nos endpoints do Windows 7 caso nenhum TPM esteja disponível ou caso tenha sido desabilitada através do GPO.

A unidade de memória flash USB deve ser formatada com NTFS, FAT, ou FAT32. O formato exFAT não é compatível. Além disso, a unidade de memória flash USB deve ser gravável.

Se todas as condições forem atendidas, o diálogo de instalação da proteção de pen drive será exibido e o usuário deverá conectar uma unidade de memória flash USB que será usada para armazenar o código.

O usuário pode clicar em **Reiniciar e Encriptar** para imediatamente reiniciar o computador e começar a encriptação.

2.6 Configurações das políticas de grupo do BitLocker

O Sophos Central define automaticamente algumas políticas de grupo, para que os administradores não precisem preparar os computadores para encriptação de dispositivo.

Caso os ajustes já tenham sido definidos pelos administradores, os valores configurados não serão sobrescritos.

Em **Editor de Políticas de Grupo Local** em **Configuração do Computador > Modelos Administrativos > Componentes do Windows > Encriptação da Unidade de Disco do BitLocker > Unidades de Disco do Sistema Operacional**, você encontrará as seguintes políticas:

Política	Ajuste	Valor definido pelo Sophos Central	Comentário
Permitir desbloqueio de rede na inicialização		Habilitado	Você pode permitir o desbloqueio de uma rede BitLocker pré-configurada para continuar trabalhando após ter habilitado a Encriptação de Dispositivo Central.
Exigir autenticação adicional na inicialização	Permite o BitLocker sem um TPM compatível	Verificado	Ajustado para o Windows 8 caso nenhum TPM esteja disponível, para permitir a utilização de uma senha no momento da inicialização para desbloquear o disco do sistema.
Exigir autenticação adicional na inicialização	Configurar PIN de inicialização do TPM	Permitir PIN de inicialização com TPM	Se a configuração da política de Encriptação de Dispositivo **Requer autenticação na inicialização** estiver configurada e o sistema possuir um TPM, esta configuração de política de grupo permitirá a proteção da unidade de disco do sistema por TPM, e o usuário também será solicitado a inserir um PIN.
Permitir PINs avançados para inicialização	n/d	Habilitado	Ajustado para permitir a utilização de PINs alfanuméricos para proteger a unidade de disco do sistema com TPM. Caso não puder ser ajustado, serão permitidos apenas dígitos.

Política	Ajuste	Valor definido pelo Sophos Central	Comentário
Configurar a mensagem de recuperação de pré-inicialização e URL	Selecionar uma opção para a mensagem de recuperação de pré-inicialização	Usar mensagem de recuperação padrão e URL	Definido para usar a mensagem padrão da Sophos e URL.
Configurar a mensagem de recuperação de pré-inicialização e URL	Opção de mensagem de recuperação personalizada	Não tem um código de recuperação? Entre em contato com a equipe de Assistência de TI ou acesse o Portal de Autoatendimento: `https://sophos.com/ssp`	
Configurar a mensagem de recuperação de pré-inicialização e URL	Opção de URL de recuperação personalizada		
Configurar o uso de encriptação baseada em hardware para unidades de dados fixos	n/d	Desabilitado	Definido para impor a encriptação baseada em software. Contudo, se a configuração existente de uma política de grupo de BitLocker exigir encriptação baseada em hardware, a configuração dessa política não será substituída.
Configurar o uso de encriptação baseada em hardware para unidades de sistemas operacionais	n/d	Desabilitado	Definido para impor a encriptação baseada em software. Contudo, se a configuração existente de uma política de grupo de BitLocker exigir encriptação baseada em hardware, a configuração dessa política não será substituída.

- Algoritmo de encriptação a ser usado: Por default, Sophos Central Device Encryption utiliza o AES-256. Existe um ajuste de política de grupo que pode ser usado para selecionar o AES-128.
- Requisitos de PIN/senha: Existem ajustes de política de grupo que podem ser usados para definir um tamanho mínimo de PIN/senha e para exigir senhas complexas.
- Encriptar todos os dados ou apenas o espaço utilizado: Se a política de grupo para volumes de inicialização e/ou de dados for configurada para exigir encriptação total de dados, ela prevalecerá sobre qualquer política do Sophos Central que permita a encriptação somente do espaço utilizado.

Algumas configurações de política de grupo podem entrar em conflito com o Sophos Central e, assim, a encriptação não pode ser habilitada. Nesse caso, é enviado um evento para o Sophos Central.

- Smart card requerido: Se uma política de grupo requerer a utilização de um smart card para o BitLocker, isso não será compatível com o Sophos Central e gerará um evento de erro.
- Encriptar todos os dados ou apenas o espaço utilizado: Se a política de grupo para volumes de inicialização e/ou de dados for configurada para encriptar somente o espaço utilizado mas a política do Sophos Central exigir encriptação total, isso gerará um evento de erro.

Se quiser encriptar aparelhos tablet (como o MS Surface Pro) e usar autenticação de inicialização, você precisa habilitar a seguinte configuração de política de grupo:

Habilitar uso da autenticação do BitLocker que exige entrada de teclado pré-inicialização em slates

Para ver mais detalhes, consulte o artigo 125772 da base de conhecimentos.

Para obter mais informações gerais sobre as configurações de política de grupo do BitLocker e do TPM, consulte Configurações das políticas de grupo do BitLocker e Configurações das políticas de grupo de serviços Trusted Platform Module.

Conceitos relacionados

Método de encriptação e relatórios (página 11)
Você pode encriptar volumes com uma encriptação baseada em software ou baseada em hardware.

Informações relacionadas

Configurações das Políticas de Grupo do BitLocker
Configurações das Políticas de Grupo do TPM
Artigo 125772 da base de conhecimentos

2.7 Limitações

Discos dinâmicos

O BitLocker não é compatível com discos dinâmicos. Os endpoints enviam um evento ao Sophos Central para notificar você que houve falha na encriptação. Isso acontece porque o volume de um sistema em um disco dinâmico não pode ser encriptado. Os volumes de dados nos discos dinâmicos são simplesmente ignorados.

Desktop Remoto

Ao usar um endpoint do Windows através de um Desktop Remoto que possua o software agente do Sophos Central instalado, não serão exibidas caixas de diálogo e a encriptação de dispositivo NÃO será obrigatória caso seja implantada uma política de encriptação. Permitir a encriptação resultaria em uma sequência de reinicialização para verificar a compatibilidade do hardware. O usuário precisa ter a capacidade de inserir o PIN / frase de segurança no ambiente de pré-inicialização, e isso não pode ser feito através do Desktop Remoto.

2.8 Método de encriptação e relatórios

Você pode encriptar volumes com uma encriptação baseada em software ou baseada em hardware.

O Device Encryption sempre usa a encriptação baseada em software para os novos volumes, mesmo que a unidade de disco suporte a encriptação baseada em hardware.

Se a unidade de disco já estiver encriptada com a encriptação baseada em hardware, ela não será alterada.

Se a configuração de uma política de grupo de BitLocker exigir encriptação baseada em hardware, ela não será alterada.

Na página **Computadores**, você pode filtrar computadores de acordo com seu estado de encriptação, por exemplo, método de encriptação ou computadores que não estão encriptados.

A página de detalhes de um computador mostra o método de encriptação e o algoritmo usados para um volume.

Para computadores Windows, você também pode ver **Encriptado desde**. As informações apresentadas dependem do dispositivo.

- Para computadores já encriptados com a Encriptação de Dispositivo do Sophos Central, mostra a data e a hora em que o computador foi atualizado para o Sophos Central Device Encryption versão 2.1.
- Para computadores encriptados usando outro produto de encriptação, mostra a data e a hora em que o Sophos Central Device Encryption foi instalado.
- Para computadores novos encriptados com o Sophos Central Encryption 2.1 (ou posterior), mostra a data e a hora da encriptação.

O relatório **Status da criptografia** mostra o status de criptografia dos seus computadores.

Você pode ver quais dos seus computadores estão encriptados, quais são os tipos de volume encriptados e quais os computadores que estão em conformidade com as suas políticas de criptografia. Você também pode saber como seus computadores se autenticam e como eles são encriptados.

Conceitos relacionados

Configurações das políticas de grupo do BitLocker (página 9)
O Sophos Central define automaticamente algumas políticas de grupo, para que os administradores não precisem preparar os computadores para encriptação de dispositivo.

Computadores

Resumo do computador

2.9 Sobre a desencriptação

Em geral, você não precisa decodificar. Caso precise excluir da desencriptação um ponto final, ou endpoint, que já foi encriptado, você pode fazê-lo removendo todos os seus usuários da política e, em seguida, desativando a encriptação.

No Windows Explorer (no endpoint), clique com o botão direito no disco do sistema e selecione **Gerenciar BitLocker**. Na caixa de diálogo da **Encriptação de Unidade de Disco do BitLocker**, clique em **Desligar BitLocker**. Apenas um Administrador Windows pode realizar esta operação.

Caso uma política de encriptação seja aplicada e um usuário com privilégios administrativos tente decodificar manualmente seu disco rígido, o Sophos Central ignora o comando do usuário e o disco permanece encriptado.

2.10 Recuperar endpoints em Windows

Caso os usuários esqueçam o PIN ou senha de seu BitLocker, é possível reaver o acesso ao seu computador de duas maneiras.

- Os usuários podem acessar o Portal de Autoatendimento Sophos; consulte Acesso do código de recuperação através do Portal de Autoatendimento. Os usuários do Windows 10 receberão instruções na tela **Recuperação de BitLocker**.
- Você pode ajudá-lo a acessar o computador. Estas instruções lhe informam o que os usuários verão e o que precisarão fazer. Eles devem:

1. Reiniciar o computador e pressionar a tecla **Esc** na tela de logon do **BitLocker**.
2. Na tela **Recuperação BitLocker**, procurar a **ID do código de recuperação**.
3. Contatar o administrador para informá-lo sobre o ID do código de recuperação.
   Você pode lhe dar o código de recuperação. Para obter ajuda sobre como acessar o código para um de seus usuários, consulte a ajuda ao Sophos Central.
4. O usuário deve fornecer o código de recuperação e, depois, seguir as instruções na tela para criar uma nova senha ou PIN.

   Em computadores com Windows 7, não se vê nenhuma instrução. É preciso redefinir o PIN/senha manualmente.

Os usuários podem acessar novamente os seus computadores. Normalmente, os volumes de dados são desbloqueados automaticamente tão logo o usuário possa acessar o volume de inicialização. Se não for esse o caso, você pode obter um código de recuperação para o volume de dados no Sophos Central do mesmo modo que para os volumes de inicialização.

Tarefas relacionadas

Acesso do código de recuperação através do Portal de Autoatendimento (página 22)
Se os usuários não conseguirem se conectar ao computador (esqueceram o PIN do BitLocker ou a senha do macOS, por exemplo), poderão usar o Portal de Autoatendimento Sophos para acessar um código de recuperação.

Informações relacionadas

Portal de autoatendimento

Ajuda do Sophos Central

3 Gerenciar encriptação FileVault

O Sophos Central Device Encryption para Mac gerencia a funcionalidade de encriptação completa de disco FileVault em Macs.

Os usuários precisam apenas da senha de login do macOS para encriptar e acessar seus dados.

3.1 Migrar para o Sophos Central Device Encryption (Mac)

Se quiser usar o Sophos Central para gerenciar endpoints do Mac que já estão encriptados com FileVault, você precisa aplicar uma política Sophos Central Device Encryption para esses endpoints, ou pontos finais.

Nota
Se estiver usando o FileVault with SafeGuard Enterprise, você deverá, primeiro, desinstalar o software **Sophos SafeGuard Device Encryption**.

Antes que os usuários possam começar:

- Você deve instalar o software do agente Sophos Central nos pontos finais.
- Você deve configurar e ativar uma política de Encriptação de Dispositivo no Sophos Central.
- Os usuários devem iniciar uma sessão em seus endpoints. Eles devem ser conectados e sincronizados com o Sophos Central. Observe que o logon remoto não é suportado.

Estas instruções lhe informam o que os usuários verão e o que precisarão fazer:

1. Quando os usuários se conectam ou quando você aplica uma política Sophos Central Device Encryption enquanto estão conectados, os usuários são informados que a Encriptação de Dispositivo foi instalada para proteger seus computadores.
2. Para ativar o Sophos Central Device Encryption, os usuários precisam fornecer a senha de login e clicar em **Criar código**.
   Um novo código de recuperação é criado e armazenado centralmente para fins de restauração. Se houver outros discos internos não encriptados, esses discos serão encriptados também. Você não precisará de uma senha de disco separada para eles.
3. Se houver discos internos que já estejam encriptados com uma senha de disco, os usuários deverão inserir a senha de disco e clicar em **Continuar**.
   Agora a senha do disco será gerenciada pelo Sophos Central. O disco é desbloqueado automaticamente durante a inicialização.

Agora o endpoint é gerenciado pelo Sophos Central Device Encryption.

3.2 Encriptação de dispositivo, passo a passo (Mac)

Siga estas etapas para encriptar Macs.

Antes que os usuários possam começar:

- Você deve instalar o software do agente Sophos Central nos pontos finais.
- Você deve configurar e ativar uma política de Encriptação de Dispositivo no Sophos Central.
- Os usuários devem iniciar uma sessão em seus endpoints. Eles devem ser conectados e sincronizados com o Sophos Central. Observe que o logon remoto não é suportado.

Estas instruções lhe informam o que os usuários verão e o que precisarão fazer.

1. Informar a senha de login após inicializar o Mac do usuário.

   Isto ativa o Sophos Device Encryption.
2. Clicar em **Encriptar** para iniciar a encriptação do disco de seu sistema ou **Adiar** para iniciar o processo mais tarde.

   Quando os usuários fornecem a senha de login e clicam em **Encriptar**, o código de recuperação é armazenado localmente no keychain e no Sophos Central.

   Todos os usuários existentes de um endpoint são adicionados automaticamente ao FileVault.

   No caso de endpoints que possuam a versão macOS 10.12 ou mais antiga, cada usuário precisará fazer o login separadamente para ser adicionado ao FileVault.

Quando o disco do sistema é encriptado, os volumes de dados internos são encriptados automaticamente. Os discos encriptados são automaticamente desbloqueados durante a inicialização do computador.

As notificações informam os usuários sobre o status de encriptação dos discos individualmente.

3.2.1 Adicionar novos usuários FileVault

Caso os usuários não sejam automaticamente adicionados ao FileVault, estas instruções lhe informam o que os novos usuários verão e o que precisarão fazer.

Eles devem:

1. Informar a senha de login e clicar em **Proceder**.
   Normalmente, os usuários podem usar a senha de login do macOS para o Mac e usar o FileVault.
2. Se ainda não houver um código de recuperação armazenado no Sophos Central, os novos usuários deverão selecionar um usuário existente do FileVault que possa autorizar a tarefa.
3. Depois, os usuários existentes do FileVault precisam fornecer a senha de login e clicar em **Continuar**.

Agora os novos usuários podem usar a senha de login do macOS para acessar o Mac e usar o FileVault.

3.3 Recuperar endpoints em Mac

Siga estes passos para recuperar Macs.

Caso os usuários esqueçam a senha de login, há várias maneiras de recuperar o acesso aos seus computadores.

- Se o usuário foi a última pessoa a se conectar ao computador, ele pode usar o Portal de Autoatendimento Sophos; veja Acesso do código de recuperação através do Portal de Autoatendimento.
- Os usuários podem inicializar o computador com um disco de inicialização Mac externo e usar comandos do Terminal para desbloquear o disco.

- Os usuários podem inicializar o computador no modo de disco de destino e usar comandos do Terminal para desbloquear o disco.
- Os usuários podem inicializar o computador com o macOS Recovery e usar comandos do Terminal para desbloquear o disco.

  Para obter informações sobre como trabalhar com comandos de terminal, consulte Desbloquear volumes HFS+ com comandos do terminal e Desbloquear volumes APFS com comandos do terminal.

Você pode ajudar os usuários a recuperar o acesso. Estas instruções lhe informam o que os usuários verão e o que precisarão fazer. Eles devem:

1. Ligar o computador endpoint e aguardar até que a **ID do Código de Recuperação** seja exibida.
   A ID do código de recuperação é exibida por apenas alguns minutos. Para vê-lo novamente, o usuário precisa reiniciar o computador.
2. Contatar o administrador para informá-lo sobre o ID do código de recuperação.
   Você pode lhe dar o código de recuperação. Para obter ajuda sobre como acessar o código para um de seus usuários, consulte a ajuda ao Sophos Central.
3. Clicar no ícone de ponto de interrogação no campo **Senha**.
   A mensagem é exibida.
4. Clicar no ícone de seta ao lado da mensagem para alternar para o campo do código de recuperação.
5. Insira o código de recuperação.

   Para usuários importados do Active Directory, você precisa seguir estes passos extras:

   - Redefina a senha existente no Active Directory. Depois, gere uma senha preliminar e entregue-a ao usuário.
   - Peça ao usuário que clique em **Cancelar** no diálogo **Redefinir senha** e insira a senha preliminar.
6. Siga as instruções na tela para criar uma nova senha.
7. Quando solicitado, clicar em **Criar Novas Chaves**.

Os usuários podem acessar novamente o volume de inicialização de seus computadores.

No caso de endpoints que possuam a versão macOS 10.12 ou mais antiga, um novo código de recuperação será criado e armazenado no Sophos Central. Um código de recuperação pode ser usado apenas uma vez. Se, no futuro, você precisar restaurar seu computador novamente, será necessário acessar um novo código de recuperação.

No caso de endpoints que possuam a versão macOS 10.13 e Apple File System (APFS), não será criado um novo código de recuperação. O código de recuperação existente continua válido.

Tarefas relacionadas

Acesso do código de recuperação através do Portal de Autoatendimento (página 22)
Se os usuários não conseguirem se conectar ao computador (esqueceram o PIN do BitLocker ou a senha do macOS, por exemplo), poderão usar o Portal de Autoatendimento Sophos para acessar um código de recuperação.

Desbloquear volumes HFS+ com comandos do Terminal (página 17)
É possível usar os comandos de Terminal para desbloquear volumes encriptados. Os comandos nesta seção se aplicam a endpoints que possuem a versão macOS 10.12 ou mais antiga, com volumes formatados com HFS+.

Desbloquear volumes APFS com comandos do Terminal (página 17)
É possível usar os comandos de Terminal para desbloquear volumes encriptados. Os comandos nesta seção se aplicam a endpoints que possuem a versão macOS 10.13 e Apple File System (APFS).

Informações relacionadas

Recuperação de macOS

Como selecionar um disco de inicialização diferente

Ajuda do Sophos Central

3.3.1 Desbloquear volumes HFS+ com comandos do Terminal

É possível usar os comandos de Terminal para desbloquear volumes encriptados. Os comandos nesta seção se aplicam a endpoints que possuem a versão macOS 10.12 ou mais antiga, com volumes formatados com HFS+.

Estas instruções lhe informam o que os usuários verão e o que precisarão fazer. Eles devem:

1. Abrir o aplicativo **Terminal** e executar `diskutil corestorage list`.
   É exibida uma lista de todos os volumes conectados.
2. Procurar o nome de volume (`LV Name`) que desejam restaurar e anotar a identificação do `Volume lógico`.
3. Contatar o administrador e solicitar o código de recuperação usando a identificação do `Volume lógico` como o ID do código de recuperação.
   Você lhe dá o código de recuperação. Para obter ajuda sobre como acessar o código para um de seus usuários, consulte a ajuda ao Sophos Central.
4. Inserir o código de recuperação no diálogo de senha do disco para desbloquear o disco. Alternativamente, os usuários podem usar o comando `diskutil corestorage unlockVolume` e inserir o código de recuperação no aplicativo **Terminal** para desbloquear o disco.

Agora o disco pode ser acessado no Finder.

Informações relacionadas

Ajuda do Sophos Central

3.3.2 Desbloquear volumes APFS com comandos do Terminal

É possível usar os comandos de Terminal para desbloquear volumes encriptados. Os comandos nesta seção se aplicam a endpoints que possuem a versão macOS 10.13 e Apple File System (APFS).

Estas instruções lhe informam o que os usuários verão e o que precisarão fazer. Eles devem:

1. Abrir o aplicativo **Terminal** e executar `diskutil apfs list`.
   É exibida uma lista de todos os volumes conectados.
2. Procurar pelo nome do volume que deseja recuperar e anotar a identificação do volume, por exemplo `Volume disk1s1`.
3. Contatar o administrador e solicitar o código de recuperação usando a identificação do volume como a ID do código de recuperação.
   Você lhe dá o código de recuperação. Para obter ajuda sobre como acessar o código para um de seus usuários, consulte a ajuda ao Sophos Central.
4. Inserir o código de recuperação no diálogo de senha do disco para desbloquear o disco. Alternativamente, os usuários podem usar o comando `diskutil apfs unlockVolume` e inserir o código de recuperação no aplicativo **Terminal** para desbloquear o disco.

Agora o disco pode ser acessado no Finder.

Informações relacionadas
Ajuda do Sophos Central

3.3.3 Erro: Falha ao armazenar código de recuperação

Em algumas raras ocasiões, o sistema poderá falhar ao armazenar o código de recuperação localmente (na keychain) ou no Sophos Central.

Isso significa que não é possível restaurar a máquina se os usuários esquecerem suas senhas. Para diminuir o risco, é exibida uma mensagem de erro com o código de recuperação, e o usuário é solicitado a copiar o código de recuperação.

O sistema tentará repetidamente armazenar o código de recuperação no Sophos Central. Assim que conseguir, os usuários serão informados que um novo código de recuperação passou a ser gerenciado pelo Sophos Central e que eles podem destruir a cópia do código de recuperação.

3.4 Status do Device Encryption (Mac)

Os usuários podem acessar informações sobre o status de encriptação usando o aplicativo **Sophos Device Encryption**. Ele está instalado no diretório `Applications` e pode ser iniciado via Finder, Launchpad ou Spotlight.

O aplicativo **Sophos Device Encryption** fornece as seguintes informações:

- Status da política: A primeira linha informa os usuários se o endpoint, ou ponto final, é gerenciado ou não pelo Sophos Device Encryption.
- Status do usuário: A segunda linha informa os usuários o que eles podem e não podem fazer.
- Status do disco: É exibida uma lista de todos os discos internos. Se o nome do disco estiver acinzentado, o disco não está montado. Um ícone ao lado do nome do disco indica o status do disco. Os seguintes status estão disponíveis:
  - Verde: O disco está totalmente encriptado e o código de recuperação está armazenado de modo centralizado.
  - Amarelo: O disco está totalmente encriptado, mas o código de recuperação não está armazenado no Sophos Central. Isso pode acontecer quando o Sophos Central não está acessível. Se a encriptação do disco não for necessária, pode ser que o código de recuperação simplesmente não exista. Em geral, esse é o caso quando o disco não é gerenciado pelo Sophos Central Device Encryption e foi encriptado usando as ferramentas do sistema operacional.
  - Amarelo + ponto de exclamação: O disco está totalmente encriptado, existe uma política que requer que o disco seja encriptado, mas não há código de recuperação disponível.
  - Vermelho: O disco não está encriptado, mas há uma política ativa que requer que o disco seja encriptado.
  - Cinza: O disco não está encriptado e a política não requer encriptação ou não há nenhuma política.
  - Barra de status + **Encriptando**: O disco está sendo encriptado no momento.
  - Barra de status + **Decodificando**: O disco está sendo decodificado no momento.

Nota
Caso um usuário com privilégios administrativos em um endpoint Mac tente decodificar manualmente seu disco rígido com uma política de encriptação aplicada, o Sophos Central não poderá cancelar isso e o disco será decodificado. Quando a decodificação é concluída, é solicitada a senha do usuário para habilitar o FileVault, e o disco é novamente encriptado.

- Status de recuperação: Na parte inferior da janela, os usuários são informados se os códigos de recuperação estão ou não disponíveis para os seus discos.

Alternativamente, você pode acessar informações sobre o status do Device Encryption via ferramenta de linha de comando. A ferramenta está instalada em `/usr/local/bin/seadmin`. Os seguintes comandos estão disponíveis:

- `help`: Exibe uma lista de comandos disponíveis.
- `status`: Exibe a última sincronização do software de encriptação e o intervalo de sincronização.
- `--device-encryption`: Exibe a política de encriptação atual e o status de encriptação e recuperação de todos os discos internos.

4 Arquivos protegidos por senha para o compartilhamento seguro

Você pode ativar esta opção em uma política de **Encriptação do dispositivo**.

Nota
O recurso estará disponível apenas no Central Device Encryption 2.0 ou posterior. Disponível apenas para Windows.

Você pode proteger arquivos de até 50 MB.

Habilitar menu contextual com o clique do botão direito: Se você ativar esta opção, a opção **Criar arquivo protegido por senha** aparecerá no menu acionado pelo botão direito. Os usuários podem anexar arquivos protegidos por senha a e-mails quando enviam dados confidenciais a destinatários fora da rede corporativa. Os arquivos são encapsulados em um novo arquivo HTML com conteúdo encriptado.

Os destinatários podem abrir o arquivo clicando duas vezes nele e digitando a senha. Eles podem enviar o arquivo recebido de volta e protegê-lo com a mesma senha ou com uma nova senha, ou podem criar um novo arquivo protegido por senha.

Habilitar o Suplemento do Outlook: Esta opção adiciona a encriptação de anexos de e-mail ao Outlook. Os usuários podem proteger anexos selecionando **Proteger anexos** na faixa de opções do Outlook. Todos os anexos não protegidos são encapsulados em um novo anexo HTML com conteúdo encriptado que é enviado por e-mail.

Sempre perguntar como proceder com os arquivos anexados: Se você ativar esta opção, os usuários deverão escolher como enviar os anexos sempre que a mensagem contiver um. Eles podem enviá-los com ou sem senha de proteção.

Você pode inserir domínios excluídos para os quais a opção **Sempre perguntar como proceder com os arquivos anexados** não se aplica, por exemplo, o domínio da sua organização. Se os destinatários pertencerem a tal domínio, os remetentes não serão indagados sobre como desejam lidar com os anexos.

Digite apenas nomes de domínio completos e separe-os por vírgula.

Informações relacionadas
Política de Encriptação de Dispositivos

5 Solicitar aos usuários que alterem a senha/PIN

Existem duas formas de solicitar aos usuários que alterem a sua senha.

Nota
Esta opção está disponível apenas para Windows.

- Utilize a opção **Exigir novo PIN/senha de autenticação dos usuários** na política de encriptação.

  Esta opção é desativada por padrão. Ela força a alteração da senha ou do PIN do BitLocker após o tempo especificado. Após os usuários alterarem a senha ou PIN, é registrado um evento.

  Nota
  O recurso estará disponível apenas no Central Device Encryption 2.0 ou posterior.

- Utilize a opção **Disparar alteração de senha/PIN** na guia **Resumo** da página de detalhes de um computador.

  Isso exige que os usuários alterarem a senha ou PIN do BitLocker imediatamente. Uma mensagem é exibida após a solicitação ser enviada com sucesso.

No endpoint, os usuários são solicitados a criar uma nova senha ou PIN do BitLocker. Se os usuários fecharem a caixa de diálogo sem digitar nada, o diálogo voltará a ser exibido após 30 segundos. Isso para quando digitarem algo. Depois que a caixa de diálogo for fechada cinco vezes sem alterar a senha ou o PIN, um alerta é registrado.

Informações relacionadas
Política de Encriptação de Dispositivos
Resumo do computador

6 Acesso do código de recuperação através do Portal de Autoatendimento

Se os usuários não conseguirem se conectar ao computador (esqueceram o PIN do BitLocker ou a senha do macOS, por exemplo), poderão usar o Portal de Autoatendimento Sophos para acessar um código de recuperação.

Com o código de recuperação, eles voltarão a ter acesso ao computador.

Para habilitar os usuários a recuperarem seus computadores no Portal de Autoatendimento, vá até **Sophos Central > Pessoas > Usuários**, selecione um ou mais usuários e clique no botão **Link de configuração de E-mail**. No diálogo a seguir, selecione **E-mail de instalação/boas-vindas do Sophos Central Self Service** para enviar um link de ativação aos usuários por e-mail. Ao seguirem as instruções no e-mail, os usuários poderão usar o Portal de Autoatendimento Sophos para restaurar seus computadores.

Estas instruções lhe informam o que os usuários verão e o que precisarão fazer. Eles devem:

1. Iniciar uma sessão no Portal de Autoatendimento Sophos utilizando outro computador.
2. Ir para a página **Encriptação de Dispositivo**.
   Será exibida uma lista de todos os computadores aos quais o usuário foi o último a estar conectado. Se alguém conectou-se a um computador nesse meio tempo, o usuário não poderá ganhar novamente acesso a tal computador através do Portal de Autoatendimento.
3. Selecionar um computador da lista e clicar no botão **Acessar** na coluna **CÓDIGO DE RECUPERAÇÃO**.
   Aparecerá uma caixa de diálogo com o código de recuperação.
4. Ligar seus próprios computadores e ir para a página de recuperação.
   - Windows: Pressione a tecla **Esc** para alternar para a tela **Recuperação do BitLocker**.
   - Mac: Clique no ícone de ponto de interrogação no campo **Senha** para alternar para a página de recuperação do FileVault.
5. Insira o código de recuperação.

Os usuários podem acessar novamente os seus computadores.

Informações relacionadas

Portal de autoatendimento

7 Mais informações

Windows

- Perguntas frequentes: artigo 124819 na base de conhecimentos
- Perguntas frequentes sobre o BitLocker
- Configurações das Políticas de Grupo do BitLocker
- Fundamentos do TPM
- Configurações das Políticas de Grupo do TPM
- Apresentação técnica sobre a administração do módulo de plataforma confiável

Mac

- Perguntas frequentes: artigo 125982 na base de conhecimentos
- Configuração do FileVault: Usar o FileVault para criptografar o disco de inicialização no Mac
- Códigos de recuperação do FileVault: Definir uma chave reserva do FileVault para os computadores de sua instituição
- Redefinição de Senha: Alterar ou redefinir a senha de uma conta de usuário do macOS

Informações relacionadas

Perguntas frequentes sobre o BitLocker
Configurações das Políticas de Grupo do BitLocker
Configurações das Políticas de Grupo do TPM
Fundamentos do TPM
Apresentação técnica sobre a administração do módulo de plataforma confiável
Usar o FileVault para criptografar o disco de inicialização no Mac
Definir uma chave reserva do FileVault para os computadores de sua instituição
Alterar ou redefinir a senha de uma conta de usuário do macOS
Artigo 124819 da base de conhecimentos
Artigo 125982 da base de conhecimentos

8 Navegadores da web compatíveis

Os seguintes navegadores são atualmente compatíveis:

- Microsoft Internet Explorer 11 e Microsoft Edge.
- Google Chrome.
- Mozilla Firefox.
- Apple Safari (somente Mac).

Recomendamos que você instale ou atualize para uma versão compatível conforme a lista acima e que sempre tenha em execução a versão mais recente. Nossa meta é nos manter atualizados e atender às mais recentes versões do Google Chrome, Mozilla Firefox e Apple Safari, bem como às anteriores. Se um navegador incompatível for detectado, você será redirecionado para https://central.sophos.com/unsupported.

Nota
O Sophos Central Admin não é compatível com dispositivos móveis.

9 Obter ajuda adicional

Para obter ajuda da Sophos Support:

1. Clique em **Ajuda**, na área superior direita da interface de usuário, e selecione **Criar Solicitação de Atendimento**.
2. Preencha o formulário. Seja o mais exato possível, de modo que o suporte técnico posso ajudar você de maneira eficiente.
3. Opcionalmente, selecione a opção para permitir que o suporte acesse a sua sessão no Sophos Central diretamente para poder melhor ajudá-lo.
4. Clique em **Enviar**.

A Sophos entrará em contato com você dentro de 24 horas.

Nota
Se tiver selecionado a opção para permitir que o suporte acesse a sessão no Sophos Central, esta função será habilitada quando você clicar em **Enviar**. A Assistente remota será desabilitada automaticamente após 72 horas. Para desabilitá-la antes, clique no nome da sua conta (área superior direita da interface de usuário), selecione **Detalhes da conta** e clique na guia **Suporte da Sophos**.

Enviar feedback

Para enviar comentários e sugestões à Sophos Support:

1. Clique em **Ajuda**, na área superior direita da interface de usuário, e selecione **Dar feedback**.
2. Preencha o formulário.
3. Clique em **Enviar**.

Ajuda adicional

Você também encontrará assistência técnica conforme abaixo:

- Visitando a Comunidade Sophos em community.sophos.com/ e pesquisando por usuários que estão passando pelo mesmo problema.
- Visitando a base de conhecimentos de suporte da Sophos em www.sophos.com/en-us/support.aspx.

10 Avisos legais