# Dell Data Protection | Personal Edition

Guia de Instalação v8.13

## Notas, avisos e advertências

**NOTA: Uma NOTA indica informações importantes que ajudam você a usar melhor o seu produto.**

**CUIDADO: Um AVISO indica possíveis danos ao hardware ou perda de dados e ensina como evitar o problema.**

**ATENÇÃO: Uma ADVERTÊNCIA indica possíveis danos à propriedade, risco de lesões corporais ou mesmo risco de vida.**



**Guia de Instalação do Personal Edition**

2017 - 04

Rev. A01

# Índice

1

# Visão geral do Personal Edition

Este guia presume que o Security Tools será instalado com o Personal Edition.

## Personal Edition

O Personal Edition tem como objetivo proteger os dados no seu computador, mesmo em caso de perda ou roubo.

Para preservar a segurança dos seus dados sigilosos, o Personal Edition criptografa os dados no seu computador Windows. Sempre é possível acessar os dados quando você estiver logado no computador, mas usuários não autorizados não terão acesso a esses dados protegidos. Dados sempre permanecem criptografados na unidade de disco, mas, como a criptografia ocorre em segundo plano, não é preciso mudar a maneira de trabalhar com os aplicativos e dados.

Normalmente, o Encryption Client descriptografa os dados à medida que você trabalha com eles. É possível que um aplicativo tente acessar um arquivo enquanto o Encryption Client está fazendo sua criptografia ou descriptografia. Se isso acontecer, após um ou dois segundos, o Encryption Client mostrará uma caixa de diálogo com a opção de aguardar ou cancelar a criptografia/descriptografia. Se você optar por esperar, o Encryption Client liberará o arquivo assim que a operação estiver concluída (geralmente, em alguns segundos).

## Security Tools

A finalidade do Security Tools é fornecer uma solução de segurança completa para o suporte do Advanced Authentication.

O Security Tools oferece suporte a múltiplos fatores para autenticação do Windows, com senhas, leitores de impressão digital e cartões inteligentes (com ou sem contato), além de inscrição automática, senhas de uso único (OTP – One-time Password) e login em uma etapa (SSO – Single Sign-on).

O Security Console é a interface do Security Tools que guia os usuários pelo processo de configuração de suas credenciais e perguntas para autorrecuperação, com base na política definida pelo administrador local.

A ferramenta Configurações de administrador está disponível para usuários com privilégios de administrador e é usada para configurar políticas de autenticação e opções de recuperação, gerenciar usuários e definir configurações avançadas, além de configurações específicas para credenciais suportadas para login no Windows.

Consulte Definir as configurações de administrador do Security Tools e também o *Guia do usuário do Dell Console* para saber como usar os aplicativos do Security Tools.

## Entre em contato com o Dell ProSupport

Ligue para 877-459-7304, extensão 4310039 para obter suporte por telefone, 24 horas por dia, 7 dias na semana, para o seu produto Dell Data Protection.

Há também disponível o serviço de suporte on-line para os produtos Dell Data Protection no site dell.com/support. O suporte on-line inclui drivers, manuais, orientações técnicas, perguntas frequentes e problemas emergentes.

Quando telefonar, tenha em mãos o código de serviço, para nos ajudar a garantir que possamos direcioná-lo rapidamente ao especialista técnico correto.

Para obter os números de telefone fora dos Estados Unidos, consulte Números de telefone internacionais do Dell ProSupport.

2

# Requisitos do Personal Edition

Esses requisitos detalham tudo que é necessário para a instalação do Personal Edition.

## Encryption Client

- É necessário ter um código de direito para instalar satisfatoriamente o Personal Edition. O código de direito é fornecido quando você compra o Personal Edition. Dependendo de como você comprar o Personal Edition, você pode precisar instalar manualmente o direito. Em caso afirmativo, siga as instruções simples que acompanham o código de direito. Se o Personal Edition for instalado usando o Dell Digital Delivery, a instalação do direito é executada pelo serviço do Dell Digital Delivery. Os mesmos arquivos binários são usados pelo Enterprise Edition e pelo Personal Edition. O código de direito informa ao instalador a versão a ser instalada.
- A Dell recomenda fortemente o uso de uma senha do Windows (se ela ainda não existir) para proteger o acesso aos seus dados criptografados. Criar uma senha para o seu computador impede que outras pessoas façam login na sua conta de usuário sem a sua senha.
  a Vá para o Painel de controle do Windows (**Iniciar** > **Painel de controle**).
  b Clique no ícone **Contas de usuário**.
  c Clique em **Criar uma senha para sua conta**.
  d Digite a senha e digite-a novamente.
  e Opcionalmente, adicione uma dica de senha.
  f Clique em **Criar senha**.
  g Reinicie o computador.
- As práticas recomendadas de TI devem ser seguidas durante a implementação. Isso inclui, sem limitações, ambientes de teste controlados para testes iniciais e implantações escalonadas para os usuários.
- A conta de usuário que executa a instalação/upgrade/desinstalação precisa ser a de um usuário Admin local ou de domínio, que pode ser temporariamente atribuída por uma ferramenta de implementação, como o Microsoft SMS ou o Dell KACE. Não há suporte para um usuário que não é administrador mas possui privilégios elevados.
- Faça backup de todos os dados importantes antes de iniciar a instalação/desinstalação/upgrade.
- Não realize alterações no computador, incluindo a inserção ou a remoção de unidades externas (USB), durante a instalação/desinstalação/upgrade.
- Para reduzir o tempo de criptografia inicial (bem como o tempo de descriptografia, se estiver desinstalando), execute o Assistente de Limpeza de Disco do Windows para remover arquivos temporários e todos os outros dados desnecessários.
- Desative o modo de suspensão durante a varredura de criptografia inicial para impedir que um computador sem supervisão entre em modo de suspensão. Nem a criptografia nem a descriptografia podem ocorrer em um computador em modo de suspensão.
- O Encryption Client não suporta configurações de inicialização dupla, pois existe a possibilidade de criptografar arquivos de sistema do outro sistema operacional e isto pode interferir na sua operação.
- O instalador mestre não oferece suporte a atualizações de componentes anteriores à versão v8.0. Extraia os instaladores filho do instalador mestre e faça upgrade do componente individualmente. Se tiver perguntas ou preocupações, entre em contato com o Dell ProSupport.
- O cliente Encryption agora suporta o modo Audit. O modo Audit permite que os administradores implementem o cliente Encryption como parte da imagem corporativa, em vez de usar um SCCM de terceiros ou soluções similares para implementar o cliente Encryption. Para obter instruções sobre como instalar o cliente Encryption em uma imagem corporativa, consulte http://www.dell.com/support/article/us/en/19/SLN304039.
- O TPM é usado para selar a GPK. Entretanto, se estiver executando o cliente Encryption, limpe o TPM no BIOS antes de instalar um novo sistema operacional no computador cliente.
- O Encryption Client foi testado e é compatível com McAfee, o cliente da Symantec, Kaspersky e MalwareBytes. Há exclusões inseridas no código em vigor para esses fornecedores de antivírus a fim de evitar incompatibilidades entre a varredura do antivírus e a criptografia. O Encryption Client também foi testado com o Kit de ferramentas de experiência de mitigação aprimorada da Microsoft.

Se sua organização usa um fornecedor de antivírus que não está na lista, consulte o artigo do banco de conhecimento SLN298707 ou Entre em contato com o Dell ProSupport para obter ajuda.

- Não há suporte para upgrade de sistema operacional instalado quando o Encryption Client está instalado. Desinstale e descriptografe o Encryption Client, faça o upgrade para o novo sistema operacional e depois reinstale o Encryption Client.

  Além disso, não há suporte para reinstalação de sistema operacional. Para reinstalar o sistema operacional, faça um backup do computador de destino, formate o computador, instale o sistema operacional e, depois, faça a recuperação dos dados criptografados seguindo os procedimentos de recuperação estabelecidos.
- Verifique periodicamente www.dell.com/support para obter a documentação e recomendações técnicas mais recentes.

# Pré-requisitos do Encryption Client

- O Microsoft .Net Framework 4.5.2 (ou posterior) é necessário para o instalador mestre e os clientes secundários do instalador.

  Todos os computadores enviados de fábrica pela Dell vêm com o Microsoft .Net Framework 4.5.2 (ou posterior) pré-instalado. No entanto, se você não estiver realizando a instalação em um hardware da Dell ou estiver fazendo a atualização do cliente em equipamentos mais antigos da Dell, será necessário verificar qual versão do Microsoft .Net está instalada e atualizar a versão **antes de instalar o cliente** a fim de evitar falhas de atualização/instalação. Para verificar a versão do Microsoft .Net instalado, siga estas instruções no computador de instalação: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Para instalar o Microsoft .Net Framework 4.5.2, vá até https://www.microsoft.com/en-us/download/details.aspx?id=42643.
- O instalador mestre instala o Microsoft Visual C++ 2012 Update 4 se ele não estiver instalado no computador. **Quando estiver usando o instalador filho**, você precisará instalar esse componente antes de instalar o Encryption Client.

| Pré-requisito |
| --- |
| • Visual C++ 2012 Update 4 ou Redistributable Package mais recente (x86 e x64) |
| • Microsoft SQL Server Compact 3.5 SP2 (x86 e x64) |

# Hardware do Encryption Client

- A tabela a seguir detalha o hardware de computador suportado.

| Hardware |
| --- |
| • Os requisitos mínimos de hardware precisam atender às especificações mínimas do sistema operacional |

- A tabela a seguir detalha o hardware de computador opcional suportado.

| Hardware integrado opcional |
| --- |
| • TPM 1.2 ou 2.0 |

# Sistemas operacionais do Encryption Client

- A tabela a seguir detalha os sistemas operacionais suportados.

| Sistemas operacionais Windows (32 e 64 bits) |
| --- |
| • Windows 7 SP0-SP1: Enterprise, Professional, Ultimate |
| • Windows Embedded Standard 7 com modelo de compatibilidade de aplicativo (sem suporte para criptografia de hardware) |
| • Windows 8: Enterprise, Pro |
| • Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition |

**Sistemas operacionais Windows (32 e 64 bits)**

- Windows Embedded 8.1 Industry Enterprise (sem suporte para criptografia de hardware)
- Windows 10: Education, Enterprise, Pro
- VMWare Workstation 5.5 e mais recentes

> **NOTA: Sem suporte para o modo UEFI no Windows 7, Windows Embedded Standard 7 ou Windows Embedded 8.1 Industry Enterprise.**

# Sistemas operacionais para External Media Shield (EMS)

- A seguinte tabela detalha os sistemas operacionais suportados para acesso a mídias protegidas pelo EMS.

> **NOTA: A mídia externa precisa ter aproximadamente 55 MB disponíveis, além de espaço livre na mídia igual ao maior arquivo a ser criptografado para hospedar o EMS.**

> **NOTA:**
> O Windows XP só é suportado ao usar o EMS Explorer.

**Sistemas operacionais Windows suportados para acessar mídia protegida por EMS (32 e 64 bits)**

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate, Home Premium
- Windows 8: Enterprise, Pro, Consumer
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

**Sistemas operacionais Mac suportados para acessar mídias protegidas por EMS (kernels de 64 bits)**

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- Mac OS Sierra 10.12.0

# Suporte a idiomas do Encryption Client

- O Encryption Client é compatível com interfaces de usuário multi-idiomas (MUI) e suporta os idiomas a seguir.

**Suporte a idiomas**

- EN - Inglês
- ES - Espanhol
- FR - Francês
- IT - Italiano
- DE - Alemão
- JA - Japonês
- KO - Coreano
- PT-BR - Português, Brasil
- PT-PT - Português, Portugal (ibérico)

# Cliente de Autenticação avançada

- Ao usarem o Advanced Authentication, os usuários estarão protegendo o acesso ao computador com o uso das credenciais do Advanced Authentication que são gerenciadas e inscritas usando o Security Tools. O Security Tools se tornará o gerenciador principal das credenciais de autenticação para login no Windows, incluindo, senha, impressão digital e cartões inteligentes do Windows. Senha

com imagem, código numérico e impressão digital inscrita usando o sistema operacional da Microsoft não serão reconhecidos durante o login no Windows

Para continuar usando o sistema operacional Microsoft para gerenciar as credenciais de usuário, não instale ou desinstale o Security Tools.

- O recurso de Senha de uso único (OTP - One-time Password) do Security Tools exige que um TPM esteja presente, ativado e possua um proprietário. O OTP não é suportado com TPM 2.0. Para limpar e definir a propriedade do TPM, consulte https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2.

# Hardware do cliente de autenticação avançada

- A tabela a seguir detalha o hardware de autenticação suportado.

**Leitores de cartões inteligentes e de impressão digital**

- Validity VFS495 em modo seguro
- Leitor Dell ControlVault Swipe
- UPEK TCS1 FIPS 201 Secure Reader 1.6.3.379
- Leitores USB Authentec Eikon e Eikon To Go

**Cartões sem contato**

- Cartões sem contato que usam leitores de cartões sem contato integrados em laptops Dell específicos

**Cartões inteligentes**

- Cartões inteligentes PKCS #11 usando o cliente ActivIdentity

  **NOTA: O cliente ActivIdentity não é pré-carregado e precisa ser instalado separadamente.**
- Cartões CSP
- Cartões de acesso comum (CACs)
- Cartões Classe B/SIPR Net

- Os drivers e o firmware para Dell ControlVault, leitores de impressão digital e cartões inteligentes (conforme mostrado abaixo) não estão incluídos nos arquivos executáveis do instalador mestre ou do instalador filho. Os drivers e o firmware precisam ser mantidos atualizados e podem ser obtidos por download em http://www.dell.com/support, selecionando o modelo do seu computador. Faça download dos drivers e firmware adequados com base em seu hardware de autenticação.

  - Dell ControlVault
  - Leitor de impressão digital de indicadores biométricos NEXT
  - Driver 495 do leitor de impressão digital Validity
  - Driver de cartão inteligente O2Micro

  No caso de instalação em hardware que não seja da Dell, faça download dos drivers e do firmware atualizados no site do fornecedor. As instruções de instalação dos drivers do Dell ControlVault são fornecidas em Drivers do Dell ControlVault.
- A tabela a seguir detalha os modelos de computador Dell com suporte para cartões SIPR Net.

**Modelos de computador Dell - Suporte para cartão Classe B/SIPR Net**

- Latitude E6440
- Latitude E6540
- Precision M2800
- Precision M4800
- Precision M6800
- Latitude 14 Rugged Extreme
- Latitude 12 Rugged Extreme
- Latitude 14 Rugged

# Sistemas operacionais do cliente de autenticação avançada

**Sistemas operacionais Windows**

- A tabela a seguir detalha os sistemas operacionais suportados.

| Sistemas operacionais Windows (32 e 64 bits) |
|---|
| • Windows 7 SP0-SP1: Enterprise, Professional, Ultimate<br>• Windows 8: Enterprise, Pro<br>• Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition<br>• Windows 10: Education, Enterprise, Pro |

**NOTA: O modo UEFI não é suportado no Windows 7.**

**Sistemas operacionais de dispositivos móveis**

- Os seguintes sistemas operacionais móveis são suportados com o recurso de Senha de uso único do Security Tools.

| Sistemas operacionais Android |
|---|
| • 4.0 - 4.0.4 (Ice Cream Sandwich)<br>• 4.1 - 4.3.1 (Jelly Bean)<br>• 4.4 - 4.4.4 (KitKat)<br>• 5.0 - 5.1.1 (Lollipop) |

| Sistemas operacionais iOS |
|---|
| • iOS 7.x<br>• iOS 8.x |

| Sistemas operacionais Windows Phone |
|---|
| • Windows Phone 8.1<br>• Windows 10 Mobile |

# Suporte a idiomas do cliente de autenticação avançada

- O cliente de Advanced Authentication é compatível com interfaces de usuário multi-idiomas (MUI) e suporta os seguintes idiomas. O Modo UEFI e a Autenticação de pré-inicialização não são suportados em russo, em chinês tradicional e em chinês simplificado.

| Suporte a idiomas | |
|---|---|
| • EN - Inglês | • KO - Coreano |
| • FR - Francês | • ZH-CN - Chinês, simplificado |
| • IT - Italiano | • ZH-TW - Chinês, tradicional/Taiwan |
| • DE - Alemão | • PT-BR - Português, Brasil |
| • ES - Espanhol | • PT-PT - Português, Portugal (ibérico) |
| • JA - Japonês | • RU - Russo |

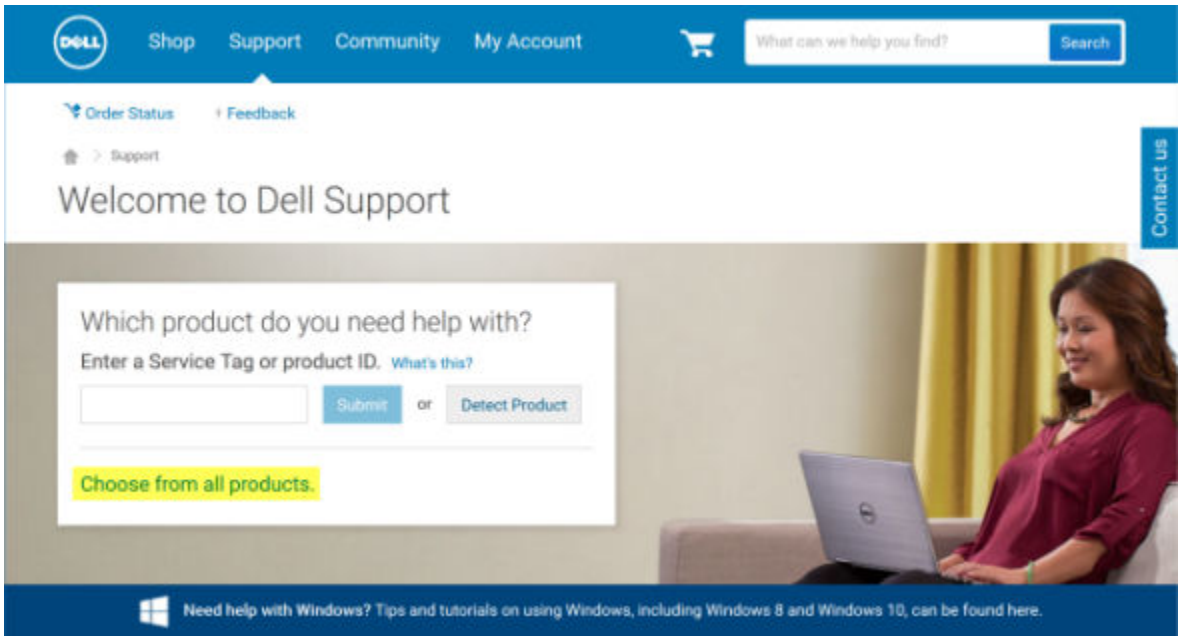
Vá para Obter software.

# Faça o download do software

Esta seção detalha as informações sobre como obter o software em dell.com/support. Se você já tiver o software, você pode ignorar esta seção.

Acesse dell.com/support para começar.

1 Na página Suporte Dell, selecione **Escolha entre todos os produtos**.




2 Selecione **Software e segurança** da lista de produtos.

3 Selecione **Soluções de segurança de ponto de extremidade** na seção *Software e segurança*.
Depois de fazer essa seleção uma vez, o site se lembrará.

4 Selecione o produto Dell Data Protection.
Exemplos:

**Dell Encryption**

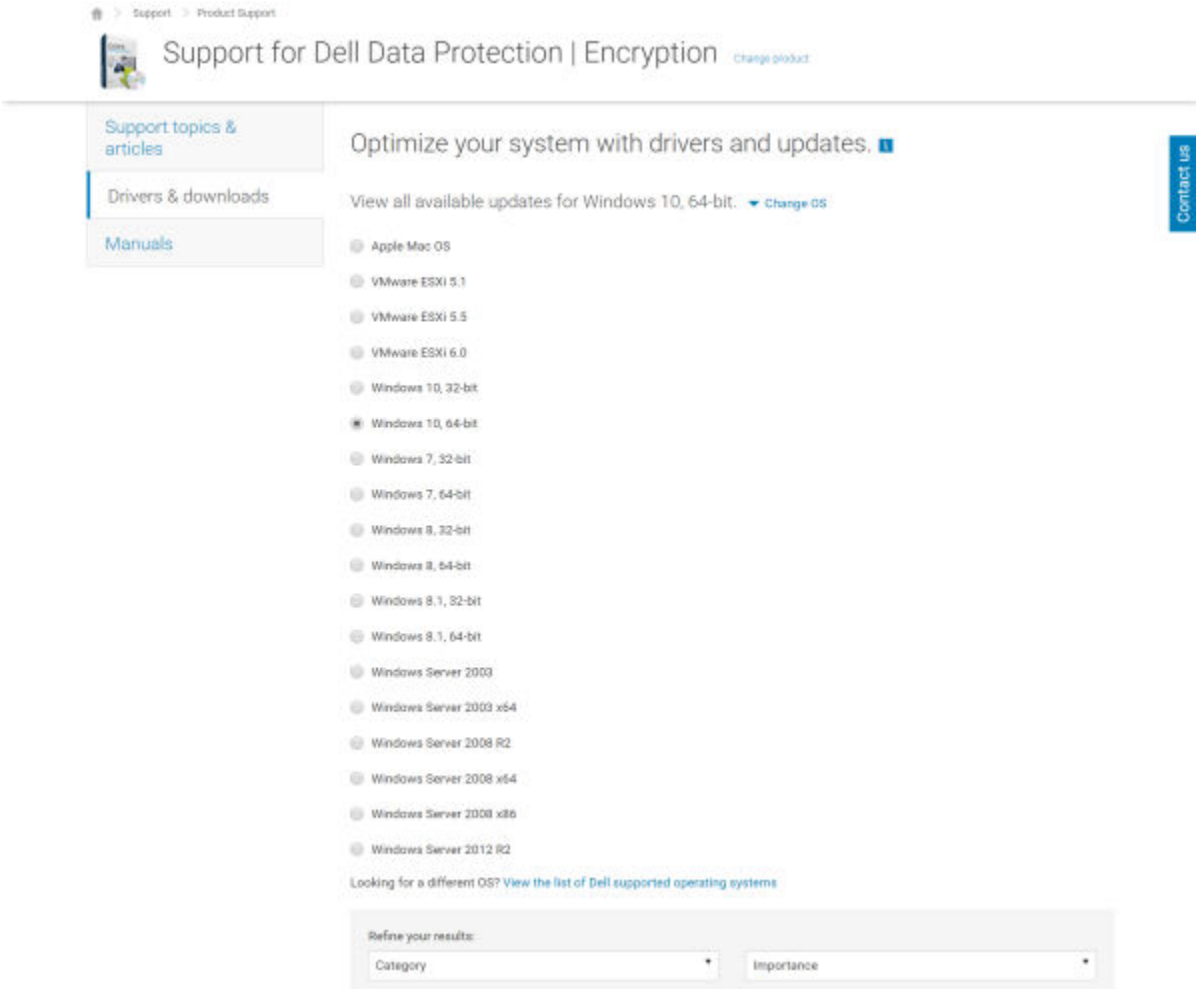
**Dell Endpoint Security Suite**

**Dell Endpoint Security Suite Enterprise**

5 Selecione **Drivers e downloads**.

6 Selecione o tipo de sistema operacional do cliente desejado.

7 Selecione **Dell Data Protection (4 arquivos)** no resultado. A sequência descrita acima é apenas um exemplo, por isso, pode ser um pouco diferente. Por exemplo, pode ser que não haja 4 arquivos para você escolher.




8 Selecione **Fazer download de arquivo** ou **Adicionar à lista de download nº XX**.
Vá para Instalar Personal Edition.

# 4

# Instalar o Personal Edition

Você pode instalar o Personal Edition usando o instalador mestre (recomendado) ou extraindo os instaladores filhos do instalador mestre. De qualquer uma das formas, o Personal Edition pode ser instalado pela interface do usuário, pela linha de comando ou por scripts e usando qualquer tecnologia push disponível para a sua organização.

Os usuários devem consultar os seguintes arquivos de ajuda para obter ajuda com o aplicativo:

- Consulte a *Ajuda de criptografia Dell* para aprender como usar o recurso do Encryption Client. Acesse a ajuda em **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
- Consulte a *Ajuda EMS* para aprender sobre os recursos do External Media Shield. Acesse a ajuda em **<Install dir>:\Program Files\Dell \Dell Data Protection\Encryption\EMS**.
- Consulte a *ajuda do Security Tools* para saber como usar os recursos do Advanced Authentication. Acesse a ajuda em **<Install dir>: \Program Files\Dell\Dell Data Protection\Security Tools \Help**.

# Escolher um método de instalação

Há dois métodos para instalar o cliente. Selecione **um**:

- Instalar o Personal Edition usando o instalador mestre - RECOMENDADO
- Instalar o Personal Edition usando os instaladores filhos

# Instalar o Personal Edition usando o instalador mestre - RECOMENDADO

Para instalar o Personal Edition, o instalador deve encontrar o direito apropriado no computador. Se o direito apropriado não for encontrado, o Personal Edition não poderá ser instalado.

- O instalador do Dell Data Protection é comumente conhecido como instalador mestre, pois ele instala vários clientes. No caso do Personal Edition, ele instala o Encryption Client e o cliente do Advanced Authentication.
- Se a instalação for realizada com a interface do usuário do instalador mestre, o Personal Edition pode ser instalado em um computador de cada vez.
- Os arquivos de log do instalador mestre estão localizados na pasta **C:\ProgramData\Dell\Dell Data Protection\Installer.**

Selecione um método:

- Instalação usando a interface do usuário
- Instalação usando a linha de comando

**Instalação usando a interface do usuário**

1. Instale o direito no computador de destino, se necessário.
2. Copie o arquivo DDPSetup.exe para o computador local.
3. Clique duas vezes em DDPSetup.exe para iniciar o instalador.
4. Uma caixa de diálogo será mostrada indicando o status da instalação dos pré-requisitos. A instalação demora vários minutos.
5. Clique em **Avançar** na tela de boas-vindas.
6. Leia o contrato de licença, concorde com os termos e clique em **Avançar**.

7 Clique em **Avançar** para instalar o Personal Edition no local padrão de **C:\Program Files\Dell\Dell Data Protection\.**

8 O Security Tools é instalado por padrão e não pode ser desmarcado. Isso está listado como Security Framework no instalador.
O Advanced Authentication é instalado por padrão e não pode ser desmarcado.

Clique em **Avançar**.

9 Clique em **Instalar** para iniciar a instalação.
Uma janela de status é exibida. A instalação demora vários minutos.

10 Selecione **Sim, quero reiniciar meu computador agora** e clique em **Concluir**.

11 Quando o computador tiver sido reiniciado, faça a autenticação no Windows.

A instalação de Personal Edition + Security Tools está concluída.

O Assistente de configuração do Personal Edition e a Configuração são cobertos separadamente.

Após a execução do Assistente de configuração do Personal Edition e da Configuração, abra o Security Tools Administrator Console.

O restante desta seção fornece mais detalhes sobre as tarefas de instalação e pode ser pulado. Vá para Assistentes de configuração do Security Tools e do Personal Edition.

**Instalação usando a linha de comando**

- Instale o direito no computador de destino, se necessário.
- Opções:

  Para uma instalação por linha de comando, as opções precisam ser especificadas primeiro. A tabela a seguir detalha as opções disponíveis para a instalação.

| Opção | Significado |
|---|---|
| -y -gm2 | Passar dados para o autoextrator |
| /s | Modo silencioso |
| /z | Passar dados para a variável de sistema CMDLINE do InstallScript |

- Parâmetros:

  A tabela a seguir detalha os parâmetros disponíveis para a instalação.

| Parâmetros |
|---|
| InstallPath=caminho para local alternativo de instalação. |
| FEATURE=PE |

- Exemplo de instalação por linha de comando

  Embora a reinicialização seja suprimida nesses exemplos, uma reinicialização será necessária adiante. Não será possível iniciar a criptografia até o computador ser reinicializado.

  Lembre-se de cercar um valor que contenha um ou mais caracteres especiais, como um espaço em branco, com aspas com caractere de escape.

  As linhas de comando diferenciam letras maiúsculas de minúsculas.

- O seguinte exemplo instala o Personal Edition e o Security Tools (instalação silenciosa, sem reinicialização e instalado no local padrão **C:\Program Files\Dell\Dell Data Protection**).

```
DDPSetup.exe -y -gm2 /S /z"\"FEATURE=PE\""
```

- O seguinte exemplo instala o Personal Edition e o Security Tools (instalação silenciosa, sem reinicialização e instalado no local padrão **C:\Program Files\Dell\My_New_Folder**).

  ```
  DDPSetup.exe -y -gm2 /S /z"\"FEATURE=PE, InstallPath=C:\Program Files\Dell\My_New_Folder\""
  ```

  Quando o computador for reiniciado, faça a autenticação no Windows.

  A instalação de Personal Edition + Security Tools está concluída.

  O Assistente de configuração do Personal Edition e a Configuração são cobertos separadamente.

  Após a execução do Assistente de configuração do Personal Edition e da Configuração, abra o Security Tools Administrator Console.

  O restante desta seção fornece mais detalhes sobre as tarefas de instalação e pode ser pulado. Vá para Assistentes de configuração do Security Tools e do Personal Edition.

# Instalar o Personal Edition usando os instaladores filhos

Para Instalar o Personal Edition usando os instaladores filhos, os arquivos filhos executáveis precisam antes ser extraídos do instalador mestre. Consulte Extrair os instaladores filhos do instalador mestre. Quando terminar, retorne para esta seção.

**Instalação por linha de comando**

- Parâmetros e opções de linha de comando fazem distinção entre maiúsculas e minúsculas.
- Lembre-se de cercar um valor que contenha um ou mais caracteres especiais, como um espaço em branco na linha de comando, com aspas como caractere de escape.
- Use esses instaladores para instalar os clientes usando uma instalação com scripts, arquivos em lote ou qualquer outra tecnologia push disponível para sua organização.
- A reinicialização foi suprimida nos exemplos de instalação por linha de comando. Entretanto, uma eventual reinicialização é necessária. Não será possível iniciar a criptografia até o computador ser reinicializado.
- Arquivos de log: O Windows cria arquivos de log de instalação para cada instalador filho, para o usuário logado em %temp%, os quais podem ser encontrados em **C:\Users\<UserName>\AppData\Local\Temp.**

  Se você decidir adicionar um arquivo de log distinto quando executar o instalador, verifique se o arquivo de log tem um nome único, pois os arquivos de log de instalador filho não são acrescidos. O comando padrão .msi pode ser usado para criar um arquivo de log usando **/l*v C:\<any directory>\<any log file name>.log**.
- Todos os instaladores filhos usam as mesmas opções de exibição e opções .msi básicas, exceto onde indicado, para as instalações por linha de comando. As opções precisam ser especificadas antes. A opção /v é necessária e utiliza um argumento. Outros parâmetros vão dentro de um argumento que é passado para a opção /v.

  Opções de exibição podem ser especificadas no final do argumento passado para a opção /v para obter o comportamento esperado. Não use /q e /qn na mesma linha de comando. Use apenas ! e - depois de /qb.

| Opção | Significado |
|---|---|
| /v | Passa as variáveis para o .msi dentro do *.exe |
| /s | Modo silencioso |
| /i | Modo de instalação |

| Opção | Significado |
|---|---|
| /q | Não há caixa de diálogo de andamento, reinicia-se após a conclusão do processo |
| /qb | Caixa de diálogo de andamento com o botão **Cancelar**, solicita a reinicialização |

| Opção | Significado |
|---|---|
| /qb- | Caixa de diálogo de andamento com o botão **Cancelar**, reinicia-se após a conclusão do processo |
| /qb! | Caixa de diálogo de andamento sem o botão **Cancelar**, solicita a reinicialização |
| /qb!- | Caixa de diálogo de andamento sem o botão **Cancelar**, reinicia-se após a conclusão do processo |
| /qn | Sem interface do usuário |

**Instalar drivers**

- Os drivers e o firmware para Dell ControlVault, leitores de impressão digital e cartões inteligentes não estão contidos nos arquivos executáveis do instalador mestre ou dos instaladores filhos. Os drivers e o firmware precisam ser mantidos atualizados e podem ser obtidos por download em http://www.dell.com/support, selecionando o modelo do seu computador. Faça download dos drivers e firmware adequados com base em seu hardware de autenticação.
  - Dell ControlVault
  - Leitor de impressão digital de indicadores biométricos NEXT
  - Driver 495 do leitor de impressão digital Validity
  - Driver de cartão inteligente O2Micro

  No caso de instalação em hardware que não seja da Dell, faça download dos drivers e do firmware atualizados no site do fornecedor.
- Em seguida:

**Instalar os clientes do Advanced Authentication**

- Os usuários fazem login na PBA usando suas credenciais do Windows.
- Localize o arquivo em **C:\extracted\Security Tools** e em **C:\extracted\Security Tools\Authentication.**

Exemplo de instalação por linha de comando

**\Security Tools**

- O seguinte exemplo instala o Security Framework (instalação silenciosa, sem reinicialização e é instalado no local padrão C:\Program Files\Dell\Dell Data Protection).

```
EMAgent_XXbit_setup.exe /s /v"/norestart /qn"
```

> **NOTA:**
> Esse cliente é necessário no Advanced Authentication v8.x.

*Em seguida*:

**\Security Tools\Authentication**

- O seguinte exemplo instala Security Tools (instalação silenciosa, sem reinicialização e é instalado no local padrão C:\Program Files\Dell\Dell Data Protection).

```
setup.exe /s /v"/norestart /qn"
```

*Em seguida*:

**Instalar o Encryption Client**

- Analise os requisitos do Encryption Client caso sua organização esteja usando um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign. É necessário fazer uma mudança na configuração do registro do computador cliente para permitir a validação do certificado.

- Localize o arquivo em **C:\extracted\Encryption.**

  Exemplo de instalação por linha de comando

- O exemplo a seguir instala o Personal Edition, Encrypt for Sharing, oculta os ícones de superposição, não mostra caixa de diálogo, não mostra barra de andamento e suprime a reinicialização.

  ```
  DDPE_XXbit_setup.exe /s /v"HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
  ```

  Quando o computador for reiniciado, faça a autenticação no Windows.

  A instalação de Personal Edition + Security Tools está concluída. O Assistente de configuração do Personal Edition e a Configuração são cobertos separadamente.

  Vá para Assistentes de configuração do Security Tools e do Personal Edition.

# Assistentes de configuração do Security Tools e do Personal Edition

Faça login com seu nome de usuário e senha do Windows. Você acessará imediatamente o Windows. A interface pode parecer diferente do que você está acostumado a ver.

1 O UAC pode solicitar a você que execute o aplicativo. Em caso afirmativo, clique em Sim.

2 Após a reinicialização da instalação inicial, o assistente de ativação do Security Tools é mostrado. Clique em **Avançar**.

3 Digite uma nova Senha de administrador de criptografia (EAP - Encryption Administrator Password) e digite-a novamente. Clique em **Avançar**.

4 Informe um local de backup em uma unidade de rede ou em uma mídia removível para armazenar as informações de recuperação e clique em **Avançar**.

5 Clique em **Aplicar** para iniciar a ativação do ST.

6 Depois de concluir o assistente de ativação do Security Tools, abra o assistente de configuração do Personal Edition a partir do ícone do DDP na bandeja do sistema (pode ser que abra por conta própria).

Esse Assistente de configuração o ajuda a usar criptografia para proteger as informações deste computador. Enquanto o assistente não for concluído, não será possível iniciar a criptografia.

Leia a tela de boas-vindas e clique em **Avançar**.

7 Selecione um modelo de política. O modelo de política estabelece as configurações padrão de políticas para criptografia.

Você poderá facilmente aplicar um modelo de política diferente ou personalizar o modelo selecionado no Console de gerenciamento local quando a configuração inicial estiver concluída.

Clique em **Avançar**.

8 Leia e confirme o aviso de senha do Windows. Se quiser criar uma senha do Windows agora, consulte Requisitos.

9 Crie uma Senha de administrador de criptografia (EAP — Encryption Administrator Password) com 9 a 32 caracteres e confirme. A senha deverá conter caracteres alfabéticos, numéricos e especiais. Essa senha pode ser a mesma que a EAP configurada para o Security Tools, mas não há relação entre elas. **Anote e guarde essa senha em um local seguro**. Clique em **Avançar**.

10 Clique em **Procurar** para escolher uma unidade de rede ou um armazenamento removível e fazer o backup de suas chaves de criptografia (que são incorporadas a um aplicativo chamado LSARecovery_[nome_do_host].exe).

No caso de determinadas falhas de computador, essas chaves serão usadas para recuperar seus dados.

Além disso, alterações futuras nas políticas possivelmente exigirão que o backup das chaves de criptografia seja feito novamente. Se a unidade de rede ou o armazenamento removível estiver disponível, o backup de suas chaves de criptografia será feito em segundo plano. Entretanto, se o local não estiver disponível (por exemplo, se o dispositivo de armazenamento removível original não tiver sido inserido no computador), as alterações de política não entrarão em vigor até que o backup manual das chaves de criptografia seja feito.

> **NOTA: Para obter informações sobre como fazer o backup manual das chaves de criptografia, clique em "? > Ajuda" no canto superior direito do Console de gerenciamento local ou clique em Iniciar > Todos os programas >Dell > Dell Data Protection > Criptografia > Ajuda de criptografia.**

Clique em **Avançar**.

11 Uma lista de configurações de criptografia é mostrada na tela Confirmar configurações de criptografia. Analise os itens e clique em **Confirmar** quando estiver satisfeito com as configurações.

A configuração do computador é iniciada. Uma barra de status informa o andamento da configuração.

12 Clique em **Concluir** para concluir a configuração.

13 Uma reinicialização será necessária depois de configurar o computador para criptografia. Clique em **Reinicializar agora** ou você pode adiar a reinicialização 20 minutos por 5 vezes.

14 Depois de reinicializar o computador, abra o Console de gerenciamento local a partir do menu Iniciar para ver o status da criptografia.

A criptografia ocorre em segundo plano. O Console de gerenciamento local pode ser deixado aberto ou fechado. A criptografia dos arquivos será feita em qualquer caso. O computador pode ser usado normalmente durante a criptografia.

15 O computador reinicializará mais uma vez quando a verificação terminar.

Quando terminarem todas as varreduras de criptografia e reinicializações, você pode verificar o status de conformidade abrindo o Console de gerenciamento local. A unidade estará identificada como "Em conformidade".

Vá para Definir as configurações de administrador do Security Tools.

# Definir as Configurações de Administrador do Security Tools

As configurações padrão do Security Tools permitem que administradores e usuários usem o Security Tools imediatamente após a ativação, sem necessidade de configuração adicional. Os usuários são adicionados automaticamente como usuários do Security Tools ao iniciarem a sessão no computador com suas senhas do Windows, mas, por padrão, a autenticação por múltiplos fatores no Windows não está ativada.

Para configurar os recursos do Security Tools, você precisa ser administrador no computador.

## Alterar o local de backup e a senha do administrador

Depois da ativação do Security Tools, o local de backup e a senha do administrador podem ser alterados, caso seja necessário.

1. Como administrador, abra Security Tools pelo atalho da área de trabalho.
2. Clique no bloco **Configurações de administrador**.
3. Na caixa de diálogo Autenticação, digite a senha do administrador que foi configurada durante a ativação e clique em **OK.**
4. Clique na guia **Configurações de administrador**.
5. Na página Alterar senha de administrador, se você quiser alterar a senha, digite uma nova senha com 8 a 32 caracteres e que contenha no mínimo uma letra, um número e um caractere especial.
6. Digite a senha uma segunda vez para confirmá-la e clique em **Aplicar**.
7. Para alterar o local no qual a chave de recuperação está armazenada, selecione **Alterar local de backup** no painel esquerdo.
8. Selecione um novo local para o backup e clique em **Aplicar**.

   O arquivo de backup precisa ser salvo em uma unidade de rede ou em mídia removível. O arquivo de backup contém as chaves que são necessárias para recuperar dados neste computador. O Dell ProSupport precisa ter acesso a esse arquivo para ajudar você a recuperar os dados.

   O backup dos dados de recuperação será feito automaticamente, no local especificado. Se o local não estiver disponível (por exemplo, se a unidade USB de backup não estiver inserida), o Security Tools solicitará um local para fazer backup dos dados. Para iniciar a criptografia, será necessário acesso aos dados de recuperação.

## Configurar opções de autenticação

Os controles na guia Autenticação de configurações de administrador permitem que você defina as opções de acesso de usuário e personalize as configurações para cada uma delas.

**NOTA: A opção de Senha de uso único não é mostrada nas Opções de recuperação caso o TPM não esteja presente, ativado e com um proprietário.**

## Configurar opções de login

Na página opções de login, você pode configurar as políticas de login. Por padrão, todas as credenciais suportadas estão listadas em Opções disponíveis.

Para configurar as opções de login:

1 No painel esquerdo, em Autenticação, selecione **Opções de login**.

2 Para escolher a função que você deseja configurar, selecione a função na lista **Aplicar opções de acesso a**: **Usuários** ou **Administradores**. Todas as mudanças realizadas nessa página só serão aplicadas à função selecionada.

3 Defina as Opções disponíveis para autenticação.

Por padrão, todo método de autenticação é configurado para ser usado individualmente e não em combinação com outros métodos de autenticação. Você pode alterar os padrões das seguintes maneiras:

- Para configurar uma combinação de opções de autenticação, em Opções disponíveis, clique em para selecionar o primeiro método de autenticação. Na caixa de diálogo Opções disponíveis, selecione o segundo método de autenticação e depois clique em **OK**.

  Por exemplo, você pode solicitar impressão digital e uma senha como credenciais de acesso. Na caixa de diálogo, selecione o segundo método de autenticação que precisa ser usado juntamente com a autenticação por impressão digital.
- Para permitir que cada método de autenticação seja usado individualmente, na caixa de diálogo Opções disponíveis, deixe o segundo método de autenticação definido como **Nenhum**, e clique em **OK**.
- Para remover uma opção de entrada, sob Opções disponíveis) na página Opções de entrada, clique em **X** para remover o método.
- Para adicionar uma nova combinação de métodos de autenticação, clique em **Adicionar uma opção**.

4 Defina opções de recuperação para que os usuários recuperem o acesso deles ao computador, caso fiquem bloqueados.

- Para permitir que os usuários definam um conjunto de perguntas e respostas para uso ao obter acesso novamente ao computador, selecione **Perguntas de recuperação**.

  Para impedir o uso do recurso Perguntas de recuperação, desmarque a opção.
- Para permitir que os usuários recuperem o acesso usando um dispositivo móvel, selecione **Senha de uso único**. Quando a opção Senha de uso único (OTP) é selecionada como um método de recuperação, ela não fica disponível como uma opção de login na tela de login do Windows.

  Para usar o recurso de OTP para fazer login, desmarque a opção em Opções de recuperação. Quando desmarcada como opção de recuperação, a opção OTP aparece em uma página de login do Windows desde que no mínimo um usuário esteja inscrito na OTP.

  > **NOTA: Como administrador, você controlar como a Senha de uso único pode ser usada: para autenticação ou para recuperação. O recurso de OTP pode ser usado para autenticação ou para recuperação, mas não para ambas. A configuração afeta todos os usuários do computador ou todos os administradores com base na seleção do campo Opções de login, em Aplicar opções de login a.**

  Se a opção de Senha de uso único não for mostrada na lista em Opções de recuperação, a configuração do seu computador não oferece suporte para o recurso. Para obter mais informações, consulte Requisitos.
- Para solicitar que o usuário ligue para o atendimento caso perca ou esqueça as credenciais de login, desmarque as duas caixas de seleção em Opções de recuperação: Perguntas de recuperação e Senha de uso único.

5 Para definir um período de tempo no qual os usuários poderão inscrever suas credenciais de autenticação, selecione **Período de tolerância**.

O recurso Período de tolerância permite que você defina a data na qual uma opção de login configurada começará a ser aplicada. Você pode configurar uma opção de login antes da data na qual ela será aplicada e definir um período de tempo para permitir a inscrição dos usuários. Por padrão, a política é aplicada imediatamente.

Para alterar a data do parâmetro Aplicar Opção de Login de *Imediatamente* na caixa de diálogo Período de tolerância, clique no menu suspenso e selecione **Data especificada**. Clique na seta para baixo no lado direito do campo de data para mostrar um calendário e, em seguida, selecione uma data. A execução da política começa, aproximadamente, às 00h01 da data marcada.

Os usuários podem ser lembrados de inscrever suas credenciais necessárias no próximo login no Windows (por padrão) ou você pode configurar lembretes regulares. Selecione o intervalo de lembretes na lista suspensa *Lembrar usuário*.

**NOTA:**
O lembrete mostrado para o usuário é um pouco diferente, dependendo de se o usuário está na tela de login do Windows ou em uma sessão do Windows quando o lembrete é acionado. Os lembretes não são mostrados nas telas de login da Autenticação de pré-inicialização.

**Funcionalidade durante o período de tolerância**

Durante um Período de tolerância especificado, após cada login, a notificação Credenciais adicionais é mostrada enquanto o usuário ainda não tiver inscrito as credenciais mínimas necessárias para atender uma opção de login alterada. O conteúdo da mensagem é: *Credenciais adicionais estão disponíveis para inscrição.*

Caso haja credenciais adicionais, mas não forem obrigatórias, a mensagem será mostrada apenas uma vez depois que a política for alterada.

Clicar na notificação tem os seguintes resultados, dependendo do contexto:

- Se nenhuma credencial estiver inscrita, o assistente de instalação é mostrado, permitindo que os usuários administrativos definam as configurações relacionadas ao computador, oferecendo aos usuários a capacidade de inscrever as credenciais mais comuns.
- Após a inscrição inicial da credencial, clicar na notificação exibe o assistente de instalação no DDP Security Console.

**Funcionalidade após o término do período de tolerância**

Em todos os casos, depois que o período de tolerância termina, os usuários não podem fazer login sem ter inscrito as credenciais exigidas pela opção de login. Se um usuário tentar acessar com uma credencial ou combinação de credenciais que não atenda à opção de login, o assistente de instalação será mostrado na parte superior da tela de login do Windows.

- Se o usuário inscrever com sucesso as credenciais necessárias, será feito o login no Windows.
- Se um usuário não inscrever com sucesso as credenciais necessárias ou cancelar o assistente, ele voltará à tela de login do Windows.

6 Para salvar as configurações para a função selecionada, clique em **Aplicar**.

# Configurar autenticação do Password Manager

Na página do Password Manager, é possível configurar como os usuários se autenticam no utilitário.

Para configurar a autenticação do Password Manager:

1 No painel esquerdo, em Autenticação, selecione **Password Manager**.

2 Para escolher a função que você deseja configurar, selecione a função na lista **Aplicar opções de acesso a**: **Usuários** ou **Administradores**. Todas as mudanças realizadas nessa página só serão aplicadas à função selecionada.

3 Como opção, selecione a caixa de seleção **Não exigir autenticação** para permitir que a função do usuário selecionado seja conectada automaticamente em todos os aplicativos de software e sites de Internet com as credenciais armazenadas no Password Manager.

4 Defina as Opções disponíveis para autenticação.

Por padrão, todo método de autenticação é configurado para ser usado individualmente e não em combinação com outros métodos de autenticação. Você pode alterar os padrões das seguintes maneiras:

- Para configurar uma combinação de opções de autenticação, em Opções disponíveis, clique em para selecionar o primeiro método de autenticação. Na caixa de diálogo Opções disponíveis, selecione o segundo método de autenticação e depois clique em **OK**.

  Por exemplo, você pode solicitar impressão digital e uma senha como credenciais de acesso. Na caixa de diálogo, selecione o segundo método de autenticação que precisa ser usado juntamente com a autenticação por impressão digital.
- Para permitir que cada método de autenticação seja usado individualmente, na caixa de diálogo Opções disponíveis, deixe o segundo método de autenticação definido como **Nenhum**, e clique em **OK**.
- Para remover uma opção de entrada, sob Opções disponíveis) na página Opções de entrada, clique em **X** para remover o método.

- Para adicionar uma nova combinação de métodos de autenticação, clique em **Adicionar uma opção**.

5 Para salvar as configurações para a função selecionada, clique em **Aplicar**.

> **NOTA: Selecione o botão Configurações padrão para restaurar as configurações para seus valores originais.**

# Configurar Perguntas de recuperação

Na página Perguntas de recuperação, você pode selecionar quais perguntas serão apresentadas aos usuários quando eles definirem perguntas e respostas de recuperação pessoais. As perguntas de recuperação permitem que os usuários recuperem acesso aos seus computadores em caso de esquecimento ou expiração das senhas.

Para configurar as Perguntas de recuperação:

1 No painel esquerdo, sob Autenticação, selecione **Perguntas de recuperação**.
2 Na página Perguntas de recuperação, selecione no mínimo três perguntas pré-definidas.
3 Como opção, você pode adicionar até três perguntas personalizadas à lista para que o usuário escolha.
4 Para salvar as perguntas de recuperação, clique em **Aplicar**.

# Configurar autenticação de leitura de impressão digital

Para configurar a autenticação de leitura de impressão digital:

1 No painel esquerdo, sob Autenticação, selecione **Impressões digitais**.
2 Em Inscrições, defina o número máximo e o mínimo de dedos que um usuário pode inscrever.
3 Defina a Sensibilidade de leitura de impressão digital.

   Diminuir a sensibilidade aumenta a variação aceitável e a probabilidade de aceitar uma leitura falsa. Na configuração mais alta, o sistema pode rejeitar impressões digitais legítimas. A configuração de Maior sensibilidade diminui a taxa de aceitação de falsos para 1 a cada 10.000 leituras.
4 Para remover todas as leituras de impressões digitais e inscrições de credenciais do buffer do leitor de impressão digital, clique em **Limpar leitor**. Isso remove apenas os dados que você está adicionando no momento. Essa ação não apaga leituras e inscrições armazenadas de sessões anteriores.
5 Para salvar as configurações, clique em **Aplicar**.

# Configurar autenticação de senha de uso único

> **NOTA: O recurso de OTP exige que o módulo TPM esteja presente, ativado e tenha proprietário. Para obter instruções sobre como configurar o TPM, consulte Configuração de pré-instalação para Senha de uso único.**

Para usar o recurso Senha de uso único, o usuário gera uma senha de uso único com o Security Tools Mobile em seu dispositivo móvel e depois digita essa senha no computador. A senha pode ser usada apenas uma vez e é válida por um período limitado.

Para aprimorar ainda mais a segurança, o administrador pode garantir a segurança do aplicativo móvel exigindo uma senha.

Na página Dispositivo móvel, é possível definir as configurações que aumentam ainda mais a segurança do dispositivo móvel e da senha de uso único.

Para configurar a autenticação de senha de uso único:

1 No painel esquerdo, sob Autenticação, selecione **Dispositivo móvel**.
2 Para exigir que o usuário digite uma senha para acessar o aplicativo Security Tools Mobile no dispositivo móvel, selecione **Exigir senha**.

**NOTA: A ativação da política *Exigir senha* após dispositivos móveis terem sido inscritos com um computador cancela a inscrição de todos os dispositivos móveis. Os usuários serão solicitados a reinscrever seus dispositivos móveis uma vez que esta política seja ativada.**

Quando a caixa de seleção **Exigir senha** estiver marcada, os usuários precisarão desbloquear seu dispositivo móvel para acessar o aplicativo Security Tools Mobile. Se o bloqueio de um dispositivo não estiver presente no dispositivo móvel, a senha será necessária.

3 Para selecionar o tamanho da senha de uso único (OTP) para a configuração **Tamanho da senha de uso único**, selecione o número de caracteres da senha exigido.

4 Para selecionar o número de chances que o usuário tem para digitar a senha de uso único corretamente, escolha um número de **5** a **30** para a configuração **Tentativas autorizadas de login de usuário**.

Quando o número máximo de tentativas for alcançado, o recurso OTP será desativado até que o usuário inscreva novamente o dispositivo móvel.

**NOTA: A Dell recomenda configurar no mínimo um método adicional de autenticação além da senha de uso único.**

# Configurar a inscrição de cartão inteligente

O DDP|Security Tools oferece suporte para dois tipos de cartões inteligentes: com e sem contato.

Os cartões com contato exigem um leitor de cartão inteligente, no qual são inseridos. Esses cartões são compatíveis apenas com computadores de domínio. Cartões SIPRNet e CAC são cartões com contato. Devido à natureza avançada desses cartões, o usuário precisará escolher um certificado após inserir seu cartão para fazer login.

- Os cartões sem contato são suportados por computadores sem domínio e computadores configurados com especificações de domínio.
- Os usuários podem inscrever um cartão inteligente com contato para cada conta de usuário ou múltiplos cartões sem contato por conta.
- Os cartões inteligentes não são suportados com Autenticação de pré-inicialização.

**NOTA: Ao remover uma inscrição de cartão inteligente de uma conta com múltiplos cartões inscritos, todos os cartões têm sua inscrição cancelada ao mesmo tempo.**

Para configurar a inscrição de cartão inteligente:

Na guia Autenticação da ferramenta Configurações de administrador, selecione **Cartão inteligente**.

# Configurar permissões avançadas

1 Clique em **Avançado** para modificar as opções avançadas de usuários finais. Em *Avançado*, você pode optar por permitir que os usuários inscrevam credenciais por conta própria ou que modifiquem as credenciais inscritas, além de poder ativar o login em uma etapa.

2 Marque ou desmarque as caixas de seleção:

**Permitir que usuários inscrevam credenciais** - essa caixa de seleção é marcada por padrão. Os usuários são autorizados a inscrever credenciais sem a intervenção de um administrador. Se você desmarcar a caixa de seleção, as credenciais precisam ser inscritas pelo administrador.

**Permitir que o usuário modifique as credenciais inscritas** - essa caixa de seleção é marcada por padrão. Quando marcada, os usuários têm permissão para modificar ou apagar suas credenciais inscritas sem a intervenção de um administrador. Se você desmarcar a caixa de seleção, as credenciais não podem ser modificadas ou apagadas por um usuário comum, apenas pelo administrador.

**NOTA: Para inscrever as credenciais de um usuário, acesse a página *Usuários* da ferramenta Configurações de administrador e clique em Inscrever.**

**Permitir login em uma etapa** - o login em uma etapa é o Login único (SSO). Por padrão, a caixa de seleção é marcada. Quando esse recurso é ativado, os usuários precisam digitar suas credenciais apenas na tela de Autenticação de pré-inicialização. Os usuários são

conectados automaticamente no Windows. Se você desmarcar a caixa de seleção, o usuário pode ser solicitado a se conectar várias vezes.

> **NOTA: Essa opção não pode ser selecionada, a menos que a configuração Permitir que os usuários inscrevam credenciais também seja selecionada.**

3 Clique em **Aplicar** quando terminar.

# Gerenciar a autenticação de usuários

Os controles na guia Autenticação de configurações de administrador permitem que você defina as opções de login de usuário e defina as configurações para cada uma delas.

Para gerenciar a autenticação do usuário:

1 Como administrador, clique no bloco **Configurações de administrador**.
2 Clique na guia **Usuários** para gerenciar usuários e ver seu status de inscrição. Com esta guia, você pode:
- Inscrever novos usuários
- Adicionar ou alterar credenciais
- Remover as credenciais do usuário

> **NOTA:**
> As opções **Login** e **Sessão** mostram o status de inscrição de um usuário.
>
> Quando o status de **Login** for **OK**, todas as inscrições que o usuário precisa para iniciar a sessão foram preenchidas. Quando o status de **Sessão** for **OK**, todas as inscrições que o usuário precisa para usar o Password Manager foram preenchidas.
>
> Se o status de alguma das opções for **Não**, o usuário precisará preencher inscrições adicionais. Para saber quais inscrições ainda são necessárias, selecione a ferramenta **Configurações de administrador** e abra a guia **Usuários**. As caixas de seleção na cor cinza representam inscrições incompletas. Como opção, clique no bloco **Inscrições** e confira o status da coluna **Política** na guia **Status** onde as inscrições necessárias aparecem.

# Adicionar novos usuários

> **NOTA: Novos usuários do Windows são automaticamente adicionados quando fazem login no Windows ou inscrevem credenciais.**

1 Clique em **Adicionar Usuário** para iniciar o processo de inscrição para um usuário existente do Windows.
2 Quando a caixa de diálogo *Selecionar usuário* for mostrada, selecione **Tipos de objeto**.
3 Digite o nome de objeto de um usuário na caixa de texto e clique em **Verificar nomes**.
4 Clique em **OK** quando tiver terminado.
O Assistente de inscrição é mostrado.

Continue em Inscrever ou alterar credenciais de usuário para obter instruções.

# Inscrever ou alterar credenciais de usuário

O administrador pode inscrever ou alterar as credenciais de um usuário em nome do mesmo, mas algumas atividades de inscrição exigem a presença do usuário, como responder perguntas de recuperação e fazer a leitura de suas impressões digitais.

Para inscrever ou alterar as credenciais do usuário:

1 Em Configurações de administrador, clique na guia **Usuários**.
2 Na página Usuários, clique em **Inscrever**.
3 Na página de Boas-vindas, clique em **Avançar**.
4 Na caixa de diálogo Autenticação necessária, faça login com a senha do Windows do usuário e clique em **OK**.
5 Na página Senha, para alterar a senha do Windows do usuário, digite e confirme uma nova senha. Depois, clique em **Avançar**.
Para pular a etapa de alteração de senha, clique em **Pular**. O assistente permite que você ignore uma credencial caso não queira inscrevê-la. Para voltar uma página, clique em **Voltar**.
6 Siga as instruções em cada página e clique no botão adequado: **Avançar**, **Pular** ou **Voltar**.
7 Na página Resumo, confirme as credenciais inscritas e, após concluir a inscrição, clique em **Aplicar**.
Para retornar a uma página de inscrição de credencial e fazer uma alteração, clique em **Voltar** até chegar à página que você quer alterar.

Para obter informações mais detalhadas sobre a inscrição de uma credencial ou sobre como alterar uma credencial, consulte o *Guia do usuário do Console*.

# Remover uma credencial inscrita

1 Clique no bloco **Configurações de administrador**.
2 Clique na guia **Usuários** e localize o usuário que você quer alterar.
3 Posicione o cursor sobre a marca de seleção verde da credencial que você quer remover. A marca se transformará em ⊗
4 Clique no símbolo ⊗ e depois clique em **Sim** para confirmar a remoção.

> ⓘ **NOTA: Uma credencial não pode ser removida dessa maneira caso seja a única credencial inscrita do usuário. Além disso, a senha não pode ser removida por este método. Use o comando Remover para remover por completo o acesso de um usuário ao computador.**

# Remover todas as credenciais inscritas de um usuário

1 Clique no bloco **Configurações de administrador**.
2 Clique na guia **Usuários** e localize o usuário que você deseja remover.
3 Clique em **Remover**. O comando Remover aparece em vermelho abaixo das configurações do usuário.
Após a remoção, o usuário não conseguirá fazer login no computador, a menos que se inscreva novamente.

# Desinstalar usando o instalador mestre

- Cada componente precisa ser desinstalado separadamente, seguidos pela desinstalação do instalador mestre. Os clientes precisam ser desinstalados em uma **ordem específica para evitar falhas de desinstalação**.
- Siga as instruções em Extrair os instaladores filhos do instalador mestre para obter os instaladores filhos.
- Certifique-se de que a mesma versão do instalador mestre (e, com isso, os clientes) usada na instalação seja usada na desinstalação.
- Esse capítulo direciona você para outro capítulo que contém instruções *detalhadas* sobre como desinstalar os instaladores filho. Este capítulo explica **apenas** a última etapa, a desinstalação do instalador mestre.

Desinstale os clientes na seguinte ordem.

1 Desinstalar o Encryption Client.
2 Desinstalar o Client Security Framework.
3 Desinstalar o Advanced Authentication.

O pacote de drivers não precisa ser desinstalado.

Vá para Escolher um método de desinstalação.

# Escolher um método de desinstalação

Há dois métodos para desinstalar o instalador mestre. Selecione **um** deles:

- Desinstalar a partir de Adicionar ou Remover Programas
- Desinstalar a partir da linha de comando

# Desinstalar a partir de Adicionar ou Remover Programas

1 No painel de controle do Windows, acesse Desinstalar um programa (**Iniciar** > **Painel de controle** > **Programas e recursos** > **Desinstalar um programa.**).
2 Selecione o **Instalador do Dell Data Protection** e clique com o botão esquerdo em **Alterar** para iniciar o Assistente de instalação.
3 Leia a tela de boas-vindas e clique em **Avançar**.
4 Siga os passos para desinstalar e clique em **Concluir**.
5 Reinicie o computador e faça login no Windows.
O instalador mestre foi desinstalado.

# Desinstalar a partir da linha de comando

- O exemplo a seguir desinstala silenciosamente o instalador mestre.

```
"DDPSetup.exe" -y -gm2 /S /x
```

Reinicie o computador ao terminar.

O instalador mestre foi desinstalado.

Vá para Desinstalar usando os instaladores filhos.

# 8

# Desinstalar usando os instaladores filhos

- O usuário que executa a descriptografia e a desinstalação precisa ser um administrador local ou de domínio. Se for desinstalar por linha de comando, as credenciais do administrador de domínio são necessárias.
- Se você instalou o Personal Edition com o instalador mestre, os arquivos executáveis filhos precisam ser extraídos do instalador mestre antes da desinstalação, conforme mostrado em Extrair os instaladores filhos do instalador mestre.
- Certifique-se de que a mesma versão dos clientes usada na instalação seja usada na desinstalação.
- Planeje realizar a descriptografia durante a noite, se possível.
- Desative o modo de suspensão para impedir que um computador sem supervisão entre em modo de suspensão. A descriptografia não pode ocorrer em um computador em modo de suspensão.
- Feche todos os processos e aplicativos para reduzir as falhas devido a arquivos bloqueados.

# Desinstalar o Encryption Client

- **Antes de iniciar o processo de desinstalação**, consulte (Opcional) Criar um arquivo de log do Agente de remoção de criptografia. Este arquivo de log é útil para solucionar problemas de uma operação de desinstalação/descriptografia. Se você não pretende descriptografar arquivos durante o processo de desinstalação, não é necessário criar um arquivo de log do Agente de remoção de criptografia.
- Execute o WSScan para garantir que todos os dados sejam descriptografados após a conclusão da desinstalação, mas antes de reiniciar o computador. Consulte Usar WSScan para obter instruções.
- Periodicamente Verificar o status do Agente de remoção de criptografia. A descriptografia dos dados ainda está em andamento se o serviço Agente de remoção de criptografia estiver presente no painel Serviços.

# Escolher um método de desinstalação

Há dois métodos para desinstalar o Encryption Client. Selecione **um** deles:

- Desinstalar usando a interface do usuário
- Desinstalar a partir da linha de comando

**Desinstalar usando a interface do usuário**

1 No painel de controle do Windows, acesse Desinstalar um programa (**Iniciar** > **Painel de controle** > **Programas e recursos** > **Desinstalar um programa.**).
2 Selecione **Encryption** e clique com o botão esquerdo em **Alterar** para iniciar o Assistente de configuração do Personal Edition.
3 Leia a tela de boas-vindas e clique em **Avançar**.
4 Na tela Instalação do Agente de remoção de criptografia, selecione uma destas opções:

> **NOTA: A segunda opção está ativada por padrão. Se você quiser descriptografar arquivos, altere a seleção para a opção um.**

- Agente de remoção de criptografia — Importar chaves de um arquivo

  Para criptografia SDE, Usuário ou Comum, essa opção descriptografa os arquivos e desinstala o Encryption Client. ***Esta é a seleção recomendada.***
- Não instalar o Agente de remoção de criptografia

Essa opção desinstala o Encryption Client, *mas não descriptografa os arquivos*. Esta opção deve ser usada **somente** para fins de solução de problemas, conforme instruções do Dell ProSupport.

Clique em **Avançar**.

5 Na caixa de texto *Arquivo de backup*, digite o caminho para a unidade de rede ou para o local da mídia removível do arquivo de backup ou clique em **...** para procurar o local. O formato do arquivo é LSARecovery_[nome_do_host].exe.

Digite sua Senha de administrador de criptografia na caixa de texto Senha. Essa é a senha que foi configurada no Assistente de configuração quando o software foi instalado.

Clique em **Avançar**.

6 Na tela *Fazer login no serviço Dell Decryption Agent como*, há duas opções. Selecione **Conta de sistema local**. Clique em **Concluir**.

7 Clique em **Remover** na tela Remover o programa.

8 Clique em **Concluir** na tela Configuração concluída.

9 Reinicie o computador e faça login no Windows.

A descriptografia está agora em andamento.

O processo de descriptografia pode levar várias horas, dependendo do número de unidades que estiverem sendo descriptografadas e da quantidade de dados dessas unidades. Para verificar o processo de descriptografia, consulte Verificar o status do Agente de remoção de criptografia.

### Desinstalar a partir da linha de comando

- Parâmetros e opções de linha de comando fazem distinção entre maiúsculas e minúsculas.
- Lembre-se de cercar um valor que contenha um ou mais caracteres especiais, como um espaço em branco na linha de comando, com aspas como caractere de escape. Os parâmetros de linha de comando diferenciam letras maiúsculas de minúsculas.
- Use esses instaladores para desinstalar os clientes usando uma instalação com scripts, arquivos em lote ou qualquer outra tecnologia push disponível para sua organização.
- Arquivos de log

  O Windows cria um arquivo de log de desinstalação para cada instalador filho, para o usuário conectado em %temp%, os quais podem ser encontrados em C:\Users\<UserName>\AppData\Local\Temp.

  Se você decidir adicionar um arquivo de log distinto quando executar o instalador, verifique se o arquivo de log tem um nome único, pois os arquivos de log de instalador filho não são acrescidos. O comando padrão .msi pode ser usado para criar um arquivo de log usando /l C:\<any directory>\<any log file name>.log. A Dell não recomenda usar "/l*v" (registro em log detalhado) em uma desinstalação por linha de comando, pois o nome de usuário e a senha são gravados no arquivo de log.
- Todos os instaladores filho usam as mesmas opções de exibição e opções .msi básicas, exceto onde indicado, para desinstalações de linha de comando. As opções precisam ser especificadas antes. A opção /v é necessária e utiliza um argumento. Outros parâmetros vão dentro de um argumento que é passado para a opção /v.

  Opções de exibição podem ser especificadas no final do argumento passado para a opção /v para obter o comportamento esperado. Não use /q e /qn na mesma linha de comando. Use apenas ! e - depois de /qb.

| Opção | Significado |
|---|---|
| /v | Passa as variáveis para o .msi dentro de setup.exe |
| /s | Modo silencioso |
| /x | Modo Desinstalar |

| Opção | Significado |
|---|---|
| /q | Não há caixa de diálogo de andamento, reinicia-se após a conclusão do processo |
| /qb | Caixa de diálogo de andamento com o botão **Cancelar**, solicita a reinicialização |
| /qb- | Caixa de diálogo de andamento com o botão **Cancelar**, reinicia-se após a conclusão do processo |
| /qb! | Caixa de diálogo de andamento sem o botão **Cancelar**, solicita a reinicialização |
| /qb!- | Caixa de diálogo de andamento sem o botão **Cancelar**, reinicia-se após a conclusão do processo |
| /qn | Sem interface do usuário |

- Depois de extraído do instalador mestre, o instalador do Encryption Client pode ser encontrado em **C:\extracted\Encryption \DDPE_XXbit_setup.exe**.
- A tabela a seguir detalha os parâmetros disponíveis para a desinstalação.

| Parâmetro | Seleção |
|---|---|
| CMG_DECRYPT | Propriedade para selecionar o tipo de instalação do Encryption Removal Agent:<br>2 - Obter as chaves usando um pacote de chaves forenses<br>0 - Não instalar o Agente de remoção de criptografia |
| CMGSILENTMODE | Propriedade de desinstalação silenciosa:<br>1 - Silenciosa<br>0 - Não silenciosa |
| DA_KM_PW | A senha da conta do administrador de domínio. |
| DA_KM_PATH | O caminho para o pacote de materiais de chaves. |

- O exemplo a seguir desinstala o cliente Encryption sem instalar o Encryption Removal Agent.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=0 CMGSILENTMODE=1 DA_KM_PATH=C:\FullPathToLSA.exe
DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
```

- O exemplo a seguir desinstala o cliente Encryption usando um pacote de chaves forenses. Copie o pacote de chaves forenses no disco local e, em seguida, execute este comando.

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=2 CMGSILENTMODE=1 DA_KM_PATH=C:
\FullPathToForensicKeyBundle DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
```

Reinicie o computador ao terminar.

O processo de descriptografia pode levar várias horas, dependendo do número de unidades que estiverem sendo descriptografadas e da quantidade de dados dessas unidades. Para verificar o processo de descriptografia, consulte Verificar o status do Agente de remoção de criptografia.

# Desinstalar o Advanced Authentication

## Escolher um método de desinstalação

Há dois métodos para desinstalar o Encryption Client. Selecione **um** deles:

- Desinstalar usando a interface do usuário
- Desinstalar a partir da linha de comando

**Desinstalar usando a interface do usuário**

1. No painel de controle do Windows, acesse Desinstalar um programa (**Iniciar** > **Painel de controle** > **Programas e recursos** > **Desinstalar um programa.**).
2. Selecione **Security Tools Authentication** e clique com o botão esquerdo em **Alterar** para iniciar o Assistente de instalação.
3. Leia a tela de boas-vindas e clique em **Avançar**.
4. Digite a senha de administrador.
5. Siga os passos para desinstalar e clique em **Concluir**.
6. Reinicie o computador e faça login no Windows.

O Security Tools Authentication foi desinstalado.

**Desinstalar a partir da linha de comando**

- Depois de extraído do instalador mestre, o instalador do cliente do Advanced Authentication pode ser encontrado em C:\extracted \Security Tools\Authentication\<x64/x86>\setup.exe.
- O exemplo a seguir desinstala silenciosamente o cliente de autenticação avançada.

  ```
  setup.exe /x /s /v" /qn"
  ```

  Desligue e reinicie o computador ao terminar.

  Vá para Descrições de modelo e políticas.

# Desinstalar o Client Security Framework

## Escolher um método de desinstalação

Há dois métodos para desinstalar o Encryption Client. Selecione **um** deles:

- Desinstalar usando a interface do usuário
- Desinstalar a partir da linha de comando

**Desinstalar usando a interface do usuário**

1. No painel de controle do Windows, acesse Desinstalar um programa (**Iniciar** > **Painel de controle** > **Programas e recursos** > **Desinstalar um programa.**).
2. Selecione **Client Security Framework** e clique com o botão esquerdo em **Alterar** para iniciar o Assistente de instalação.
3. Leia a tela de boas-vindas e clique em **Avançar**.
4. Siga os passos para desinstalar e clique em **Concluir**.
5. Reinicie o computador e faça login no Windows.

Client Security Framework foi desinstalado.

**Desinstalar a partir da linha de comando**

- Depois de extraído do instalador mestre, o instalador do cliente do Client Security Framework pode ser encontrado em C:\extracted \Security Tools\EMAgent_.
- O exemplo a seguir desinstala silenciosamente o cliente SED.

  ```
  EMAgent_XXbit_setup.exe /x /s /v" /qn"
  ```

  Desligue e reinicie o computador ao terminar.

# Descrições de modelo e políticas

As dicas de contexto são mostradas quando você passa o mouse sobre uma política no Console de gerenciamento local.

## Políticas

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| Políticas de armazenamento fixo | | | | | | | | | | |
| Criptografia SDE ativada | Verdadeiro | | | | | | | | Falso | Esta política é a "política mestre" de todas as outras políticas de SDE. Se esta política estiver definida como Falsa, não haverá criptografia SDE, independentemente dos demais valores de política.<br><br>O valor Verdadeiro significa que todos os dados não criptografados por outras políticas de criptografia inteligentes serão criptografados de acordo com a política de Regras de criptografia SDE.<br><br>A alteração do valor desta política exige uma reinicialização. |
| SDE - Algoritmo de criptografia | AES256 | | | | | | | | | AES 256, AES 128, 3DES |
| SDE - Regras de criptografia | | | | | | | | | | Regras de criptografia usadas para criptografar/ descriptografar determinadas unidades, diretórios e pastas.<br><br>Se tiver dúvidas sobre a alteração dos valores padrão, entre em contato com o Dell ProSupport. |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| Políticas de configuração geral | | | | | | | | | | |
| Criptografia ativada | Verdadeiro | | | | | | | Falso | | Esta política é a " política mestra" de todas as outras políticas de Configuração geral. Um valor Falso significa que nenhuma criptografia ocorre, independentemente de outros valores de política.<br><br>O valor Verdadeiro significa que todas as políticas de criptografia estão ativadas.<br><br>A alteração do valor dessa política aciona uma nova varredura para criptografar/descriptografar arquivos. |
| Pastas comuns criptografadas | | | | | | | | | | String - máximo de 100 entradas de 500 caracteres cada (até um máximo de 2.048 caracteres)<br><br>Uma lista de pastas em unidades de ponto de extremidade que serão criptografadas ou excluídas da criptografia, que pode ser acessada por todos os usuários gerenciados que têm acesso ao ponto de extremidade.<br><br>As letras de unidades disponíveis são:<br><br>#: Refere-se a todas as unidades<br><br>f#: Refere-se a todas as unidades fixas<br><br>r#: Refere-se a todas as unidades removíveis<br><br>Importante: a substituição da proteção do diretório pode resultar em um computador que não inicializa e/ou necessitar de unidades de reformatação.<br><br>Se a mesma pasta for especificada nesta política e na política Pastas de usuário |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | criptografadas, esta política prevalecerá. |
| Algoritmo de criptografia comum | AES256 | | | | | | | | | AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES<br><br>Arquivos de paginação do sistema são criptografados usando AES 128. |
| Lista de criptografia de dados de aplicativos | winword.exe<br><br>excel.exe<br><br>powerpnt.exe<br><br>msaccess.exe<br><br>winproj.exe<br><br>outlook.exe<br><br>acrobat.exe<br><br>visio.exe<br><br>mspub.exe<br><br>notepad.exe<br><br>wordpad.exe<br><br>winzip.exe<br><br>winrar.exe<br><br>onenote.exe<br><br>onenotem.exe | | | | | | | | | String - máximo de 100 entradas de 500 caracteres cada<br><br>A Dell não recomenda adicionar explorer.exe ou iexplorer.exe à lista de criptografia de dados de aplicativos (ADE - Application Data Encryption), pois pode causar resultados inesperados ou não pretendidos. No entanto, explorer.exe é o processo usado para criar um novo arquivo Notepad na área de trabalho, usando o menu do botão direito do mouse. A configuração de criptografia pela extensão do arquivo, e não pela lista ADE, proporciona uma cobertura mais abrangente.<br><br>Faça uma lista com os nomes de aplicativos (sem caminhos) cujos arquivos novos você deseja criptografar, separados por retornos de carro. Não use curingas.<br><br>A Dell recomenda que a lista não inclua aplicativos/ instaladores que gravam arquivos essenciais do sistema. Isso pode resultar na criptografia de arquivos importantes do sistema, o que pode fazer com que o computador não consiga ser reinicializado.<br><br>Nomes de processo comuns:<br><br>outlook.exe, winword.exe, frontpg.exe, powerpnt.exe, |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | msaccess.exe, wordpad.exe, mspaint.exe, excel.exe<br><br>Os seguintes nomes de processos de sistema e instalador inseridos no código serão ignorados se especificados nesta política:<br><br>hotfix.exe, update.exe, setup.exe, msiexec.exe, wuauclt.exe, wmiprvse.exe, migrate.exe, unregmp2.exe, ikernel.exe, wssetup.exe, svchost.exe |
| Chave de ADE | Comum | | | | | | | | | Comum ou usuário<br><br>Escolha uma chave para indicar quem pode acessar arquivos criptografados pela lista de ADE e onde podem ser acessados.<br><br>Comum, se você quiser que esses arquivos sejam acessíveis a todos os usuários gerenciados no ponto de extremidade onde foram criados (o mesmo nível de acesso de Pastas criptografadas comuns) e criptografados com o algoritmo de criptografia comum.<br><br>Usuário, se você quiser que esses arquivos sejam acessíveis apenas ao usuário que os criou, apenas no ponto de extremidade onde foram criados (o mesmo nível de acesso de Pastas criptografadas do usuário) e criptografados com o algoritmo de criptografia do usuário.<br><br>Alterações a esta política não afetam os arquivos já criptografados devido a esta política. |
| Criptografar pastas | Verdadeiro | | | | | | | Falso | | Se Verdadeiro, criptografa pastas pessoais do Outlook. |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| pessoais do Outlook | | | | | | | | | | |
| Criptografar arquivos temporários | Verdadeiro | | | | | | | Falso | | Se Verdadeiro, criptografa os caminhos listados nas variáveis de ambiente TEMP e TMP, com a chave de criptografia de dados do usuário. |
| Criptografar arquivos temporários da Internet | Verdadeiro | Falso | | | | | | | | Se Verdadeiro, criptografa o caminho mostrado na lista da variável de ambiente CSIDL_INTERNET_CACHE com a chave de criptografia de dados do usuário.<br><br>Para reduzir o tempo de varredura da criptografia, o cliente limpa o conteúdo de CSIDL_INTERNET_CACHE para criptografia inicial, bem como as atualizações a esta política.<br><br>Esta política só é aplicável quando o Microsoft Internet Explorer é usado. |
| Criptografar documentos do perfil do usuário | Verdadeiro | | | | | | | | Falso | Se Verdadeiro, criptografa:<br><br>· O perfil de usuários (**C:\Users\jsmith**) com a chave de criptografia de dados do usuário<br><br>· \Users\Public com a chave de criptografia comum |
| Criptografar arquivo de paginação do Windows | Verdadeiro | | | | | | | | Falso | Se Verdadeiro, criptografa o arquivo de paginação do Windows. A alteração nesta política exige uma reinicialização. |
| Serviços gerenciados | | | | | | | | | | String - máximo de 100 entradas de 500 caracteres cada (até um máximo de 2.048 caracteres)<br><br>Quando um serviço é gerenciado por esta política, é iniciado apenas após o usuário estar conectado e o cliente estiver desbloqueado. Esta política também garante que o |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | serviço gerenciado por ela seja interrompido antes que o cliente seja bloqueado durante o logout. Além disso, esta política pode evitar que um usuário se desconecte caso o serviço não esteja respondendo.<br><br>A sintaxe é um nome de serviço por linha. Espaços no nome do serviço são suportados.<br><br>Curingas não são suportados<br><br>Serviços gerenciados não serão iniciados se um usuário não gerenciado fizer login. |
| Proteger limpeza pós-criptografia | Substituição do tipo three-pass | Substituição do tipo single-pass | | | | | | | Sem substituição | Sem substituição, Substituição do tipo single-pass, Substituição do tipo three-pass, Substituição do tipo seven-pass<br><br>Quando as pastas especificadas por outras políticas nesta categoria forem criptografadas, esta política determinará o que acontece com o resíduo não criptografado dos arquivos originais:<br><br>· A opção Sem substituição o apaga. Esse valor proporciona o processamento mais rápido da criptografia.<br><br>· A opção Substituição do tipo single-pass o substitui com dados aleatórios.<br><br>· A Substituição do tipo three-pass o substitui com um padrão normal de 1s e 0s, em seguida com seu complemento, e depois com dados aleatórios.<br><br>· A Substituição do tipo seven-pass o substitui com um padrão normal de 1s e 0s, em seguida com seu complemento, e depois com |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | dados aleatórios cinco vezes. Esse valor faz com que seja mais difícil recuperar arquivos originais da memória e produz o processamento de criptografia mais seguro. |
| Proteger arquivo de hibernação do Windows | Verdadeiro | | | | | Falso | | Verdadeiro | Falso | Quando ativado, o arquivo de hibernação será criptografado apenas quando o computador entrar em hibernação. O cliente liberará a proteção quando o computador sair da hibernação, oferecendo proteção sem afetar os usuários ou os aplicativos enquanto o computador estiver em uso. |
| Evitar hibernação não protegida | Verdadeiro | | | | | Falso | | Verdadeiro | Falso | Quando ativado, o cliente não permitirá a hibernação do computador se não conseguir criptografar os dados de hibernação. |
| Prioridade da verificação de estações de trabalho | Alto | Normal | | | | | | | | Mais alta, Alta, Normal, Baixa, Mais baixa<br><br>Especifica a prioridade relativa do Windows para varredura de pasta criptografada. |
| Pastas de usuário criptografadas | | | | | | | | | | String - máximo de 100 entradas de 500 caracteres cada (até um máximo de 2.048 caracteres)<br><br>Uma lista de pastas no disco rígido do ponto de extremidade a serem criptografadas com a Chave de Criptografia de dados do usuário ou excluídas da criptografia.<br><br>Esta política aplica-se a todas as unidades classificadas pelo Windows como discos rígidos. Você não pode usar essa política para criptografar unidades ou mídia externa cujo tipo é mostrado como disco removível. Em vez disso, use Criptografar mídia externa (EMS). |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| Algoritmo de criptografia do usuário | AES256 | | | | | | | | | AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES<br><br>Algoritmo de criptografia usado para criptografar dados no nível do usuário individual. Você pode especificar valores diferentes para diferentes usuários do mesmo ponto de extremidade. |
| Chave de criptografia de dados de usuário | Usuário | Comum | | Usuário | Comum | | | | Usuário | Comum ou usuário<br><br>Escolha uma chave para indicar quem, e onde, pode acessar arquivos criptografados pelas seguintes políticas:<br><br>· Pastas de usuário criptografadas<br><br>· Criptografar pastas pessoais do Outlook<br><br>· Criptografar arquivos temporários (somente \Documents and Settings \username\Local Settings \Temp)<br><br>· Criptografar arquivos temporários da Internet<br><br>· Criptografar documentos do perfil do usuário<br><br>Selecione:<br><br>· Comum, se você quiser que arquivos/pastas do usuário criptografados sejam acessíveis a todos os usuários gerenciados no ponto de extremidade onde foram criados (o mesmo nível de acesso de Pastas criptografadas do usuário) e que sejam criptografados com o algoritmo de criptografia comum.<br><br>· Usuário, se você quiser que esses arquivos sejam acessíveis apenas ao usuário que os criou, somente no |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | ponto de extremidade onde foram criados (o mesmo nível de acesso de Pastas criptografadas do usuário) e que sejam criptografados com o algoritmo de criptografia do usuário.<br><br>Se você optar por incorporar uma política de criptografia para criptografar partições inteiras do disco, recomenda-se usar a política de criptografia SDE padrão, em vez da Comum ou do Usuário. Isso garante que todos os arquivos criptografados do sistema operacional sejam acessíveis quando o usuário gerenciado não estiver conectado. |
| Hardware Crypto Accelerator (suportado apenas com clientes Encryption da versão v8.3 à v8.9.1) | | | | | | | | | | |
| Hardware Crypto Accelerator (HCA) | Falso | | | | | | | | | Esta é a "política mestre" de todas as outras políticas de aceleradores de criptografia por hardware (HCA - Hardware Crypto Accelerator). Se esta política estiver definida como Falso, não haverá criptografia do HCA, independentemente dos demais valores de política.<br><br>As políticas de HCA só podem ser usadas em computadores equipados com um acelerador de criptografia por hardware. |
| Volumes direcionados para criptografia | Todos os volumes fixos | | | | | | | | | Todos os volumes fixos ou apenas o volume do sistema<br><br>Especifica que volume(s) deverá(ão) ser criptografado(s). |
| Metadados forenses disponíveis na unidade criptografada HCA | Falso | | | | | | | | | Verdadeiro ou Falso<br><br>Quando Verdadeiro, metadados forenses são incluídos na unidade para |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | facilitar o laboratório forense. Metadados incluídos:<br>• ID de máquina (MCID) da máquina atual<br>• ID de dispositivo (DCID/SCID) da instalação do Shield atual<br><br>Quando Falso, os metadados forenses não são incluídos na unidade.<br><br>Alternar de Falso para Verdadeiro fará nova varredura com base nas políticas HCA para adicionar dados forenses. |
| Permitir aprovação do usuário para criptografia da unidade secundária | Falso | | | | | | | | | A opção Verdadeiro permite que os usuários decidam se unidades adicionais devem ser criptografadas. |
| Algoritmo de criptografia | AES256 | | | | | | | | | AES 256 ou AES 128 |
| Políticas de controle de portas | | | | | | | | | | |
| Sistema de controle de porta | Desativado | | | | | | | | | Habilitar ou desabilitar todas as políticas de sistema de controle de portas (PCS — Port Control System). Se esta política estiver definida como Desabilitar, nenhuma política de PCS será aplicada, independentemente de outras políticas de sistema de controle de portas.<br><br>**Nota:** as políticas de PCS exigem uma reinicialização para que a política tenha efeito. |
| Porta: slot para Express Card | Ativado | | | | | | | | | Habilitar, desabilitar ou ignorar portas expostas por meio do slot para Express Card. |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| Porta: eSATA | Ativado | | | | | | | | | Habilitar, desabilitar ou ignorar o acesso da porta a portas SATA externas. |
| Porta: PCMCIA | Ativado | | | | | | | | | Habilitar, desabilitar ou ignorar o acesso da porta a portas PCMCIA. |
| Porta: Firewire (1394) | Ativado | | | | | | | | | Habilitar, desabilitar ou ignorar o acesso da porta a portas Firewire (1394) externas. |
| Porta: SD | Ativado | | | | | | | | | Habilitar, desabilitar ou ignorar o acesso da portas a portas do cartão SD. |
| Subclasse de armazenamento: controle da unidade externa | Bloqueado | Somente leitura | | | Acesso completo | | | Somente leitura | Acesso completo | FILHO da Classe: armazenamento. Classe: o armazenamento precisa estar Ativado para usar esta política.<br><br>Essa política tem interações com PCS. Consulte Interações de EMS e PCS.<br><br>Acesso completo: a porta da unidade externa não tem restrições de dados de leitura/gravação aplicadas<br><br>Somente leitura: permite o recurso de leitura. Gravação de dados está desativada<br><br>Bloqueado: é porta é bloqueada para leitura/gravação<br><br>Essa política é baseada em ponto de extremidade e não pode ser substituída por uma política de usuário. |
| Porta: dispositivo de transferência de memória (MTD) | Ativado | | | | | | | | | Habilitar, desabilitar ou ignorar o acesso às portas do Dispositivo de transferência de memória (MTD — Memory Transfer Device). |
| Classe: armazenamento | Ativado | | | | | | | | | PAI para as próximas 3 políticas. Ative esta política para usar as três seguintes políticas de armazenamento |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | de subclasse. A desativação desta política desativa as três políticas de armazenamento de subclasse, independentemente de seus valores. |
| Subclasse de armazenamento: controle da unidade ótica | Somente leitura | UDF somente | | | | Acesso completo | UDF somente | Acesso completo | | FILHO da Classe: armazenamento. Classe: o armazenamento precisa estar Ativado para usar esta política.<br><br>Acesso completo: a porta da unidade óptica não tem restrições de dados de leitura/gravação aplicadas<br><br>UDF somente: bloqueia todas as gravações de dados que não estejam no formato UDF (gravação de CD/DVD e ISO). Leitura de dados está ativada.<br><br>Somente leitura: permite o recurso de leitura. Gravação de dados está desativada<br><br>Bloqueado: é porta é bloqueada para leitura/gravação<br><br>Essa política é baseada em ponto de extremidade e não pode ser substituída por uma política de usuário.<br><br>Universal Disk Format (UDF — Formato de disco universal) é uma implementação da especificação conhecida como ISO/IEC 13346 e ECMA-167. É um sistema de arquivos neutro, aberto a fornecedores, para armazenamento de dados de computador em uma ampla variedade de mídia.<br><br>Essa política tem interações com PCS. Consulte Interações de EMS e PCS. |
| Subclasse de armazenamento: controle da | Bloqueado | Somente leitura | | | | Acesso completo | Somente leitura | Acesso completo | | FILHO da Classe: armazenamento. Classe: o armazenamento precisa estar Ativado para usar esta política. |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| unidade de disquete | | | | | | | | | | Acesso completo: a porta da unidade de disco não tem restrições de dados de leitura/gravação aplicadas<br><br>Somente leitura: permite o recurso de leitura. Gravação de dados está desativada<br><br>Bloqueado: é porta é bloqueada para leitura/gravação<br><br>Essa política é baseada em ponto de extremidade e não pode ser substituída por uma política de usuário. |
| Classe: dispositivo portátil do Windows | Ativado | | | | | | | | | PAI para a próxima política. Ative esta política para ativar o dispositivo portátil de subclasse do Windows : política de armazenamento. A desativação desta política desativa o dispositivo portátil de subclasse do Windows : política de armazenamento, independentemente de seu valor.<br><br>Controla o acesso a todos os WPDs. |
| Dispositivo portátil de subclasse do Windows : armazenamento | Ativado | | | | | | | | | FILHO da Classe: dispositivo portátil do Windows<br><br>Classe: o dispositivo portátil do Windows precisa estar Ativado para usar esta política.<br><br>Acesso completo: a porta não tem restrições de dados de leitura/gravação aplicadas.<br><br>Somente leitura: permite o recurso de leitura. Os dados de gravação são desativados.<br><br>Bloqueado: a porta é bloqueada para leitura/gravação. |
| Classe: dispositivo de interface humana | Ativado | | | | | | | | | Controle o acesso a todos os HID (teclado e mouse). |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | **Nota:** o bloqueio no nível da porta USB e o bloqueio no nível da classe de dispositivos de interface humana (HID - Human Interface Device) serão processados apenas se o tipo de chassi do computador puder ser identificado como um formato de laptop ou de notebook. O BIOS do computador é usado para a identificação do chassi. |
| Classe: outra | Ativado | | | | | | | | | Controla o acesso a todos os dispositivos não cobertos por outras classes. |
| Políticas de armazenamento removível | | | | | | | | | | |
| Criptografar mídia externa (EMS) | Verdadeiro | | | | | Falso | | Verdadeiro | Falso | Esta política é a "política mestra" de todas as outras políticas de Armazenamento removível. O valor Falso significa que não há criptografia de armazenamento removível, independentemente de outros valores de política.<br><br>O valor Verdadeiro significa que todas as políticas de criptografia de Armazenamento removível estão ativadas.<br><br>Essa política tem interações com PCS. Consulte Interações de EMS e PCS. |
| Excluir criptografia de CD/DVD (EMS) | Falso | | | | | | | | Verdadeiro | Se Falso, criptografa dispositivos de CD/DVD.<br><br>Essa política tem interações com PCS. Consulte Interações de EMS e PCS. |
| EMS - Acesso a mídia não protegida | Bloquear | | Somente leitura | | | Acesso completo | | Somente leitura | Acesso completo | Bloqueado, Somente leitura, Acesso completo<br><br>Essa política tem interações com PCS. Consulte Interações de EMS e PCS.<br><br>Quando esta política está definida para Bloquear o |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | acesso, você não tem acesso ao armazenamento removível, a menos que ele seja criptografado.<br><br>A escolha de Somente leitura ou Acesso completo permite que você decida qual armazenamento removível criptografar.<br><br>Se você optar por não criptografar o armazenamento removível e esta política estiver definida como acesso completo, você terá pleno acesso de leitura/gravação ao armazenamento removível.<br><br>Se você optar por não criptografar o armazenamento removível e essa política for definida como Somente leitura, não será possível ler ou apagar os arquivos no armazenamento removível não criptografado, mas o cliente não permitirá que os arquivos sejam editados ou adicionados ao armazenamento removível a menos que seja criptografado. |
| EMS - Algoritmo de criptografia | AES256 | | | | | | | | | AES 256, Rijndael 256, AES 128, Rijndael 128, 3DES |
| EMS - Fazer varredura da mídia externa | Verdadeiro | Falso | | | | | | | | Se Verdadeiro, permite que o EMS faça varredura no armazenamento removível cada vez que ele for inserido.<br><br>Quando esta política está como Falso e a política Criptografar mídia externa (EMS) está como Verdadeiro, o EMS só criptografa arquivos novos e alterados.<br><br>Uma varredura ocorre em cada inserção, para que o EMS possa captar qualquer arquivo adicionado ao armazenamento removível sem autenticação. Você pode adicionar arquivos |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | ao armazenamento removível caso decida não autenticar, mas não pode acessar os dados criptografados. Os arquivos adicionados não serão criptografados neste caso. Assim, na próxima vez que você autenticar a mídia removível para trabalhar com dados criptografados, o EMS irá verificar e criptografar todos os arquivos que possam ter sido adicionados sem criptografia. |
| EMS - Acessar dados criptografados em dispositivo não protegido | Verdadeiro | | | | | | | | | Se Verdadeiro, permite que o usuário acesse dados criptografados no armazenamento removível, independentemente de o ponto de extremidade estar criptografado ou não. |
| Lista de dispositivos do EMS permitidos | | | | | | | | | | Esta política permite a especificação dos dispositivos de mídia externos que devem ser excluídos da criptografia do EMS. Todos os dispositivos de mídia externos que não estiverem nesta lista serão protegidos. Máximo de 150 dispositivos com até 500 caracteres por PNPDeviceID. Máximo permitido de 2048 caracteres no total.<br><br>Para localizar o PNPDeviceID do armazenamento removível:<br><br>1 Insira o dispositivo de armazenamento removível em um computador com Shield.<br>2 Abra o EMSService.log em C:\Programdata\Dell\Dell Data Protection\Encryption\EMS.<br>3 Localize "PNPDeviceID="<br><br>Por exemplo: 14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDeviceID = USBSTOR\DISK&VEN_SEAGATE& |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | PROD_USB&REV_0409\2HC015KJ&0<br><br>Especifique o seguinte na política Lista de dispositivos do EMS permitidos:<br><br>VEN=Fornecedor (exemplo: USBSTOR \DISK&VEN_SEAGATE)<br><br>PROD=Nome do produto/do modelo (exemplo: &PROD_USB); também exclui da criptografia do EMS todas as unidades USB do Seagate; um valor VEN (exemplo: USBSTOR \DISK&VEN_SEAGATE) deve preceder esse valor<br><br>REV=Revisão do firmware (exemplo: &REV_0409); também exclui o modelo específico que está sendo usado; os valores VEN e PROD devem preceder esse valor<br><br>Número de série (exemplo: \2HC015KJ&0); exclui apenas este dispositivo; os valores VEN, PROD e REV devem preceder esse valor<br><br>Delimitadores permitidos: tabulações, vírgulas, ponto e vírgula, caractere hexadecimal 0x1E (caractere separador de registros) |
| EMS - Caracteres alfanuméricos obrigatórios na senha | Verdadeiro | | | | | | | | | Se Verdadeiro, exige uma ou mais letras na senha. |
| EMS - Caracteres maiúsculos e minúsculos obrigatórios na senha | Verdadeiro | Falso | | | | | | | | Se Verdadeiro, exige pelo menos uma letra maiúscula e uma letra minúscula na senha. |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| EMS - Número de caracteres obrigatórios na senha | 8 | | | | | 6 | | 8 | | 1-40 caracteres<br><br>Número mínimo de caracteres obrigatórios na senha. |
| EMS - Caracteres numéricos obrigatórios na senha | Verdadeiro | Falso | | | | | | | | Se Verdadeiro, exige um ou mais caracteres numéricos na senha. |
| EMS - Tentativas permitidas de senha | 2 | 3 | | | | 4 | | 3 | | 1-10<br><br>Número de vezes que o usuário pode tentar digitar a senha correta. |
| EMS - Caracteres especiais obrigatórios na senha | Verdadeiro | Falso | | | | | | | Verdadeiro | Se Verdadeiro, exige um ou mais caracteres especiais na senha. |
| EMS - Período de espera | 30 | | | | | | | | | 0-5000 segundos<br><br>Número de segundos que o usuário precisa esperar entre a primeira e a segunda rodada de tentativas de digitação do código de acesso. |
| EMS - Incremento no período de espera | 30 | 20 | | | | 10 | 30 | 10 | | 0-5000 segundos<br><br>Tempo incremental a adicionar ao período de espera anterior, após cada rodada malsucedida de tentativas de digitação do código de acesso. |
| EMS - Regras de criptografia | | | | | | | | | | Regras de criptografia para criptografar/não criptografar determinadas unidades, diretórios e pastas.<br><br>É permitido um total de 2.048 caracteres. Os caracteres "Espaço" e "Enter" usados para inclusão de linhas são contados como caracteres usados. Todas as regras que excederem o limite de 2.048 caracteres serão ignoradas. |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | Dispositivos de armazenamento que incorporam conexões multi-interface, como Firewire, USB, eSATA etc. podem exigir o uso de EMS e de regras de codificação para codificar o dispositivo. Isso é necessário em razão das diferenças na forma em que o sistema operacional Windows lida com dispositivos de armazenamento com base no tipo de interface. Consulte Como criptografar um iPod com o EMS. |
| EMS - Bloquear acesso a mídia que não pode ser protegida | Verdadeiro | | | | | | | | Falso | Bloqueie o acesso a qualquer armazenamento removível menor que 17 MB e que, portanto, não tem capacidade de armazenamento insuficiente para hospedar blindagem de mídia removível (como um disquete de 1,44 MB).<br><br>Todo o acesso será bloqueado se Criptografar mídia externa e esta política tiverem o valor Verdadeiro. Se Criptografar mídia externa for Verdadeiro, mas essa política for Falso, os dados poderão ser lidos do armazenamento removível não criptografável, mas o acesso de gravação à mídia será bloqueado.<br><br>Se Criptografar mídia externa for Falso, esta política não terá nenhum efeito e o acesso ao armazenamento removível não criptografável não será afetado. |
| Políticas de controle de experiência do usuário | | | | | | | | | | |
| Forçar reinicialização após atualização | Verdadeiro | | | | | | | | Falso | Ao configurar o valor como Verdadeiro, o computador é reinicializado imediatamente para permitir o processamento da criptografia ou de atualizações relacionadas à política baseada em |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | dispositivo, como System Data Encryption (SDE). |
| Duração de cada atraso para reinicialização | 5 | 10 | | | | 20 | | 15 | | O número de minutos de atraso quando o usuário escolhe adiar a reinicialização da política baseada em dispositivo. |
| Número de atrasos permitidos para reinicialização | 1 | | | | | 5 | | 3 | | O número de vezes que o usuário poderá adiar a reinicialização da política baseada em dispositivo. |
| Suprimir aviso de retenção de arquivo | Falso | | | | | | | | | Esta política controla se o usuário vê pop-ups de notificação se um aplicativo tentar acessar um arquivo enquanto o cliente o estiver processando. |
| Mostrar controle de processamento de criptografia local | Falso | | Verdadeiro | | | | | Falso | | Ao configurar o valor como Verdadeiro, o usuário verá uma opção de menu no ícone de bandeja do sistema que permite que ele pause/reinicie a criptografia/descriptografia (dependendo do que o Shield estiver fazendo no momento).<br>**NOTA: Autorizar um usuário a pausar a criptografia pode permitir que ele impeça o Shield de criptografar ou descriptografar totalmente os dados de acordo com a política.** |
| Permitir a criptografia apenas quando a tela estiver bloqueada | Falso | | Opcional do usuário | | | | | Falso | | Verdadeiro, Falso, Opcional do usuário<br><br>Quando Verdadeiro, não haverá nenhuma criptografia ou descriptografia de dados enquanto o usuário estiver trabalhando ativamente. O cliente só processará dados quando a tela estiver bloqueada. |

| Política | Alta proteção para todas as unidades fixas e externas | Norma PCI | Norma sobre violação de dados | Norma HIPAA | Proteção básica para todas as unidades fixas e externas (padrão) | Proteção básica para todas as unidades fixas | Proteção básica apenas para a unidade do sistema | Proteção básica para unidades externas | Criptografia desativada | Descrição |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | Opcional do usuário adiciona uma opção no ícone da bandeja do sistema que permite ao usuário ativar ou desativar esse recurso.<br><br>Quando Falso, o processamento da criptografia ocorrerá a qualquer momento, mesmo quando o usuário estiver trabalhando.<br><br>A ativação dessa opção prolongará consideravelmente o tempo necessário para concluir a criptografia ou descriptografia. |

# Descrições de modelos

## Alta proteção para todas as unidades fixas e externas

Esse modelo de política foi criado para as organizações que têm como objetivo principal reforçar a segurança e evitar riscos em toda a empresa. É melhor usada quando a segurança é muito mais importante do que a facilidade de uso, e a necessidade de exceções com políticas menos seguras para certos usuários, grupos ou dispositivos é mínima.

Este modelo de política:

- é uma configuração altamente restrita, que proporciona ainda mais proteção.
- oferece proteção à unidade do sistema e a todas as unidades fixas.
- criptografa todos os dados de dispositivos de armazenamento removíveis e evita o uso de dispositivos de armazenamento removíveis não criptografados.
- oferece controle de unidade óptica somente para leitura.

## Norma PCI direcionada

O Padrão PCI de Segurança de Dados (PCI DSS - Payment Card Industry Data Security Standard) é um padrão multiuso que inclui requisitos de gerenciamento de segurança, políticas, procedimentos, arquitetura de rede, projeto de software e outras importantes medidas de proteção. Esse padrão abrangente tem como objetivo definir as diretrizes para que as organizações protejam de forma proativa os dados das contas dos clientes.

Este modelo de política:

- oferece proteção à unidade do sistema e a todas as unidades fixas.
- solicita aos usuários que criptografem os dispositivos de armazenamento removíveis.
- possibilita a gravação de CD/DVDs apenas UDF. A configuração do controle de porta permite acesso de leitura a todas as unidades ópticas.

# Direcionada à Norma sobre violação de dados

A lei Sarbanes-Oxley exige controle adequado das informações financeiras. Como muitas dessas informações residem em formato eletrônico, a criptografia é o ponto de controle principal quando esses dados são armazenados ou transferidos. As diretrizes da lei Gramm-Leach-Bliley (GLB) (também conhecida como Lei de Modernização dos Serviços Financeiros) não exigem criptografia. Entretanto, o Conselho de Investigação Federal de Instituições Financeiras (FFIEC) faz a seguinte recomendação: "As instituições financeiras devem implantar a criptografia a fim de reduzir o risco de divulgação ou alteração de informações confidenciais armazenadas ou transmitidas". O projeto de lei 1386 do senado da Califórnia (California's Database Security Breach Notification Act) tem como objetivo proteger os cidadãos da Califórnia contra roubo de identidade exigindo que as organizações que tiveram sua segurança computacional violada notifiquem todos os indivíduos afetados. A única forma de uma organização evitar notificar os clientes é provar que todas as informações pessoais foram criptografadas antes da violação do sistema de segurança.

Este modelo de política:

- oferece proteção à unidade do sistema e a todas as unidades fixas.
- solicita aos usuários que criptografem os dispositivos de armazenamento removíveis.
- possibilita a gravação de CD/DVDs apenas UDF. A configuração do controle de porta permite acesso de leitura a todas as unidades ópticas.

# Direcionada à Norma HIPAA

A Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) exige que as organizações de saúde implantem um número de proteções técnicas a fim de garantir a confidencialidade e a integridade de todas as informações individuais identificáveis relacionadas à saúde.

Este modelo de política:

- oferece proteção à unidade do sistema e a todas as unidades fixas.
- solicita aos usuários que criptografem os dispositivos de armazenamento removíveis.
- possibilita a gravação de CD/DVDs apenas UDF. A configuração do controle de porta permite acesso de leitura a todas as unidades ópticas.

# Proteção básica para todas as unidades fixas e externas (padrão)

Esse modelo de política oferece a configuração recomendada, que proporciona alto nível de proteção sem causar impactos significativos na facilidade de uso do sistema.

Este modelo de política:

- oferece proteção à unidade do sistema e a todas as unidades fixas.
- solicita aos usuários que criptografem os dispositivos de armazenamento removíveis.
- possibilita a gravação de CD/DVDs apenas UDF. A configuração do controle de porta permite acesso de leitura a todas as unidades ópticas.

# Proteção básica para todas as unidades fixas

Este modelo de política:

- oferece proteção à unidade do sistema e a todas as unidades fixas.

- possibilita a gravação de CD/DVDs em qualquer formato suportado. A configuração do controle de porta permite acesso de leitura a todas as unidades ópticas.

  Esse modelo de política não:

- fornece criptografia para dispositivos de armazenamento removíveis.

# Proteção básica apenas para a unidade do sistema

Este modelo de política:

- fornece proteção para a unidade do sistema, geralmente a unidade C:, onde o sistema operacional é carregado.
- possibilita a gravação de CD/DVDs em qualquer formato suportado. A configuração do controle de porta permite acesso de leitura a todas as unidades ópticas.

  Esse modelo de política não:

- fornece criptografia para dispositivos de armazenamento removíveis.

# Proteção básica para unidades externas

Este modelo de política:

- fornece proteção para os dispositivos de armazenamento removíveis.
- possibilita a gravação de CD/DVDs apenas UDF. A configuração do controle de porta permite acesso de leitura a todas as unidades ópticas.

  Esse modelo de política não:

- fornece proteção à unidade do sistema (geralmente a unidade C:, onde o sistema operacional é carregado) ou a outras unidades fixas.

# Criptografia desativada

Esse modelo de política não oferece proteção por criptografia. Ao usar esse modelo, tome medidas adicionais para proteger seus dispositivos contra perda e roubo.

Esse modelo é útil para organizações que preferem iniciar sem nenhuma criptografia ativa durante a transição para segurança. Assim que a organização se adaptar à implantação, a criptografia pode ser moderadamente ativada por meio do ajuste de políticas individuais ou da aplicação de modelos mais sólidos para toda ou parte da organização.

Vá para Configuração de pré-instalação para Senha de uso único.

10

# Configuração de pré-instalação para Senha de uso único

Esses recursos do Personal Edition precisam ser configurados **antes** de começar a instalação.

## Inicializar o TPM

- É preciso ser membro do grupo de administradores locais ou ter função equivalente.
- O computador precisa estar equipado com BIOS e módulo TPM compatíveis.

Essa tarefa é necessária se você estiver usando uma senha de uso único (OTP).

- Siga as instruções disponíveis em http://technet.microsoft.com/en-us/library/cc753140.aspx.

# Extrair os instaladores filhos do instalador mestre

- Para instalar cada cliente individualmente, extraia os arquivos executáveis filhos do instalador.
- Se o instalador mestre tiver sido usado na instalação, os clientes precisam ser desinstalados individualmente. Use esse processo para extrair os clientes do instalador mestre para que eles possam ser usados para desinstalação.

1 Na mídia de instalação Dell, copie o arquivo`DDPSetup.exe` para o computador local.

2 Abra um prompt de comando no mesmo local do arquivo`DDPSetup.exe` e digite:

```
DDPSetup.exe /z"\"EXTRACT_INSTALLERS=C:\extracted\""
```

O caminho de extração não pode ter mais de 63 caracteres.

Antes de começar a instalação, certifique-se de que todos os pré-requisitos foram atendidos e que todos os softwares necessários foram instalados para cada instalador filho que você planeja instalar. Consulte Requisitos para obter detalhes.

Os instaladores filhos extraídos estão localizados em **C:\extracted\.**

Vá para Solução de problemas.

# Solução de problemas

**Fazer upgrade para a Atualização de Aniversário do Windows 10**

Os computadores instalados com o Encryption devem usar um pacote de atualização do Windows 10 especialmente configurado para atualizar para a Atualização de Aniversário do Windows 10. A versão configurada do pacote de upgrade garante que o Dell Data Protection possa gerenciar o acesso aos seus arquivos criptografados para não serem danificados durante o processo de upgrade.

Para fazer o upgrade para a versão de Aniversário do Windows 10, siga as instruções no seguinte artigo:

http://www.dell.com/support/article/us/en/19/SLN298382

# Solução de problemas do cliente Encryption

## Upgrade para a Atualização de Aniversário do Windows 10

Para fazer o upgrade para a versão Atualização de Aniversário do Windows 10, siga as instruções no seguinte artigo: http://www.dell.com/support/article/us/en/19/SLN298382.

## (Opcional) Criar um arquivo de log do Agente de remoção de criptografia

- Antes de iniciar o processo de desinstalação, você terá a opção de criar um arquivo de log do Agente de remoção de criptografia. Este arquivo de log é útil para solucionar problemas de uma operação de desinstalação/descriptografia. Se você não pretende descriptografar arquivos durante o processo de desinstalação, não é necessário criar esse arquivo de log.
- O arquivo de log do Agente de remoção de criptografia não será criado até que o serviço Agente de remoção de criptografia seja concluído, o que não acontece até o computador ser reiniciado. Quando o cliente tiver sido desinstalado com êxito e o computador estiver totalmente descriptografado, o arquivo de log será apagado permanentemente.
- O caminho do arquivo de log é **C:\ProgramData\Dell\Dell Data Protection\Encryption.**
- Crie a seguinte entrada de registro no computador que você pretende descriptografar.

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=dword:2

  0: nenhum registro em log

  1: registra os erros que impedem a execução do Serviço

  2: registra os erros que impedem a descriptografia de dados completa (nível recomendado)

  3: registra as informações sobre todos os volumes e arquivos de descriptografia

  5: registra as informações de depuração

# Localizar a versão do TSS

- O TSS é um componente que faz interface com o TPM. Para localizar a versão do TSS, acesse (local padrão) **C:\Program Files\Dell \Dell Data Protection\Drivers\TSS\bin > tcsd_win32.exe**. Clique com o botão direito no arquivo e selecione **Propriedades**. Verifique a versão do arquivo na guia **Detalhes**.

# Interações de EMS e PCS

**Para garantir que a mídia não está como somente leitura e a porta não está bloqueada**

A política EMS - Acesso a mídia não protegida interage com a política Sistema de controle de portas - Classe de armazenamento: Controle de unidade externa. Se você pretende definir a política EMS - Acesso a mídia não protegida como *Acesso completo*, verifique se a política Classe de armazenamento: Controle de unidade externa também está definida como *Acesso completo*, para garantir que a mídia não esteja definida para somente leitura e que a porta não esteja bloqueada.

**Para criptografar dados gravados em CD/DVD:**

- Defina Criptografar mídia externa (EMS) = Verdadeiro.
- Defina Excluir criptografia de CD/DVD (EMS) = Falso.
- Definir Subclasse de armazenamento: Controle de unidade óptica = UDF somente.

# Usar WSScan

- O WSScan permite que você garanta que todos os dados sejam descriptografados ao desinstalar o cliente Encryption, bem como visualizar o status de criptografia e identificar arquivos não criptografados que devem ser criptografados.
- Privilégios do administrador são necessários para executar este utilitário.

**Execute o WSScan**

1 Copie o WSScan.exe da mídia de instalação Dell para o computador Windows a ser verificado.

2 Inicie uma linha de comando no local acima e digite **wsscan.exe** no prompt de comando. O WSScan é aberto.

3 Clique em **Avançado**.

4 Selecione o tipo de unidade a ser analisada no menu suspenso: *Todas as unidades*, *Unidades fixas*, *Unidades removíveis* ou *CDROM/ DVDROM*.

5 Selecione o tipo de relatório de criptografia desejado no menu suspenso: *Arquivos criptografados*, *Arquivos não criptografados*, *Todos os arquivos* ou *Arquivos não criptografados em violação*:

- *Arquivos criptografados* - Para garantir que todos os dados sejam descriptografados ao desinstalar o cliente Encryption. Siga seu processo existente para descriptografar dados, como emitir uma atualização de política de descriptografia. Após descriptografar os dados, mas antes de fazer uma reinicialização, execute o WSScan para garantir que todos os dados sejam descriptografados.
- *Arquivos não criptografados* - Para identificar os arquivos não criptografados, com uma indicação se os arquivos devem ser criptografados (S/N).
- *Todos os arquivos* - Para mostrar uma lista de todos os arquivos criptografados e não criptografados, com a indicação se os arquivos devem ser criptografados (S/N).
- *Arquivos não criptografados em violação* - Para identificar os arquivos não criptografados que devem ser criptografados.

6 Clique em **Pesquisar**.

OU

1 Clique em **Avançado** para alternar a exibição para **Simples** para verificar uma pasta específica.

2 Acesse Configurações de varredura e digite o caminho da pasta no campo **Caminho de pesquisa**. Se este campo for usado, a seleção na caixa suspensa será ignorada.

3 Se você não quiser gravar a saída de WSScan em um arquivo, desmarque a caixa de seleção **Saída para arquivo**.

4 Se quiser, altere o caminho padrão e o nome do arquivo em *Caminho*.

5 Selecione **Adicionar a arquivo existente** se você não deseja substituir nenhum arquivo de saída WSScan existente.

6 Escolha o formato de saída:

- Selecione Formato de relatório para obter uma lista de estilo de relatório de saída verificada. Este é o formato padrão.
- Selecione "Arquivo delimitado por valor" para gerar um arquivo que pode ser importado para um aplicativo de planilha. O delimitador padrão é "|", embora ele possa ser alterado para até 9 caracteres alfanuméricos, de espaço ou pontuação.
- Selecione a opção 'Valores entre aspas' para incluir cada valor entre aspas duplas.
- Selecione 'Arquivo de largura fixa' para gerar um arquivo não delimitado que contenha uma linha contínua de informações de comprimento fixo sobre cada arquivo criptografado.

7 Clique em **Pesquisar**.

Clique em **Parar pesquisa** para parar sua pesquisa. Clique em **Clear** (Apagar) para apagar as mensagens mostradas.

**Saída de WSScan**

As informações de WSScan sobre arquivos criptografados contêm as seguintes informações.

Exemplo de saída:

[2015-07-28 07:52:33] SysData.07vdlxrsb._SDENCR_: "c:\temp\Dell - test.log" ainda é criptografado em AES256

| Saída | Significado |
|---|---|
| Marca de data/hora | A data e hora em que o arquivo foi verificado. |
| Tipo de criptografia | O tipo de criptografia usada para criptografar o arquivo.<br><br>**SysData:** chave de criptografia do SDE.<br><br>**Usuário:** chave de criptografia do usuário.<br><br>**Comum:** chave de criptografia comum.<br><br>O WSScan não mostra arquivos que foram criptografados com o recurso Criptografar para compartilhamento. |
| KCID | A identificação do computador-chave.<br><br>Como mostrado no exemplo acima, "**7vdlxrsb**"<br><br>Se você estiver verificando uma unidade de rede mapeada, o relatório de verificação não retornará um KCID. |
| UCID | O ID do usuário.<br><br>Como mostrado no exemplo acima, "**_SDENCR_**"<br><br>O UCID é compartilhado por todos os usuários do computador. |
| Arquivo | O caminho do arquivo criptografado.<br><br>Como mostrado no exemplo acima, "**c:\temp\Dell - test.log**" |
| Algoritmo | O algoritmo de criptografia que está sendo usado para criptografar o arquivo.<br><br>Como mostrado no exemplo acima, "**ainda é criptografado em AES256**"<br><br>Rijndael 128<br><br>Rijndael 256 |

| Saída | Significado |
|---|---|
| | AES 128 |
| | AES 256 |
| | 3DES |

# Verificar o status do agente de remoção de criptografia

O Agente de remoção de criptografia mostra o status na área de descrição do painel Serviços (Iniciar > Executar... > services.msc > OK) da seguinte maneira. Atualize periodicamente o Serviço (realce o Serviço > clique com o botão direito > Atualizar) para atualizar seu status.

- **Aguardando a desativação de SDE** – O cliente Encryption ainda está instalado, ainda está configurado, ou ambos. A descriptografia não iniciará até o cliente Encryption ser desinstalado.
- **Varredura inicial** – o serviço está realizando uma varredura inicial, calculando o número de arquivos e bytes criptografados. A varredura inicial ocorre uma vez.
- **Varredura de descriptografia** – o serviço está descriptografando arquivos e possivelmente solicitando a descriptografia de arquivos bloqueados.
- **Descriptografar na reinicialização (parcial)** – a varredura de descriptografia está concluída e alguns arquivos bloqueados (mas não todos) precisam ser descriptografados na próxima reinicialização.
- **Descriptografar na reinicialização** – a varredura de descriptografia está concluída e todos os arquivos bloqueados precisam ser descriptografados na próxima reinicialização.
- **Não foi possível descriptografar todos os arquivos** – a varredura de descriptografia está concluída, mas não foi possível descriptografar todos os arquivos. Esse status significa que uma das seguintes situações ocorreu:
  - Não foi possível agendar os arquivos bloqueados para descriptografia porque eles eram muito grandes ou ocorreu um erro durante a solicitação para desbloqueá-los.
  - Ocorreu um erro de entrada/saída durante a descriptografia de arquivos.
  - Não foi possível descriptografar os arquivos por política.
  - Os arquivos estão marcados como se devessem ser criptografados.
  - Ocorreu um erro durante a varredura de descriptografia.
  - Em todos os casos, um arquivo de log é criado (se o registro em log estiver configurado) quando LogVerbosity=2 (ou superior) é definido. Para solucionar o problema, defina o detalhamento do log como 2 e reinicie o serviço Agente de remoção de criptografia para forçar outra varredura de descriptografia.
- **Concluída** – A varredura de descriptografia está concluída. O Serviço, o executável, o driver e o executável do driver ficam agendados para serem apagados na próxima reinicialização.

# Como criptografar um iPod com o EMS

Essas regras desativam ou ativam a criptografia para essas pastas e tipos de arquivos em todos os dispositivos removíveis - não apenas no iPod. Tenha cuidado ao definir regras.

- Não recomendamos o uso do iPod Shuffle, pois podem ocorrer resultados inesperados.
- À medida que os iPods mudam, essas informações também podem mudar, por isso recomenda-se cautela ao permitir o uso de iPods em computadores habilitados com EMS.
- Como os nomes das pastas nos iPods dependem do modelo do iPod, recomendamos criar uma política de exclusão que abranja todos os nomes de pasta, em todos os modelos de iPod.
- Para garantir que a criptografia de um iPod via EMS não torne o dispositivo inutilizável, digite as seguintes regras na política Regras de criptografia de EMS:

  -R#:\Calendars

  -R#:\Contacts

-R#:\iPod_Control

-R#:\Notes

-R#:\Photos

- Você também pode forçar a criptografia de tipos específicos de arquivos nos diretórios acima. A adição das seguintes regras assegura que arquivos ppt, pptx, doc, docx, xls e xlsx sejam criptografados nos diretórios *excluídos* da criptografia pelas regras anteriores:

  ^R#:\Calendars;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Contacts;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\iPod_Control;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Notes;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Photos;ppt.doc.xls.pptx.docx.xlsx

- A substituição dessas cinco regras pela seguinte regra forçará a criptografia de arquivos ppt, pptx, doc, docx, xls e xlsx em qualquer diretório do iPod, incluindo Calendários, Contatos iPod_Control, Notas e Fotos.

  ^R#:\;ppt.doc.xls.pptx.docx.xlsx

- As regras foram testadas nos seguintes iPods:

  - iPod Video 30 GB quinta geração

  - iPod Nano 2 GB segunda geração

  - iPod Nano 4 GB segunda geração

# Drivers Dell ControlVault

## Atualização dos drivers e firmware Dell ControlVault

- Os drivers e firmware Dell ControlVault instalados de fábrica nos computadores Dell estão desatualizados e precisam ser atualizados. Siga o procedimento adiante e na ordem em que ele é apresentado.
- Se uma mensagem de erro for mostrada durante a instalação do cliente solicitando que você saia do instalador para atualizar os drivers do Dell ControlVault, você pode desconsiderar completamente essa mensagem para continuar a instalação do cliente. Os drivers (e firmware) Dell ControlVault podem ser atualizados após a instalação do cliente ser concluída.

**Download dos drivers mais recentes**

1 Vá para support.dell.com.
2 Selecione o modelo do seu computador.
3 Selecione **Drivers e Downloads**.
4 Selecione o **Sistema operacional** do computador em questão.
5 Expanda a categoria **Segurança**.
6 Faça o download e salve os drivers Dell ControlVault.
7 Faça o download e salve o firmware Dell ControlVault.
8 Copie os drivers e o firmware nos computadores de destino, se necessário.

**Instale o driver Dell ControlVault.**

1 Navegue até a pasta na qual você fez o download do arquivo de instalação do driver.
2 Clique duas vezes no driver Dell ControlVault para abrir o arquivo executável autoextraível.

**DICA:**

Instale o driver primeiro. O nome de arquivo do driver *quando este documento foi criado* é ControlVault_Setup_2MYJC_A37_ZPE.exe.

3 Clique em **Continue** (Continuar) para começar.

4 Clique em **OK** para descompactar os arquivos do driver no local padrão **C:\Dell\Drivers\<Nova pasta>**.

5 Clique em **Sim** para criar uma nova pasta.

6 Clique em **Ok** quando for mostrada a mensagem de que a descompactação foi bem-sucedida.

7 A pasta que contém os arquivos deve ser mostrada após a extração. Se ela não for mostrada, navegue até à pasta na qual você extraiu os arquivos. Neste caso, a pasta é **JW22F**.

8 Clique duas vezes em **CVHCI64.MSI** para abrir o instalador de drivers. [este exemplo é **CVHCI64.MSI** neste modelo (CVHCI para um computador de 32 bits)].

9 Clique em **Avançar** na tela de Boas-vindas.

10 Clique em **Avançar** para instalar os drivers no local padrão **C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.**

11 Selecione a opção **Concluir** e clique em **Avançar**.

12 Clique em **Instalar** para iniciar a instalação dos drivers.

13 Opcionalmente marque a caixa para mostrar o arquivo de log do instalador. Clique em **Concluir** para sair do assistente.

### Verificação da instalação de drivers

- O Gerenciador de dispositivos terá um dispositivo Dell ControlVault (e outros dispositivos) dependendo da configuração de hardware e do sistema operacional.

### Instalação do firmware Dell ControlVault

1 Navegue até a pasta na qual você fez o download do arquivo de instalação do firmware.

2 Clique duas vezes no firmware Dell ControlVault para abrir o arquivo executável autoextraível.

3 Clique em **Continuar** para começar.

4 Clique em **OK** para descompactar os arquivos do driver no local padrão **C:\Dell\Drivers\<Nova pasta>**.

5 Clique em **Sim** para criar uma nova pasta.

6 Clique em **Ok** quando for mostrada a mensagem de que a descompactação foi bem-sucedida.

7 A pasta que contém os arquivos deve ser mostrada após a extração. Se ela não for mostrada, navegue até à pasta na qual você extraiu os arquivos. Selecione a pasta **firmware**.

8 Clique duas vezes em **ushupgrade.exe** para abrir o instalador do firmware.

9 Clique em **Iniciar** para começar o upgrade do firmware.

**IMPORTANTE:**

Se estiver fazendo o upgrade de uma versão mais antiga do firmware, será solicitado que você digite a senha de administrador. Digite `Broadcom` como a senha e clique em **Enter** se essa caixa de diálogo for mostrada.

Várias mensagens de status serão mostradas.

10 Clique em **Reiniciar** para concluir o upgrade do firmware.

A atualização dos drivers e firmware Dell ControlVault foi concluída.

# Configurações de registro

Esta seção detalha todas as configurações de registro aprovadas pelo Dell ProSupport para computadores clientes locais.

# Encryption Client

**(Opcional) Criar um arquivo de log do Agente de remoção de criptografia**

- Antes de iniciar o processo de desinstalação, você terá a opção de criar um arquivo de log do Agente de remoção de criptografia. Este arquivo de log é útil para solucionar problemas de uma operação de desinstalação/descriptografia. Se você não pretende descriptografar arquivos durante o processo de desinstalação, não é necessário criar esse arquivo de log.
- O arquivo de log do Agente de remoção de criptografia não será criado até que o serviço Agente de remoção de criptografia seja concluído, o que não acontece até o computador ser reiniciado. Quando o cliente tiver sido desinstalado com êxito e o computador estiver totalmente descriptografado, o arquivo de log será apagado permanentemente.
- O caminho do arquivo de log é **C:\ProgramData\Dell\Dell Data Protection\Encryption.**
- Crie a seguinte entrada de registro no computador que você pretende descriptografar.

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=dword:2

  0: nenhum registro em log

  1: registra os erros que impedem a execução do Serviço

  2: registra os erros que impedem a descriptografia de dados completa (nível recomendado)

  3: registra as informações sobre todos os volumes e arquivos de descriptografia

  5: registra as informações de depuração

**Usar cartões inteligentes com o login do Windows**

- Para usar cartões inteligentes com a autenticação do Windows, o seguinte valor de registro precisará ser configurado no computador cliente:

  [HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

  "MSSmartcardSupport"=dword:1

**Preservar os arquivos temporários durante a instalação**

- Por padrão, todos os arquivos temporários no diretório c:\windows\temp são automaticamente apagados durante a instalação. A exclusão dos arquivos temporários acelera a criptografia inicial e ocorre antes da varredura de criptografia inicial.

  Entretanto, se a sua organização usa um aplicativo de terceiro que exige que a estrutura de arquivos dentro do diretório \temp seja preservada, você deve evitar esta exclusão.

  Para desativar a exclusão de arquivo temporário, crie ou modifique a configuração de registro da seguinte forma:

  [HKLM\SOFTWARE\CREDANT\CMGShield]

  "DeleteTempFiles"=REG_DWORD:0

  Não apagar os arquivos temporários aumenta o tempo da criptografia inicial.

**Alterar o comportamento padrão do prompt de usuário para iniciar ou atrasar a criptografia**

- O Encryption Client mostra o prompt `duração de cada atraso de atualização de política` durante cinco minutos a cada vez. Se o usuário não responder ao prompt, o próximo atraso será iniciado. O prompt de atraso final inclui uma contagem regressiva e uma barra de progresso, e é exibido até que o usuário responda, ou o atraso final expirar e o logout ou reinicialização necessários ocorra.

Você pode alterar o comportamento do prompt de usuário para iniciar ou atrasar a criptografia, para impedir o processamento de criptografia após não obter nenhuma resposta do usuário. Para fazer isso, configure o registro com o seguinte valor:

[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"SnoozeBeforeSweep"=DWORD:1

Nenhum valor diferente de zero alterará o comportamento para suspensão. Sem nenhuma interação do usuário, o processamento de criptografia será atrasado até o número de atrasos permitidos configurável. O processamento da criptografia começará quando o atraso final expirar.

Calcule o máximo possível de atrasos da seguinte forma (um atraso máximo envolveria o usuário nunca responder a um prompt de atraso, cada um do qual é exibido por 5 minutos):

(NÚMERO DE ATRASOS DE ATUALIZAÇÃO DE POLÍTICA PERMITIDOS × DURAÇÃO DE CADA ATRASO DE ATUALIZAÇÃO DE POLÍTICA) + (5 MINUTOS × [NÚMERO DE ATRASOS DE ATUALIZAÇÃO DE POLÍTICA PERMITIDOS - 1])

**Alterar o uso padrão da chave SDUser**

- O System Data Encryption (SDE) é forçado com base no valor da política para as Regras de Criptografia do SDE. Diretórios adicionais são protegidos por padrão quando a política Criptografia do SDE Ativada é selecionada. Para obter mais informações, pesquise as "Regras de Criptografia do SDE" no AdminHelp. Quando o cliente Encryption estiver processando uma atualização de política que inclui uma política do SDE ativa, o diretório de perfil do usuário atual é criptografado por padrão com a chave SDUser (uma chave do usuário) em vez da chave SDE (uma chave do dispositivo). A chave SDUser também é usada para criptografar arquivos ou pastas que são copiados (não movidos) em um diretório do usuário que não é criptografado com o SDE.

  Para desativar a chave SDUser e usar a chave do SDE para criptografar esses diretórios do usuário, crie a seguinte entrada do registro no computador:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]

  "EnableSDUserKeyUsage"=dword:00000000

  Se esta chave do registro não estiver presente ou estiver configurada para qualquer outro valor diferente de 0, a chave SDUser será usada para criptografar esses diretórios do usuário.

# Cliente de autenticação avançada

**Desativar cartão inteligente e serviços biométricos (opcional)**

Se não quiser que o Security Tools altere os serviços associados aos cartões inteligentes e dispositivos biométricos para um tipo de inicialização "automática", é possível desativar o recurso de inicialização de serviço.

Quando desativado, Security Tools não tentará iniciar estes três serviços:

- SCardSvr – Gerencia o acesso a cartões inteligentes lidos pelo computador. Se esse serviço for interrompido, este computador será incapaz de ler cartões inteligentes. Se esse serviço for desativado, quaisquer serviços que dependerem explicitamente dele não serão iniciados.
- SCPolicySvc – Permite que o sistema seja configurado para bloquear a área de trabalho do usuário após a remoção do cartão inteligente.
- WbioSrvc – O serviço biométrico do Windows oferece aos aplicativos de clientes a capacidade de capturar, comparar, manipular e armazenar dados biométricos sem obter acesso direto a nenhum hardware biométrico nem amostras. O serviço é hospedado em um processo privilegiado de SVCHOST.

  Desativar esse recurso também cancela avisos associados aos serviços necessários que não estão em execução.
- Por padrão, se a chave de registro não existir ou se o valor estiver definido como 0, esse recurso é ativado.

  [HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

SmartCardServiceCheck=REG_DWORD:0

Defina como 0 para ativar.

Defina como 1 para desativar.

**Usar cartões inteligentes com o login do Windows**

- Para usar cartões inteligentes com a autenticação do Windows, o seguinte valor de registro precisará ser configurado no computador cliente:

  [HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

  "MSSmartcardSupport"=dword:1

  Vá para Glossário.

# 13

# Glossário

Advanced Authentication – O produto Advanced Authentication oferece opções totalmente integradas de leitor de impressões digitais, cartão inteligente e cartão inteligente sem contato. O Advanced Authentication ajuda a gerenciar esses diversos métodos de autenticação de hardware, oferece suporte para login com unidades de criptografia automática, SSO e gerencia credenciais e senhas de usuário. Além disso, o Advanced Authentication pode ser usado para acessar não apenas computadores, mas também qualquer site, SaaS ou aplicativo. Depois que os usuários registram suas credenciais, o Advanced Authentication permite o uso dessas credenciais para fazer login no dispositivo e realizar a troca de senha.

Senha de administrador de criptografia (EAP) - A EAP é uma senha administrativa exclusiva de cada computador. A maioria das configurações feitas no Console de gerenciamento local exige essa senha. Essa senha é a mesma que será solicitada se você precisar usar o arquivo LSARecovery_[nome_do_host].exe para recuperar os dados. Anote e guarde essa senha em um local seguro.

Cliente Encryption - O cliente Encryption é o componente presente no dispositivo que impõe as políticas de segurança, independentemente de o endpoint estar conectado ou não à rede e de ter sido perdido ou roubado. Criando um ambiente de computação confiável para endpoints, o cliente Encryption opera como uma camada acima do sistema operacional do dispositivo e fornece autenticação imposta de forma sistemática, criptografia e autorização, para maximizar a proteção de informações confidenciais.

Chaves de criptografia – Na maioria dos casos, o cliente Encryption usa a chave de usuário e mais duas chaves de criptografia adicionais. Entretanto, existem exceções: todas as políticas do SDE e a política Secure Windows Credentials (Credenciais seguras do Windows) usam a chave do SDE. As políticas Criptografar arquivo de paginação do Windows e Proteger arquivo de hibernação do Windows usam suas próprias chaves, a GPK (General Purpose Key, chave para finalidades gerais). A chave Comum torna os arquivos acessíveis a todos os usuários gerenciados no dispositivo em que foram criados. A chave Usuário torna os arquivos acessíveis apenas para o usuário que os criou, apenas no dispositivo em que foram criados. A chave Roaming de usuário torna os arquivos acessíveis apenas ao usuário que os criou, em qualquer dispositivo protegido do Windows (ou Mac).

Varredura de criptografia – Uma varredura de criptografia é o processo de verificar as pastas a serem criptografadas em um endpoint protegido para garantir que os arquivos contidos nelas estejam no estado de criptografia adequado. As operações habituais de criação de arquivo e alteração de nome não acionam uma varredura de criptografia. É importante entender quando uma varredura de criptografia pode ocorrer e o que pode influenciar os tempos de varredura resultantes, da seguinte forma: - Uma varredura de criptografia ocorrerá após o recebimento inicial de uma política com criptografia ativada. Isso pode ocorrer imediatamente após a ativação se sua política tiver criptografia ativada. - Se a política "Verificar estação de trabalho no login" estiver ativada, as pastas especificadas para criptografia serão verificadas toda vez que o usuário fizer login. - Uma varredura pode ser acionada novamente por certas mudanças de política subsequentes. Qualquer mudança de política relacionada à definição das pastas de criptografia, algoritmos de criptografia e uso de chave de criptografia (comum x usuário) ativará uma varredura. Além disso, alternar entre a ativação e a desativação da criptografia acionará uma varredura de criptografia.

Senha de uso único (OTP) - Uma senha de uso único só pode ser usada uma vez e é válida apenas por um período limitado de tempo. A OTP exige que o TPM esteja presente, ativado e possua um proprietário. Para ativar a Senha de uso único, um dispositivo móvel é emparelhado com o computador usando o Security Console e o aplicativo Security Tools Mobile. O aplicativo Security Tools Mobile gera no dispositivo móvel a senha utilizada para fazer login no computador na tela de login do Windows. Conforme a política, o recurso de OTP pode ser usado para recuperar o acesso ao computador em caso de vencimento ou esquecimento da senha, desde que a OTP não tenha sido usada para o login no computador. O recurso de OTP pode ser usado para autenticação ou para recuperação, mas não para ambos. A segurança da Senha de uso único é superior a de alguns outros métodos de autenticação, pois a senha gerada pode ser utilizada apenas uma vez e vence em pouco tempo.

PBA (Preboot Authentication, Autenticação de pré-inicialização) – O recurso de PBA serve como uma extensão do BIOS ou do firmware de inicialização e garante um ambiente seguro e à prova de falsificação externo ao sistema operacional, como uma camada de autenticação confiável. A PBA impede a leitura de qualquer informação do disco rígido, como o sistema operacional, até o usuário confirmar que tem as credenciais corretas.

Logon único (SSO) - o SSO simplifica o processo de logon quando a autenticação multifatores está ativada, tanto na pré-inicialização como no logon do Windows. Se ativado, a autenticação será necessária na pré-inicialização apenas, e os usuários serão automaticamente conectados ao Windows. Se não estiver ativado, a autenticação talvez seja necessária mais de uma vez.

System Data Encryption (SDE) - O SDE foi projetado para criptografar arquivos do sistema operacional e de programas. Para atingir este objetivo, o SDE precisa ser capaz de abrir sua chave enquanto o sistema operacional estiver sendo inicializado. A intenção é evitar que um invasor altere ou ataque o sistema operacional off-line. O SDE não se destina a dados de usuário. Criptografia comum e de chave de usuário são destinadas a dados confidenciais do usuário, pois exigem uma senha de usuário para desbloquear as chaves de criptografia. As políticas de SDE não criptografam os arquivos necessários para que o sistema operacional comece o processo de inicialização. As políticas de SDE não exigem autenticação de pré-inicialização e não interferem no Registro mestre de inicialização de nenhuma forma. Quando o computador é inicializado, os arquivos criptografados ficam disponíveis antes de qualquer usuário fazer login (para ativar ferramentas de backup e recuperação, SMS e gerenciamento de patches). Desativar a criptografia SDE aciona a descriptografia automática de todos os arquivos e diretórios criptografados do SDE para os usuários relevantes, independentemente de outras políticas de SDE, como, por exemplo, Regras de criptografia SDE.

Módulo TPM (Trusted Platform Module - Módulo de plataforma confiável) – É um chip de segurança com três funções principais: armazenamento seguro, medição e confirmação. O cliente Encryption usa o TPM para sua função de armazenamento seguro. O TPM pode também fornecer recipientes criptografados para o vault de software. O TPM é também necessário para uso com o recurso de Senha de uso único.