Dell Data Protection | Endpoint Security Suite Enterprise

Guia de Instalação Básica v1.4

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 Básica do Endpoint Security Suite Enterprise

2017 - 04

Rev. A01

Índice

1 Introdução 5
Antes de começar 5
Usar este guia 5
Entre em contato com o Dell ProSupport 5

2 Requisitos 7
Todos os clientes 7
Todos os clientes - Pré-requisitos 7
Todos os clientes - Hardware 7
Todos os clientes - Suporte a idiomas 8
Cliente Encryption 8
Pré-requisitos do cliente Encryption 9
Sistemas operacionais do cliente Encryption 9
Sistemas operacionais do External Media Shield (EMS) 9
Cliente Advanced Threat Prevention 10
Sistemas operacionais do Advanced Threat Prevention 10
Portas do Advanced Threat Prevention 10
Verificação da integridade da imagem do BIOS 11
Cliente SED 11
Pré-requisitos do Cliente de SED 12
Hardware do cliente SED 12
Sistemas operacionais do Cliente de SED 12
Cliente Advanced Authentication 13
Hardware do cliente de autenticação avançada 13
Sistemas operacionais do cliente de autenticação avançada 13
Cliente BitLocker Manager 14
Pré-requisitos do cliente BitLocker Manager 14
Sistemas operacionais do cliente BitLocker Manager 15

3 Instalar usando o instalador mestre do ESS 16
Instalar de forma interativa usando o instalador mestre do ESS 16
Instalar por linha de comando usando o instalador mestre do ESS 17

4 Desinstalar usando o instalador mestre do ESS 20
Desinstalar o instalador mestre do ESS 20
Desinstalação por linha de comando 20

5 Desinstalar usando os instaladores filhos 21
Desinstalar o cliente Encryption e Server Encryption 22
Processo 22
Desinstalação por linha de comando 22
Desinstalar o Advanced Threat Prevention 24
Desinstalação por linha de comando 24

Desinstalar clientes SED e Advanced Authentication....24
Processo....24
Desativar o PBA....24
Desinstalar o cliente de SED e os clientes Advanced Authentication....25
Desinstalar o cliente BitLocker Manager....25
Desinstalação por linha de comando....25

6 Provisionar um locatário para o Advanced Threat Prevention....26
Fazer o provisionamento de um locatário....26

7 Configurar Atualização automática do agente do Advanced Threat Prevention....27

8 Extrair os instaladores filhos do instalador mestre do ESS....28

9 Configurar o Key Server para desinstalação do cliente Encryption ativado no EE Server....29
Painel Serviços - Adicionar usuário da conta de domínio....29
Arquivo de configuração do servidor de chaves - Adicionar usuário para comunicação com o EE Server....29
Painel Serviços - Reiniciar o serviço do servidor de chaves....30
Remote Management Console - Adicionar administrador forense....30

10 Usar o utilitário de download administrativo (CMGAd)....31
Usar o utilitário de download administrativo no modo forense....31
Usar o utilitário de download administrativo no modo administrativo....32

11 Solução de problemas....33
Todos os clientes - solução de problemas....33
Solução de problemas do cliente Encryption e Server Encryption....33
Upgrade para a Atualização de Aniversário do Windows 10....33
Ativação em um sistema operacional de servidor....33
Interações de EMS e PCS....36
Usar WSScan....36
Verificar o status do agente de remoção de criptografia....38
Solução de problemas do cliente do Advanced Threat Prevention....38
Encontrar o código do produto com o Windows PowerShell....38
Provisionamento do Advanced Threat Prevention e comunicação do agente....39
Processo de verificação de integridade da imagem do BIOS....41
Drivers Dell ControlVault....42
Atualização dos drivers e firmware Dell ControlVault....42

12 Glossário....45

1

Introdução

Este guia detalha como instalar e configurar o aplicativo usando o instalador mestre do ESS. Este guia fornece assistência básica de instalação. Consulte o *Guia de Instalação Avançada* se precisar de informações sobre a instalação de instaladores filhos, configuração do EE Server/VE Server ou informações além da assistência básica para o instalador mestre ESS.

Todas as informações sobre as políticas e suas descrições podem ser encontradas no AdminHelp.

Antes de começar

1 Instale o EE Server/VE Server antes de implantar clientes. Localize o guia correto conforme mostrado abaixo, siga as instruções descritas e retorne para este guia.

- *Guia de instalação e migração do DDP Enterprise Server*
- *Guia de Instalação e de Início Rápido do DDP Enterprise Server – Virtual Edition*

Verifique se as políticas estão definidas conforme desejado. Procure através do AdminHelp, disponível a partir do **?** no canto direito da tela. O AdminHelp é uma ajuda no nível de página desenvolvida para ajudar você a definir e modificar políticas e compreender as suas opções com o EE Server/VE Server.

2 Provisionar um locatário para o Advanced Threat Prevention. Um locatário precisa ser provisionado no DDP Server para que a imposição de políticas do Advanced Threat Prevention possa ser ativada.

3 Leia completamente o capítulo Requisitos deste documento.

4 Implemente os clientes para os usuários finais.

Usar este guia

Use este guia na seguinte ordem.

- Consulte Requisitos para obter os pré-requisitos do cliente.
- Selecione uma das seguintes opções:
  - Instalar de forma interativa usando o instalador mestre do ESSE

    ou
  - Instalar por linha de comando usando o instalador mestre do ESSE

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.

Requisitos

Todos os clientes

- 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.
- Não realize alterações no computador, incluindo a inserção ou a remoção de unidades externas (USB), durante a instalação.
- Verifique se a porta de saída 443 está disponível para se comunicar com o EE Server/VE Server se os clientes do instalador mestre do ESSE forem habilitados usando o Dell Digital Delivery (DDD). A funcionalidade de habilitação não funcionará se a porta 443 estiver bloqueada por qualquer motivo. O DDD não será usado se a instalação for feita usando instaladores filhos.
- Verifique periodicamente www.dell.com/support para obter a documentação e recomendações técnicas mais recentes.

Todos os clientes - Pré-requisitos

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

  Todos os computadores enviados da fábrica da Dell são pré-instalados com a versão completa do Microsoft .Net Framework 4.5.2 (ou posterior). 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, acesse https://www.microsoft.com/en-us/download/details.aspx?id=42643.
- Os drivers e o firmware para o ControlVault, leitores de impressão digital e cartões inteligentes (conforme mostrado abaixo) não estão incluídos nos arquivos executáveis do instalador filho nem do instalador mestre do ESSE. Os drivers e o firmware precisam ser mantidos atualizados, e podem ser obtidos por download acessando o site http://www.dell.com/support e selecionando o modelo do computador. Faça download dos drivers e firmware adequados com base em seu hardware de autenticação.

  - ControlVault
  - NEXT Biometrics Fingerprint Driver
  - 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 ControlVault são fornecidas em Atualização dos drivers e firmware Dell ControlVault.

Todos os clientes - Hardware

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

Hardware

- Os requisitos mínimos de hardware precisam atender às especificações mínimas do sistema operacional.

Todos os clientes - Suporte a idiomas

- Os clientes Encryption Advanced Threat Prevention e BitLocker Manager são compatíveis com interfaces de usuário multi-idiomas (MUI) e suportam os idiomas a seguir: Os dados do Advanced Threat Prevention são mostrados no Remote Management Console apenas em inglês.

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)

- Os clientes da unidade de criptografia automática (SED - Self-Encrypting Drive) e do Advanced Authentication são compatíveis com interfaces de usuário multi-idiomas (MUI) e suportam os idiomas a seguir. 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
- FR - Francês
- IT - Italiano
- DE - Alemão
- ES - Espanhol
- JA - Japonês
- KO - Coreano
- ZH-CN - Chinês, simplificado
- ZH-TW - Chinês, tradicional/Taiwan
- PT-BR - Português, Brasil
- PT-PT - Português, Portugal (ibérico)
- RU - Russo

Cliente Encryption

- O computador cliente precisa ter conectividade de rede para realizar a ativação.
- Desative o modo de suspensão durante a varredura inicial de criptografia para impedir que um computador não supervisionado entre em modo de suspensão. Nem a criptografia nem a descriptografia podem ocorrer em um computador em modo de suspensão.
- O cliente Encryption 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 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 cliente Encryption 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 http://www.dell.com/support/Article/us/en/19/SLN298707 ou entre em contato com o Dell ProSupport para obter ajuda.
- Não há suporte para upgrade de sistema operacional instalado quando o cliente Encryption está instalado. Desinstale e descriptografe o cliente Encryption, faça o upgrade para o novo sistema operacional e depois reinstale o cliente Encryption.

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.

Pré-requisitos do cliente Encryption

- O instalador mestre do ESSE instala o Microsoft Visual C++ 2012 Update 4 caso não esteja instalado no computador.

Pré-requisito

- Visual C++ 2012 Update 4 ou Redistributable Package mais recente (x86 e x64)

Sistemas operacionais do cliente Encryption

- 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
- 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 em Windows 7, Windows Embedded Standard 7 ou Windows Embedded 8.1 Industry Enterprise.

Sistemas operacionais do 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

Cliente Advanced Threat Prevention

- O cliente Advanced Threat Prevention não pode ser instalado sem que o cliente Dell Client Security Framework (EMAgent) seja detectado no computador. Se você tentar fazer a instalação, ela falhará.
- Para concluir a instalação do Advanced Threat Prevention quando o Dell Enterprise Server/VE que gerencia o cliente estiver em execução no Modo conectado, o computador deve ter conectividade de rede. No entanto, a conectividade de rede ***não*** é necessária para a instalação do Advanced Threat Prevention quando o Dell Server que gerencia o cliente estiver em execução no Modo desconectado.
- Para fazer o provisionamento de um locatário para o Advanced Threat Prevention, o Dell Server precisa ter conectividade com a Internet.

  NOTA: A conectividade com a Internet não é necessária quando o Dell Server estiver em execução no Modo desconectado.
- Os recursos opcionais Firewall cliente e Proteção da Web ***não*** devem ser instalados em computadores cliente que sejam gerenciados pelo Dell Enterprise Server/VE em execução no Modo desconectado.
- Aplicativos antivírus, antimalware e antispyware de outros fornecedores podem entrar em conflito com o cliente Advanced Threat Prevention. Se possível, desinstale esses aplicativos. O Windows Defender não é um software conflitante. Aplicativos de firewall são permitidos.

  Se não for possível desinstalar outros aplicativos antivírus, antimalware e antispyware, você precisa adicionar exclusões ao Advanced Threat Protection no Dell Server e também aos outros aplicativos. Para obter instruções sobre como adicionar exclusões ao Advanced Threat Protection no Dell Server, consulte http://www.dell.com/support/article/us/en/04/SLN300970. Para obter uma lista de exclusões para adicionar aos outros aplicativos antivírus, consulte http://www.dell.com/support/article/us/en/19/SLN301134.

Sistemas operacionais do Advanced Threat Prevention

- A tabela a seguir detalha os sistemas operacionais suportados.

Sistemas operacionais Windows (32 e 64 bits)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Portas do Advanced Threat Prevention

- Os agentes do Advanced Threat Prevention são gerenciados pela plataforma SaaS do console de gerenciamento e se comunicam com ela. A porta 443 (https) é usada para a comunicação e precisa estar aberta no firewall para que os agentes consigam se comunicar com o console. O console é hospedado pelo Amazon Web Services e não possui IP fixo. Se a porta 443 estiver bloqueada por algum motivo, não será possível fazer o download das atualizações, de modo que os computadores podem não ter a proteção mais atual. Certifique-se de que os computadores cliente possam acessar os URLs da seguinte forma.

Uso	Protocolo de aplicativo	Protocolo de transporte	Número da porta	Destino	Direção
Toda a comunicação	HTTPS	TCP	443	Permitir todo o tráfego https para *.cylance.com	Saída

Verificação da integridade da imagem do BIOS

Se a política *Ativar certificação de BIOS* estiver selecionada no Remote Management Console, o locatário do Cylance valida um hash do BIOS nos sistemas dos usuários finais para garantir que o BIOS não foi modificado na versão de fábrica da Dell, o que é um possível vetor de ataque. Se uma ameaça for detectada, uma notificação é passada para o DDP Server e o administrador de TI é alertado no Remote Management Console. Para obter uma visão geral do processo, consulte Processo de verificação de integridade da imagem do BIOS.

NOTA: Não é possível usar uma imagem de fábrica personalizada com esse recurso, pois o BIOS foi modificado.

Modelos de computador Dell compatíveis com a Verificação de integridade da imagem do BIOS

- Latitude 3470
- Latitude 3570
- Latitude 7275
- Latitude 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7270
- Latitude E7470
- Latitude Rugged 5414
- Latitude Rugged 7214 Extreme
- Latitude Rugged 7414
- OptiPlex 3040
- OptiPlex 3240
- OptiPlex 5040
- OptiPlex 7040
- OptiPlex 7440
- Precision Mobile Workstation 3510
- Precision Mobile Workstation 5510
- Precision Workstation 3620
- Precision Workstation 7510
- Precision Workstation 7710
- Precision Workstation T3420
- Venue 10 Pro 5056
- Venue Pro 5855
- Venue XPS 12 9250
- XPS 13 9350
- XPS 9550

Cliente SED

- O computador precisa ter uma conexão de rede cabeada para instalar satisfatoriamente o SED Management.
- IPv6 não é compatível.
- Esteja preparado para desligar e reiniciar o computador após você aplicar políticas e estar pronto para iniciar a aplicação delas.
- Computadores equipados com unidades de criptografia automática não podem ser usados com placas de HCA. Há incompatibilidades que impedem o provisionamento do HCA. A Dell não comercializa computadores com unidades de criptografia automática que oferecem suporte ao módulo de HCA. Esta configuração não-suportada seria uma configuração de reposição.
- Se o computador destinado para criptografia estiver equipado com uma unidade de criptografia automática, certifique-se de que a opção *O usuário precisa mudar a senha no próximo login* do Active Directory esteja desativada. A Autenticação de pré-inicialização não é compatível com essa opção do Active Directory.
- A DELL recomenda que você não altere o método de autenticação depois que a PBA tiver sido ativada. Se for necessário mudar para um método de autenticação diferente, você precisará:

  - Remova todos os usuários da PBA.

  ou

  - Desative a PBA, altere o método de autenticação e ative novamente a PBA.

IMPORTANTE:
Em função da natureza do RAID e das SEDs, o gerenciamento de SED não suporta o RAID. O problema de *RAID=On* com SEDs é que o RAID exige acesso ao disco para ler e gravar dados relacionados ao RAID em um alto setor não disponível em uma SED bloqueada desde o início e não consegue aguardar para ler esses dados até o usuário ter feito login. Altere a operação de SATA no BIOS de *RAID=On* para *AHCI* para resolver o problema. Se o sistema operacional não tiver os drivers de controlador AHCI pré-instalados, o sistema mostrará a tela azul quando alterado de *RAID=On* para *AHCI*.

- O SED Management não é suportado com Server Encryption ou Advanced Threat Prevention em um SO de servidor.

Pré-requisitos do Cliente de SED

- O instalador mestre do ESSE instalará o Microsoft Visual C++2010 SP1 **e** o Microsoft Visual C++ 2012 Update 4 caso ainda não estejam instalados no computador.

Pré-requisitos

- Visual C++ 2010 SP1 ou Redistributable Package mais recente (x86 e x64)
- Visual C++ 2012 Update 4 ou Redistributable Package mais recente (x86 e x64)

Hardware do cliente SED

Teclados internacionais

- A tabela a seguir mostra os teclados internacionais compatíveis com Autenticação de pré-inicialização em UEFI e computadores não compatíveis com UEFI.

Suporte a teclado internacional - UEFI

- DE-CH - Alemão da Suíça
- DE-FR - Francês da Suíça

Suporte a teclado internacional - Non-UEFI

- AR - Árabe (usando letras latinas)
- DE-CH - Alemão da Suíça
- DE-FR - Francês da Suíça

Sistemas operacionais do Cliente de SED

- A tabela a seguir detalha os sistemas operacionais suportados.

Sistemas operacionais Windows (32 e 64 bits)

- Windows 7 SP0-SP1: Enterprise, Professional (suportado com o modo de Inicialização herdada, mas não com UEFI)

  NOTA:
  O modo de inicialização herdada é suportado no Windows 7. O UEFI não é suportado no Windows 7.

- Windows 8: Enterprise, Pro,

Sistemas operacionais Windows (32 e 64 bits)

- Windows 8.1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

Cliente Advanced Authentication

- Ao usarem o Advanced Authentication, os usuários estarão protegendo o acesso ao computador com o uso de credenciais de autenticação avançadas 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.

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 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

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

Sistemas operacionais Windows (32 e 64 bits)

- Windows 8: Enterprise, Pro
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- 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)
- 4.1 - 4.3.1 (Jelly Bean)
- 4.4 - 4.4.4 (KitKat)
- 5.0 - 5.1.1 (Lollipop)

Sistemas operacionais iOS

- iOS 7.x
- iOS 8.x

Sistemas operacionais Windows Phone

- Windows Phone 8.1
- Windows 10 Mobile

Cliente BitLocker Manager

- Considere a revisão dos Requisitos do Microsoft BitLocker caso o BitLocker ainda não esteja implementado no ambiente,
- Verifique se a partição de PBA já está configurada. Se o BitLocker Manager for instalado antes de a partição de PBA ser configurada, o BitLocker não poderá ser ativado e o BitLocker Manager não ficará operacional.
- O teclado, o mouse e os componentes de vídeo precisam estar diretamente conectados ao computador. Não use um interruptor KVM para gerenciar os periféricos, visto que ele pode interferir na capacidade do computador de identificar corretamente o hardware.
- Ligue e ative o TPM. O BitLocker Manager assumirá a propriedade do TPM e não exigirá uma reinicialização. Entretanto, se uma posse do TPM já existir, o BitLocker Manager iniciará o processo de configuração de criptografia (nenhuma reinicialização será necessária). A questão é que o TPM precisa ter um "proprietário" e estar ativado.
- O BitLocker Manager não é suportado com o Server Encryption ou com o Advanced Threat Prevention em um SO de servidor.

Pré-requisitos do cliente BitLocker Manager

- O instalador mestre do ESSE instalará o Microsoft Visual C++2010 SP1 **e** o Microsoft Visual C++ 2012 Update 4 caso ainda não estejam instalados no computador.

Pré-requisitos

- Visual C++ 2010 SP1 ou Redistributable Package mais recente (x86 e x64)
- Visual C++ 2012 Update 4 ou Redistributable Package mais recente (x86 e x64)

Sistemas operacionais do cliente BitLocker Manager

- A tabela a seguir detalha os sistemas operacionais suportados.

Sistemas operacionais Windows

- Windows 7 SP0-SP1: Enterprise, Ultimate (32 e 64 bits)
- Windows 8: Enterprise (64 bits)
- Windows 8.1: Enterprise Edition, Pro Edition (64 bits)
- Windows 10: Education, Enterprise, Pro
- Windows Server 2008 R2: Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2012
- Windows Server 2012 R2: Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2016

3

Instalar usando o instalador mestre do ESS

- Parâmetros e opções de linha de comando fazem distinção entre maiúsculas e minúsculas.
- Para instalar usando portas que não são as portas padrão, use os instaladores filhos em vez do instalador mestre do ESS.
- Os arquivos de log do instalador mestre do ESS estão localizados em **C:\ProgramData\Dell\Dell Data Protection\Installer.**
- Oriente os usuários a consultar o documento e os arquivos de ajuda a seguir para obter ajuda com o aplicativo:
  - Consulte a *Ajuda de criptografia Dell* para aprender como usar o recurso do cliente Encryption. Acesse a ajuda em **<Diretório de instalação>:\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 **<Diretório de instalação>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
  - Consulte a *Ajuda do Endpoint Security Suite Enterprise* para aprender como usar os recursos de Advanced Authentication, e Advanced Threat Prevention. Acesse a ajuda em **<Diretório de instalação>:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Help**.
- Os usuários devem atualizar suas políticas, clicando com o botão direito no ícone do Dell Data Protection na bandeja do sistema e selecionando **Verificar se há atualizações de políticas** depois de a instalação terminar.
- O instalador mestre ESS instala todo o conjunto de produtos. Há dois métodos de instalação usando o instalador mestre do ESS. Escolha um dos métodos a seguir.
  - Instalar de forma interativa usando o instalador mestre do ESSE

  ou

  - Instalar por linha de comando usando o instalador mestre do ESSE

Instalar de forma interativa usando o instalador mestre do ESS

- O instalador mestre do ESS pode ser localizado em:
  - **Sua conta de FTP na Dell** - Localize o kit de instalação em DDP-Endpoint-Security-Suite-1.x.x.xxx.zip.
- Use essas instruções para instalar o Dell Endpoint Security Suite Enterprise interativamente usando o instalador mestre ESSE. Este método pode ser usado para instalar o conjunto de produtos no computador de uma vez.

1. Localize **DDPSuite.exe** na mídia de instalação da Dell. Copie-o para o computador local.
2. Clique duas vezes em **DDPSuite.exe** para iniciar o instalador. Isso pode levar vários minutos.
3. Clique em **Avançar** na caixa de diálogo de Boas-vindas.
4. Leia o contrato de licença, aceite os termos e condições e clique em **Avançar**.
5. No campo **Enterprise Server Name** (Nome do Enterprise Server), digite o nome de host totalmente qualificado do EE Server/VE Server que gerenciará o usuário de destino, como server.organization.com.

   No campo **Device Server URL** (URL do Device Server), digite o URL do Device Server (Security Server) com o qual o cliente se comunicará.

   O formato será https://server.organization.com:**8443**/xapi**/** (incluindo a barra final).

   Clique em **Avançar**.
6. Clique em **Avançar** para instalar o produto no local padrão **C:\Program Files\Dell\Dell Data Protection\. A Dell recomenda instalar somente no local padrão**, pois podem ocorrer problemas ao instalar em outros locais.

7 Selecione os componentes a serem instalados.

A opção *Security Framework* instala a estrutura de segurança subjacente e o Security Tools, o cliente de autenticação avançada que gerencia múltiplos métodos de autenticação, incluindo PBA e credenciais como impressões digitais e senhas.

A *Advanced Authentication* (Autenticação avançada) instala os arquivos e serviços necessários para a Autenticação avançada.

A opção *Encryption* instala o cliente Encryption, o qual impõe a política de segurança, esteja o computador conectado ou não à rede, seja perdido ou roubado.

Threat Protection instala os clientes Threat Protection, que são uma proteção contra malwares e antivírus e fazem verificações em busca de vírus, spywares e programas indesejados; o firewall do cliente, que monitora a comunicação entre o computador e os recursos na rede e na Internet; e a filtragem da Web, que mostra classificações de segurança ou bloqueia o acesso a sites durante a navegação on-line.

A opção *BitLocker Manager* instala o cliente do BitLocker Manager, projetado para aprimorar a segurança das implantações do BitLocker simplificando e reduzindo o custo de propriedade através do gerenciamento centralizado das políticas de criptografia do BitLocker.

O *Advanced Threat Protection* instala o cliente Advanced Threat Prevention, que é a proteção antivírus de última geração que usa ciência algorítmica e aprendizagem de máquina para identificar, classificar e impedir a execução ou os danos ao endpoint por ameaças cibernéticas conhecidas e desconhecidas.

A *Proteção da Web e firewall* instala os recursos opcionais de Proteção da Web e firewall. O Firewall cliente verifica o tráfego de entrada e saída em relação à sua lista de regras. A Proteção na Web monitora a navegação na Web e os downloads para identificar ameaças e impor a ação definida pela política ao detectar uma ameaça, com base nas classificações de sites.

> **NOTA: O Threat Protection e o Advanced Threat Prevention não podem estar no mesmo computador. O instalador impede automaticamente a seleção de ambos os componentes. Caso você queira instalar o Threat Protection, faça download do Guia de instalação avançada do Endpoint Security Suite.**

Clique em **Avançar** quando terminar de selecionar.

8 Clique em **Instalar** para iniciar a instalação. A instalação tomará alguns minutos.

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

A instalação está concluída.

Instalar por linha de comando usando o instalador mestre do ESS

- As opções precisam ser especificadas primeiro em uma instalação de linha de comando. Outros parâmetros vão dentro de um argumento que é passado para a opção /v.

Opções

- A tabela a seguir descreve as opções que podem ser usadas com o instalador mestre do ESSE .

Opção	Descrição
-y -gm2	Pré-extração do instalador mestre do ESS . As opções -y e -gm2 precisam ser usadas juntas. Não as separe.
/s	Instalação silenciosa
/z	Passa as variáveis para o .msi dentro de DDPSuite.exe

Parâmetros

- A tabela a seguir descreve os parâmetros que podem ser usados com o instalador mestre do ESS . O instalador mestre do ESSE não pode excluir componentes individuais, mas pode receber comandos para especificar quais componentes devem ser instalados.

Parâmetro	Descrição
SUPPRESSREBOOT	Suprime a reinicialização automática após a conclusão da instalação. Pode ser usado no modo SILENCIOSO.
Servidor	Especifica a URL do EE Server/VE Server.
InstallPath	Especifica o caminho da instalação. Pode ser usado no modo SILENCIOSO.
FEATURES	Especifica os componentes que podem ser instalados no modo SILENCIOSO. ATP = ***Somente*** Advanced Threat Prevention em um SO de servidor; Advanced Threat Prevention ***e*** Encryption em um SO de estação de trabalho DE-ATP = Advanced Threat Prevention e Encryption em um SO de servidor. Use ***somente*** para instalação em um SO de servidor. Esta é a instalação padrão em um SO se o parâmetro FEATURES não for especificado. DE = ***Somente*** Drive Encryption (cliente Encryption) Use ***somente*** para instalação em um SO de servidor. BLM = BitLocker Manager SED = Gerenciamento de unidade de criptografia automática (EMAgent/Manager, Drivers PBA/GPE) (Disponível somente quando instalado em um SO de estação de trabalho) ATP-WEBFIREWALL = Firewall cliente e Proteção da Web em um SO de estação de trabalho DE-ATP-WEBFIREWALL = Firewall cliente e Proteção da Web em um SO de servidor **NOTA: Para atualizações do Enterprise Edition ou a partir do Endpoint Security Suite Enterprise anterior à v1.4, o ATP-WEBFIREWALL ou o DE-ATP-WEBFIREWALL *devem* ser especificados para que sejam instalados no Firewall cliente e na Proteção da Web. Não especifique o ATP-WEBFIREWALL ou o DE-ATP-WEBFIREWALL ao instalar um cliente que será gerenciado pelo Dell Enterprise Server/VE em execução no Disconnected Mode (Modo desconectado).**
BLM_ONLY=1	Precisa ser usado em conjunto com o uso de FEATURES=BLM na linha de comando para excluir o plugin de gerenciamento de SED.

Exemplo de linha de comando

- Os parâmetros de linha de comando diferenciam letras maiúsculas de minúsculas.
- (Em um SO de estação de trabalho) Este exemplo instala todos os componentes usando o instalador mestre do ESSE em portas padrão, de forma silenciosa, no local padrão C:\Program Files\Dell\Dell Data Protection\, e o configura para usar o EE Server/VE Server especificado.

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com\""
```

- (Em um SO de estação de trabalho) Este exemplo instala o Advanced Threat Prevention e Encryption usando ***somente*** o instalador mestre do ESSE em portas padrão, de forma silenciosa, no local padrão C:\Program Files\Dell\Dell Data Protection\, e o configura para usar o EE Server/VE Server especificado.

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP\""
```

- (Em um SO de estação de trabalho) Este exemplo instala o Advanced Threat Prevention, Encryption e SED Management usando o instalador mestre do ESSE em portas padrão, de forma silenciosa e com reinicialização suprimida, no local padrão C:\Program Files\Dell\Dell Data Protection\, e o configura para usar o EE Server/VE Server especificado.

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP-SED,
SUPPRESSREBOOT=1\""
```

- (Em um SO de estação de trabalho) Este exemplo instala Advanced Threat Prevention, Encryption, Proteção da Web e Firewall cliente usando o instalador mestre do ESSE em portas padrão, de forma silenciosa, no local padrão C:\Program Files\Dell\Dell Data Protection\, e o configura para usar o EE Server/VE Server especificado.

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP-WEBFIREWALL\""
```

- (Em um SO de servidor) Este exemplo instala o Advanced Threat Prevention e Encryption usando ***somente*** o instalador mestre do ESSE em portas padrão, de forma silenciosa, no local padrão C:\Program Files\Dell\Dell Data Protection\, e o configura para usar o EE Server/VE Server especificado.

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE-ATP\""
```

- (Em um SO de servidor) Este exemplo instala Advanced Threat Prevention, Encryption, Proteção da Web e Firewall cliente usando o instalador mestre do ESSE em portas padrão, de forma silenciosa, no local padrão C:\Program Files\Dell\Dell Data Protection\

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE-ATP-WEBFIREWALL\""
```

- (Em um SO de servidor) Este exemplo instala o Advanced Threat Prevention usando ***somente*** o instalador mestre do ESSE em portas padrão, de forma silenciosa, no local padrão C:\Program Files\Dell\Dell Data Protection\, e o configura para usar o EE Server/VE Server especificado.

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP\""
```

- (Em um SO de servidor) Este exemplo instala ***somente*** o Encryption usando o instalador mestre do ESSE em portas padrão, de forma silenciosa, no local padrão C:\Program Files\Dell\Dell Data Protection\, e o configura para usar o EE Server/VE Server especificado.

```
"DDPSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE\""
```

Desinstalar usando o instalador mestre do ESS

- Cada componente precisa ser desinstalado separadamente, seguido pela desinstalação do instalador mestre do ESS. 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 do ESSE para obter os instaladores filhos.
- Certifique-se de usar, para a desinstalação, a mesma versão do instalador mestre do ESSE (e, por consequência, dos clientes) usada para a instalação.
- Esse capítulo direciona você para outros capítulos que contêm instruções *detalhadas* sobre como desinstalar os instaladores filho. Este capítulo explica **apenas** a última etapa, que desinstala o instalador mestre do ESS .
- Desinstale os clientes na seguinte ordem.

  a Desinstalar o cliente Encryption.

  b Desinstalar o Advanced Threat Prevention.

  c Desinstalar SED e clientes de autenticação avançada (desinstala a Dell Client Security Framework, que não pode ser desinstalada até que a Advanced Threat Prevention seja desinstalada).

  d Desinstalar o cliente BitLocker Manager
- Prossiga para Desinstalar o instalador mestre do ESSE.

Desinstalar o instalador mestre do ESS

Agora que todos os clientes individuais foram desinstalados, o instalador mestre do ESS pode ser desinstalado.

Desinstalação por linha de comando

- O exemplo a seguir desinstala silenciosamente o instalador mestre do ESS.

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

  Reinicie o computador ao terminar.

Desinstalar usando os instaladores filhos

- Para desinstalar cada cliente individualmente, os arquivos executáveis filhos precisam primeiro ser extraídos do instalador mestre do ESSE, como mostrado em Extrair os instaladores filhos do instalador mestre do ESSE . Como alternativa, execute uma instalação administrativa para extrair o .msi.
- Certifique-se de que as mesmas versões dos clientes usadas na instalação sejam usadas na desinstalação.
- 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 arquivos de log de desinstalação do instalador filho exclusivos para o usuário logado em %temp%, localizados 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:\<qualquer diretório>\<qualquer nome de arquivo de log>.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.

Switch	Significado
/v	Passa as variáveis para o .msi dentro de setup.exe. O conteúdo deve estar sempre entre aspas e com texto sem formatação.
/s	Modo silencioso
/x	Modo Desinstalar
/a	Instalação administrativa (copiará todos os arquivos dentro do .msi)

NOTA:
Com /v, as opções padrão da Microsoft estarão disponíveis. Para obter uma lista de opções, consulte https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx .

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

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

Desinstalar o cliente Encryption e Server Encryption

- Para reduzir o tempo de descriptografia, execute o assistente de Limpeza de Disco do Windows para remover arquivos temporários e outros dados desnecessários.
- 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 de descriptografia devido a arquivos bloqueados.
- Depois que a desinstalação estiver concluída e a descriptografia estiver em execução, desative toda a conectividade de rede. Caso contrário, novas políticas que reativem a criptografia poderão ser adquiridas.
- Siga seu processo existente para descriptografar dados, como emitir uma atualização de política.
- O Windows Shields atualizam o EE Server/VE Server para mudar o status para *Desprotegido* no início de um processo de desinstalação do Shield. Entretanto, caso o cliente não consiga entrar em contato com o EE Server/VE Server, independentemente do motivo, o status não poderá ser atualizado. Nesse caso, você precisará *Remover o endpoint* manualmente no Remote Management Console. Caso sua organização use esse fluxo de trabalho para fins de conformidade, a Dell recomenda que você verifique se a opção *Desprotegido* foi configurada conforme esperado, seja no Remote Management Console ou no Compliance Reporter.

Processo

- O Key Server (e o EE Server) precisa ser configurado antes da desinstalação no caso do uso da opção **Fazer download de chaves do servidor do Encryption Removal Agent**. Consulte Configurar o Key Server para desinstalação do cliente Encryption ativado no EE Server para obter instruções. Não é necessário realizar nenhuma ação antes disso se o cliente a ser desinstalado estiver ativado em um VE Server, uma vez que o VE Server não usa o Key Server.
- Você precisa usar o Dell Administrative Utility (CMGAd) antes de iniciar o Encryption Removal Agent se estiver usando a opção **Importar chaves de um arquivo do Encryption Removal Agent**. Esse utilitário é usado para obter o pacote de chaves de criptografia. Consulte Usar o Administrative Download Utility (CMGAd) para obter instruções. O utilitário pode ser encontrado na mídia de instalação Dell.

Desinstalação por linha de comando

- Once extracted from the ESSE master installer, the Encryption client installer can be located at **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: 3 - Use o pacote LSARecovery 2 - Use o material de chave forense previamente baixado 1 - Fazer download das chaves do Dell Server

Parâmetro	Seleção
	0 - Não instalar o Agente de remoção de criptografia
CMGSILENTMODE	Propriedade de desinstalação silenciosa: 1 - Silenciosa 0 - Não silenciosa
Propriedades necessárias	
DA_SERVER	FQHN para o EE Server que hospeda a sessão de negociação.
DA_PORT	Porta no EE Server para solicitação (o padrão é 8050).
SVCPN	Nome de usuário, no formato UPN, ao qual o serviço do Key Server está conectado no EE Server.
DA_RUNAS	Contexto do nome de usuário no formato compatível com SAM em que a solicitação de extração de chave será feita. Esse usuário precisa estar na lista do Key Server no EE Server.
DA_RUNASPWD	Senha do usuário runas.
FORENSIC_ADMIN	A conta de administrador forense no Dell Server, que pode ser usada para solicitações forenses para desinstalações ou chaves.
FORENSIC_ADMIN_PWD	A senha da conta de administrador forense.
Propriedades opcionais	
SVCLOGONUN	Nome de usuário no formato UPN para login no serviço Encryption Removal Agent como parâmetro.
SVCLOGONPWD	Senha para login como usuário.

- O exemplo a seguir desinstala silenciosamente o cliente Encryption e faz download das chaves de criptografia do EE Server.

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1 DA_SERVER=server.organization.com
  DA_PORT=8050 SVCPN=administrator@organization.com DA_RUNAS=domain\username
  DA_RUNASPWD=password /qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  CMG_DECRYPT="1" CMGSILENTMODE="1" DA_SERVER="server.organization.com" DA_PORT="8050"
  SVCPN="administrator@domain.com" DA_RUNAS="domain\username" DA_RUNASPWD="password" /qn
  ```

  Reinicie o computador ao terminar.

- O exemplo a seguir desinstala silenciosamente o cliente Encryption e faz download das chaves de criptografia usando uma conta de administrador forense.

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1
  FORENSIC_ADMIN=forensicadmin@organization.com FORENSIC_ADMIN_PWD=tempchangeit /qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn CMG_DECRYPT=1 CMGSILENTMODE=1
  FORENSIC_ADMIN=forensicadmin@organization.com FORENSIC_ADMIN_PWD=tempchangeit
  REBOOT=REALLYSUPPRESS
  ```

  Reinicie o computador ao terminar.

IMPORTANTE:

A Dell recomenda as seguintes ações quando você usar uma senha de administrador forense na linha de comando:

1 Criar uma conta de Administrador forense no Console de gerenciamento remoto para fazer a desinstalação silenciosa.
2 Usar uma senha temporária para essa conta que seja exclusiva dessa conta e desse período.
3 Após o término da desinstalação silenciosa, remova a conta temporária da lista de administradores ou altere sua senha.

NOTA:

Alguns clientes mais antigos podem precisar de caracteres de escape, como "\", ao redor dos valores de parâmetros. Por exemplo:

```
DDPE_XXbit_setup.exe /x /v"CMG_DECRYPT=\"1\" CMGSILENTMODE=\"1\" DA_SERVER=
\"server.organization.com\" DA_PORT=\"8050\" SVCPN=\"administrator@organization.com\"
DA_RUNAS=\"domain\username\" DA_RUNASPWD=\"password\" /qn"
```

Desinstalar o Advanced Threat Prevention

Desinstalação por linha de comando

- O exemplo a seguir desinstala o cliente Advanced Threat Prevention. ***Este comando deve ser executado a partir de um prompt de comando administrativo.***

  ```
  wmic path win32_product WHERE (CAPTION LIKE "%%CYLANCE%%") call uninstall
  ```

  Desligue e reinicie o computador e, em seguida, desinstale o componente Dell Client Security Framework.

- **IMPORTANTE: Se você instalou clientes SED e Advanced Authentication ou ativou a Autenticação de pré-inicialização, siga as instruções de desinstalação descritas em Desinstalar clientes SED e Advanced Authentication.**

  O exemplo a seguir desinstala somente o componente Dell Client Security Framework e não os clientes SED e Advanced Authentication.

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

Desinstalar clientes SED e Advanced Authentication

- É preciso ter uma conexão de rede com o EE Server/VE Server para desativar o recurso PBA.

Processo

- Desative o PBA, o que vai remover todos os dados de PBA do computador e desbloquear as chaves da SED.
- Desinstalar o cliente SED.
- Desinstalar o cliente de autenticação avançada.

Desativar o PBA

1 Como um administrador Dell, faça login no Remote Management Console.
2 No painel esquerdo, clique em > **Proteger e gerenciar endpoints**.
3 Selecione o Tipo de endpoint apropriado.
4 Selecione Mostrar >*Visível*, *Oculto* ou *Todos*.
5 Se você souber o nome de host do computador, digite-o no campo Nome de host (há suporte para caracteres curinga). Você pode deixar o campo em branco para ver todos os computadores. Clique em **Pesquisar**.

   Se você não souber o nome de host, navegue pela lista para localizar o computador.

   Um computador ou uma lista de computadores é mostrado com base em seu filtro de pesquisa.

6 Selecione o ícone **Detalhes** do computador desejado.
7 Clique em **Políticas de segurança** no menu superior.
8 Selecione **Unidades de criptografia automática** no menu **Categoria de política**.
9 Expanda a área **Administração de SED** e altere as políticas **Ativar gerenciamento de SED** e **Ativar PBA** de `True` para ***`False`***.
10 Clique em **Salvar**.
11 No painel à esquerda, clique em **Ações** > **Confirmar políticas**.
12 Clique em **Aplicar alterações**.

Aguarde a política ser propagada a partir do EE Server/VE Server para o computador de destino para fazer a desativação.

Desinstale os clientes de autenticação e SED após o PBA ser desativado.

Desinstalar o cliente de SED e os clientes Advanced Authentication

Desinstalação por linha de comando

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

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

Desligue e reinicie o computador ao terminar.

Em seguida:

- O exemplo a seguir desinstala silenciosamente o cliente de autenticação avançada.

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

Desligue e reinicie o computador ao terminar.

Desinstalar o cliente BitLocker Manager

Desinstalação por linha de comando

- Depois de extraído do instalador mestre do ESS, o instalador do cliente BitLocker pode ser localizado em C:\extracted\Security Tools \EMAgent_XXbit_setup.exe.
- O exemplo a seguir desinstala silenciosamente o cliente BitLocker Manager.

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

Reinicie o computador ao terminar.

Provisionar um locatário para o Advanced Threat Prevention

Se sua organização está usando o Advanced Threat Prevention, um locatário precisa ser provisionado no Dell Server antes que o modo de imposição das políticas do Advanced Threat Prevention se torne ativa.

Pré-requisitos

- Precisa ser realizado por um administrador com a função Administrador de sistema.
- É necessária conectividade com a Internet para provisionar no Dell Server.
- É necessária conectividade do cliente com a Internet para exibir a integração do serviço online do Advanced Threat Prevention no Remote Management Console.
- O provisionamento é baseado em um token gerado a partir de um certificado durante o provisionamento.
- As licenças do Advanced Threat Prevention precisam estar presentes no Dell Server.

Fazer o provisionamento de um locatário

1 Faça login no Remote Management Console e vá até **Gerenciamento de serviços**.

2 Clique em **Configurar serviço Advanced Threat Protection**. Importe as suas licenças do ATP se ocorrer uma falha neste ponto.

3 A configuração guiada começa após as licenças serem importadas. Clique em **Avançar** para começar.

4 Leia e concorde com o Contrato de licença do usuário final (a caixa de seleção está **desmarcada** por padrão) e clique em **Avançar**.

5 Forneça as credenciais de identificação ao DDP Server para o provisionamento do locatário. Clique em **Avançar**. *Não é suportado fazer o provisionamento de um locatário existente da marca Cylance.*

6 Faça download do certificado. Ele será necessário para fazer a recuperação em cenários de desastre com o DDP Server. O backup desse certificado não é feito automaticamente através do utilitário de upgrade v9.2. Faça backup do certificado em um local seguro disponível em outro computador. Marque a caixa de seleção para confirmar que você fez o backup do certificado e clique em **Avançar**.

7 A configuração foi concluída. Clique em **OK**.

Configurar Atualização automática do agente do Advanced Threat Prevention

No Remote Management Console do Dell Server, você pode se inscrever para receber atualizações automáticas do agente do Advanced Threat Prevention. A inscrição para receber atualizações do agente automáticas permite aos clientes fazer download automaticamente das atualizações e aplicá-las a partir do servidor do Advanced Threat Prevention. As atualizações são liberadas mensalmente.

NOTA: Atualizações automáticas do agente são suportadas com o Dell Server v9.4.1 ou posterior.

Receber atualizações automáticas do agente

Para se inscrever para receber atualizações automáticas do agente:

1. No painel esquerdo do Remote Management Console, clique em **Gerenciamento** > **Gerenciamento de serviços**.
2. Na guia **Ameaças avançadas**, em Atualização automática do agente, clique no botão **Ativar** e, em seguida, clique no botão **Salvar preferências**.

   Pode demorar alguns minutos para que as informações sejam preenchidas e as atualizações automáticas, exibidas.

Para de receber atualizações automáticas do agente

Para parar de receber atualizações automáticas do agente:

1. No painel esquerdo do Remote Management Console, clique em **Gerenciamento** > **Gerenciamento de serviços**.
2. Na guia **Ameaças avançadas**, em Atualização automática do agente, clique no botão **Desativar** e, em seguida, clique no botão **Salvar preferências**.

Extrair os instaladores filhos do instalador mestre do ESS

- O instalador mestre do ESS não é um *desinstalador* mestre. Cada cliente precisa ser desinstalado individualmente, seguido pela desinstalação do instalador mestre do ESS. Use esse processo para extrair os clientes do instalador mestre do ESS para que possam ser usados para desinstalação.

1 A partir da mídia de instalação da Dell, copie o arquivo **DDPSuite.exe** para o computador local.

2 Abra um prompt de comando no mesmo local em que se encontra o arquivo **DDPSuite.exe** e digite:

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

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

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

Configurar o Key Server para desinstalação do cliente Encryption ativado no EE Server

- Esta seção explica como configurar os componentes para uso com autenticação/autorização Kerberos usando um EE Server. O VE Server não usa o Key Server.
- Se a autorização/autenticação do Kerberos for usada, então o servidor que contém o componente do Servidor de chaves terá de fazer parte do domínio afetado.
- Uma vez que o VE Server não usa o Key Server, a desinstalação típica é afetada. Quando um cliente Encryption ativado em um VE Server é desinstalado, a recuperação de chave forense padrão através do Security Server é usada, em vez do método Kerberos do Key Server. Consulte Desinstalação por linha de comando para obter mais informações.

Painel Serviços - Adicionar usuário da conta de domínio

1 No EE Server, navegue até o painel Serviços (Iniciar > Executar... > services.msc > OK).

2 Clique com o botão direito no Key Server e selecione **Propriedades**.

3 Selecione a guia Login e, em seguida, a opção **Esta conta:**.

No campo *Esta conta:*, adicione o usuário da domínio de domínio. Este usuário do domínio precisa ter no mínimo direitos de administrador local na pasta do servidor de chaves (ele precisar poder gravar no arquivo de configuração do servidor de chaves, e poder gravar no arquivo log.txt.).

Digite e confirme a senha para o usuário de domínio.

Clique em **OK**

4 Reinicie o serviço do Key Server (deixe o painel Serviços aberto para continuar a operação).

5 Navegue até <Diretório de instalação do servidor de chaves> log.txt para verificar se o serviço foi iniciado corretamente.

Arquivo de configuração do servidor de chaves - Adicionar usuário para comunicação com o EE Server

1 Navegue até <Diretório de instalação do servidor de chaves>.

2 Abra ***Credant.KeyServer.exe.config*** com um editor de texto.

3 Vá para <add key="user" value="superadmin" /> e altere o valor "superadmin" para o nome do usuário apropriado (você também pode deixar como "superadmin").

4 Vá até <add key="epw" value="<valor criptografado da senha>" /> e altere "epw" para "senha". Depois altere "<valor criptografado da senha>" para a senha do usuário na etapa 3. Esta senha será criptografada novamente quando o EE Server for reiniciado.

Se estiver usando "superadmin" na etapa 3 e a senha superadmin não for "changeit", ela precisará ser alterada aqui. Salve e feche o arquivo.

Painel Serviços - Reiniciar o serviço do servidor de chaves

1 Volte para o painel Serviços (Iniciar > Executar... > services.msc > OK).
2 Reinicie o serviço do Key Server.
3 Navegue até <Diretório de instalação do servidor de chaves> log.txt para verificar se o serviço foi iniciado corretamente.
4 Feche o painel Serviços.

Remote Management Console - Adicionar administrador forense

1 Se necessário, faça login no Remote Management Console.
2 Clique em **Populações** > **Domínios**.
3 Selecione o domínio adequado.
4 Clique na guia **Key Server**.
5 No campo Account (Conta), adicione o usuário que realizará as atividades de administrador. O formato é DOMÍNIO\Nome de usuário. Clique em **Adicionar conta**.
6 Clique em **Usuários** no menu à esquerda. Na caixa de pesquisa, procure o nome de usuário adicionado na Etapa 5. Clique em **Search** (Pesquisar).
7 Assim que o usuário correto for localizado, clique na guia **Admin**.
8 Selecione **Administrador forense** e clique em **Atualizar**.

Agora os componentes estão configurados para a autorização/autenticação do Kerberos.

Usar o utilitário de download administrativo (CMGAd)

- Este utilitário possibilita fazer download de um pacote de materiais de chaves para uso em um computador não conectado a um EE Server/VE Server.
- O utilitário usa um dos métodos a seguir para fazer download de um pacote de chaves, dependendo do parâmetro de linha de comando passado ao aplicativo:
  - Forensic Mode (Modo forense) - Usado se "-f" for incluído na linha de comando ou se nenhum parâmetro de linha de comando for usado.
  - Admin Mode (Modo administrativo) - Usado se "-a" for incluído na linha de comando.

    Os arquivos de log podem ser encontrados em C:\ProgramData\CmgAdmin.log

Usar o utilitário de download administrativo no modo forense

1 Clique duas vezes em **cmgad.exe** para abrir o utilitário ou abra um prompt de comando onde o CMGAd está localizado e digite **`cmgad.exe -f`** (ou **`cmgad.exe`**).

2 Digite as informações a seguir (alguns campos podem já estar preenchidos).

URL do servidor de dispositivos: URL do Security Server (Device Server) totalmente qualificado. O formato é https://securityserver.domain.com:8443/xapi/.

Administrador da Dell: nome do administrador com credenciais de administrador forense (habilitado no Remote Management Console), por exemplo, jdoe

Senha: senha do administrador forense

MCID: ID da máquina, por exemplo, machineID.domain.com

DCID: Oito primeiros dígitos da ID Shield de 16 dígitos

> **DICA:**
> Normalmente, especificar o MCID *ou* DCID é suficiente. No entanto, se você souber ambos, é útil digitar os dois. Cada parâmetro contém diferentes informações sobre o cliente e o computador cliente.

Clique em **Next** (Avançar).

3 No campo Passphrase: (Senha:), digite uma senha para proteger o arquivo de download. A senha deve ter no mínimo oito caracteres e conter pelo menos um caractere alfabético e um numérico. Confirme a senha.

Aceite o nome e o local padrão onde o arquivo será salvo ou clique em ... para selecionar um local diferente.

Clique em **Next** (Avançar).

Uma mensagem indicando que o material de chave foi desbloqueado corretamente é mostrada. Os arquivos estão acessíveis agora.

4 Clique em **Concluir** quando terminar.

Usar o utilitário de download administrativo no modo administrativo

O VE Server não usa o Key Server, de forma que o modo administrativo não pode ser usado para obter um pacote de chaves de um VE Server. Use o modo forense para obter um pacote de chaves se o cliente estiver ativado em um VE Server.

1 Abra um prompt de comando onde o CMGAd está localizado e digite **`cmgad.exe -a`**.

2 Digite as informações a seguir (alguns campos podem já estar preenchidos).

Servidor: nome de Host totalmente qualificado do Key Server, por exemplo, keyserver.domain.com

Número da porta: a porta padrão é 8050

Conta de servidor: o usuário de domínio com o qual o Key Server está sendo executado. O formato é domínio\nome de usuário. O usuário de domínio executando o utilitário precisa estar autorizado a fazer download no Key Server

MCID: ID da máquina, por exemplo, machineID.domain.com

DCID: oito primeiros dígitos da ID Shield de 16 dígitos

> **DICA:**
> Normalmente, especificar o MCID *ou* DCID é suficiente. No entanto, se você souber ambos, é útil digitar os dois. Cada parâmetro contém diferentes informações sobre o cliente e o computador cliente.

Clique em **Next** (Avançar).

3 No campo Passphrase: (Senha:), digite uma senha para proteger o arquivo de download. A senha deve ter no mínimo oito caracteres e conter pelo menos um caractere alfabético e um numérico.

Confirme a senha.

Aceite o nome e o local padrão onde o arquivo será salvo ou clique em ... para selecionar um local diferente.

Clique em **Next** (Avançar).

Uma mensagem indicando que o material de chave foi desbloqueado corretamente é mostrada. Os arquivos estão acessíveis agora.

4 Clique em **Concluir** quando terminar.

Solução de problemas

Todos os clientes - solução de problemas

- Os arquivos de log do instalador mestre do **ESSE estão localizados em** C:\ProgramData\Dell\Dell Data Protection\Installer.
- O Windows cria **arquivos de log de desinstalação do instalador filho** exclusivos para o usuário logado em %temp%, localizados em **C:\Users\<UserName>\AppData\Local\Temp.**
- O Windows cria arquivos de log referentes a pré-requisitos do cliente, como Visual C++, para o usuário logado em %temp%, localizados em **C:\Users\<UserName>\AppData\Local\Temp. Por exemplo, C:\Users\<NomeDoUsuário>\AppData\Local\Temp \dd_vcredist_amd64_20160109003943.log**
- Siga as instruções em http://msdn.microsoft.com para verificar a versão do Microsoft .Net instalada no computador onde será feita a instalação.

  Acesse https://www.microsoft.com/en-us/download/details.aspx?id=30653 para baixar a versão completa do Microsoft .Net Framework 4.5.
- Consulte *Dell Data Protection | Security Tools Compatibility* se o computador onde será feita a instalação tem (ou já teve) o Dell Access instalado. O DDP|A não é compatível com esse conjunto de produtos.

Solução de problemas do cliente Encryption e Server 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.

Ativação em um sistema operacional de servidor

Quando o Encryption estiver instalado em um sistema operacional de servidor, a ativação exige duas fases de ativação: ativação inicial e ativação do dispositivo.

Solução de problemas da ativação inicial

A ativação inicial falha quando:

- Um UPN válido não pode ser construído usando as credenciais fornecidas.
- As credenciais não são encontradas no vault empresarial.
- As credenciais usadas para ativar não são as credenciais do administrador do domínio.

Mensagem de erro: Nome de usuário desconhecido ou senha incorreta

O nome de usuário ou a senha não correspondem.

Possível solução: Tente fazer login novamente, garantindo que você digite o nome de usuário e a senha corretamente.

Mensagem de erro: A ativação falhou porque a conta de usuário não tem direitos de administrador de domínio.

As credenciais usadas para ativar não têm direitos de administrador de domínio ou o nome de usuário do administrador não estava no formato UPN.

Possível solução: Na caixa de diálogo Ativação, digite as credenciais para um administrador de domínio, no formato UPN.

Mensagens de erro: Não foi possível estabelecer uma conexão com o servidor.

ou

`The operation timed out.`

O Server Encryption não conseguiu se comunicar usando a porta 8449 por HTTPS com o DDP Security Server.

Possíveis soluções

- Conecte-se diretamente à rede e tente ativar novamente.
- Caso esteja conectado por VPN, tente se conectar diretamente à rede e tente ativar novamente.
- Verifique o URL do DDP Server para garantir que corresponde ao URL fornecido pelo administrador. O URL e outros dados que o usuário digitou no instalador ficam armazenados no registro. Verifique a correção dos dados em [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] e [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet].
- Desconecte o servidor da rede. Reinicie o servidor e reconecte-se à rede.

Mensagem de erro: Falha na ativação porque o servidor não foi capaz de atender a esta solicitação.

Possíveis soluções

- O Server Encryption não pode ser ativado em um servidor preexistente; a versão do DDP Server precisa ser 9.1 ou superior. Se necessário, faça upgrade de seu DDP Server para a versão 9.1 ou superior.
- Verifique o URL do DDP Server para garantir que corresponde ao URL fornecido pelo administrador. O URL e outros dados que o usuário digitou no instalador ficam armazenados no registro.
- Verifique a correção dos dados em [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] e [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet].

Processo de ativação inicial

O diagrama a seguir ilustra uma ativação inicial bem-sucedida.

O processo de ativação inicial do Server Encryption precisa de um usuário ativo para acessar o servidor. O usuário pode ser de qualquer tipo: usuário de domínio ou não, conectado por área de trabalho remota ou interativo, mas ele precisa ter acesso às credenciais do administrador do domínio.

A caixa de diálogo Ativação mostra quando uma das duas opções a seguir ocorre:

- Um novo usuário (não gerenciado) faz login no computador.
- Quando um novo usuário clica com o botão direito no ícone do cliente Encryption na bandeja do sistema e seleciona Activate Dell Encryption (Ativar Dell Encryption).

O processo de ativação inicial ocorre da seguinte forma:

1 O usuário faz login.
2 Ao detectar um novo usuário (não gerenciado), a caixa de diálogo Ativar é mostrada. O usuário clica em **Cancelar**.
3 O usuário abre a caixa Sobre do Server Encryption para confirmar que ele está sendo executado no modo de servidor.
4 O usuário clica com o botão direito no ícone do cliente Encryption na bandeja do sistema e seleciona **Activate Dell Encryption (Ativar Dell Encryption)**.
5 O usuário digita as credenciais do administrador no domínio na caixa de diálogo Ativar.

> **NOTA:**
> A necessidade de credenciais do administrador do domínio é uma medida de segurança que impede que um Server Encryption seja implementado em outros ambientes de servidor que não sejam compatíveis com ele. Para desativar a necessidade de credenciais do administrador do domínio, consulte Antes de começar.

6 O DDP Server verifica as credenciais no vault empresarial (Active Directory ou equivalente) para confirmar que as credenciais sejam do administrador do domínio.

7 Um UPN é construído usando as credenciais.

8 Com o UPN, um DDP Server cria uma nova conta de usuário para o usuário de servidor virtual, e armazena as credenciais no vault do DDP Server.

A **conta de usuário de servidor virtual** é para uso exclusivo do cliente Encryption. Ela será usada para autenticar com o servidor, para lidar com chaves de criptografia comuns e para receber atualizações de política.

> **NOTA:**
> A autenticação DPAPI e de senha são desativadas para esta conta de forma que *somente* o usuário do servidor virtual possa acessar as chaves de criptografia no computador. Esta conta não corresponde a nenhuma outra conta de usuário no computador ou no domínio.

9 Quando a ativação for bem-sucedida, o usuário reinicia o computador, que dá início à segunda parte da ativação, a autenticação e a ativação do dispositivo.

Solucionar problemas de autenticação e ativação do dispositivo

A ativação do dispositivo falha quando:

- A ativação inicial falhou.
- Não foi possível estabelecer uma conexão com o servidor.
- Não foi possível validar o certificado de confiança.

Depois da ativação, quando o computador é reiniciado, o Server Encryption faz login automaticamente como o usuário do servidor virtual, solicitando a chave Computador do DDP Enterprise Server. Isso ocorre mesmo antes de qualquer usuário poder fazer login.

- Abra a caixa de diálogo Sobre para confirmar que o Server Encryption está autenticado e no modo Servidor.
- Se o Shield ID estiver vermelho, a criptografia ainda não foi ativada.
- No Remote Management Console, a versão de um servidor com o Server Encryption instalado é listada como *Shield para Server*.
- Se a obtenção da chave Computador falhar devido a um problema de rede, o Server Encryption se registrará para notificações de rede com o sistema operacional.
- Se a obtenção da chave Computador falhar:
  - O login de usuário do servidor virtual ainda ocorrerá satisfatoriamente.
  - Configure a política *Intervalo de nova tentativa após falha de rede* para realizar tentativas de obtenção de chave em um intervalo programado.

    Consulte AdminHelp, disponível no Remote Management Console, para obter detalhes sobre a política *Intervalo de nova tentativa após falha*.

Processo de autenticação e ativação do dispositivo

O diagrama a seguir ilustra a ativação do dispositivo e autenticação bem-sucedida.

1 Quando reinicializado após uma ativação inicial bem-sucedida, um computador com Server Encryption autentica automaticamente usando a conta de usuário de servidor virtual e executa o cliente Encryption no modo de servidor.

2 O computador verifica seu estado de ativação do dispositivo com o DDP Server:

- Se o computador não tiver sido previamente ativado no dispositivo, o DDP Server atribui ao computador um MCID, um DCID e um certificado de confiança, e armazena todas as informações no vault do DDP Server.

- Se o computador tiver sido previamente ativado pelo dispositivo, o DDP Server verifica o certificado de confiança.

3 Depois que o DDP Server atribui o certificado de confiança ao servidor, ele pode acessar suas chaves de criptografia.

4 A ativação do dispositivo ocorre com sucesso.

> **NOTA:**
> Quando o cliente Encryption está sendo executado no modo de servidor, ele precisa ter acesso ao mesmo certificado usado para a ativação do dispositivo para acessar as chaves de criptografia.

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

Saída	Significado
	Rijndael 256
	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.

Solução de problemas do cliente do Advanced Threat Prevention

Encontrar o código do produto com o Windows PowerShell

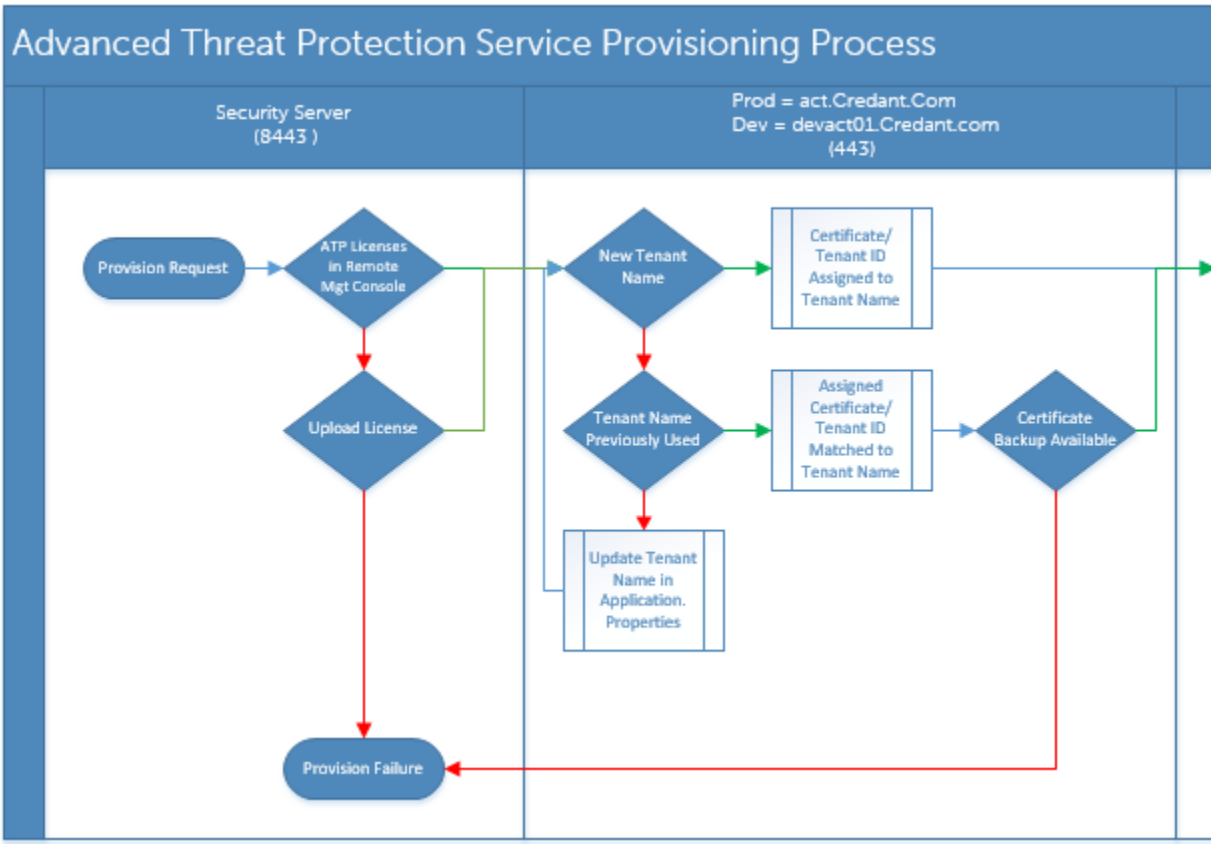
- Você pode identificar facilmente o código do produto, se ele mudar no futuro, usando este método.

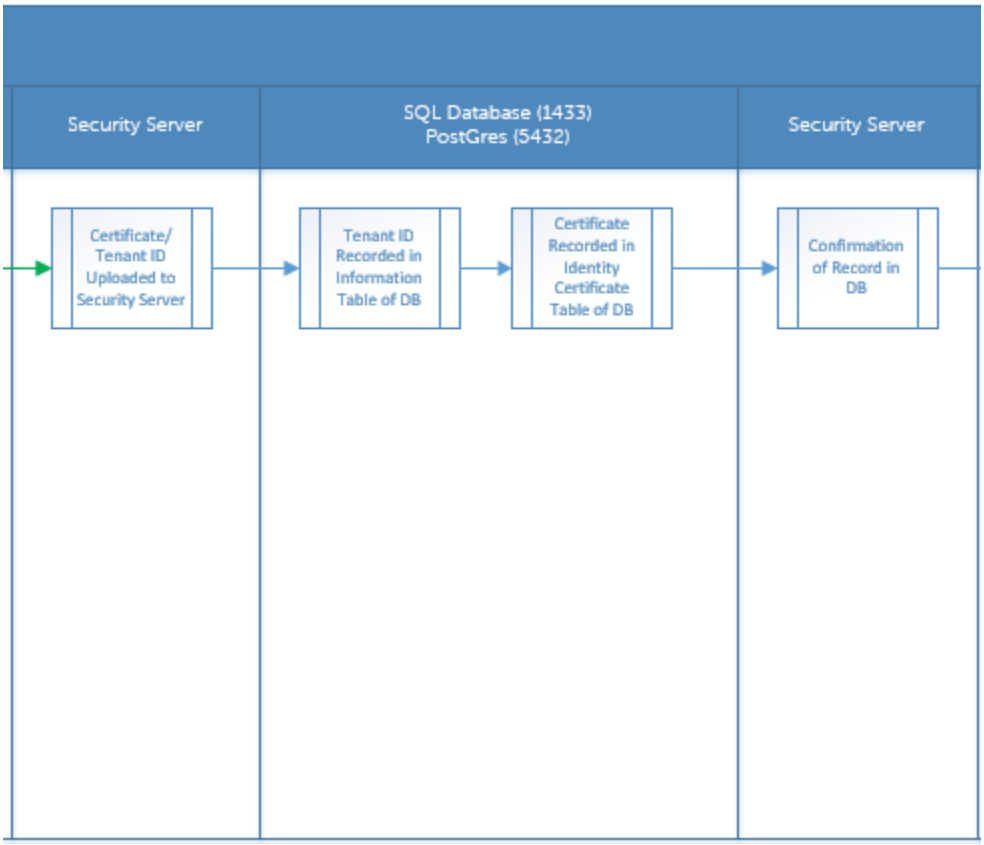
  ```
  Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT
  IdentifyingNumber, Name, LocalPackage
  ```

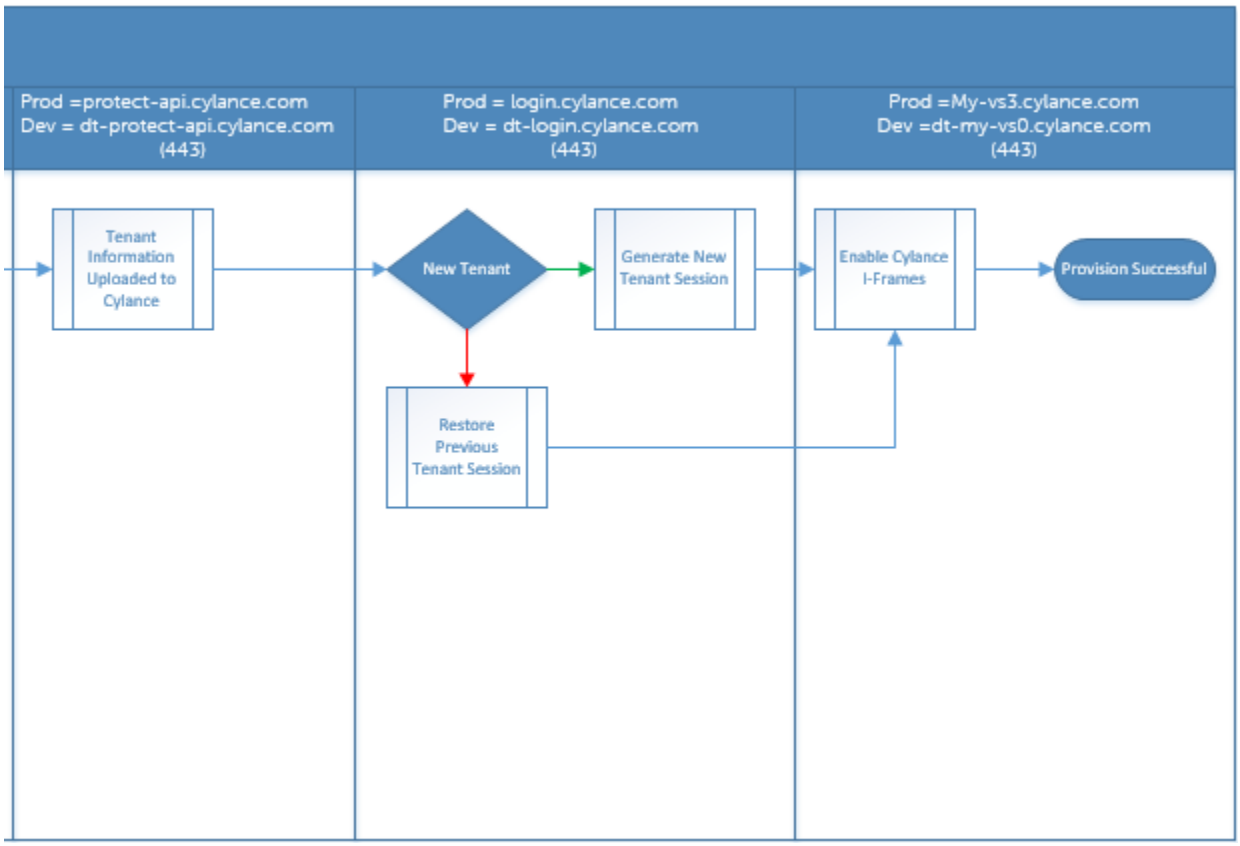
  O resultado será o caminho inteiro e o nome do arquivo .msi (o nome hexadecimal do arquivo convertido).

Provisionamento do Advanced Threat Prevention e comunicação do agente

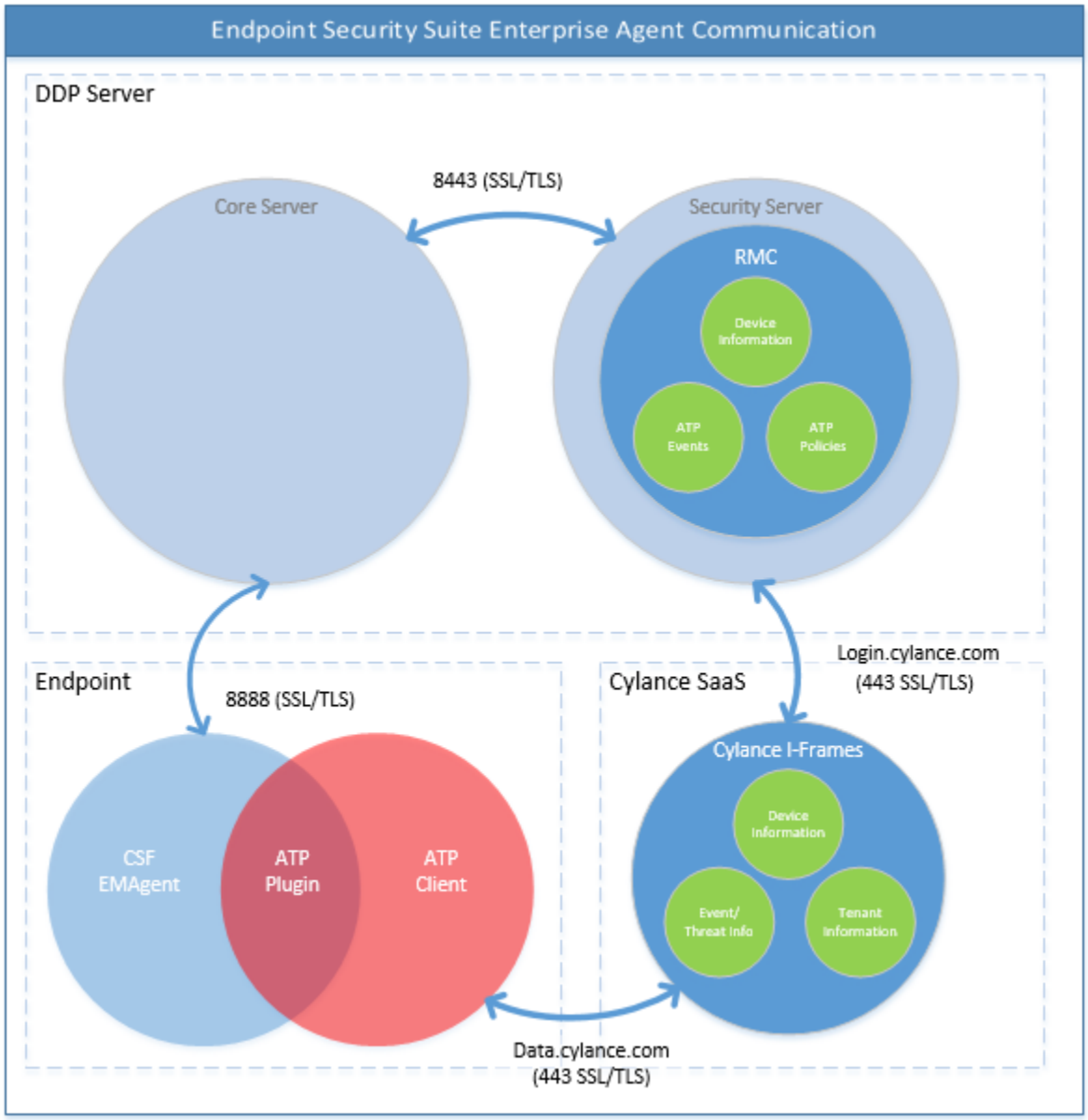
Os diagramas a seguir ilustram o processo de provisionamento do serviço Advanced Threat Prevention.





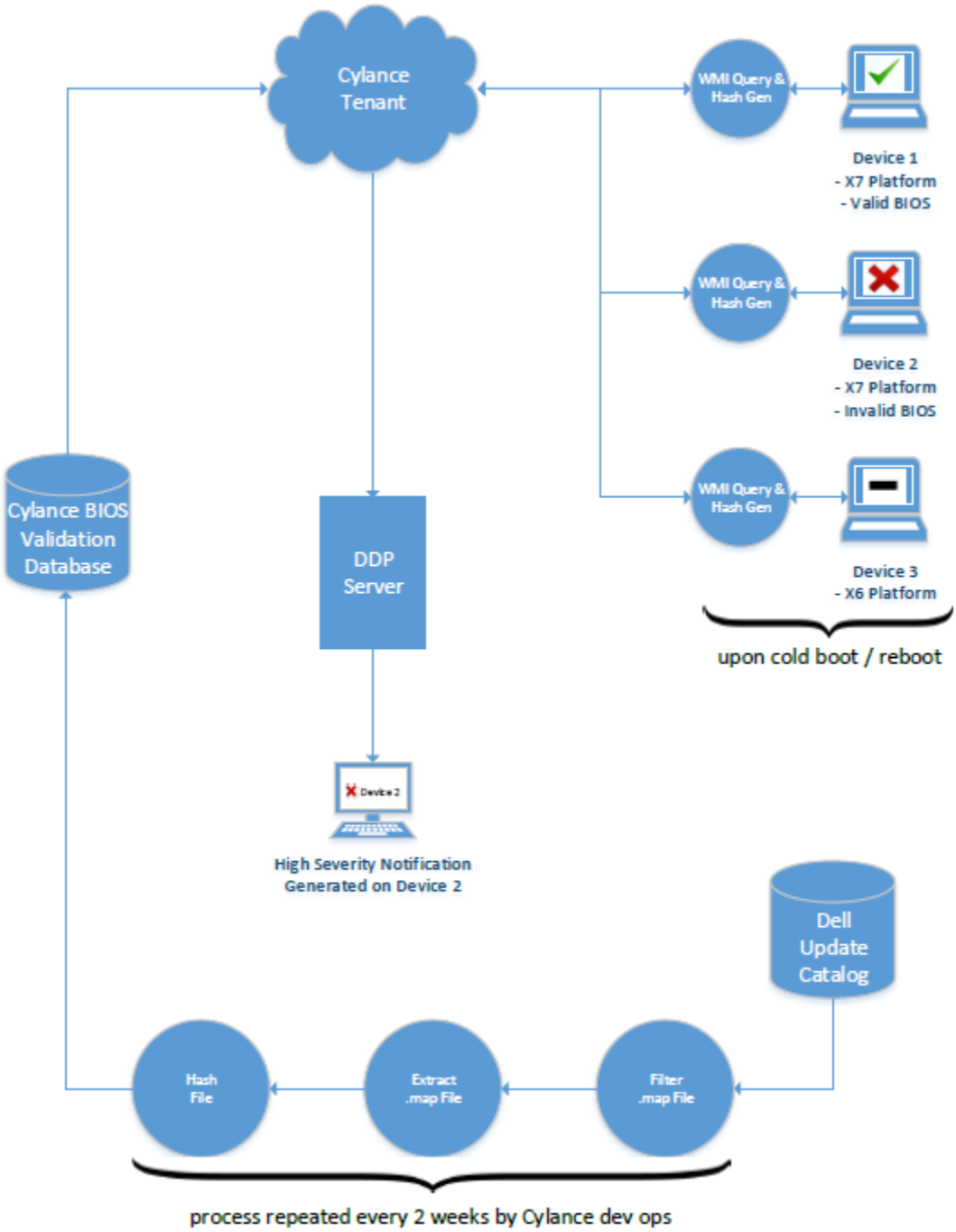


O diagrama a seguir ilustra o processo de comunicação do agente do Advanced Threat Prevention.



Processo de verificação de integridade da imagem do BIOS

O diagrama a seguir ilustra o processo de verificação de integridade da imagem do BIOS. Para obter uma lista dos modelos de computador Dell compatíveis com a verificação de integridade da imagem do BIOS, consulte Requisitos - Verificação de integridade da imagem do BIOS.



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.

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.

Advanced Threat Prevention – O produto Advanced Threat Prevention é a proteção antivírus de última geração que usa aprendizado automatizado e ciência de algoritmos para identificar, classificar e impedir que ameaças virtuais conhecidas e desconhecidas sejam executadas ou comprometam endpoints. O recurso opcional Client Firewall monitora a comunicação entre o computador e os recursos na rede e na Internet, interceptando comunicações potencialmente maliciosas. O recurso opcional Proteção na web bloqueia sites perigosos e os downloads desses sites ao navegar e fazer pesquisas on-line, com base em classificações de segurança e relatórios de sites.

BitLocker Manager – O Windows BitLocker foi projetado para ajudar a proteger computadores Windows ao criptografar os dados e os arquivos do sistema operacional. Para melhorar a segurança das implantações do BitLocker e simplificar e reduzir o custo de propriedade, a Dell fornece um console de gerenciamento único e central que trata de muitas preocupações de segurança e oferece uma abordagem integrada para gerenciar a criptografia em outras plataformas diferentes do BitLocker, sejam elas físicas, virtuais ou na nuvem. O BitLocker Manager oferece suporte para criptografia por BitLocker para sistemas operacionais, unidades fixas e BitLocker To Go. O BitLocker Manager permite que você integre perfeitamente o BitLocker às suas necessidades de criptografia existentes e gerencie o BitLocker com mínimo esforço ao mesmo tempo em que aperfeiçoa a segurança e a conformidade. O BitLocker Manager fornece gerenciamento integrado para recuperação de chaves, gerenciamento e imposição de políticas, gerenciamento de TPM automatizado, conformidade FIPS e relatórios de conformidade.

Desativar - A desativação ocorre quando o gerenciamento de SED é definido como Desligado no Remote Management Console. Quando o computador é desativado, o banco de dados de PBA é removido, e não haverá mais nenhum registro de usuário em cache.

EMS - External Media Shield - Esse serviço do cliente Dell Encryption aplica políticas à mídia removível e aos dispositivos de armazenamento externo.

Código de acesso do EMS - Esse serviço do Dell Enterprise Server/VE permite a recuperação de dispositivos protegidos pelo External Media Shield em que o usuário se esquece da senha e não consegue mais fazer login. A conclusão desse processo permite ao usuário redefinir a senha configurada na mídia removível ou dispositivo de armazenamento externo.

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.

Ponto de extremidade - um computador ou dispositivo de hardware móvel que é gerenciado pelo Dell Enterprise Server/VE.

Limpeza de criptografia – Uma limpeza de criptografia é o processo de verificar as pastas a serem criptografadas em um ponto de extremidade gerenciado 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 limpeza. 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.

SED Management – O SED Management fornece uma plataforma para gerenciar com segurança as SEDs (self-encrypting drives, unidades de criptografia automática). Embora as SEDs forneçam sua própria criptografia, elas carecem de uma plataforma para gerenciar a criptografia e as políticas disponíveis. O SED Management é um componente central e escalonável de gerenciamento, que permite proteger e gerenciar seus dados com mais eficácia. O SED Management garante que você possa administrar sua empresa de forma mais rápida e descomplicada.

Usuário de servidor – Uma conta de usuário virtual criada pelo Dell Server Encryption com o objetivo de processar chaves de criptografia e atualizações de política. Essa conta de usuário não corresponde a nenhuma outra no computador nem no domínio e não tem nome de usuário ou senha que podem ser usados fisicamente. A conta recebe um valor de UCID exclusivo no Remote Management Console do Dell Enterprise Server/VE.