Endpoint Security Suite Enterprise

Guia de instalação básica v2.1

Notas, avisos e advertências

NOTA: Uma NOTA indica informações importantes que ajudam a melhorar a utilização do produto.

AVISO: Um AVISO indica potenciais danos do hardware ou a perda de dados e explica como evitar o problema.

ADVERTÊNCIA: Uma ADVERTÊNCIA indica potenciais danos no equipamento, lesões pessoais ou mesmo morte.

2018 - 11

Rev. A01

Índice

1 Introdução 6
- Antes de começar 6
- Utilizar este guia 6
- Contacte o Dell ProSupport 6

2 Requisitos 7
- Todos os clientes 7
  - Todos os clientes - Pré-requisitos 7
  - Todos os clientes - Hardware 7
  - Todos os clientes - Localização 8
- Cliente Encryption 8
  - Pré-requisitos do Encryption Client 8
  - Sistemas operativos do Encryption Client 8
  - Sistemas operativos do Encryption Client com ativação diferida 9
  - Sistemas operativos do Encryption External Media 9
- Full Disk Encryption 10
  - Pré-requisitos do cliente da Full Disk Encryption 10
  - Hardware do cliente da Full Disk Encryption 11
  - Sistemas operativos do cliente da Full Disk Encryption 11
- Cliente Advanced Threat Prevention 11
  - Sistemas operativos do Advanced Threat Prevention 11
  - Portas do Advanced Threat Prevention 12
  - Verificação da integridade de imagem do BIOS 12
- Client Firewall e Web Protection Client 13
  - Sistemas operativos de Client Firewall e Web Protection Client 13
  - Portas do Client Firewall e Web Protection Client 13
- Cliente SED 13
  - Hardware do cliente SED 15
  - Teclados internacionais do cliente SEDLocalização do cliente SEDSistemas operativos do cliente SED 15
- Cliente BitLocker Manager 16
  - Hardware do cliente BitLocker Manager 16
  - Sistemas operativos do cliente BitLocker Manager 16

3 Instalar utilizando o instalador principal 18
- Instalar interativamente utilizando o instalador principal 18
- Instalar por linha de comandos utilizando o instalador principal 19

4 Desinstalar o instalador principal 22
- Desinstalar o instalador principal do Endpoint Security Suite Enterprise 22
  - Desinstalação por linha de comando 22

5 Desinstalar utilizando os instaladores subordinados 23
- Desinstalar o Encryption e o Server Encryption Client 24

Processo....24
Desinstalação por linha de comando....24
Desinstalar o Advanced Threat Prevention....26
Desinstalação por linha de comando....26
Desinstalar o cliente SED....26
Processo....26
Desativar a PBA....26
Desinstalar o cliente SED....27
Desinstalar o cliente BitLocker Manager....27
Desinstalação por linha de comando....27

6 Desinstalador do Data Security....28
Desinstalar Endpoint Security Suite Enterprise....28

7 Configurar um inquilino....29
Configurar um inquilino....29

8 Configurar a atualização automática do Advanced Threat Prevention....30

9 Extrair os instaladores subordinados....31

10 Configurar o Key Server....32
Painel de Serviços - Adicionar utilizador da conta do domínio....32
Ficheiro de configuração do Key Server - Adicionar utilizador para comunicação com o Security Management Server....32
Painel de Serviços - Reiniciar o serviço Key Server....33
Management Console - Adicionar administrador forense....33

11 Utilizar o Administrative Download Utility (CMGAd)....34
Utilize o Administrative Download Utility no Modo forense....34
Utilize o Administrative Download Utility no Modo de administrador....35

12 Resolução de problemas....36
Todos os clientes - Resolução de problemas....36
Todos os clientes - Estado de Proteção....36
Resolução de problemas do Encryption e do Server Encryption Client....36
Atualização para o Windows 10 Creators Update....36
Ativação num sistema operativo de servidor....37
Interações de PCS e Encryption External Media....39
Utilizar o WSScan....39
Verificar o estado do Encryption Removal Agent....41
Resolução de problemas do cliente Advanced Threat Prevention....42
Encontrar o código do produto com o Windows PowerShell....42
Aprovisionamento e comunicação do agente do Advanced Threat Prevention....42
Processo de verificação da integridade de imagem do BIOS....44
Controladores do Dell ControlVault....45
Atualização de controladores e firmware do Dell ControlVault....45

13 Glossário..... 48

1

Introdução

Este guia explica como instalar e configurar a aplicação utilizando o instalador principal do Endpoint Security Suite Enterprise. Este guia proporciona assistência de instalação básica. Consulte o *Guia de instalação avançada* caso necessite de informações sobre a instalação dos instaladores subordinados, a configuração do Security Management Server/Security Management Server Virtual ou informações além da assistência básica com o instalador principal do Endpoint Security Suite Enterprise.

Todas as informações sobre políticas e as respetivas descrições podem ser encontradas em AdminHelp.

Antes de começar

1 Instale o Dell Server antes de implementar os clientes. Localize o guia correto como mostrado abaixo, siga as instruções e, em seguida, volte a este guia.

- *Security Management Server Installation and Migration Guide (Guia de instalação e migração do Security Management Server)*
- *Security Management Server Virtual Quick Start Guide and Installation Guide (Guia de instalação e guia de início rápido do Security Management Server Virtual)*
- Certifique-se de que as políticas foram definidas da forma pretendida. Navegue no AdminHelp, disponível através de **?** no canto superior direito do ecrã. O AdminHelp é uma ajuda ao nível da página concebida para o ajudar a definir e modificar a política e a compreender as suas opções relativamente ao seu Dell Server.

2 Aprovisionar um inquilino para o Advanced Threat Prevention. Deve ser aprovisionado um inquilino no Dell Server antes da ativação da aplicação de políticas do Advanced Threat Prevention.

3 Leia atentamente o capítulo Requisitos deste documento.

4 Implemente os clientes para utilizadores.

Utilizar este guia

Utilize este guia pela seguinte ordem.

- Consulte Requisitos para obter informações sobre os pré-requisitos do cliente.
- Selecione uma das seguintes ações:
  - Instalar interativamente utilizando o instalador principal

    ou
  - Instalar por linha de comandos utilizando o instalador principal

Contacte o Dell ProSupport

Contacte o número 877-459-7304, extensão 4310039 para obter suporte telefónico permanente (24 x 7) para o seu produto Dell.

Adicionalmente, o suporte online para os produtos Dell encontra-se disponível em dell.com/support. O suporte online inclui controladores, manuais, conselhos técnicos, FAQ e problemas emergentes.

Ajude-nos a garantir que o direcionamos rapidamente para o especialista técnico mais indicado para si tendo o seu Código de serviço ou Código de serviço expresso disponível quando nos contactar.

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

2

Requisitos

Todos os clientes

- Durante a implementação, devem ser seguidas as melhores práticas de TI. Estas incluem, entre outras, ambientes de teste controlados para os testes iniciais e a implementação progressiva para os utilizadores.
- A conta de utilizador que realiza a instalação/atualização/desinstalação deve ser um utilizador administrador local ou de domínio, o qual pode ser atribuído temporariamente por uma ferramenta de implementação, como o Microsoft SCCM ou Quest KACE. Não são suportados utilizadores não administradores com privilégios elevados.
- Realize uma cópia de segurança de todos os dados importantes antes de iniciar a instalação/desinstalação.
- Não realize alterações no computador, incluindo inserir ou remover unidades externas (USB) durante a instalação.
- Os administradores devem assegurar a disponibilidade de todas as portas necessárias.
- Assegure-se de verificar periodicamente a página www.dell.com/support para procurar a documentação mais atual e Conselhos técnicos.
- **NOTA: A linha de produtos Dell Data Security não é compatível com as versões do Windows Insider Preview.**

Todos os clientes - Pré-requisitos

- O instalador principal instala os seguintes pré-requisitos se ainda não estiverem instalados no computador.

Pré-requisito
– Visual C++ 2012 Update 4 ou Redistributable Package posterior (x86 e x64)
– Visual C++ 2015 Update 3 ou Redistributable Package posterior (x86 e x64)

O Visual C++ 2015 requer o Windows Update KB2999226, ao instalar no Windows 7.

É necessário o Microsoft .Net Framework 4.5.2 (ou posterior) para os clientes de instalador principal e de instalador subordinado do Endpoint Security Suite Enterprise . O instalador *não* instala o componente Microsoft .Net Framework.

Para verificar a versão instalada do Microsoft .Net, siga estas instruções no computador onde pretende efetuar a instalação: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Para instalar o Microsoft .Net Framework 4.5.2, aceda a https://www.microsoft.com/en-us/download/details.aspx?id=42643.

Todos os clientes - Hardware

- A tabela seguinte apresenta o hardware de computador mínimo suportado.

Hardware
– Processador Intel Pentium ou AMD
– 500 MB de espaço livre em disco
– 2 GB de RAM

NOTA: É necessário espaço livre em disco adicional para encriptar os ficheiros no ponto final. Este tamanho varia de acordo com as políticas e do tamanho da unidade.

Todos os clientes - Localização

- Os clientes Encryption, Advanced Threat Prevention e BitLocker Manager estão em conformidade com a norma MUI (Multilingual User Interface - Interface de utilizador multilíngue) e estão localizados nos seguintes idiomas. O Full Disk Encryption só é suportado com sistemas operativos em inglês. Os dados do Advanced Threat Prevention apresentados na Management Console apenas estão disponíveis em inglês.

Suporte de idiomas

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

Cliente Encryption

- O computador cliente deve ter conectividade de rede para ativar.
- Desative o modo de suspensão durante o varrimento de encriptação inicial para impedir a suspensão do computador caso este se encontre sem supervisão. A encriptação não é possível num computador em suspensão (tal como não é possível a desencriptação).
- O cliente Encryption não suporta configurações de duplo arranque, uma vez que é possível encriptar ficheiros de sistema do outro sistema operativo, o que poderia interferir com o respetivo funcionamento.
- O cliente de encriptação é validado face a fornecedores de antivírus líderes do sector. Existem exclusões implementadas para estes fornecedores de produtos anti-vírus, para evitar incompatibilidades entre a monitorização anti-vírus e a encriptação. O cliente Encryption foi também testado com o Microsoft Enhanced Mitigation Experience Toolkit.

  Se a sua organização utilizar um antivírus de um fornecedor não indicado na lista, consulte http://www.dell.com/support/article/us/en/19/SLN288353/ ou contacte o Dell ProSupport para obter assistência.
- Não são suportadas reinstalações de sistema operativo no local. Para realizar a reinstalação do sistema operativo, faça uma cópia de segurança do computador em questão, realize a limpeza do computador, instale o sistema operativo e, em seguida, realize a recuperação dos dados encriptados seguindo os procedimentos de recuperação estabelecidos.

Pré-requisitos do Encryption Client

Sistemas operativos do Encryption Client

- A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos Windows (32 e 64 bits)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 com modelo de compatibilidade de aplicações
- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10: Education, Enterprise, Pro Version 1607 (Atualização de Aniversário/Redstone 1) até à versão 1803 (Atualização de abril de 2018/Redstone 4)

Sistemas operativos Windows (32 e 64 bits)

- VMware Workstation 12.5 e posterior

NOTA:
Ao utilizar o modo UEFI, a política de hibernação segura não é suportada.

Sistemas operativos do Encryption Client com ativação diferida

- A ativação diferida permite que a conta de utilizador do Active Directory utilizada durante a ativação seja independente da conta utilizada para iniciar sessão no endpoint. Em vez de o fornecedor de serviços de rede capturar as informações de autenticação, o utilizador especifica a conta baseada no Active Directory manualmente quando solicitado. Depois de serem introduzidas as credenciais, a informação de autenticação é enviada de uma forma segura para o Dell Server que a valida relativamente aos domínios do Active Directory configurados. Para obter mais informações, consulte http://www.dell.com/support/article/us/en/19/sln306341.
- A tabela seguinte apresenta os sistemas operativos suportados com ativação diferida.

Sistemas operativos Windows (32 e 64 bits)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 com modelo de compatibilidade de aplicações
- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10: Education, Enterprise, Pro Version 1607 (Atualização de Aniversário/Redstone 1) até à versão 1803 (Atualização de abril de 2018/Redstone 4)

Sistemas operativos do Encryption External Media

- A tabela seguinte indica os sistemas operativos compatíveis ao aceder a suportes de dados protegidos pelo Encryption External Media.

NOTA:
O suporte de dados externo tem de ter aproximadamente 55 MB disponíveis, bem como espaço livre no suporte de dados igual ao maior ficheiro a encriptar para alojar o Encryption External Media.

Sistemas operativos Windows compatíveis para aceder a suportes de dados protegidos pelo Encryption External Media (32 e 64 bits)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows Embedded Standard 7 com modelo de compatibilidade de aplicações
- Windows 8: Enterprise, Pro
- Windows 8.1: Enterprise, Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10: Education, Enterprise, Pro Version 1607 (Atualização de Aniversário/Redstone 1) até à versão 1803 (Atualização de abril de 2018/Redstone 4)

Sistemas operativos Mac compatíveis para aceder a suportes de dados protegidos pelo Encryption External Media (kernels de 64 bits)

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 – 10.13.6
- macOS Mojave 10.14

Full Disk Encryption

A Full Disk Encryption **apenas** pode ser instalada através da interface da linha de comandos (CLI). Se pretender instalar a Full Disk Encryption, transfira o Guia de instalação avançada do Endpoint Security Suite Enterprise para obter instruções.

- A Full Disk Encryption requer ativação num Dell Server de versão v9.8.2 ou posterior.
- Atualmente, a Full Disk Encryption não é suportada em computadores do sistema anfitrião virtualizado.
- As encriptações Full Disk Encryption de configurações de várias unidades não são suportadas.
- Os fornecedores de credenciais externos não funcionarão com funcionalidades FDE instaladas e todos serão desativados quando a PBA for ativada.
- O computador cliente deve ter conectividade de rede ou um código de acesso para ativar.
- O computador tem de possuir uma ligação de rede com fios para que um utilizador de smart card possa iniciar sessão através da Autenticação de pré-arranque pela primeira vez.
- As atualizações de funcionalidades do sistema operativo não são suportadas com o Full Disk Encryption.
- É necessária uma ligação com fios para que a PBA comunique com o Dell Server.
- Não pode estar presente um SED no computador de destino.
- A Full Disk Encryption não é compatível com o BitLocker ou o BitLocker Manager. Não instale a Full Disk Encryption num computador que tenha o BitLocker ou o BitLocker Manager instalado.
- Qualquer unidade NVMe que esteja a ser utilizada para PBA - O modo de funcionamento SATA do BIOS tem de ser definido para RAID ON, uma vez que a gestão de PBA da Dell não é compatível com AHCI nas unidades NVMe.
- Qualquer unidade NVMe que esteja a ser utilizada para PBA - O modo de arranque do BIOS tem de ser UEFI e as ROM de opção de legado têm de estar desativadas.
- Qualquer unidade não-NVMe que esteja a ser utilizada para PBA - O modo de funcionamento SATA do BIOS tem de ser definido para AHCI, uma vez que a gestão de PBA da Dell não é compatível com o RAID nas unidades não-NVMe.
  - O modo RAID ligado não é suportado, porque o acesso de leitura e escrita de dados relacionados com RAID (num setor que não esteja disponível numa unidade não-NVMe bloqueada) não está acessível durante o arranque e não poderá aguardar para ler estes dados até o utilizador ter iniciado sessão.
  - O sistema operativo falhará quando alterado de RAID ligado > AHCI, se os controladores do AHCI não estiverem pré-instalados. Para obter instruções sobre como alterar de RAID > AHCI (ou vice-versa), consulte http://www.dell.com/support/article/us/en/19/SLN306460.

    A Dell recomenda a versão 15.2.0.0 ou posterior do controlador Intel Rapid Storage Technology, com unidades NVMe.
- Desative o modo de suspensão durante o varrimento de encriptação inicial para impedir a suspensão do computador caso este se encontre sem supervisão. A encriptação não é possível num computador em suspensão (tal como não é possível a desencriptação).
- O cliente da Full Disk Encryption não é compatível com configurações de duplo arranque, uma vez que é possível encriptar ficheiros de sistema do outro sistema operativo, o que poderia interferir com o respetivo funcionamento.
- Não são suportadas reinstalações de sistema operativo no local. Para realizar a reinstalação do sistema operativo, faça uma cópia de segurança do computador em questão, realize a limpeza do computador, instale o sistema operativo e, em seguida, realize a recuperação dos dados encriptados seguindo os procedimentos de recuperação estabelecidos.
- **NOTA: É necessária uma palavra-passe com Autenticação de pré-arranque. A Dell recomenda a definição de um comprimento mínimo da palavra-passe, de acordo com as políticas de segurança internas.**

NOTA: A Full Disk Encryption deve ser configurada com os algoritmos de encriptação definidos como AES 256 e o modo de encriptação definido como CBC.

Pré-requisitos do cliente da Full Disk Encryption

- É necessário o Microsoft .Net Framework 4.5.2 (ou posterior) O instalador *não* instala o componente Microsoft .Net Framework.

Para verificar a versão instalada do Microsoft .Net, siga estas instruções no computador onde pretende efetuar a instalação: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Para instalar o Microsoft .Net Framework 4.5.2, aceda a https://www.microsoft.com/en-us/download/details.aspx?id=42643.

Hardware do cliente da Full Disk Encryption

- A tabela seguinte indica o hardware suportado.

Hardware opcional incorporado
– TPM 1.2 ou 2.0

Sistemas operativos do cliente da Full Disk Encryption

- A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos Windows (64 bits)
– Windows 7 SP1: Enterprise, Professional, Ultimate (modo de arranque Legacy necessário)
– Windows 10: Education, Enterprise, Pro Version 1607 (Atualização de Aniversário/Redstone 1) até à versão 1803 (Atualização de abril de 2018/Redstone 4) (modo de arranque UEFI necessário)

Cliente Advanced Threat Prevention

- Para concluir a instalação do Advanced Threat Prevention, quando o Dell Server que gere o cliente estiver em execução no Modo ligado (predefinido), o computador tem de estar ligado à rede. No entanto, ***não*** é necessário haver ligação à rede durante a instalação do Advanced Threat Prevention quando o Dell Server que gere está em execução no modo Desligado.
- Para configurar um inquilino para o Advanced Threat Prevention, o Dell Server tem de estar ligado à Internet.
- As funcionalidades opcionais de Client Firewall e Proteção Web ***não*** devem ser instaladas nos computadores cliente que são geridos pelo Dell Server em execução no modo Desligado.
- As aplicações de antivírus, antimalware e antispyware de outros fabricantes podem entrar em conflito com o cliente Advanced Threat Prevention. Desinstale estas aplicações, se possível. O software passível de originar conflitos não inclui o Windows Defender. São permitidas aplicações de firewall.

  Se não for possível desinstalar outras aplicações de antivírus, antimalware e antispyware, tem de adicionar exclusões ao Advanced Threat Prevention no Dell Server e às outras aplicações. Para obter instruções sobre como adicionar exclusões ao Advanced Threat Prevention no Dell Server, consulte http://www.dell.com/support/article/us/en/04/SLN300970. Para obter uma lista de exclusões a adicionar às outras aplicações de antivírus, consulte http://www.dell.com/support/article/us/en/04/sln301562.

Sistemas operativos do Advanced Threat Prevention

- A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos Windows (32 e 64 bits)
– Windows 7 SP1: Enterprise, Professional, Ultimate
– Windows Embedded Standard 7
– Windows 8: Enterprise, Pro

Sistemas operativos Windows (32 e 64 bits)

- Windows 8.1: Enterprise, Pro
- Windows 10: Education, Enterprise, Pro Version 1607 (Atualização de Aniversário/Redstone 1) até à versão 1803 (Atualização de abril de 2018/Redstone 4)
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016

Portas do Advanced Threat Prevention

- Os agentes do Advanced Threat Prevention são geridos por e informam a plataforma SaaS da consola de gestão. A porta 443 (https) é utilizada para comunicação e deve estar aberta na firewall para que os agentes comuniquem com a consola. A consola é alojada por Amazon Web Services e não tem quaisquer IP fixos. Se, por qualquer motivo, a porta 443 estiver bloqueada, não é possível transferir as atualizações, pelo que os computadores poderão não dispor da proteção mais recente. Certifique-se de que os computadores cliente conseguem aceder aos URL, da seguinte forma.

Utilizar	Protocolo de aplicação	Protocolo de transporte	Número da porta	Destino	Direção
Todas as comunicações	HTTPS	TCP	443	Todo o tráfego https para *.cylance.com	Porta de saída

Para obter informações detalhadas sobre os URL que estão a ser utilizados, consulte: http://www.dell.com/support/article/us/en/19/SLN303898

Verificação da integridade de imagem do BIOS

Se a política *Ativar a garantia do BIOS* for selecionada na Management Console, o inquilino Cylance valida o hash do BIOS nos computadores de endpoint para assegurar que o BIOS não foi modificado face à versão de fábrica da Dell, o qual é um possível vetor de ataques. Se for detetada uma ameaça, é transmitida uma notificação para o Dell Server e o administrador de TI é alertado na Management Console. Para uma descrição geral do processo, consulte Processo de verificação da integridade de imagem do BIOS.

NOTA: Não é possível utilizar uma imagem de fábrica personalizada com esta funcionalidade, uma vez que o BIOS foi modificado.

Modelos de computador Dell suportados pela Verificação da integridade de 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
- Estação de trabalho móvel Precision 3510
- Estação de trabalho móvel Precision 5510
- Estação de trabalho Precision 3620
- Estação de trabalho Precision 7510
- Estação de trabalho Precision 7710
- Estação de trabalho Precision T3420
- Venue 10 Pro 5056
- Venue Pro 5855
- XPS 12 9250
- XPS 13 9350
- XPS 9550

Client Firewall e Web Protection Client

- Para instalar o Client Firewall e o Web Protection com êxito, o computador deve ter ligação à rede.
- Antes de instalar o Client Firewall e o Web Protection Client, elimine as aplicações antivírus, antimalware, anti-spyware e de firewall de outros fornecedores para evitar falhas na instalação. O software passível de originar conflitos não inclui o Windows Defender e o Endpoint Security Suite Enterprise.
- A funcionalidade de Proteção Web é suportada apenas no Internet Explorer.

Sistemas operativos de Client Firewall e Web Protection Client

- A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos Windows (32 e 64 bits)
– Windows 7 SP1: Enterprise, Professional, Ultimate
– Windows 8: Enterprise, Pro
– Windows 8.1: Enterprise, Pro
– Windows 10: Education, Enterprise, Pro Version 1607 (Atualização de Aniversário/Redstone 1) até à versão 1803 (Atualização de abril de 2018/Redstone 4)

Portas do Client Firewall e Web Protection Client

- Para se certificar de que o Client Firewall e o Web Protection Client recebem as mais recentes atualizações do Client Firewall e Web Protection, as portas 443 e 80 devem estar disponíveis para comunicar com os vários servidores de destino. Se, por qualquer motivo, as portas estiverem bloqueadas, as atualizações da assinatura antivírus (ficheiros DAT) não poderão ser transferidas, pelo que os computadores poderão não dispor da proteção mais recente. Certifique-se de que os computadores cliente conseguem aceder aos URL, da seguinte forma.

Utilizar	Protocolo de aplicação	Protocolo de transporte	Número da porta	Destino	Direção	Notas
Serviço de reputação	SSL	TCP	443	tunnel.web.trustedsource.org	Porta de saída	
Feedback do serviço de reputação	SSL	TCP	443	gtifeedback.trustedsource.org	Porta de saída	
Atualização da base de dados de reputação de URL	HTTP	TCP	80	list.smartfilter.com	Porta de saída	
Pesquisa de reputação do URL	SSL	TCP	443	tunnel.web.trustedsource.org	Porta de saída	

Cliente SED

- Para instalar a gestão SED com êxito, o computador deve possuir uma ligação à rede com fios.
- O computador tem de possuir uma ligação de rede com fios para que um utilizador de smart card possa iniciar sessão através da Autenticação de pré-arranque pela primeira vez.
- Os fornecedores de credenciais externos não funcionarão com o SED Management instalado e todos serão desativados quando a PBA for ativada.

- O IPv6 não é suportado.
- O SED Manager não é suportado com configurações de várias unidades.
- Atualmente, o SED Manager não é suportado em computadores do sistema anfitrião virtualizado.
- Prepare-se para encerrar e reiniciar o computador após aplicar as políticas e quando estiver pronto para começar a implementá-las.
- Os computadores equipados com unidades de encriptação automática não podem ser utilizados com placas HCA. Existem incompatibilidades que impedem o aprovisionamento do HCA. A Dell não vende computadores com unidades de encriptação automática compatíveis com o módulo HCA. Esta configuração não suportada seria uma configuração pós-venda.
- Se o computador destinado à encriptação estiver equipado com uma unidade de encriptação automática, certifique-se de que a opção do Active Directory, *O utilizador deve alterar a palavra-passe no próximo início de sessão*, está desativada. A Autenticação de pré-arranque não suporta esta opção do Active Directory.
- A Dell recomenda que não mude o método de autenticação depois de a PBA ter sido ativada. Se for necessário mudar para um método de autenticação diferente, deve:

  – Elimine todos os utilizadores da PBA.

  ou

  – Desative a PBA, altere o método de autenticação e, em seguida, volte a ativar a PBA.

  IMPORTANTE:

  Devido à natureza do RAID e SED, a gestão de SED não suporta RAID. O problema de *RAID=On* nas SED é que o RAID necessita de acesso ao disco para ler e gravar dados relacionados com o RAID num setor elevado não disponível numa SED bloqueada desde o arranque, e não pode esperar até o utilizador iniciar sessão para ler estes dados. Para solucionar este problema, altere a operação SATA no BIOS de *RAID=On* para *AHCI*. Se o sistema operativo não incluir controladores AHCI pré-instalados, o sistema operativo irá falhar quando alterar de *RAID=On* para *AHCI*.

- A configuração de unidades de encriptação automática para o SED Management da Dell difere entre unidades NVMe e não-NVMe (SATA), conforme se segue.

  – Qualquer unidade NVMe que esteja a ser utilizada como SED - O modo de funcionamento SATA do BIOS tem de ser definido para RAID ligado, uma vez que o SED Management da Dell não suporta o AHCI em unidades NVMe.

  – Qualquer unidade NVMe que esteja a ser utilizada como SED - O modo de arranque do BIOS tem de ser UEFI e as ROMs de opção de legado devem ser desativadas.

  – Qualquer unidade não-NVMe que esteja a ser utilizada como SED - O modo de funcionamento SATA do BIOS tem de ser definido para AHCI, uma vez que o SED Management da Dell não suporta o RAID com unidades não-NVMe.

    ◦ O modo RAID ligado não é suportado, porque o acesso de leitura e escrita de dados relacionados com RAID (num setor que não esteja disponível numa unidade não-NVMe bloqueada) não está acessível durante o arranque e não poderá aguardar para ler estes dados até o utilizador ter iniciado sessão.

    ◦ O sistema operativo falhará quando alterado de RAID ligado > AHCI, se os controladores do AHCI não estiverem pré-instalados. Para obter instruções sobre como alterar de RAID > AHCI (ou vice-versa), consulte http://www.dell.com/support/article/us/en/19/SLN306460.

  As SED compatíveis com OPAL suportadas requerem controladores Intel Rapid Storage Technology atualizados, localizados em http://www.dell.com/support. A Dell recomenda a versão 15.2.0.0 ou posterior do controlador Intel Rapid Storage Technology, com unidades NVMe.

  NOTA: Os controladores Intel Rapid Storage Technology dependem da plataforma. Pode encontrar o controlador do sistema na ligação acima consoante o modelo do computador.

- O SED Management não é suportado com o Server Encryption ou o Advanced Threat Prevention no sistema operativo de um servidor.
- **NOTA: É necessária uma palavra-passe com Autenticação de pré-arranque. A Dell recomenda a definição de um comprimento mínimo da palavra-passe, de acordo com as políticas de segurança internas.**

Hardware do cliente SED

Teclados internacionais do cliente SED

- A tabela que se segue indica teclados internacionais suportados com Autenticação de pré-arranque em computadores UEFI e não-UEFI.

Suporte de teclado internacional - UEFI

- DE-FR - Francês (Suíça)
- DE-CH - Alemão (Suíça)
- EN-US - Inglês (América)
- EN-GB - Inglês (Reino Unido)
- EN-CA - Inglês (Canadá)

Suporte de teclado internacional - Non-UEFI

- AR - Árabe (utilizando letras latinas)
- DE-FR - Francês (Suíça)
- DE-CH - Alemão (Suíça)
- EN-US - Inglês (América)
- EN-GB - Inglês (Reino Unido)
- EN-CA - Inglês (Canadá)

Localização do cliente SED

O cliente SED está em conformidade com a norma MUI (Interface de Utilizador Multilíngue) e está localizado nos seguintes idiomas. O modo UEFI e Autenticação de pré-arranque são suportados nos seguintes idiomas, **exceto** em russo, chinês tradicional ou chinês simplificado.

Suporte de idiomas

- EN - Inglês
- FR - Francês
- IT - Italiano
- DE - Alemão
- ES - Espanhol
- KO - Coreano
- ZH-CN - Chinês simplificado
- ZH-TW - Chinês tradicional/Taiwan
- PT-BR - Português, Brasil
- PT-PT - Português, Portugal (Ibérico)

Suporte de idiomas

- JA - Japonês
- RU - Russo

Sistemas operativos do cliente SED

- A tabela seguinte apresenta os sistemas operativos compatíveis.

Sistemas operativos Windows (32 e 64 bits)
– Windows 7 SP0-SP1: Enterprise, Professional, Ultimate (suportado com o modo de Arranque Legacy, mas não UEFI)
– Windows 8: Enterprise, Pro,
– Windows 8.1: Enterprise, Pro
– Windows 10: Education, Enterprise, Pro Version 1607 (Atualização de Aniversário/Redstone 1) até à versão 1803 (Atualização de abril de 2018/Redstone 4)

NOTA:
As unidades de encriptação automática NVMe não são suportadas no Windows 7.

Cliente BitLocker Manager

- Se o BitLocker ainda não tiver sido implementado no seu ambiente, pondere a revisão dos requisitos do Microsoft BitLocker,
- Certifique-se de que a partição de PBA já está configurada. Se o BitLocker Manager for instalado antes da configuração da partição de PBA, não é possível ativar o BitLocker e o BitLocker Manager não irá funcionar.
- É necessário um Dell Server para utilizar o BitLocker Manager.
- Certifique-se de que está disponível um certificado de assinatura na base de dados. Para obter mais informações, consulte http://www.dell.com/support/article/us/en/19/sln307028.
- O teclado, o rato e os componentes de vídeo devem estar ligados diretamente ao computador. Não utilize um comutador KVM para gerir periféricos, uma vez que o comutador KVM pode interferir com a capacidade do computador para identificar corretamente o hardware.
- Ligue e ative o TPM. O BitLocker Manager assume a propriedade do TPM e não necessita de reinício. No entanto, se um TPM já tiver um proprietário, o BitLocker Manager inicia o processo de configuração da encriptação (não é necessário o reinício). O importante é que o TPM tenha um proprietário e esteja ativo.
- O BitLocker Manager não é suportado com o Server Encryption ou o Advanced Threat Prevention no sistema operativo de um servidor.

Hardware do cliente BitLocker Manager

- A tabela seguinte indica o hardware suportado.

Hardware opcional incorporado
– TPM 1.2 ou 2.0

Sistemas operativos do cliente BitLocker Manager

- A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos Windows
– Windows 7 SP0-SP1: Enterprise, Ultimate (32 e 64 bits)
– Windows 8: Enterprise (64 bits)

Sistemas operativos Windows

- Windows 8.1: Enterprise Edition, Pro Edition (64 bits)
- Windows 10: Enterprise, Pro Version 1607 (Atualização de Aniversário/Redstone 1) até à versão 1803 (Atualização de abril de 2018/Redstone 4)
- Windows Server 2008 R2: Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2012 R2: Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2016

As atualizações do Windows KB3133977 e KB3125574 **não podem** estar instaladas, se instalar o BitLocker Manager no Windows 7.

3

Instalar utilizando o instalador principal

- As opções e parâmetros da linha de comandos são sensíveis a maiúsculas e minúsculas.
- Para instalar utilizando portas não predefinidas, utilize os instaladores subordinados em vez do instalador principal.
- Os ficheiros de registo do instalador principal do Endpoint Security Suite Enterprise encontram-se em **C:\ProgramData\Dell\Dell Data Protection\Installer.**
- Dê a instrução aos utilizadores para consultar o seguinte documento e ficheiros de ajuda para assistência de aplicação:
  - Consulte a *Dell Encrypt Help (Ajuda do Dell Encrypt)* para saber como utilizar a funcionalidade do Encryption Client. Aceda à ajuda a partir de **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help**.
  - Consulte a *Encryption External Media Help (Ajuda do Encryption External Media)* para saber como utilizar as funcionalidades do Encryption External Media. Aceda à ajuda a partir de **<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS**.
  - Consulte a *Ajuda do Endpoint Security Suite Enterprise* para saber como utilizar as funcionalidades do Advanced Threat Prevention. Aceda à ajuda a partir de **<Install dir>:\Program Files\Dell\Dell Data Protection\Client Security Framework\Help**.
- Após a conclusão da instalação, os utilizadores devem atualizar as respetivas políticas clicando com o botão direito do rato no ícone do Dell Encryption, na área de notificação e selecionando **Procurar atualizações de políticas**.
- O instalador principal instala todo o conjunto de produtos. Existem dois métodos para instalar utilizando o instalador principal. Escolha uma das seguintes opções.
  - Instalar interativamente utilizando o instalador principal

  ou

  - Instalar por linha de comandos utilizando o instalador principal

Instalar interativamente utilizando o instalador principal

- O instalador principal do Endpoint Security Suite Enterprise pode ser localizado em:
  - **Na sua conta FTP Dell** - localize o pacote de instalação em Endpoint-Security-Suite-Ent-1.x.x.xxx.zip.
- Utilize estas instruções para instalar ou atualizar interativamente o Dell Endpoint Security Suite Enterprise utilizando o instalador principal do Endpoint Security Suite Enterprise. Este método pode ser utilizado para instalar o conjunto de produtos num computador de cada vez.

1. Localize o **DDSSuite.exe** no suporte multimédia de instalação Dell. Copie-o para o computador local.
2. Faça duplo clique em **DDSSuite.exe** para iniciar o instalador. Isto poderá demorar vários minutos.
3. Clique em **Seguinte** na caixa de diálogo Bem-vindo.
4. Leia o contrato de licença, aceite os termos e condições e clique em **Seguinte**.
5. Em *Nome de Dell Management Server no local*, introduza o nome de anfitrião totalmente qualificado do Dell Server para gerir o utilizador pretendido, por exemplo, server.organization.com.

   Em *URL do Dell Device Server*, introduza o URL do Dell Server com o qual o cliente irá comunicar.

   o formato é https://server.organization.com:**8443**/xapi**/** (incluindo a barra inclinada para a direita no final).

   Clique em **Seguinte**.
6. Clique em **Seguinte** para instalar os produtos na localização predefinida **C:\Program Files\Dell\Dell Data Protection\. Dell recommends installing in the default location only**, uma vez que poderão surgir problemas ao efetuar a instalação noutras localizações.
7. Selecione os componentes a serem instalados.

O *Security Framework* instala a framework de segurança subjacente.

Encriptação instala o cliente Encryption, o componente que aplica a política de segurança, quer um computador esteja ligado à rede, desligado da rede, seja perdido ou roubado.

O *Threat Protection* instala os clientes Threat Protection, que são uma proteção contra malware e antivírus para verificação da existência de vírus, spyware e programas indesejáveis, Client Firewall para monitorizar a comunicação entre o computador e os recursos na rede e na Internet e o filtro Web, para apresentação de classificações de segurança ou bloqueio do acesso a Web sites durante a navegação online.

O *BitLocker Manager* instala o cliente BitLocker Manager, concebido para melhorar a segurança das implementações do BitLocker pela simplificação e redução do custo de propriedade através da gestão centralizada das políticas de encriptação do BitLocker.

O *Advanced Threat Prevention* instala o cliente Advanced Threat Prevention, que é uma proteção antivírus de última geração que utiliza ciência algorítmica e aprendizagem automática (machine learning) para identificar, classificar e evitar que as ameaças virtuais, conhecidas e desconhecidas, sejam executadas ou danifiquem os endpoints.

Web Protection and Firewall instala as funcionalidades opcionais Web Protection e Firewall. O Client Firewall verifica todo o tráfego de entrada e de saída com base na respetiva lista de regras. A Proteção Web monitoriza a navegação online e as transferências para identificar ameaças e implementar ações definidas pela política quando uma ameaça é detetada, com base em classificações para Web sites.

NOTA: Se tentar instalar a funcionalidade opcional do Advanced Threat Prevention num PC com Windows 10, atualização de outubro de 2018 (Redstone 5) ou posterior, é apresentado um aviso de incompatibilidade.

NOTA: Se tentar instalar as funcionalidades opcionais Web Protection e Firewall num PC com Windows 10, atualização de abril de 2018 (Redstone 5) ou posterior, é apresentado um aviso de incompatibilidade.

Clique em **Seguinte** quando concluir as suas seleções.

8 Clique em **Instalar** para dar início à instalação. A instalação demora vários minutos.

9 Selecione **Sim, desejo reiniciar o computador agora** e clique em **Concluir**.

A instalação está concluída.

Instalar por linha de comandos utilizando o instalador principal

- Numa instalação com linha de comandos, primeiro é necessário especificar as opções. Outros parâmetros vão dentro de um argumento que é passado para a opção /v.

Opções

- A tabela seguinte descreve as opções que podem ser utilizadas com o instalador principal do Endpoint Security Suite Enterprise.

NOTA: Se a sua organização requer a utilização de fornecedores de credenciais externos, o Encryption Management Agent tem de ser instalado ou atualizado com o parâmetro FEATURE=BLM ou FEATURE=BASIC.

NOTA: O Advanced Threat Prevention não é compatível com a atualização de 10 outubro de 2018 do Windows 10 (Redstone 5) ou posterior.

Opção	Descrição
-y -gm2	Pré-extração do instalador principal do Endpoint Security Suite Enterprise. As opções -y e -gm2 devem ser utilizadas em conjunto.

Opção	Descrição
	Não separe as opções.
/S	Instalação silenciosa
/z	Passa variáveis para o .msi dentro do DDSSuite.exe

Parâmetros

- A tabela seguinte descreve os parâmetros que podem ser utilizados com o instalador principal do Endpoint Security Suite Enterprise. O instalador principal do Endpoint Security Suite Enterprise não pode excluir componentes individuais, mas pode receber comandos para especificar os componentes que devem ser instalados.

Parâmetro	Descrição
SUPPRESSREBOOT	Elimina o reinício automático após a conclusão da instalação. Pode ser utilizado no modo SILENCIOSO.
SERVIDOR	Especifica o URL do Dell Server.
InstallPath	Especifica o caminho da instalação. Pode ser utilizado no modo SILENCIOSO.
FUNÇÕES	Especifica os componentes que podem ser instalados no modo SILENCIOSO. ATP = Advanced Threat Prevention *apenas* DE-ATP = Advanced Threat Prevention e Encryption. Esta é a opção de instalação predefinida, se o parâmetro FEATURES não for especificado DE = Cliente de Encriptação de Unidade apenas BLM = BitLocker Manager SED = SED Management (controladores EMAgent/Manager, PBA/GPE)(Disponível apenas quando instalado no sistema operativo de uma estação de trabalho) ATP-WEBFIREWALL = Advanced Threat Prevention com Client Firewall e Web Protection DE-ATP-WEBFIREWALL = Encryption e Advanced Threat Prevention com Client Firewall e Web Protection **NOTA: Para atualizações a partir do Encryption Enterprise ou a partir de uma versão anterior à v1.4 do Endpoint Security Suite Enterprise, é *obrigatório* que ATP-WEBFIREWALL ou DE-ATP-WEBFIREWALL sejam especificados de forma a instalar o Client Firewall e o Web Protection. Não especifique ATP-WEBFIREWALL ou DE-ATP-WEBFIREWALL ao instalar um cliente a ser gerido pelo Dell Server em execução no modo Desligado.**
BLM_ONLY=1	Deve ser utilizado com FEATURES=BLM na linha de comandos para excluir o plug-in de Gestão SED.

Exemplo de linha de comandos

- Os parâmetros da linha de comandos são sensíveis a maiúsculas e minúsculas.
- (No sistema operativo de uma estação de trabalho) Este exemplo instala todos os componentes utilizando o instalador principal do Endpoint Security Suite Enterprise em portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\ e configura-os para utilizar o Dell Server especificado.

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

- (No sistema operativo de uma estação de trabalho) Este exemplo instala o Advanced Threat Prevention e o Encryption ***apenas*** utilizando o instalador principal do Endpoint Security Suite Enterprise em portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\ e configura-os para utilizar o Dell Server especificado.

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

- (No sistema operativo de uma estação de trabalho) Este exemplo instala o Advanced Threat Prevention, o Encryption e o SED Management utilizando o instalador principal do Endpoint Security Suite Enterprise nas portas padrão, de forma silenciosa, com um

reinício suprimido, na localização predefinida C:\Program Files\Dell\Dell Data Protection\ e configura-os para utilizar o Dell Server especificado.

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

- (No sistema operativo de uma estação de trabalho) Este exemplo instala o Advanced Threat Prevention, o Encryption, o Web Protection e o Client Firewall utilizando o instalador principal do Endpoint Security Suite Enterprise nas portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\ e configura-os para utilizar o Dell Server especificado.

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

- (No sistema operativo de uma estação de trabalho) Este exemplo instala ***apenas*** o Advanced Threat Prevention e o Encryption utilizando o instalador principal do Endpoint Security Suite Enterprise nas portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\ e configura-os para utilizar o Dell Server especificado.

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

- (No sistema operativo de um servidor) Este exemplo instala o Advanced Threat Prevention, o Encryption, o Web Protection e o Client Firewall utilizando o instalador principal do Endpoint Security Suite Enterprise nas portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\

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

- (No sistema operativo de um servidor) Este exemplo instala o Advanced Threat Prevention ***apenas*** utilizando o instalador principal do Endpoint Security Suite Enterprise nas portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\ e configura-o para utilizar o Dell Server especificado.

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

- (No sistema operativo de um servidor) Este exemplo instala o Encryption ***apenas*** utilizando o instalador principal do Endpoint Security Suite Enterprise nas portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\ e configura-o para utilizar o Dell Server especificado.

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

4

Desinstalar o instalador principal

- A Dell recomenda a utilização do Desinstalador do Data Security para remover o conjunto de aplicações do Data Security.
- Cada componente deve ser desinstalado separadamente e, depois, deve ser efetuada a desinstalação do instalador principal do Endpoint Security Suite Enterprise. Os clientes devem ser desinstalados numa **ordem específica para impedir falhas na desinstalação**.
- Sigas as instruções que constam em Extrair os Instaladores Subordinados do Instalador Principal para obter instaladores subordinados.
- Certifique-se de que é utilizada a mesma versão do instalador principal (e, por conseguinte, clientes) do Endpoint Security Suite Enterprise.
- Este capítulo direciona-o para outros capítulos que contêm instruções *detalhadas* sobre como desinstalar os instaladores subordinados. Este capítulo explica **apenas** o último passo da desinstalação do instalador principal.
- Desinstale os clientes pela seguinte ordem.

  a Desinstalar o Encryption Client.

  b Desinstalar o Advanced Threat Prevention

  c Desinstalar o cliente SED (esta opção desinstala o Dell Encryption Management Agent, que não pode ser desinstalado antes de desinstalar o Advanced Threat Prevention).

  d Desinstalar o cliente BitLocker Manager
- Avance para Desinstalar o instalador principal.

Desinstalar o instalador principal do Endpoint Security Suite Enterprise

Após desinstalar todos os clientes individuais, o instalador principal pode ser desinstalado.

Desinstalação por linha de comando

- O seguinte exemplo desinstala o instalador principal do Endpoint Security Suite Enterprise de forma silenciosa.

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

  Reinicie o computador quando concluído.

5

Desinstalar utilizando os instaladores subordinados

- A Dell recomenda a utilização do Desinstalador do Data Security para remover o conjunto de aplicações do Data Security.
- Para desinstalar cada cliente individualmente, primeiro é necessário extrair os ficheiros executáveis subordinados do instalador principal do Endpoint Security Suite Enterprise, conforme descrito em Extrair os Instaladores Subordinados do Instalador Principal. Em alternativa, execute uma instalação administrativa para extrair o .msi.
- Certifique-se de que são utilizadas as mesmas versões do cliente para a desinstalação e para a instalação.
- As opções e parâmetros da linha de comandos são sensíveis a maiúsculas e minúsculas.
- Certifique-se de que inclui um valor que contenha um ou mais caracteres especiais, como um espaço em branco na linha de comandos, entre aspas duplas de escape. Os parâmetros da linha de comandos são sensíveis a maiúsculas e minúsculas.
- Utilize estes instaladores para desinstalar os clientes utilizando uma instalação com script, com ficheiros batch ou qualquer outra tecnologia push disponível na sua organização.
- Ficheiros de registo - O Windows cria ficheiros de registo de desinstalação do instalador subordinado únicos para o utilizador com sessão iniciada em %temp%, localizados em **C:\Users\<UserName>\AppData\Local\Temp.**

  Se decidir adicionar um ficheiro de registo separado quando executar o instalador, certifique-se de que ficheiro de registo tem um nome único uma vez que os ficheiros de registo de instalador subordinado não são acrescentados. O comando padrão .msi pode ser utilizado para criar um ficheiro de registo utilizando /l **C:\<any directory>\<any log file name>.log**. A Dell não recomenda a utilização de "/l*v" (registo verboso) na desinstalação através da linha de comandos, uma vez que o nome de utilizador/palavra-passe são guardados no ficheiro de registo.
- Todos os instaladores subordinados utilizam as mesmas opções de apresentação e parâmetros .msi básicos, exceto quando indicado, para as desinstalações através da linha de comandos. As opções devem ser especificadas em primeiro lugar. A opção /v é obrigatória e necessita de um argumento. Outros parâmetros vão dentro de um argumento que é passado para a opção /v.

  As opções de apresentação podem ser especificadas no final do argumento passado para a opção /v para alcançar o comportamento esperado. Não utilize /q e /qn na mesma linha de comandos. Utilize apenas ! e - após /qb.

Opção	Significado
/v	Passa variáveis para o .msi dentro do setup.exe. O conteúdo deve estar sempre dentro de aspas de texto simples.
/s	Modo silencioso
/x	Modo de desinstalação
/a	Instalação administrativa (copia todos os ficheiros contidos no .msi)

NOTA:
Com /v, as opções predefinidas da Microsoft ficam 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	Sem caixa de diálogo de Progresso, reinicia-se após a conclusão do processo
/qb	Caixa de diálogo de Progresso com botão **Cancelar**, solicita o reinício

Opção	Significado
/qb-	Caixa de diálogo de Progresso com botão **Cancelar**, reinicia-se após a conclusão do processo
/qb!	Caixa de diálogo de Progresso sem botão **Cancelar**, solicita o reinício
/qb!-	Caixa de diálogo de Progresso sem botão **Cancelar**, reinicia-se após a conclusão do processo
/qn	Sem interface de utilizador

Desinstalar o Encryption e o Server Encryption Client

- Para reduzir o tempo de desencriptação, execute o Assistente de Limpeza de Disco do Windows para remover ficheiros temporários e outros dados desnecessários.
- Se possível, programe a desencriptação para ser feita durante a noite.
- Desative o modo de suspensão para impedir a suspensão do computador caso este se encontre sem supervisão. A desencriptação não é possível num computador em suspensão.
- Encerre todos os processos e aplicações para minimizar as falhas de desencriptação devidas a ficheiros bloqueados.
- Uma vez que a desinstalação está concluída e a desencriptação está em progresso, desative toda a conectividade à rede. Caso contrário, podem ser adquiridas novas políticas que voltam a ativar a encriptação.
- Siga o processo de desencriptação de dados existente, como, por exemplo, a emissão de uma atualização de política.
- O Dell Encryption e o Encryption External Media atualizam o Dell Server para alterar o estado para *Desprotegido* no início de um processo de desinstalação do Cliente de Encriptação. No entanto, caso o cliente não consiga contactar o Dell Server, independentemente do motivo, não é possível atualizar o estado. Neste caso, terá de *Remover o Endpoint* manualmente na Management Console. Se a sua organização utilizar este fluxo de trabalho por motivos de conformidade, a Dell recomenda que verifique se o estado *Desprotegido* foi definido da forma esperada na Management Console ou no Compliance Reporter.

Processo

- O Key Server (e o Security Management Server) deve ser configurado antes da desinstalação se estiver a utilizar a opção **Transferir chaves a partir do servidor do Encryption Removal Agent**. Consulte Configurar o Key Server para desinstalação do Encryption Client ativado no Security Management Server para obter instruções. Não é necessária qualquer ação anterior se o cliente a ser desinstalado estiver ativado num Security Management Server Virtual, uma vez que o Security Management Server Virtual não utiliza o Key Server.
- Deve utilizar o Dell Administrative Utility (CMGAd) antes de iniciar o Encryption Removal Agent se estiver a utilizar a opção **Importar chaves a partir de um ficheiro do Encryption Removal Agent**. Este utilitário é utilizado para obter o pacote de chave de encriptação. Consulte Utilizar o Administrative Download Utility (CMGAd) para obter instruções. O utilitário pode estar localizado no suporte de instalação Dell.

Desinstalação por linha de comando

- Uma vez extraído do instalador principal do Endpoint Security Suite Enterprise, o instalador do Encryption Client pode ser localizado em **C:\extracted\Encryption\DDPE_XXbit_setup.exe**.
- A tabela seguinte descreve os parâmetros disponíveis para a desinstalação.

Parâmetro	Seleção
CMG_DECRYPT	Propriedade para selecionar o tipo de instalação do Encryption Removal Agent 3 - Utilizar o pacote LSARecovery 2 - Utilizar material da chave forense anteriormente transferido

Parâmetro	Seleção
	1 - Transferir chaves do Dell Server 0 – Não instalar o Encryption Removal Agent
CMGSILENTMODE	Propriedade para a desinstalação silenciosa: 1 – Silenciosa 0 – Não silenciosa
Propriedades obrigatórias	
DA_SERVER	FQHN para o Security Management Server anfitrião da sessão de negociação.
DA_PORT	Porta do Security Management Server para pedidos (a predefinição é 8050).
SVCPN	Nome de utilizador no formato UPN no qual o serviço Key Server tem sessão iniciada no Security Management Server.
DA_RUNAS	Nome de utilizador no formato compatível com SAM, sendo o pedido de recuperação de chaves realizado neste contexto. Este utilizador necessita de estar na lista do Key Server do Security Management Server.
DA_RUNASPWD	Palavra-passe do utilizador runas.
FORENSIC_ADMIN	A conta de administrador forense no Dell Server, que pode ser utilizada para pedidos forenses para desinstalações ou chaves.
FORENSIC_ADMIN_PWD	A palavra-passe da conta de administrador forense.
Propriedades opcionais	
SVCLOGONUN	Nome de utilizador no formato UPN para o início de sessão do serviço Encryption Removal Agent como parâmetro.
SVCLOGONPWD	Palavra-passe para início de sessão como utilizador.

- O seguinte exemplo desinstala silenciosamente o Encryption Client e transfere as chaves de encriptação a partir do Security Management 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 quando concluído.

- O seguinte exemplo desinstala silenciosamente o Encryption Client e transfere as chaves de encriptação utilizando 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 quando concluído.

IMPORTANTE:

A Dell recomenda as seguintes ações ao utilizar uma palavra-passe de administrador forense na linha de comandos:

1. Crie uma conta de administrador forense na Management Console para realizar a desinstalação silenciosa.
2. Utilize uma palavra-passe temporária exclusiva para essa conta e para esse período de tempo.
3. Após a conclusão da desinstalação silenciosa, remova a conta temporária da lista de administradores ou altere a respetiva palavra-passe.

NOTA:

Alguns clientes mais antigos poderão requerer caracteres de \" à volta dos valores dos 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 seguinte desinstala o cliente Advanced Threat Prevention. ***Este comando tem de ser executado a partir de uma linha de comandos administrativa.***

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

  Encerre e reinicie o computador e, em seguida, desinstale o componente Dell Encryption Management Agent.

- **IMPORTANTE: Se tiver instalado o cliente SED ou tiver ativado a autenticação de pré-arranque, siga as instruções de desinstalação apresentadas em Desinstalar o cliente SED.**

  O seguinte exemplo desinstala apenas o componente Dell Encryption Management Agent e não o cliente SED.

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

Desinstalar o cliente SED

- Para desativar a PBA, é necessária uma ligação de rede ao Dell Server.

Processo

- Desativar a PBA, o que remove todos os dados da PBA do computador e desbloqueia as chaves SED.
- Desinstalar o software de cliente SED.

Desativar a PBA

1. Como administrador Dell, inicie sessão na Management Console.
2. No painel esquerdo, clique em **Populações** > **Endpoints**.
3. Selecione o Tipo de endpoint adequado.
4. Selecione Mostrar >*Visível*, Oculto ou *Todos*.

5 Se souber o Nome de anfitrião do computador, introduza-o no campo Nome de anfitrião (os caracteres universais são suportados). Pode deixar o campo em branco, de modo a que sejam apresentados todos os computadores. Clique em **Procurar**.

Se não souber o Nome de anfitrião, procure na lista até encontrar o computador.

É apresentado um computador ou lista de computadores com base no seu filtro de pesquisa.

6 Selecione o nome de anfitrião do computador pretendido.

7 Clique em **Políticas de segurança** no menu superior.

8 Selecione **Unidades de encriptação automática** na página **Categoria de política**.

9 Altere a **Unidade de encriptação automática (SED)** e a política de *On* para ***Off***.

10 Clique em **Guardar**.

11 No painel do lado esquerdo, clique na faixa **Consolidar políticas**.

12 Clique em **Consolidar políticas**.

Aguarde que a política seja propagada do Dell Server para o computador onde pretende efetuar a desativação.

Desinstale os clientes SED e de Autenticação depois da PBA ser desativada.

Desinstalar o cliente SED

Desinstalação por linha de comando

- Uma vez extraído do instalador principal, o instalador do cliente SED pode ser localizado em C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe.
  - O seguinte exemplo desinstala o cliente SED de forma silenciosa.

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

    Encerre e reinicie o computador quando concluído.

Desinstalar o cliente BitLocker Manager

Desinstalação por linha de comando

- Uma vez extraído do instalador principal do Endpoint Security Suite Enterprise , o instalador do cliente BitLocker pode ser localizado em C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe.
- O seguinte exemplo desinstala o cliente BitLocker Manager de forma silenciosa.

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

  Reinicie o computador quando concluído.

6

Desinstalador do Data Security

Desinstalar Endpoint Security Suite Enterprise

A Dell fornece o Data Security Uninstaller como o desinstalador principal. Este utilitário reúne os produtos instalados atualmente e remove-os na ordem apropriada.

O Data Security Uninstaller está disponível na seguinte localização: C:\Program Files (x86)\Dell\Dell Data Protection

Para obter mais informações ou para utilizar a interface de linha de comandos (CLI), consulte o artigo BDC SLN307791.

Os registos são gerados em C:\ProgramData\Dell\Dell Data Protection\ para todos os componentes que são removidos.

Para executar o utilitário, abra a respetiva pasta, clique com o botão direito do rato em **DataSecurityUninstaller.exe** e **execute-o como administrador**.

Clique em **Seguinte**.

Opcionalmente, desmarque a remoção de qualquer aplicação e clique em **Seguinte**.

NOTA: As dependências necessárias são automaticamente selecionadas ou desmarcadas.

Para remover aplicações sem instalar o Encryption Removal Agent, escolha **Não instalar o Encryption Removal Agent** e selecione **Seguinte**.

Selecione **Encryption Removal Agent - Transferir chaves a partir do servidor**.

Introduza as credenciais totalmente qualificadas de um administrador forense e selecione **Seguinte**.

Selecione **Remover** para iniciar a desinstalação.

Clique em **Terminar** para concluir a remoção e reinicie o computador. **Reiniciar o computador depois de clicar em terminar** está selecionado por predefinição.

A desinstalação e remoção estão concluídas.

7

Configurar um inquilino

Deve ser aprovisionado um inquilino no Dell Server antes da ativação da aplicação de políticas do Advanced Threat Prevention.

Pré-requisitos

- Tem de ser efetuado por um administrador com função de administrador de sistema.
- Deve ter ligação à Internet para configuração no Dell Server.
- Tem de ter ligação à Internet no cliente para visualizar a integração do serviço online do Advanced Threat Prevention na Management Console.
- A configuração tem como base um token que é gerado a partir de um certificado durante a configuração.
- As licenças do Advanced Threat Prevention devem estar presentes no Dell Server.

Configurar um inquilino

1 Como administrador Dell, inicie sessão na Management Console.

2 No painel esquerdo da Management Console, clique em **Gestão > Gestão de serviços**.

3 Clique em **Configurar serviço Advanced Threat Protection**. Se ocorrer qualquer falha neste momento, importe as suas licenças Advanced Threat Prevention.

4 A configuração com assistente é iniciada imediatamente após as licenças serem importadas. Clique em **Seguinte** para começar.

5 Leia e aceite o EULA e clique em **Seguinte**.

6 Disponibilize credenciais de identificação no Dell Server para configuração do Inquilino. Clique em **Seguinte**. *A configuração de um Inquilino existente da marca Cylance não é suportada.*

7 Transfira o Certificado. Este é necessário para recuperação em caso de desastres no Dell Server. Não é efetuada uma cópia de segurança deste Certificado. Efetue uma cópia de segurança do Certificado numa localização segura num computador diferente. Selecione a caixa de verificação para confirmar que efetuou uma cópia de segurança do Certificado e clique em **Seguinte**.

8 A configuração está concluída. Clique em **OK**.

8

Configurar a atualização automática do Advanced Threat Prevention

Na Management Console, pode inscrever-se para receber atualizações automáticas do agente Advanced Threat Prevention. A subscrição da receção de atualizações automáticas do agente permite aos clientes transferir e aplicar autoatualizações a partir do serviço de Advanced Threat Prevention. As atualizações são mensais.

NOTA:
As autoatualizações do agente são suportadas com o Dell Server v9.4.1 ou posterior.

Receber autoatualizações do agente

Para se inscrever e receber autoatualizações do agente:

1 No painel esquerdo da Management Console, clique em **Gestão** > **Gestão de Serviços**.
2 No separador *Advanced Threats*, sob *Atualização automática do agente*, clique em **Ligar** e, em seguida, clique em **Guardar preferências**.
Poderá demorar alguns momentos até as informações serem propagadas e as autoatualizações serem apresentadas.

Deixar de receber autoatualizações do agente

Para deixar de receber autoatualizações do agente:

1 No painel esquerdo da Management Console, clique em **Gestão** > **Gestão de Serviços**.
2 No separador *Advanced Threats*, sob *Atualização automática do agente*, clique em **Desligar** e, em seguida, clique em **Guardar preferências**.

9

Extrair os instaladores subordinados

- O instalador principal não é um *desinstalador* principal. Cada cliente tem de ser desinstalado separadamente, seguido pela desinstalação do instalador principal. Utilize este processo para extrair os clientes do instalador principal para que possam ser utilizados para a desinstalação.

1 A partir do suporte multimédia de instalação Dell, copie o ficheiro **DDSSuite.exe** para o computador local.

2 Abra uma linha de comandos na mesma localização do ficheiro **DDSSuite.exe** e introduza:

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

O caminho de extração não pode exceder os 63 caracteres.

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

Configurar o Key Server

- Esta secção explica como configurar componentes para utilização com a autenticação/autorização Kerberos ao utilizar um Security Management Server. O Security Management Server Virtual não utiliza o Key Server.
- Se for necessário utilizar a autenticação/autorização Kerberos, o servidor que contém o componente Key Server tem de fazer parte do domínio afetado.
- Dado que o Security Management Server Virtual não utiliza o Key Server, a desinstalação típica é afetada. Quando um Encryption Client ativado num Security Management Server Virtual é desinstalado, é utilizada a recuperação de chave forense padrão através do Security Server, em vez do método Kerberos do Key Server. Consulte Desinstalação por linha de comando para obter mais informações.

Painel de Serviços - Adicionar utilizador da conta do domínio

1 No Security Management Server, navegue até ao painel de Serviços (Iniciar > Executar... > services.msc > OK).

2 Clique com o botão direito do rato em Key Server e selecione **Propriedades**.

3 Selecione o separador Iniciar sessão e selecione a opção **Esta conta:**.

Em *Esta conta:*, adicione o utilizador da conta do domínio. Este utilizador do domínio necessita possuir, pelo menos, direitos administrativos locais para a pasta do Key Server (necessita poder gravar no ficheiro de configuração do Key Server e também ter a capacidade de gravar no ficheiro log.txt).

Introduza e confirme a palavra-passe para o utilizador do domínio.

Clique em **OK**.

4 Reinicie o serviço do Key Server (deixe o painel de serviços aberto para o continuar a utilizar).

5 Navegue até <Key Server install dir> log.txt para verificar se o serviço foi iniciado adequadamente.

Ficheiro de configuração do Key Server - Adicionar utilizador para comunicação com o Security Management Server

1 Navegue até <Key Server install dir>.

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

3 Aceda a <add key="user" value="superadmin" /> e altere o valor "superadmin" para o nome do utilizador pretendido (pode também manter "superadmin").

4 Aceda a <add key="epw" value="<encrypted value of the password>" /> e altere "epw" para "password". Em seguida, altere o "<encrypted value of the password>" para a palavra-passe do utilizador indicada no Passo 3. Esta palavra-passe é novamente encriptada quando reiniciar o Security Management Server.

Se, no Passo 3, utilizou "superadmin" e a palavra-passe do superadmin não for "changeit", deve ser alterada aqui. Guarde e feche o ficheiro.

Painel de Serviços - Reiniciar o serviço Key Server

1 Volte ao painel de Serviços (Iniciar > Executar > services.msc > OK).
2 Reinicie o serviço Key Server.
3 Navegue até <Key Server install dir> log.txt para verificar se o serviço foi iniciado adequadamente.
4 Feche o painel Serviços.

Management Console - Adicionar administrador forense

1 Como administrador Dell, inicie sessão na Management Console.
2 Clique em **Populações** > **Domínios**.
3 Selecione o Domínio adequado.
4 Clique no separador **Key Server**.
5 Em *Conta*, adicione o utilizador que irá efetuar as atividades de administrador. O formato é DOMÍNIO\Nome de utilizador. Clique em **Adicionar conta**.
6 Clique em **Utilizadores** no menu à esquerda. Na caixa de pesquisa, procure o nome de utilizador adicionado no Passo 5. Clique em **Procurar**.
7 Depois de encontrar o utilizador correto, clique no separador **Administrador**.
8 Selecione **Administrador forense** e clique em **Atualizar**.

Os componentes estão agora configurados para autenticação/autorização Kerberos.

11

Utilizar o Administrative Download Utility (CMGAd)

- Este utilitário permite a transferência de um pacote de material de chave para utilização num computador que não está ligado a um servidor Security Management Server/Security Management Server Virtual.
- Este utilitário utiliza um dos seguintes métodos para transferir um pacote de chave, dependendo do parâmetro da linha de comandos passado à aplicação:
  - Modo forense - Utilizado se -f é passado na linha de comandos ou se não é utilizado qualquer parâmetro de linha de comandos.
  - Modo de administrador - Utilizado se -a é passado na linha de comandos.

  Os ficheiros de registo podem ser localizados em **C:\ProgramData\CmgAdmin.log**

Utilize o Administrative Download Utility no Modo forense

1 Clique duas vezes em **cmgad.exe** para iniciar o utilitário ou abrir uma linha de comandos onde o CMGAd está localizado e introduza **`cmgad.exe -f`** (ou **`cmgad.exe`**).

2 Introduza a seguinte informação (alguns campos podem ser pré-preenchidos).

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

Administrador Dell: Nome do administrador com credenciais de administrador forense (ativado na Remote Management Console), por exemplo, jdoe

Palavra-passe: Palavra-passe de administrador forense

MCID: ID do computador, por exemplo, machineID.domain.com

DCID: Primeiros oito dígitos da ID Shield de 16 dígitos

> **SUGESTÃO:**
> Normalmente, é suficiente especificar o MCID *ou* DCID. No entanto, se ambos são conhecidos, é útil introduzir os dois. Cada parâmetro contém informação diferente sobre o cliente e o computador cliente.

Clique em **Seguinte**.

3 No campo Frase de acesso:, escreva uma frase de acesso para proteger o ficheiro de transferência. A frase de acesso deve ter pelo menos oito caracteres de comprimento, e conter pelo menos um carácter alfabético e um carácter numérico. Confirme a frase de acesso.

Aceite o nome e localização padrão onde o ficheiro será guardado ou clique em ... para selecionar uma localização diferente.

Clique em **Seguinte**.

É apresentada uma mensagem, indicando que o material de chave foi desbloqueado satisfatoriamente. Os ficheiros estão agora acessíveis.

4 Clique em **Concluir** quando tiver terminado.

Utilize o Administrative Download Utility no Modo de administrador

O Security Management Server Virtual não utiliza o Key Server, pelo que o modo de Administrador não pode ser utilizado para obter um pacote de chave a partir de um Security Management Server Virtual. Utilize o Modo forense para obter o pacote de chaves se o cliente estiver ativado num Security Management Server Virtual.

1 Abra uma linha de comandos onde o CMGAd está localizado e introduza **`cmgad.exe -a`**.

2 Introduza a seguinte informação (alguns campos podem ser pré-preenchidos).

Servidor: Nome de anfitrião totalmente qualificado do Key Server, por exemplo, keyserver.domain.com

Número da porta: A porta predefinida é 8050

Conta do servidor: O utilizador do domínio de execução do Key Server. O formato é domain\username. O utilizador do domínio que está a executar o utilitário deve estar autorizado para realizar a transferência a partir do Key Server

MCID: ID do computador, por exemplo, machineID.domain.com

DCID: Primeiros oito dígitos da ID Shield de 16 dígitos

SUGESTÃO:

Normalmente, é suficiente especificar o MCID *ou* DCID. No entanto, se ambos são conhecidos, é útil introduzir os dois. Cada parâmetro contém informação diferente sobre o cliente e o computador cliente.

Clique em **Seguinte**.

3 No campo Frase de acesso:, escreva uma frase de acesso para proteger o ficheiro de transferência. A frase de acesso deve ter pelo menos oito caracteres de comprimento, e conter pelo menos um carácter alfabético e um carácter numérico.

Confirme a frase de acesso.

Aceite o nome e localização padrão onde o ficheiro será guardado ou clique em ... para selecionar uma localização diferente.

Clique em **Seguinte**.

É apresentada uma mensagem, indicando que o material de chave foi desbloqueado satisfatoriamente. Os ficheiros estão agora acessíveis.

4 Clique em **Concluir** quando tiver terminado.

12

Resolução de problemas

Todos os clientes - Resolução de problemas

- **Os ficheiros de registo do instalador principal do Endpoint Security Suite Enterprise** encontram-se em **C:\ProgramData\Dell\Dell Data Protection\Installer.**
- O Windows cria **ficheiros de registo de instalação do instalador subordinado** únicos para o utilizador com sessão iniciada em %temp %, localizados em **C:\Users\<NomeDeUtilizador>\AppData\Local\Temp.**
- O Windows cria ficheiros de registo para pré-requisitos do cliente, como Visual C++, para o utilizador com sessão iniciada em %temp%, localizados em **C:\Users\<NomeDeUtilizador>\AppData\Local\Temp. Por exemplo, C:\Users\<NomeDeUtilizador>\AppData\Local \Temp\dd_vcredist_amd64_20160109003943.log**
- Siga as instruções apresentadas em http://msdn.microsoft.com para verificar a versão do Microsoft .Net instalada no computador onde pretende efetuar a instalação.

  Aceda a https://www.microsoft.com/en-us/download/details.aspx?id=30653 para transferir a versão completa do Microsoft .Net Framework 4.5.2 ou posterior.
- Consulte *este documento* se o computador onde pretende efetuar a instalação tiver (ou teve anteriormente) o Dell Access instalado. O DDP|A não é compatível com este conjunto de produtos.

Todos os clientes - Estado de Proteção

Foi implementado um novo método para determinar o estado protegido de um dispositivo no Dell Security Management Server v9.8.2. Anteriormente, a área de estado protegido do endpoint no dashboard da consola de gestão apenas indicaria o estado de encriptação por dispositivo.

O estado protegido é indicado agora se forem cumpridos todos os critérios a seguir enunciados:

- O Advanced Threat Prevention está instalado e ativado.
- O Web Protection ou o Client Firewall está instalado e a política do Web Protection ou do Client Firewall está ativada.
- O Dell Data Guardian está instalado e ativado.
- A gestão de unidades de encriptação automática está instalada, ativada e a Autenticação de pré-arranque (PBA) está ativada.
- O BitLocker Manager está instalado, ativado e a encriptação foi concluída.
- O Dell Encryption (Mac) está instalado e ativado e a encriptação baseada em políticas foi implementada.
- O Dell Encryption (Windows) está instalado, ativado, a encriptação baseada em políticas foi definida para o ponto final e os varrimentos do dispositivo estão concluídos.

Resolução de problemas do Encryption e do Server Encryption Client

Atualização para o Windows 10 Creators Update

Para atualizar para a versão Windows 10, atualização de outubro de 2018, siga as instruções apresentadas no seguinte artigo: http://www.dell.com/support/article/us/en/19/SLN298382.

Ativação num sistema operativo de servidor

Quando o Encryption está instalado num sistema operativo de servidor, a ativação requer duas fases de ativação: a ativação inicial e a ativação do dispositivo.

Resolução de problemas da ativação inicial

A ativação inicial falha quando:

- Não é possível construir um UPN válido utilizando as credenciais fornecidas.
- As credenciais não se encontram no cofre da empresa.
- As credenciais utilizadas para ativação não são as credenciais do administrador do domínio.

Mensagem de erro: Nome de utilizador desconhecido ou palavra-passe inválida

O nome de utilizador ou a palavra-passe não correspondem.

Solução possível**:** Tente iniciar sessão novamente, certificando-se que introduz o nome de utilizador e palavra-passe corretos.

Mensagem de erro: a ativação falhou porque a conta de utilizador não possui direitos de administrador do domínio.

As credenciais utilizadas para ativação não possuem direitos de administrador do domínio ou o nome de utilizador do administrador não está no formato UPN.

Solução possível**:** na caixa de diálogo Ativação, introduza as credenciais de um administrador do domínio no formato UPN.

Mensagens de erro: Não foi possível estabelecer a ligação ao servidor.

ou

```
The operation timed out.
```

O Server Encryption não consegue comunicar com a porta 8449 através de HTTPS no Dell Server.

Soluções Possíveis

- Ligue diretamente à sua rede e tente novamente ativar.
- Se estiver ligado via VPN, tente ligar diretamente à rede e tente novamente ativar.
- Verifique o URL do Dell Server para garantir que corresponde ao URL fornecido pelo administrador. O URL e outros dados que o utilizador introduziu no programa de instalação estão armazenados no registo. 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 à rede.

Mensagem de erro: Ocorreu uma falha na ativação, uma vez que o Servidor não suporta este pedido.

Soluções Possíveis

- Não é possível ativar o Server Encryption num servidor legado; a versão do Dell Server deve ser a versão 9.1 ou superior. Se necessário, faça uma atualização do seu Dell Server para a versão 9.1 ou superior.
- Verifique o URL do Dell Server para garantir que corresponde ao URL fornecido pelo administrador. O URL e outros dados que o utilizador introduziu no programa de instalação estão armazenados no registo.
- 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 seguinte ilustra uma ativação inicial bem-sucedida.

O processo de ativação inicial do Server Encryption requer o acesso de um utilizador real ao servidor. O utilizador pode ser de qualquer tipo: utilizador de domínio ou de fora do domínio, ligado ao ambiente de trabalho remoto ou interativo, mas este deve ter acesso a credenciais de administrador do domínio.

A caixa de diálogo Ativação é apresentada numa das duas situações seguintes:

- Um utilizador novo (não gerido) inicia sessão no computador.
- Quando um utilizador novo clica com o botão direito do rato no ícone do Encryption Client no tabuleiro do sistema e seleciona Ativar o Dell Encryption.

O processo de ativação inicial é o seguinte:

1 O utilizador inicia sessão.
2 Ao detetar um utilizador novo (não gerido), a caixa de diálogo Ativar é apresentada. O utilizador clica em **Cancelar**.
3 O utilizador abre a caixa "Acerca de" do Server Encryption para confirmar se está em execução no modo de Servidor.
4 O utilizador clica com o botão direito do rato no ícone do Encryption Client na área de notificação e seleciona **Ativar o Dell Encryption**.
5 O utilizador introduz as credenciais de Administrador de domínio na caixa de diálogo Ativar.

> **NOTA:**
> O requisito de credenciais de administrador do domínio é uma medida de segurança que impede que o Server Encryption seja implementado noutros ambientes de servidor que não suportam o mesmo. Para desativar o requisito de credenciais de administrador do domínio, consulte Antes de começar.

6 O Dell Server verifica as credenciais no cofre da empresa (Active Directory ou equivalente) para confirmar se as mesmas são as credenciais do administrador do domínio.
7 Um UPN é construído utilizando as credenciais.
8 Com o UPN, o Dell Server cria uma nova conta de utilizador para o utilizador do servidor virtual e guarda as credenciais no cofre do Dell Server.

A **conta de utilizador do servidor virtual** destina-se a utilização exclusiva do Encryption Client. Esta é utilizada para a autenticação no servidor, para a gestão de chaves de encriptação Comuns e para receção de atualizações de política.

> **NOTA:**
> A palavra-passe e a autenticação DPAPI estão desativadas para esta conta de modo a que *apenas* o utilizador do servidor virtual tenha acesso a chaves de encriptação no computador. Esta conta não corresponde a qualquer outra conta de utilizador no computador ou no domínio.

9 Quando a ativação for bem-sucedida, o utilizador reinicia o computador, o que inicia a segunda fase, a autenticação e a ativação do dispositivo.

Resolução de problemas de autenticação e ativação do dispositivo

A ativação do dispositivo falha quando:

- Ocorre uma falha da ativação inicial.
- Não é possível estabelecer a ligação ao servidor.
- Não é possível validar o certificado de confiança.

Após a ativação, quando o computador é reiniciado, o Server Encryption inicia automaticamente sessão como utilizador do servidor virtual, solicitando a chave de Computador ao Dell Server. Ocorre mesmo antes de qualquer utilizador iniciar sessão.

- Abra a caixa de diálogo "Acerca de" para confirmar se o Server Encryption está autenticado e no modo de Servidor.
- Se a ID do Cliente de Encriptação apresentar cor vermelha, a encriptação ainda não foi ativada.
- Na Management Console, a versão de um servidor com o Server Encryption instalado é indicada como *Proteção para servidor*.
- Se a obtenção da chave de Computador falhar devido a uma falha de rede, o Server Encryption regista-se para receber notificações de rede do sistema operativo.

- Se a obtenção da chave de Computador falhar:
  - O início de sessão do utilizador no servidor virtual é, ainda assim, bem-sucedido.
  - Defina a política *Intervalo de Tempo entre Tentativas em caso de Falha de rede* para efetuar tentativas de obtenção da chave com um intervalo de tempo definido.

    Consulte AdminHelp, disponível na Management Console, para obter detalhes sobre a política *Intervalo entre tentativas em caso de falha de rede*.

Autenticação e ativação de dispositivos

O diagrama seguinte ilustra a autenticação e ativação do dispositivo bem-sucedidas.

1 Quando reiniciar após uma ativação inicial bem-sucedida, um computador com Server Encryption efetua automaticamente a autenticação utilizando a conta de utilizador do servidor virtual e executa o Encryption Client no modo de Servidor.

2 O computador verifica o respetivo estado de ativação de dispositivos com o Dell Server:

   - Se o computador não tiver ativado o dispositivo anteriormente, o Dell Server atribui um MCID, um DCID e um certificado de confiança ao computador e guarda todas as informações no cofre do Dell Server.
   - Se o computador tiver anteriormente ativado o dispositivo, o Dell Server verifica o certificado de confiança.

3 Depois de o Dell Server atribuir o certificado de confiança ao servidor, este pode aceder às respetivas chaves de encriptação.

4 A ativação do dispositivo é bem-sucedida.

> **NOTA:**
> Quando estiver em execução no modo de Servidor, o Encryption Client deve ter acesso ao mesmo certificado utilizado na ativação do dispositivo para aceder às chaves de encriptação.

Interações de PCS e Encryption External Media

Para garantir que o suporte multimédia não está definido como apenas de leitura e que a porta não está bloqueada

A política Aceder a suportes multimédia desprotegidos do EMS interage com o Sistema de controlo das portas - Classe: Armazenamento > Subclasse de armazenamento: Política de controlo da unidade externa. Se pretender definir a política Aceder a suportes multimédia desprotegidos do EMS como *Acesso total*, certifique-se de que a política de Subclasse de armazenamento: Controlo da unidade externa também está definida como *Acesso total* para garantir que o suporte de dados não está definido como só de leitura e que a porta não está bloqueada.

Para encriptar os dados gravados em CD/DVD

- Defina a encriptação de suportes de dados do Windows = Ligado.
- Defina EMS: Excluir encriptação de CD/DVD = não selecionado.
- Defina a Subclasse de armazenamento: Controlo da unidade ótica = Apenas UDF.

Utilizar o WSScan

- O WSScan permite-lhe assegurar que todos os dados são desencriptados quando desinstalar o Encryption Client, para além de visualizar o estado de encriptação e identificar ficheiros desencriptados que devem ser encriptados.
- São necessários privilégios de administrador para executar este utilitário.

Execute a

1 Copie WSScan.exe do suporte de instalação Dell para o computador Windows a verificar.

2 Inicie uma linha de comandos na localização acima e introduza **wsscan.exe** na mesma. O WSScan é iniciado.

3 Clique em **Avançadas**.

4 Selecione o tipo de unidade a analisar: *Todas as unidades, Unidades fixas*, *Unidades amovíveis* ou *CDROM/DVDROM*.

5 Selecione o tipo de relatório de encriptação: *Ficheiros encriptados*, *Ficheiros não encriptados*, *Todos os ficheiros* ou *Ficheiros não encriptados em violação*:

- *Ficheiros encriptados* - Para assegurar que todos os dados são desencriptados quando desinstalar o Encryption Client. Siga o processo de desencriptação de dados existente, por exemplo, a emissão de uma atualização de política de desencriptação. Após desencriptar os dados, mas antes de reiniciar para preparar a desinstalação, execute o WSScan para garantir que todos os dados estão desencriptados.
- *Ficheiros desencriptados* - Para identificar ficheiros que não estão encriptados, com indicação se os ficheiros devem ser encriptados (S/N).
- *Todos os ficheiros* - Para indicar todos os ficheiros encriptados e desencriptados, com indicação se os ficheiros devem ser encriptados (S/N).
- *Ficheiros desencriptados em violação* - Para identificar ficheiros que não estão encriptados e deviam estar.

6 Clique em **Procurar**.

OU

1 Clique em **Avançadas** para alternar a visualização para **Simples** para analisar uma pasta particular.

2 Aceda a Definições de análise e introduza o caminho da pasta no campo *Caminho da pesquisa*. Se este campo for utilizado, a seleção no menu é ignorada.

3 Caso não pretenda gravar os resultados de saída do WSScan num ficheiro, desmarque a caixa de verificação **Saída para ficheiro**.

4 Se pretender, altere o caminho e o nome de ficheiro predefinidos em *Caminho*.

5 Selecione **Adicionar a ficheiro existente** se não pretende substituir quaisquer ficheiros de saída WSScan existentes.

6 Escolha o formato de saída:

- Selecione Formato de relatório para obter uma lista de estilos de relatório de saída de análise. Este é o formato predefinido.
- Selecione Ficheiro de valor delimitado para uma saída que possa ser importada para uma aplicação de folha de cálculo. O delimitador predefinido é "|", embora possa ser alterado para, no máximo, 9 carateres alfanuméricos, um espaço ou sinais de pontuação do teclado.
- Selecione a opção Valores cotados para colocar cada valor entre aspas duplas.
- Selecione Ficheiro de largura fixa para uma saída não delimitada, com uma linha contínua de informações de comprimento fixo acerca de cada ficheiro encriptado.

7 Clique em **Procurar**.

Clique em **Parar a pesquisa** para parar a sua pesquisa. Clique em **Limpar** para eliminar as mensagens apresentadas.

Resultado do WSScan

As informações do WSScan acerca dos ficheiros encriptados contêm os seguintes dados.

Exemplo de saída:

[2015-07-28 07:52:33] SysData.7vdlxrsb._SDENCR_: "c:\temp\Dell - test.log" continua encriptado por AES256

Saída	Significado
Carimbo de data/hora	A data e a hora em que o ficheiro foi analisado.
Tipo de encriptação	O tipo de encriptação utilizado para encriptar o ficheiro. **SysData:** chave SDE. **Utilizador:** chave de encriptação do utilizador. **Comum:** chave de encriptação Comum. O WSScan não indica ficheiros encriptados utilizando o Encrypt for Sharing.
KCID	A ID do computador principal.

Saída	Significado
	Tal como apresentado no exemplo acima, "**7vdlxrsb**"
	Se estiver a analisar uma unidade de rede mapeada, o relatório da análise não apresenta uma KCID.
UCID	A ID do utilizador.
	Tal como apresentado no exemplo acima, "**_SDENCR_**"
	A UCID é partilhada por todos os utilizadores desse computador.
Ficheiro	O caminho do ficheiro encriptado.
	Tal como apresentado no exemplo acima, "**c:\temp\Dell - test.log**"
Algoritmo	O algoritmo de encriptação utilizado para encriptar o ficheiro.
	Tal como apresentado no exemplo acima, "**continua encriptado por AES256**"
	RIJNDAEL 128
	RIJNDAEL 256
	AES-128
	AES-256
	3DES

Verificar o estado do Encryption Removal Agent

O Encryption Removal Agent apresenta o respetivo estado na área de descrição do painel de Serviços (Iniciar > Executar > services.msc > OK) da seguinte forma. Atualize periodicamente o serviço (destaque o serviço > clique com o botão direito do rato > Atualizar) para atualizar o respetivo estado.

- **A aguardar a desativação do SED** – O cliente Encryption continua instalado, continua configurado, ou ambos. A desencriptação não será iniciada antes de o cliente Encryption ser desinstalado.
- **Varrimento inicial** – O serviço está a realizar um varrimento inicial, calculando o número de ficheiros encriptados e de bytes. O varrimento inicial ocorre uma vez.
- **Varrimento de desencriptação** – O serviço está a desencriptar ficheiros e, possivelmente, a solicitar a desencriptação de ficheiros bloqueados.
- **Desencriptar no reinício (parcial)** – O varrimento de desencriptação está concluído e alguns ficheiros bloqueados (mas não todos) serão desencriptados no próximo reinício.
- **Desencriptar no reinício** – O varrimento de desencriptação está concluído e todos os ficheiros bloqueados serão desencriptados no próximo reinício.
- **Não foi possível desencriptar todos os ficheiros** – O varrimento de desencriptação foi concluído, mas não foi possível desencriptar todos os ficheiros. Este estado significa que ocorreu uma das seguintes situações:
  - Não foi possível agendar a desencriptação dos ficheiros bloqueados, uma vez que eram demasiado grandes ou ocorreu um erro ao realizar o pedido de desbloqueio dos mesmos.
  - Ocorreu um erro de entrada/saída ao desencriptar os ficheiros.
  - Não foi possível desencriptar os ficheiros através da política.
  - Os ficheiros estão marcados como devendo estar encriptados.
  - Ocorreu um erro durante o varrimento de desencriptação.
  - Em todos os casos, é criado um ficheiro de registo (se estiver configurada a criação de registos) quando estiver definido LogVerbosity=2 (ou superior). Para a resolução de problemas, defina a verbosidade do registo para 2 e reinicie o serviço do Agente de Remoção de Encriptação para forçar outro varrimento de desencriptação.

- **Concluído** - O varrimento da desencriptação está concluído. É agendada a eliminação do serviço, do executável, do controlador e do executável do controlador para a reinicialização de sistema seguinte.

Resolução de problemas do cliente Advanced Threat Prevention

Encontrar o código do produto com o Windows PowerShell

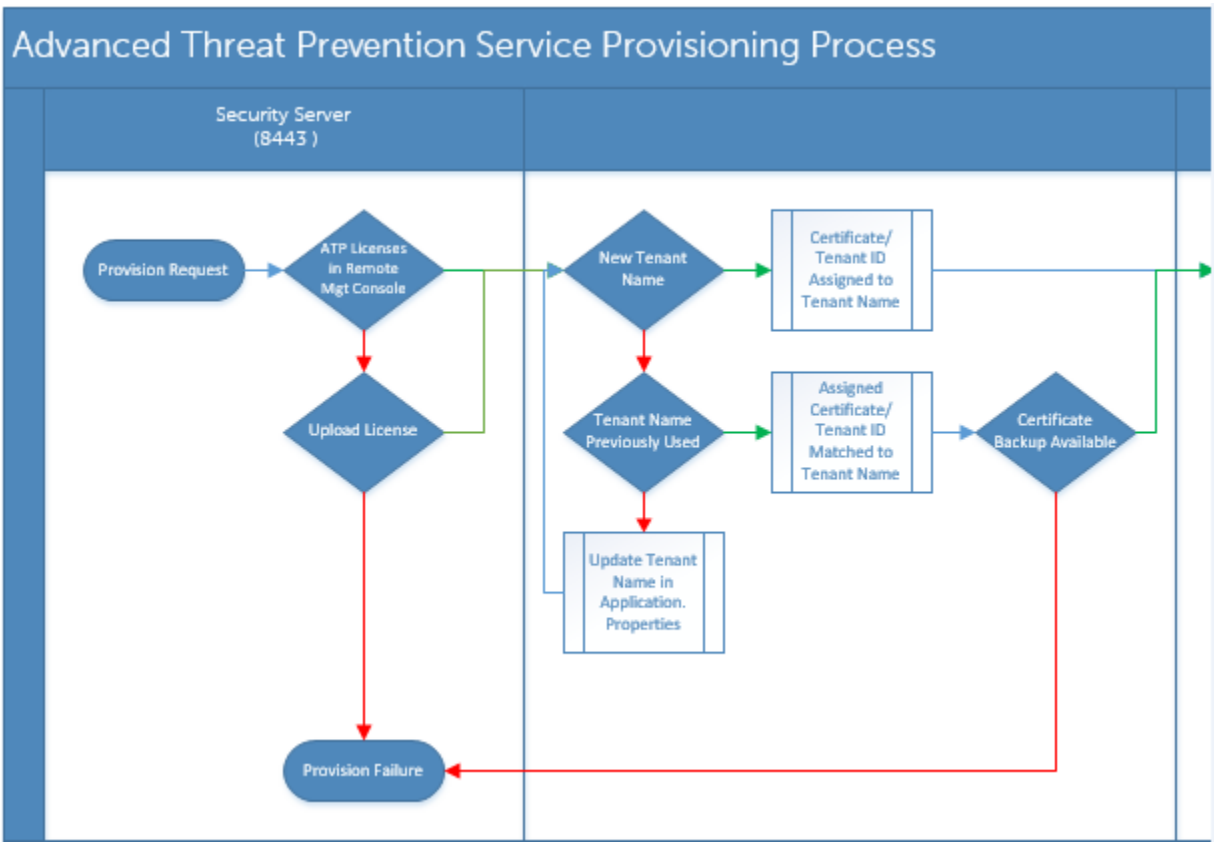
- Pode identificar facilmente o código do produto, se o código do produto mudar no futuro, utilizando este método.

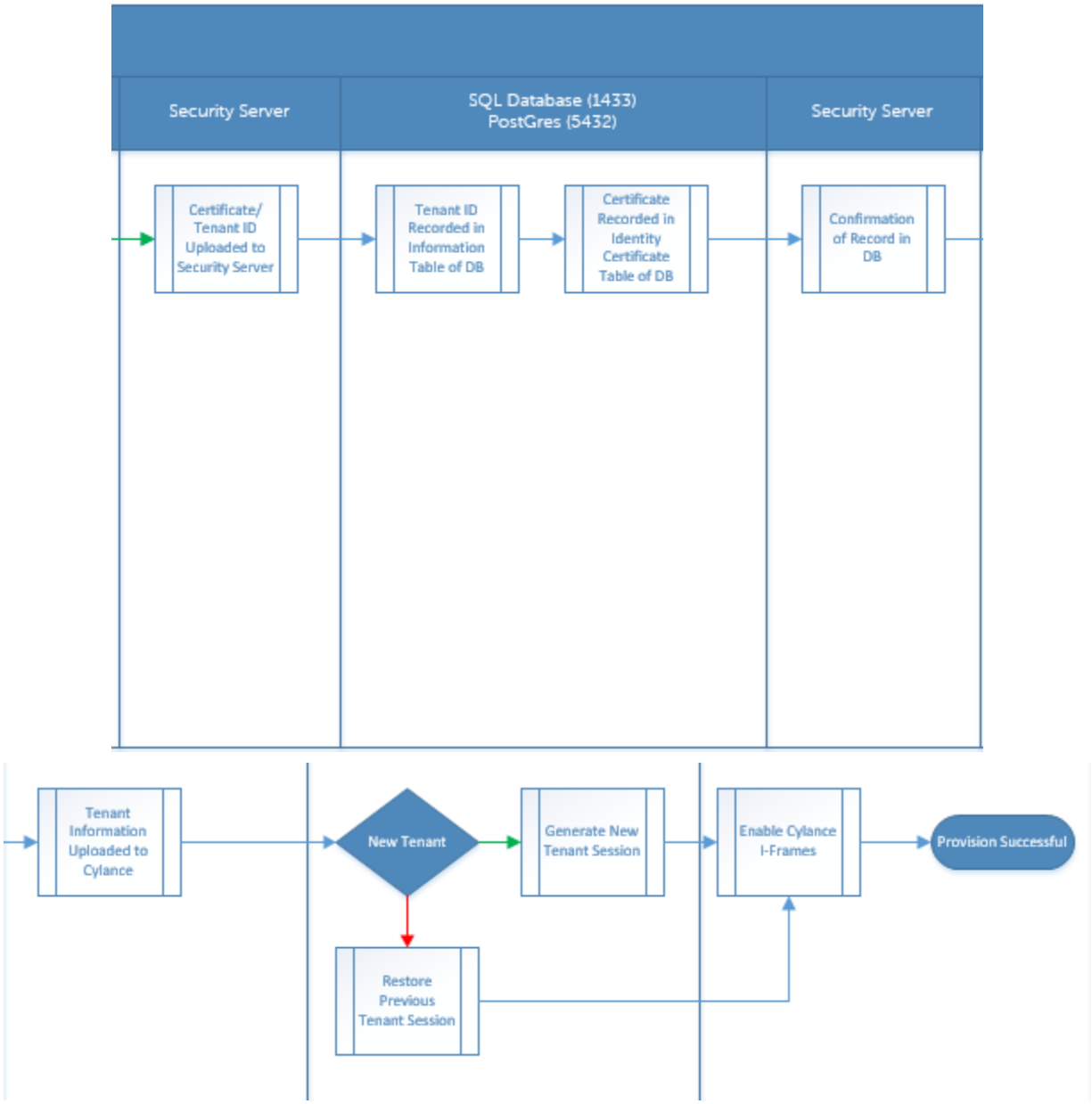
  ```
  Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT
  IdentifyingNumber, Name, LocalPackage
  ```

  O resultado é o caminho completo e o nome do ficheiro .msi (o nome hexadecimal convertido do ficheiro).

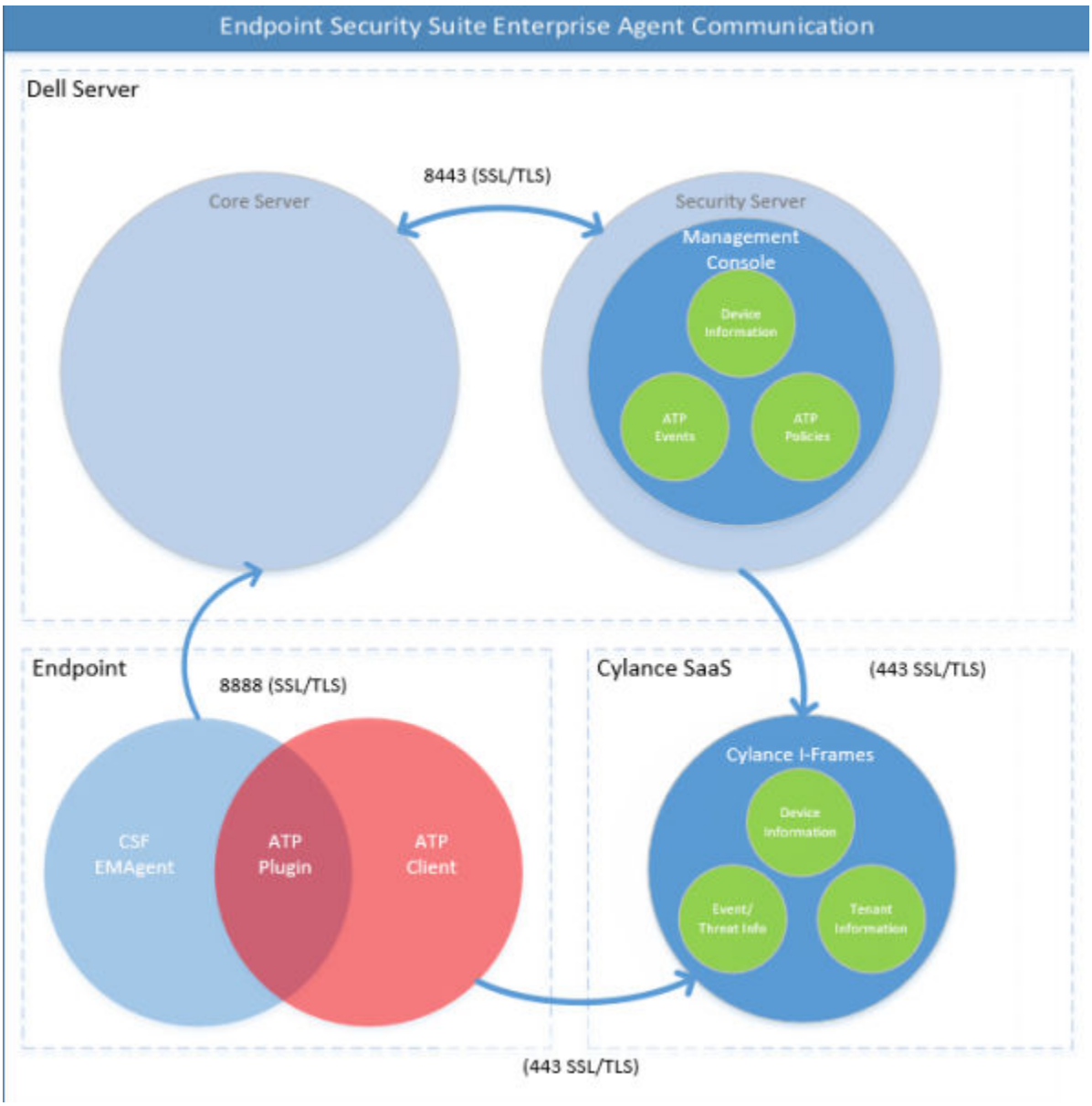
Aprovisionamento e comunicação do agente do Advanced Threat Prevention

Os diagramas seguintes ilustram o processo de aprovisionamento do serviço do Advanced Threat Prevention.



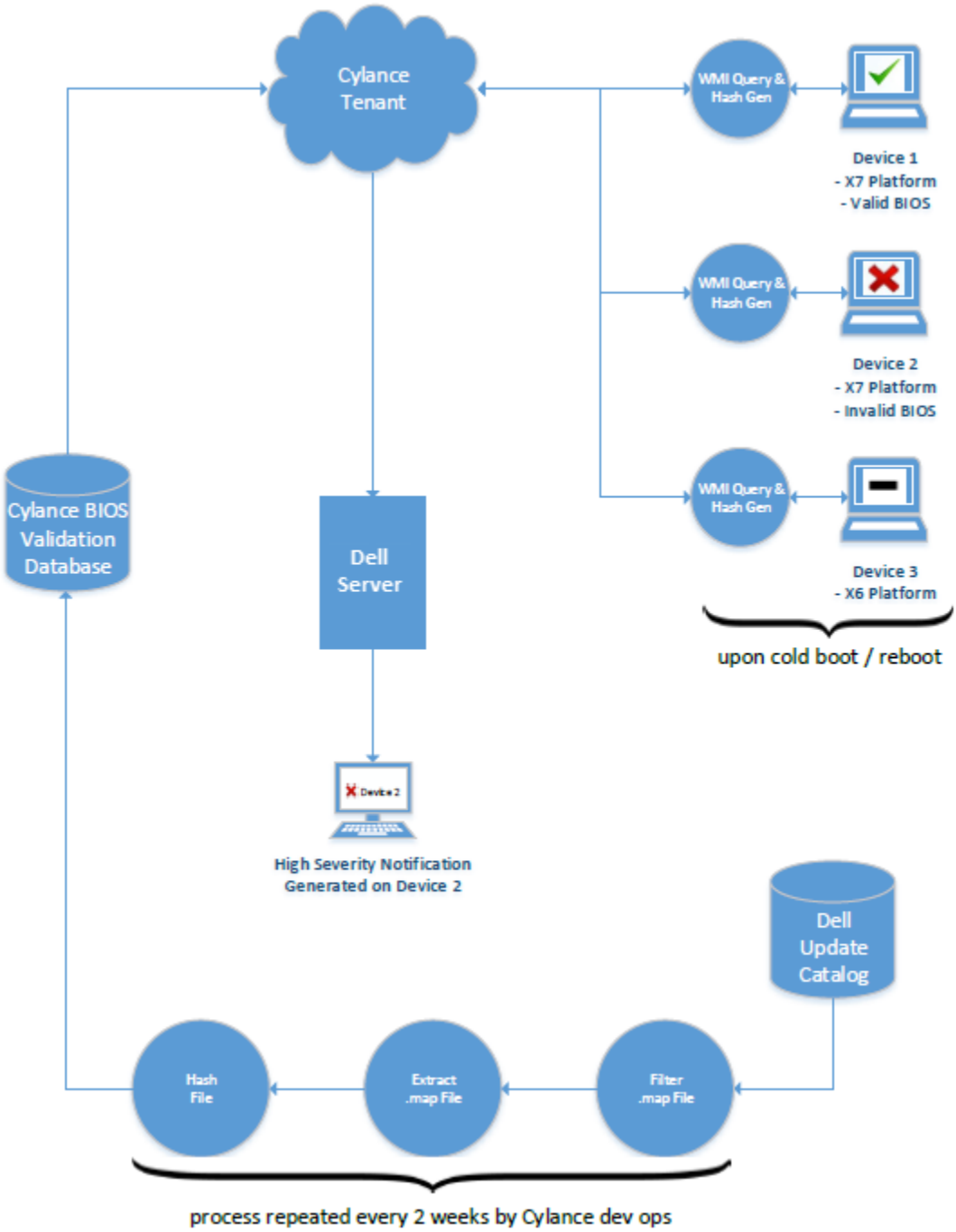


O diagrama seguinte ilustra o processo de comunicação do agente do Advanced Threat Prevention.



Processo de verificação da integridade de imagem do BIOS

O diagrama seguinte ilustra o processo de verificação da integridade de imagem do BIOS. Para aceder a uma lista de modelos de computador Dell suportados pela verificação da integridade de imagem do BIOS, consulte Requisitos - Verificação da integridade de imagem do BIOS.



Controladores do Dell ControlVault

Atualização de controladores e firmware do Dell ControlVault

Os controladores e firmware do Dell ControlVault instalados de fábrica nos computadores Dell estão desatualizados e devem ser atualizados mediante o procedimento abaixo descrito e na ordem em que se encontra.

Se uma mensagem de erro for apresentada durante a instalação do cliente e lhe pedir para sair do programa de instalação para atualizar os controladores do Dell ControlVault, pode seguramente dispensar a mensagem para continuar a instalação do cliente. Os controladores (e firmware) do Dell ControlVault podem ser atualizados após a conclusão da instalação do cliente.

Transferência dos controladores mais recentes

1 Aceda a support.dell.com.
2 Selecione o modelo do seu computador.
3 Selecione **Controladores e transferências**.
4 Selecione o **Sistema operativo** do computador de destino.
5 Expanda a categoria **Segurança**.
6 Transfira e guarde os controladores do Dell ControlVault.
7 Transfira e guarde o firmware do Dell ControlVault.
8 Copie os controladores e o firmware nos computadores de destino, se necessário.

Instale o controlador do Dell ControlVault

Navegue até à pasta para onde transferiu o ficheiro de instalação do controlador.

Clique duas vezes no controlador do Dell ControlVault para iniciar o ficheiro executável de extração automática.

:

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

Clique em **Continuar** para iniciar.

Clique em **Ok** para descomprimir os ficheiros de controladores na localização predefinida em C:\Dell\Drivers\<Nova Pasta>.

Clique em **Sim** para permitir a criação de uma nova pasta.

Clique em **Ok** quando for apresentada a mensagem de que a descompressão dos ficheiros foi bem-sucedida.

A pasta que contém os ficheiros deve ser apresentada após a extração. Caso não seja apresentada, navegue até à pasta na qual extraiu os ficheiros. Neste caso, a pasta é **JW22F**.

Clique duas vezes em **CVHCI64.MSI** para iniciar o programa de instalação dos controladores. [este exemplo é **CVHCI64.MSI** neste modelo (CVHCI para um computador de 32 bits)].

Clique em **Seguinte** no ecrã de boas-vindas.

Clique em **Seguinte** para instalar os controladores na localização predefinida de C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.

Selecione a opção **Completo** e clique em **Seguinte**.

Clique em **Instalar** para iniciar a instalação dos controladores.

Opcionalmente, marque a caixa para apresentar o ficheiro de registo do programa de instalação. Clique em **Concluir** para sair do assistente.

Verificação da instalação dos controladores

O Gestor de dispositivos terá um dispositivo Dell ControlVault (e outros dispositivos) dependendo da configuração de hardware e do sistema operativo.

Instalação do firmware do Dell ControlVault

1 Navegue até à pasta para onde transferiu o ficheiro de instalação do firmware.
2 Clique duas vezes no firmware do Dell ControlVault para iniciar o ficheiro executável de extração automática.
3 Clique em **Continuar** para iniciar.
4 Clique em **Ok** para descomprimir os ficheiros de controladores na localização predefinida em C:\Dell\Drivers\<Nova Pasta>.
5 Clique em **Sim** para permitir a criação de uma nova pasta.
6 Clique em **Ok** quando for apresentada a mensagem de que a descompressão dos ficheiros foi bem-sucedida.
7 A pasta que contém os ficheiros deve ser apresentada após a extração. Caso não seja apresentada, navegue até à pasta na qual extraiu os ficheiros. Selecione a pasta de **firmware**.
8 Clique duas vezes em **ushupgrade.exe** para iniciar o programa de instalação do firmware.

9 Clique em **Iniciar** para iniciar a atualização do firmware.

:

No caso de atualização a partir de uma versão mais antiga de firmware, pode ser-lhe solicitada a palavra-passe de administrador. Introduza **Broadcom** como palavra-passe e clique em **Enter** se esta caixa de diálogo for apresentada.

Várias mensagens de estado serão apresentadas.

10 Clique em **Reiniciar** para concluir a atualização do firmware.

A atualização dos controladores e do firmware do Dell ControlVault foi concluída.

13

Glossário

Advanced Threat Prevention - O produto Advanced Threat Prevention é uma proteção antivírus de última geração que utiliza ciência algorítmica e aprendizagem automática (machine learning) para identificar, classificar e evitar que as ameaças virtuais, conhecidas e desconhecidas, sejam executadas ou danifiquem os endpoints. A funcionalidade opcional Client Firewall monitoriza as comunicações entre o computador e recursos na rede e na Internet e intercepta comunicações potencialmente maliciosas. A funcionalidade opcional de Web Protection bloqueia Websites e transferências de Websites que não são seguros durante a navegação e pesquisa online, com base em classificações de segurança e relatórios para Websites.

BitLocker Manager - O BitLocker do Windows foi concebido para ajudar a proteger computadores Windows através da encriptação de ficheiros do sistema operativo e dados. Para melhorar a segurança das implementações do BitLocker e para simplificar e reduzir o custo de propriedade, a Dell fornece uma consola de gestão central e única que aborda muitas preocupações de segurança e oferece uma abordagem integrada para gerir a encriptação através de outras plataformas que não o BitLocker, seja de forma física, virtual ou baseada na nuvem. O BitLocker Manager suporta a encriptação do BitLocker para sistemas operativos, unidades fixas e BitLocker To Go. O BitLocker Manager permite-lhe integrar o BitLocker diretamente nas suas necessidades de encriptação existentes e gerir o BitLocker com o mínimo de esforço enquanto agiliza a segurança e conformidade. O BitLocker Manager fornece gestão integrada para a recuperação de chaves, gestão e aplicação de políticas, gestão TPM automatizada, conformidade FIPS e relatórios de conformidade.

Desativar - A desativação ocorre quando o SED Management é desligado na Management Console. Após a desativação do computador, a base de dados da PBA é eliminada e deixa de existir registo dos utilizadores em cache.

Encryption External Media - Este serviço dentro do Dell Encryption Client aplica políticas a suportes de dados amovíveis e a dispositivos de armazenamento externos.

Código de acesso do Encryption External Media - Este serviço do Dell Server permite a recuperação de dispositivos protegidos pelo Encryption External Media, caso o utilizador se esqueça da palavra-passe e já não consiga iniciar sessão. Concluir este processo permite ao utilizador repor a palavra-passe definida no suporte de dados.

Encryption Client - O Encryption Client é o componente no dispositivo que aplica as políticas de segurança, quer o endpoint esteja ligado à rede, desligado da rede, ou seja perdido ou roubado. Ao criar um ambiente de computação fidedigno para endpoints, o cliente Encryption funciona como uma camada no topo do sistema operativo do dispositivo e proporciona autenticação, encriptação e autorização aplicadas de forma consistente para maximizar a proteção de informações sensíveis.

Endpoint - Um computador que é gerido pelo Dell Server.

Varrimento de encriptação - Um varrimento de encriptação é o processo de análise das pastas a serem encriptadas num ponto final gerido para assegurar que os ficheiros contidos estão no estado de encriptação adequado. As operações comuns de criação e mudança de nome de ficheiros não acionam um varrimento de encriptação. É importante entender quando pode ocorrer um varrimento de encriptação e o que pode afetar os tempos de varrimento resultantes, da seguinte forma: - Um varrimento de encriptação ocorre após a receção inicial de uma política com a encriptação ativada. Isto pode ocorrer imediatamente depois da ativação se a sua política tem a encriptação ativada. - Se a política Analisar ambiente de trabalho ao iniciar sessão estiver ativada, as pastas especificadas para a encriptação são submetidas a varrimento em cada início de sessão do utilizador. - Um varrimento pode ser acionado novamente sob determinadas alterações de política subsequentes. Qualquer alteração de política relacionada com a definição das pastas de encriptação, algoritmos de encriptação, utilização da chave de encriptação (utilizador de versos comuns), aciona um varrimento. Adicionalmente, a alternância entre a encriptação ativada e desativada aciona um varrimento de encriptação.

Gestão SED - A Gestão SED disponibiliza uma plataforma para gerir de forma segura as unidades de encriptação automática. Embora as SEDs forneçam a sua própria encriptação, carecem de uma plataforma para gerir a sua encriptação e políticas disponíveis. A Gestão de SED é uma componente de gestão central e escalável que lhe permite proteger e gerir os seus dados de forma mais eficaz. O SED Management assegura que pode administrar a sua empresa de forma mais rápida e fácil.

Utilizador de servidor – Uma conta de utilizador virtual criada pelo Dell Server Encryption para gestão das atualizações de políticas e chaves de encriptação. Esta conta de utilizador não corresponde a nenhuma outra conta de utilizador do computador ou do domínio, não tendo um nome de utilizador ou uma palavra-passe que possam ser fisicamente utilizados. Um valor UCID exclusivo é atribuído à conta na Management Console.