Dell Data Protection | Endpoint Security Suite Enterprise

Guia de instalação avançada v1.4

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.

Guia de instalação avançada do Endpoint Security Suite Enterprise

2017 - 04

Rev. A01

Índice

1

Introdução

Este guia explica como instalar e configurar o Advanced Threat Protection, o o cliente Encryption, o cliente de gestão de SED, a Advanced Authentication e o BitLocker Manager.

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

Antes de começar

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

- *Guia de instalação e migração do DDP Enterprise Server*
- *DDP Enterprise Server - Guia de instalação e Guia de início rápido do Virtual Edition*

Certifique-se de que as políticas foram definidas da forma pretendida. Navegue no AdminHelp, disponível através de **?** no lado 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 EE Server/VE Server.

2 Aprovisionar um inquilino para o Advanced Threat Prevention. Deve ser aprovisionado um inquilino no Servidor DDP 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 finais.

Utilizar este guia

Utilize este guia pela seguinte ordem.

- Consulte Requisitos para obter informações sobre os pré-requisitos do cliente, hardware do computador e informações, limitações e modificações de registo especiais do software necessárias às funcionalidades.
- Se necessário, consulte Configuração da pré-instalação para Palavra-passe monouso, UEFI SED e BitLocker.
- Se os seus clientes forem elegíveis para utilizar o Dell Digital Delivery (DDD), consulte Definir GPO no controlador do domínio para ativar elegibilidades.
- Se instalar clientes utilizando o instalador principal do ESSE , consulte:
  - Instalar interativamente utilizando o instalador principal do ESSE

    ou
  - Instalar por linha de comandos utilizando o instalador principal do ESSE
- Se instalar clientes utilizando os instaladores subordinados, os ficheiros executáveis do instalador subordinado devem ser extraídos do instalador principal do ESSE . Consulte Extrair os instaladores subordinados do instalador principal do ESSE e, em seguida, regresse aqui.
  - Instalar instaladores subordinados através da linha de comandos:
    - Instalar controladores - Transfira os controladores e firmware adequados com base no seu hardware de autenticação.
    - Instalar o Encryption Client - utilize estas instruções para instalar o Encryption Client, que é o componente que aplica a política de segurança, quer o computador esteja ligado à rede, desligado da rede, ou seja perdido ou roubado.

- Instalar o cliente Advanced Threat Prevention - utilize estas instruções para instalar o cliente Advanced Threat Prevention, que é uma proteção antivírus de última geração que utiliza ciência algorítmica e aprendizagem por máquina para identificar, classificar e evitar que as ameaças virtuais, conhecidas e desconhecidas, sejam executadas ou danifiquem endpoints.
- Instalar o Web Protection e Firewall - utilize estas instruções para instalar as funcionalidades *opcionais* Web Protection e Firewall. O Client Firewall é uma firewall com monitorização de estado que 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.
- Instalar os clientes de Gestão de SED e Advanced Authentication - utilize estas instruções para instalar software de encriptação para SED. Embora as SED forneçam a sua própria encriptação, carecem de uma plataforma para gerir a sua encriptação e políticas. Com a Gestão de SED, todas as políticas, o armazenamento e a recuperação de chaves de encriptação ficam disponíveis numa só consola, reduzindo o risco de os computadores ficarem desprotegidos em caso de perda de acesso ou acesso não autorizado.

  O cliente Advanced Authentication gere vários métodos de autenticação, incluindo PBA para SED, Início de sessão único (SSO) e credenciais do utilizador, como impressões digitais e palavras-passe. Além disso, fornece recursos de Advanced Authentication para aceder a Web sites e aplicações.
- Instalar o cliente BitLocker Manager - utilize estas instruções para instalar o cliente BitLocker Manager, concebido para melhorar a segurança das implementações do BitLocker e para simplificar e reduzir o custo de propriedade.

  NOTA:
  A maioria dos instaladores subordinados pode ser instalado interativamente, mas as instalações não são descritas neste guia. Contudo, o instalador subordinado do cliente Advanced Threat Prevention apenas pode ser instalado por linha de comandos.

- Consulte Cenários normalmente utilizados para obter scripts dos nossos cenários mais comuns.

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 Data Protection.

Adicionalmente, o suporte online para os produtos Dell Data Protection 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 disponível quando nos contactar.

Para número de telefone fora dos Estados Unidos, consulte Dell ProSupport International Phone Numbers (Números de telefone internacionais do Dell ProSupport).

Requisitos

Todos os clientes

Estes requisitos aplicam-se a todos os clientes. Os requisitos indicados nas outras seções aplicam-se a clientes específicos.

- 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, que poderá ser atribuído temporariamente por uma ferramenta de implementação, como o Microsoft SMS ou Dell 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.
- Se os clientes do instalador principal do ESSE estiverem autorizados a utilizar o Dell Digital Delivery (DDD), certifique-se de que a porta de saída 443 está disponível para comunicar com o EE Server/VE Server. A funcionalidade de elegibilidade não funcionará se a porta 443 estiver bloqueada (por qualquer motivo). O DDD não é utilizado se a instalação for efetuada utilizando os instaladores subordinados.
- Assegure-se de verificar periodicamente a página www.dell.com/support para procurar a documentação mais atual e Conselhos técnicos.

Todos os clientes - Pré-requisitos

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

  Todos os computadores enviados da fábrica da Dell são previamente equipados com a versão completa do Microsoft .Net Framework 4.5.2 (ou posterior). No entanto, se não instalar em hardware Dell ou se atualizar o cliente num hardware Dell mais antigo, deve verificar qual a versão do Microsoft .Net instalada e atualizar a versão, **antes de instalar o cliente** para impedir falhas na instalação/atualização. 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.
- Os controladores e firmware do ControlVault, leitores de impressão digital e de smart cards (conforme abaixo ilustrado) não estão incluídos nos ficheiros executáveis do instalador principal ou do instalador subordinado do ESSE . Os controladores e firmware têm de ser mantidos atualizados e podem ser transferidos a partir de http://www.dell.com/support e selecionando o seu modelo de computador. Transfira os controladores e firmware adequados com base no seu hardware de autenticação.

  - ControlVault
  - NEXT Biometrics Fingerprint Driver
  - Validity FingerPrint Reader 495 Driver
  - O2Micro Smart Card Driver

  Se estiver a realizar a instalação em hardware não Dell, transfira os controladores e firmware atualizados a partir do Web site do fornecedor correspondente. As instruções de instalação dos controladores do ControlVault estão disponíveis em Atualizar firmware e controladores do Dell ControlVault.

Todos os clientes - Hardware

- A tabela seguinte apresenta o hardware de computador suportado.

Hardware
• Os requisitos mínimos de hardware necessitam atender as especificações mínimas do sistema operativo.

Todos os clientes - Suporte de idiomas

- Os clientes Encryption, Advanced Threat Prevention e BitLocker Manager estão em conformidade com a norma Interface de Utilizador Multilingue (MUI) e suportam os seguintes idiomas. Os dados do Advanced Threat Prevention apresentados na Remote Management Console apenas estão disponíveis em inglês.

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

- Os clientes SED e Advanced Authentication são uma Interface de Utilizador Multilingue (MUI) compatível e suportam os seguintes idiomas. O modo UEFI e a Autenticação de pré-arranque não são suportados em russo, chinês tradicional ou chinês simplificado.

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

Cliente Encryption

- O computador cliente deve ter conectividade de rede para ativar.
- Para reduzir o tempo de encriptação inicial, execute o Assistente de limpeza de disco do Windows para remover ficheiros temporários e quaisquer outros dados desnecessários.
- 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 Encryption agora suporta o modo Audit. O modo Audit permite que os administradores implementem o cliente Encryption como parte da imagem corporativa, em vez de usar um SCCM de terceiros ou uma solução similar para implementar o cliente

Encryption. Para instruções sobre como instalar o cliente Encryption numa imagem corporativa, consulte http://www.dell.com/support/article/us/en/19/SLN304039.

- O cliente Encryption foi sujeito a testes e é compatível com McAfee, com o cliente Symantec, Kaspersky e MalwareBytes. 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/SLN298707 ou contacte o Dell ProSupport para obter assistência.
- O TPM é utilizado para selar o GPK. Assim, se o cliente Encryption Client for executado, limpe o TPM no BIOS antes de proceder à instalação de um novo sistema operativo no computador cliente.
- Não é suportada a atualização de versão do sistema operativo com o cliente Encryption instalado. Desinstale e desencripte o cliente Encryption, atualize para o novo sistema operativo e, em seguida, reinstale o cliente Encryption.

  Para além disso, não são suportadas reinstalações de sistema operativo. 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

- O instalador principal do ESSE instala o Microsoft Visual C++ 2012 Update 4, se este ainda não estiver instalado no computador. **Quando utilizar o instalador subordinado**, é necessário instalar este componente antes de instalar o cliente Encryption.

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

Hardware do Encryption Client

- A tabela seguinte indica o hardware suportado.

Hardware opcional incorporado
• TPM 1.2 ou 2.0

Sistemas operativos do Encryption Client

- A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos Windows (32 e 64 bits)
• Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
• Windows Embedded Standard 7 com modelo de Compatibilidade entre Aplicações (a encriptação do hardware não é suportada)
• Windows 8: Enterprise, Pro
• Windows 8.1 Atualização 0-1: Enterprise Edition, Pro Edition
• Windows Embedded 8.1 Industry Enterprise (a encriptação do hardware não é suportada)
• Windows 10: Education, Enterprise, Pro
• VMware Workstation 5.5 e posterior

NOTA:
O modo UEFI não é suportado no Windows 7, Windows Embedded Standard 7 ou Windows Embedded 8.1 Industry Enterprise.

Sistemas operativos do External Media Shield (EMS)

- A tabela seguinte apresenta os sistemas operativos suportados ao aceder a suportes com proteção EMS.

  NOTA:
  O External Media deve ter, aproximadamente, 55 MB disponíveis, bem como espaço livre no suporte multimédia igual ao maior ficheiro a encriptar para alojar o EMS.

  NOTA:
  O Windows XP é suportado apenas quando se utiliza o EMS Explorer.

Sistemas operativos Windows compatíveis para aceder a suportes multimédia protegidos pelo EMS (32 e 64 bits)

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

Sistemas operativos Mac compatíveis para aceder a suportes multimédia protegidos pelo EMS (kernels de 64 bits)

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

Server Encryption Client

O Server Encryption destina-se a ser utilizado em computadores no modo de servidor, principalmente os servidores de ficheiros.

- O Server Encryption apenas é compatível com o Enterprise Edition e com o Endpoint Security Suite Enterprise.
- O Server Encryption oferece o seguinte:
  - A encriptação do software
  - Encriptação do armazenamento amovível
  - Controlo de portas

    NOTA:
    O servidor terá de suportar controlo de portas.

    As políticas de Sistema de Controlo de Portas afetam os suportes de dados amovíveis em servidores protegidos, por exemplo, controlando o acesso e a utilização das portas USB do servidor por parte dos dispositivos USB. A política de portas USB aplica-se a portas USB externas. A funcionalidade das portas USB internas não é afetada pela política de portas USB. No caso de a política de portas USB ser desativada, o teclado e rato do cliente USB não irá funcionar e o utilizador não será capaz de utilizar o computador, salvo se, antes da aplicação da política, for estabelecida uma Ligação ao Ambiente de Trabalho Remoto.

O Server Encryption destina-se a ser utilizado em:

- Servidores de ficheiros com unidades de disco locais
- Convidados de Máquina Virtual (VM) com sistema operativo de Servidor ou um sistema operativo que não seja de Servidor funcionando simplesmente como servidor de ficheiros

- Configurações suportadas:
  - Servidores equipados com unidades RAID 5 ou 10; RAID 0 (repartição) e RAID 1 (espelhamento) são suportados de forma independente um do outro.
  - Servidores equipados com unidades Multi TB RAID
  - Servidores equipados com unidades que possam ser substituídas sem ter de desligar o computador
  - O Server Encryption foi sujeito a testes e é compatível com clientes McAfee VirusScan, Symantec, Kaspersky Anti-Virus e MalwareBytes Anti-Malware. Existem exclusões pré-programadas para estes fornecedores de antivírus, por forma evitar incompatibilidades entre a deteção de vírus e a encriptação. Se a sua organização utilizar um antivírus de um fornecedor não indicado na lista, consulte o artigo KB SLN298707 ou contacte o Dell ProSupport para obter assistência.

Não Suportado

O Server Encryption não se destina a ser utilizado em:

- O Dell Data Protection Server ou servidores com bases de dados em execução para o Dell Data Protection Server
- O Server Encryption não é compatível com o Endpoint Security Suite, Personal Edition ou Security Tools.
- O Server Encryption não é suportado com o cliente de Gestão SED ou BitLocker Manager.
- A migração para ou a partir do Server Encryption não é suportada. As atualizações do External Media Edition para o Server Encryption requerem a desinstalação completa do produto ou produtos anteriores antes de instalar o Server Encryption.
- Anfitriões VM (Uma VM contém, tipicamente, múltiplos convidados VM.)
- Controladores de Domínio
- Servidores Exchange
- Servidores que alberguem bases de dados (SQL, Sybase, SharePoint, Oracle, MySQL, Exchange, etc.)
- Servidores que façam uso de qualquer uma das seguintes tecnologias:
  - Sistemas de ficheiros resilientes
  - Sistemas de ficheiros fluidos
  - Espaços de armazenamento Microsoft
  - Soluções de armazenamento de rede SAN/NAS
  - Dispositivos conectados por iSCSI
  - Software de eliminação de duplicados
  - Eliminação de duplicados de hardware
  - RAIDs divididos (múltiplos volumes num único RAID)
  - Unidades SED (RAIDs e Não-RAID)
  - Início de sessão automático (Windows OS 7, 8/8.1) para quiosques
  - Início de sessão automático (Windows OS 7, 8/8.1) para quiosques
- O Server 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.
- A atualização de sistema operativo no local não é suportada pelo Server Encryption. Para atualizar o seu sistema operativo, desinstale e desencripte o Server Encryption, atualize para o novo sistema operativo e, em seguida, instale novamente o Server Encryption.

  Além disso, não são suportadas reinstalações do sistema operativo. Se pretender reinstalar o sistema operativo, efetue uma cópia de segurança do computador de destino, limpe o computador, instale o sistema operativo e, em seguida, execute a recuperação dos dados encriptados seguindo os procedimentos de recuperação. Para obter mais informações sobre a recuperação de dados encriptados, consulte o *Guia de recuperação*.

Pré-requisitos do Server Encryption Client

- Antes de instalar o Server Encryption Client, deve instalar este componente.

Pré-requisito

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

Hardware do Server Encryption Client

Os requisitos mínimos de hardware necessitam atender as especificações mínimas do sistema operativo.

Sistemas operativos do Server Encryption Client

A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos (32 e 64 bits)

- Windows 7 SP0-SP1: Home, Enterprise, Professional, Ultimate
- Windows 8.0: Enterprise, Pro
- Windows 8.1 - Windows 8.1 Update 1: Enterprise Edition, Pro Edition
- Windows 10: Education Edition, Enterprise Edition, Pro Edition

Sistemas Operativo de Servidor Suportados

- Windows Server 2008 SP2: Standard Edition, Datacenter Edition com e sem Hyper-V, Enterprise Edition com e sem Hyper-V, Foundation Server Edition
- Windows Server 2008 R2 SP1: Standard Edition, Datacenter Edition com e sem Hyper-V, Enterprise Edition com e sem Hyper-V, Foundation Edition, Webserver Edition
- Windows Server 2012: Standard Edition, Essentials Edition, Foundation Edition, Datacenter Edition
- Windows Server 2012 R2: Standard Edition, Essentials Edition, Foundation Edition, Datacenter Edition
- Windows Server 2016: Standard Edition, Essentials Edition, Datacenter Edition

Sistemas operativos suportados com modo UEFI

- Windows 8: Enterprise, Pro
- Windows 8.1 - Windows 8.1 Update 1: Enterprise Edition, Pro Edition
- Windows 10: Education Edition, Enterprise Edition, Pro Edition

NOTA:

Num computador compatível com UEFI, depois de selecionar **Reiniciar** no menu principal, o computador reinicia-se e apresenta um de dois ecrãs de início de sessão possíveis. O ecrã de início de sessão que aparece é determinado por diferenças na arquitetura da plataforma do computador.

Sistemas operativos do External Media Shield (EMS)

A tabela seguinte apresenta os sistemas operativos suportados ao aceder a suportes com proteção EMS.

NOTA:

O External Media deve ter, aproximadamente, 55 MB disponíveis, bem como espaço livre no suporte multimédia igual ao maior ficheiro a encriptar para alojar o EMS.

NOTA:
O Windows XP é suportado apenas quando se utiliza o EMS Explorer.

Sistemas operativos Windows compatíveis para aceder a suportes multimédia protegidos pelo EMS (32 e 64 bits)

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

Sistemas Operativo de Servidor Suportados

- Windows Server 2008 SP1 ou posterior
- Windows Server 2012 R2

Sistemas operativos Mac compatíveis para aceder a suportes multimédia protegidos pelo EMS (kernels de 64 bits)

- Mac OS X Mavericks 10.9.5
- OS X Yosemite 10.10.5
- OS X El Capitan 10.11.4 e 10.11.5

Cliente Advanced Threat Prevention

- Não é possível instalar o cliente Advanced Threat Prevention sem que o cliente Dell Client Security Framework (EMAgent) seja detetado no computador. Se tentar, a instalação irá falhar.
- Para concluir a instalação do Advanced Threat Prevention, quando o Dell Enterprise Server/VE 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.

  NOTA: Não é necessário haver ligação à Internet quando o Dell Server está em execução no Modo desligado
- As funcionalidades opcionais de Client Firewall e Proteção Web ***não*** devem ser instaladas nos computadores cliente que são geridos pelo Dell Enterprise Server/VE 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 Protection no Dell Server e às outras aplicações. Para obter instruções sobre como adicionar exclusões ao Advanced Threat Protection no Dell Server, consulte http://www.dell.com/support/article/us/en/04/SLN300970. Para obter uma lista de exclusões a adicionar às outras aplicações de antivírus, consulte http://www.dell.com/support/article/us/en/19/SLN301134.

Sistemas operativos do Advanced Threat Prevention

- A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos Windows (32 e 64 bits)

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

Sistemas operativos Windows (32 e 64 bits)

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Portas do Advanced Threat Prevention

- Os agentes do Advanced Threat Prevention são 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

Verificação da integridade de imagem do BIOS

Se a política *Ativar garantia do BIOS* for selecionada na Remote Management Console, o inquilino Cylance valida o hash do BIOS nos sistemas de utilizador final para assegurar que o BIOS não foi modificado em relação à versão de fábrica da Dell, que é um possível vetor de ataques. Se for detetada uma ameaça, é transmitida uma notificação para o Servidor DDP e o administrador de TI é alertado na Remote 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

Cliente SED

- Para instalar a gestão SED com êxito, o computador deve possuir uma ligação à rede com fios.
- O IPv6 não é suportado.

- 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 apresentar um ecrã azul quando alterar de *RAID=On* to *AHCI*.
- A Gestão SED não é suportada com o Server Encryption ou o Advanced Threat Prevention num SO de servidor.

Controladores OPAL

- As SED compatíveis com OPAL suportadas requerem controladores Intel Rapid Storage Technology atualizados, localizados em http://www.dell.com/support.

Pré-requisitos do cliente SED

- O instalador principal do ESSE instala o Microsoft Visual C++2010 SP1 **e** o Microsoft Visual C++ 2012 Update 4, se estes ainda não estiverem instalados no computador. **Quando utilizar o instalador subordinado**, deve instalar estes componentes antes de instalar a gestão SED.

Pré-requisitos
• Visual C++ 2010 SP1 ou Redistributable Package posterior (x86 e x64) • Visual C++ 2012 Update 4 ou Redistributable Package posterior (x86 e x64)

Hardware do cliente SED

SED compatíveis com OPAL

- Para aceder à lista mais atualizada de SED compatíveis com Opal suportadas pela gestão SED, consulte este artigo KB: http://www.dell.com/support/article/us/en/19/SLN296720.

Modelos de computador Dell suportados com UEFI

- A tabela seguinte apresenta os modelos de computadores Dell compatíveis com UEFI.

Modelos de computador Dell - Suporte para UEFI

- Latitude 5280
- Latitude 5480
- Latitude 5580
- Latitude 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7240
- Latitude E7250
- Latitude E7260
- Latitude E7265
- Latitude E7270
- Latitude E7275
- Latitude E7280
- Latitude E7350
- Latitude E7440
- Latitude E7450
- Latitude E7460
- Latitude E7470
- Latitude E7480
- Latitude 12 Rugged Extreme
- Latitude 12 Rugged Tablet (Modelo 7202)
- Latitude 14 Rugged Extreme
- Latitude 14 Rugged
- Precision M3510
- Precision M4800
- Precision M5510
- Precision M5520
- Precision M6800
- Precision M7510
- Precision M7520
- Precision M7710
- Precision M7720
- Precision T3420
- Precision T3620
- Precision T7810
- Optiplex 3040 Micro, minitorre, fator de forma reduzido
- Optiplex 3046
- OptiPlex 3050 All-In-One
- OptiPlex 3050 Tower, fator de forma reduzido, Micro
- Optiplex 5040 minitorre, fator de forma reduzido
- OptiPlex 5050 Tower, fator de forma reduzido, Micro
- OptiPlex 7020
- Optiplex 7040 Micro, minitorre, fator de forma reduzido
- OptiPlex 7050 Tower, fator de forma reduzido, Micro
- Optiplex 3240 All-In-One
- OptiPlex 5250 All-In-One
- Optiplex 7440 All-In-One
- OptiPlex 7450 All-In-One
- OptiPlex 9020 Micro
- Venue Pro 11 (Modelos 5175/5179)
- Venue Pro 11 (Modelo 7139)

NOTA:
As funcionalidades de autenticação são suportadas com o modo UEFI nestes computadores com Windows 8, Windows 8.1 e Windows 10 com SED compatíveis com Opal qualificadas. Outros computadores com Windows 7, Windows 8, Windows 8.1 e Windows 10 em execução suportam o modo de Arranque Legado.

Teclados internacionais

- 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-CH - Alemão (Suíça)
- DE-FR - Francês (Suíça)

Suporte de teclado internacional - Non-UEFI

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

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 (suportado com o modo de Arranque Legacy, mas não UEFI)

  NOTA:
  O modo de Arranque Legacy é suportado pelo Windows 7. A UEFI não é suportada pelo Windows 7.

- Windows 8: Enterprise, Pro,
- Windows 8.1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

Cliente Advanced Authentication

- Ao utilizar Advanced Authentication, os utilizadores terão acesso seguro ao computador através de credenciais da autenticação avançada geridas e registadas utilizando o Security Tools. O Security Tools será o gestor principal das credenciais de autenticação para o Início de sessão do Windows, incluindo a palavra-passe do Windows, impressões digitais e smart cards. As credenciais de palavra-passe por imagem, PIN e impressão digital registadas através do sistema operativo da Microsoft não serão reconhecidas pelo Início de sessão do Windows.

  Para continuar a utilizar o sistema operativo da Microsoft para gerir as credenciais de utilizador, não instale ou desinstale o Security Tools.
- A funcionalidade Palavra-passe monouso (OTP) do Security Tools requer que um TPM esteja presente, ativado e que tenha proprietário. O OTP não é suportado com o TPM 2.0. Para eliminar e definir a propriedade do TPM, consulte https://technet.microsoft.com.
- Uma SED não requer um TPM para facultar a Advanced Authentication ou encriptação.

Hardware do Cliente Advanced Authentication

- A tabela seguinte lista a autenticação de hardware suportada.

Leitores de impressão digital e de smart cards

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

Cartões sem contacto

- Cartões sem contacto com leitores de cartões sem contacto incorporados nos portáteis Dell especificados

Smart Cards

- Smart Cards PKCS #11 que utilizam o cliente ActivIdentity

  NOTA:
  O cliente ActivIdentity não se encontra pré-carregado e tem de ser instalado separadamente.

- Cartões CSP
- Cartão de acesso comum (CAC)
- Cartões SIPRNet/Classe B

- A tabela seguinte apresenta os modelos de computador Dell compatíveis com cartões SIPR Net.

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

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

Sistemas operativos do Cliente Advanced Authentication

Sistemas operativos Windows

- A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos Windows (32 e 64 bits)

- Windows 7 SP0-SP1: Enterprise, Professional, Ultimate
- Windows 8: Enterprise, Pro
- Windows 8.1 Atualização 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro

NOTA: O modo UEFI não é suportado pelo Windows 7.

Sistemas operativos de dispositivos móveis

- Os sistemas operativos móveis seguintes são suportados com a funcionalidade Palavra-passe monouso do Security Tools.

Sistemas operativos para Android

- 4.0 - 4.0.4 Ice Cream Sandwich
- 4.1 - 4.3.1 Jelly Bean
- 4.4 - 4.4.4 KitKat
- 5.0 - 5.1.1 Lollipop

Sistemas operativos iOS

- iOS 7.x
- iOS 8.x

Sistemas operativos Windows Phone

- Windows Phone 8.1
- Windows 10 Mobile

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. Consulte Configuração da pré-instalação para configurar uma partição de PBA do BitLocker.
- 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 cliente BitLocker Manager irá utilizar os algoritmos com validação FIPS AES aprovados se o modo FIPS for ativado para a definição de segurança GPO "Criptografia do sistema: utilizar algoritmos compatíveis com FIPS para encriptação, hashing e assinatura" no

dispositivo e o mesmo for gerido através do nosso produto. Este modo não é forçado como predefinição para clientes encriptados pelo BitLocker, uma vez que a Microsoft atualmente sugere que os clientes não utilizem a respetiva encriptação validada por FIPS devido a vários problemas com a compatibilidade da aplicação, recuperação e encriptação de suportes multimédia: http://blogs.technet.com.

- O BitLocker Manager não é suportado com o Server Encryption ou o Advanced Threat Prevention num SO de servidor.

Pré-requisitos do cliente BitLocker Manager

- O instalador principal do ESSE instala o Microsoft Visual C++2010 SP1 **e** o Microsoft Visual C++ 2012 Update 4, se estes ainda não estiverem instalados no computador. **Quando utilizar o instalador subordinado**, deve instalar estes componentes antes de instalar o BitLocker Manager.

Pré-requisitos

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

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)
- Windows 8.1: Enterprise Edition, Pro Edition (64 bits)
- Windows 10: Education, Enterprise, Pro
- Windows Server 2008 R2: Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2012
- Windows Server 2012 R2: Standard Edition, Enterprise Edition (64 bits)
- Windows Server 2016

Opções de autenticação

- As opções de autenticação seguintes requerem hardware específico: Impressões digitais, Smart Cards, Cartões sem contacto, Cartões SIPRNet/Classe B e autenticação em computadores com UEFI. As opções seguintes requerem configurações: smart cards com Windows Authentication, smart cards com Autenticação de pré-arranque e Palavra-passe monouso. As tabelas seguintes apresentam as opções de autenticação disponíveis por sistema operativo, quando os requisitos de hardware e de configuração são cumpridos.

Cliente de encriptação

Não UEFI

	PBA					Autenticação do Windows				
	Palavra-passe	**Impressão digital**	**Smart card de contacto**	**Palavra-Passe Monouso**	**Cartão SIPR**	**Palavra-passe**	**Impressão digital**	**Smart card**	**Palavra-Passe Monouso**	**Cartão SIPR**
Windows 7 SP0-SP1						X	X[2]	X[2]	X[1]	X[2]
Windows 8						X	X[2]	X[2]	X[1]	X[2]

Não UEFI

	PBA					Autenticação do Windows				
	Palavra-passe	**Impressão digital**	**Smart card de contacto**	**Palavra-Passe Monouso**	**Cartão SIPR**	**Palavra-passe**	**Impressão digital**	**Smart card**	**Palavra-Passe Monouso**	**Cartão SIPR**
Windows 8.1 Update 0-1						X	X[2]	X[2]	X[1]	X[2]
Windows 10						X	X[2]	X[2]	X[1]	X[2]

1. Disponível quando instalado com o instalador principal ou com o pacote Advanced Authentication quando utilizar os instaladores subordinados.

2. Disponível quando os controladores de autenticação são transferidos a partir de support.dell.com.

UEFI

	PBA - em computadores Dell suportados					Autenticação do Windows				
	Palavra-passe	**Impressão digital**	**Smart card de contacto**	**Palavra-Passe Monouso**	**Cartão SIPR**	**Palavra-passe**	**Impressão digital**	**Smart card**	**Palavra-Passe Monouso**	**Cartão SIPR**
Windows 7 SP0-SP1										
Windows 8						X	X[2]	X[2]	X[1]	X[2]
Windows 8.1 Update 0-1						X	X[2]	X[2]	X[1]	X[2]
Windows 10						X	X[2]	X[2]	X[1]	X[2]

1. Disponível quando instalado com o instalador principal ou com o pacote Advanced Authentication quando utilizar os instaladores subordinados.

2. Disponível quando os controladores de autenticação são transferidos a partir de support.dell.com.

Cliente SED

Não UEFI

	PBA					Autenticação do Windows				
	Palavra-passe	**Impressão digital**	**Smart card de contacto**	**Palavra-Passe Monouso**	**Cartão SIPR**	**Palavra-passe**	**Impressão digital**	**Smart card**	**Palavra-Passe Monouso**	**Cartão SIPR**
Windows 7 SP0-SP1	X[2]		X[2 3]			X	X[3]	X[3]	X[1]	X[3]
Windows 8	X[2]		X[2 3]			X	X[3]	X[3]	X[1]	X[3]
Windows 8,1	X[2]		X[2 3]			X	X[3]	X[3]	X[1]	X[3]
Windows 10	X[2]		X[2 3]			X	X[3]	X[3]	X[1]	X[3]

1. Disponível quando instalado com o instalador principal ou com o pacote Advanced Authentication quando utilizar os instaladores subordinados.

Não UEFI

	PBA					Autenticação do Windows				
	Palavra-passe	Impressão digital	Smart card de contacto	Palavra-Passe Monouso	Cartão SIPR	Palavra-passe	Impressão digital	Smart card	Palavra-Passe Monouso	Cartão SIPR

2. Disponível quando os controladores de autenticação são transferidos a partir de support.dell.com.

3. Disponível com uma SED com OPAL suportada.

UEFI

	PBA - em computadores Dell suportados					Autenticação do Windows				
	Palavra-passe	Impressão digital	Smart card de contacto	Palavra-Passe Monouso	Cartão SIPR	Palavra-passe	Impressão digital	Smart card	Palavra-Passe Monouso	Cartão SIPR
Windows 7										
Windows 8	X[4]					X	X[2]	X[2]	X[1]	X[2]
Windows 8,1	X[4]					X	X[2]	X[2]	X[1]	X[2]
Windows 10	X[4]					X	X[2]	X[2]	X[1]	X[2]

1. Disponível quando instalado com o instalador principal ou com o pacote Advanced Authentication quando utilizar os instaladores subordinados.

2. Disponível quando os controladores de autenticação são transferidos a partir de support.dell.com.

4. Disponível com uma SED com OPAL suportada em computadores com UEFI suportados.

BitLocker Manager

Não UEFI

	PBA [5]					Autenticação do Windows				
	Palavra-passe	Impressão digital	Smart card de contacto	Palavra-Passe Monouso	Cartão SIPR	Palavra-passe	Impressão digital	Smart card	Palavra-Passe Monouso	Cartão SIPR
Windows 7						X	X[2]	X[2]	X[1]	X[2]
Windows 8						X	X[2]	X[2]	X[1]	X[2]
Windows 8,1						X	X[2]	X[2]	X[1]	X[2]
Windows 10						X	X[2]	X[2]	X[1]	X[2]
Windows Server 2008 R2 (64 bits)						X		X[2]		

1. Disponível quando instalado com o instalador principal ou com o pacote Advanced Authentication quando utilizar os instaladores subordinados.

2. Disponível quando os controladores de autenticação são transferidos a partir de support.dell.com.

5. O PIN de pré-arranque do BitLocker é gerido através da funcionalidade da Microsoft.

UEFI

	PBA[5] - em computadores Dell suportados					Autenticação do Windows				
	Palavra-passe	**Impressão digital**	**Smart card de contacto**	**Palavra-Passe Monouso**	**Cartão SIPR**	**Palavra-passe**	**Impressão digital**	**Smart card**	**Palavra-Passe Monouso**	**Cartão SIPR**
Windows 7										
Windows 8						X	X[2]	X[2]	X[1]	X[2]
Windows 8,1						X	X[2]	X[2]	X[1]	X[2]
Windows 10						X	X[2]	X[2]	X[1]	X[2]
Windows Server 2008 R2 (64 bits)						X		X[2]		

1. Disponível quando instalado com o instalador principal ou com o pacote Advanced Authentication quando utilizar os instaladores subordinados.

2. Disponível quando os controladores de autenticação são transferidos a partir de support.dell.com.

5. O PIN de pré-arranque do BitLocker é gerido através da funcionalidade da Microsoft.

3

Definições de registo

- Esta secção explica todas as definições de registo aprovadas pelo Dell ProSupport para computadores **cliente** locais, independentemente do motivo da definição de registo. Se uma configuração de registo se sobrepõe a dois produtos, será indicada em cada uma das categorias.
- Estas alterações de registo apenas devem ser efetuadas por Administradores e poderão não ser adequadas ou funcionar em todos os cenários.

Definições de registo do Encryption Client

- Se for utilizado um certificado autoassinado no Dell Server Enterprise Edition para Windows, a validação de confiança do certificado deve manter-se desativada no computador cliente (a validação de confiança está *desativada* por predefinição na Enterprise Edition para Windows). Antes de *ativar* a validação de confiança no computador cliente, devem ser cumpridos os seguintes requisitos.
  - Deve ser importado um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign, para o EE Server/VE Server.
  - A cadeia de confiança completa do certificado deve ser armazenada na keystore da Microsoft no computador cliente.
  - Para *ativar* a validação de confiança para o EE do Windows, altere o valor das seguintes entradas de registo para 0 no computador cliente.

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

    "IgnoreCertErrors"=dword:00000000

    0 = Falha se for encontrado um erro de certificado

    1= Ignora os erros
- Para utilizar smart cards com Autenticação do Windows, o valor de registo seguinte deve ser configurado no computador cliente.

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

  "MSSmartcardSupport"=dword:1
- Para criar um ficheiro de registo para o Encryption Removal Agent, crie a seguinte entrada de registo no computador destinado à desencriptação. Consulte (Opcional) Criar um ficheiro de registo do Encryption Removal Agent.

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=dword:2

  0: sem registos

  1: regista os erros que impedem a execução do Serviço

  2: regista os erros que impedem a desencriptação total dos dados (nível recomendado)

  3: regista informações acerca de todos os ficheiros e volumes de desencriptação

  5: regista as informações de depuração
- Por predefinição, durante a instalação, o ícone do tabuleiro do sistema é apresentado. Utilize a seguinte configuração de registo para ocultar o ícone do tabuleiro do sistema para todos os utilizadores geridos num computador após a instalação original. Crie ou modifique a definição de registo:

[HKLM\Software\CREDANT\CMGShield]

"HIDESYSTRAYICON"=dword:1

- Por predefinição, durante a instalação, todos os ficheiros temporários no diretório c:\windows\temp são automaticamente eliminados. A eliminação dos ficheiros temporários acelera a encriptação inicial e ocorre antes do varrimento de encriptação inicial.

  No entanto, se a sua organização utiliza uma aplicação de terceiros que exija que a estrutura de ficheiros dentro do diretório \temp seja preservada, deverá evitar esta eliminação.

  Para desativar a eliminação de ficheiros temporários, crie ou modifique a configuração de registo da seguinte forma:

  [HKLM\SOFTWARE\CREDANT\CMGShield]

  "DeleteTempFiles"=REG_DWORD:0

  A não eliminação dos ficheiros temporários aumenta o tempo de encriptação inicial.
- O Encryption Client apresenta o aviso de *duração de cada atraso de atualização de política* a cada cinco minutos. Se o utilizador não responder ao comando, o atraso seguinte é automaticamente iniciado. O comando de atraso final inclui uma contagem decrescente e uma barra de progresso e é apresentado até que o utilizador responda ou até que o atraso final expire e o encerramento/reinício solicitado ocorra.

  Pode alterar a ação do utilizador para iniciar ou atrasar a encriptação, para evitar o processamento da encriptação sem que o utilizador responda ao comando. Para isso, configure o registo com o seguinte valor de registo:

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

  "SnoozeBeforeSweep"=DWORD:1

  Qualquer valor diferente de zero irá alterar a ação predefinida para suspensão. Quando não houver interação do utilizador, o processamento da encriptação será atrasado até ao número de atrasos permitidos especificados. O processamento da encriptação inicia quando o atraso final expirar.

  Calcule o atraso máximo possível da seguinte forma (um atraso máximo implica que o utilizador nunca responda a um comando de atraso, que é apresentado durante 5 minutos):

  (NÚMERO DE ATRASOS DE ATUALIZAÇÃO DE POLÍTICAS PERMITIDOS × DURAÇÃO DE CADA ATRASO DE ATUALIZAÇÃO DE POLÍTICA) + (5 MINUTOS × [NÚMERO DE ATRASOS DE ATUALIZAÇÃO DE POLÍTICAS PERMITIDOS - 1])
- Utilize a seguinte configuração de registo para que o Encryption Client analise o EE Server/VE Server para uma atualização forçada da política. Crie ou modifique a definição de registo:

  [HKLM\SOFTWARE\Credant\CMGShield\Notify]

  "PingProxy"=valor DWORD:1

  A configuração de registo desaparece automaticamente quando terminar.
- Utilize as seguintes configurações de registo para permitir que o Encryption Client envie um inventário otimizado para o EE Server/VE Server, envie um inventário completo para o EE Server/VE Server ou envie para o EE Server/VE Server um inventário completo de todos os utilizadores ativados para o EE Server/VE Server.

  - Enviar para inventário otimizado para o EE Server/VE:

    Crie ou modifique a definição de registo:

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

    "OnlySendInvChanges"=REG_DWORD:1

    Se não existir qualquer entrada, o inventário otimizado é enviado para o EE Server/VE Server.

- Enviar inventário completo para o EE Server/VE Server:

  Crie ou modifique a definição de registo:

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

  "OnlySendInvChanges"=REG_DWORD:0

  Se não existir qualquer entrada, o inventário otimizado é enviado para o EE Server/VE Server.
- Enviar inventário completo de todos os utilizadores ativados

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

  "RefreshInventory"=REG_DWORD:1

  Esta entrada é eliminada do registo imediatamente após o processamento. Este valor é guardado no cofre, pelo que, mesmo que o computador seja reiniciado antes do carregamento do inventário, o Encryption Client mantém o pedido no carregamento do inventário bem-sucedido seguinte.

  Esta entrada substitui o valor de registo OnlySendInvChanges.

- A Ativação em intervalos é uma funcionalidade que permite dispersar as ativações de clientes ao longo de um determinado período de tempo para diminuir a carga do EE Server/VE Server durante uma implementação massiva. As ativações são atrasadas com base em períodos de tempo gerados através de um algoritmo para proporcionar uma distribuição uniforme dos tempos de ativação.

  Para utilizadores que necessitam de ativação através de VPN, poderá ser necessária um configuração de ativação em intervalos para o cliente, de modo a atrasar a ativação inicial pelo tempo suficiente para permitir ao cliente VPN estabelecer uma ligação de rede.

  IMPORTANTE:
  Configure a Ativação em intervalos apenas com a assistência da Dell ProSupport. Uma configuração incorreta dos períodos de tempo pode resultar na tentativa de ativação num EE Server/VE Server de um número elevado de clientes em simultâneo, podendo criar problemas de desempenho graves.

  Estas entradas de registo requerem o reinício do computador para que as atualizações sejam aplicadas.

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

    Ativa ou desativa a Ativação em intervalos.

    Desativado=0 (predefinição)

    Ativado=1
  - [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\CalRepeat]

    O período de tempo em segundos em que ocorre o intervalo de ativação. Utilize esta definição para substituir o período de tempo em segundos em que ocorre o intervalo de ativação. Estão disponíveis 25 200 segundos para ativações em intervalos durante um período de sete horas. A predefinição é de 86 400 segundos, o que representa um repetição diária.
  - [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\SlotIntervals]

    O intervalo dentro da repetição, ACTIVATION_SLOT_CALREPEAT, quando todos os períodos de tempo de ativação ocorrem. Apenas é permitido um intervalo. Esta configuração deve ser 0,<CalRepeat>. Uma definição diferente de 0 pode originar resultados inesperados. A configuração predefinida é de 0,86400. Para definir uma repetição de sete horas, utilize a configuração 0,25200. CALREPEAT é ativado quando um utilizador inicia sessão.
  - [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\MissThreshold]

    O número de intervalos de ativação que podem ser perdidos antes de o computador tentar ativar no início de sessão seguinte do utilizador cuja ativação foi submetida ao intervalo. Se a ativação falhar durante esta tentativa imediata, o cliente retoma as tentativas de ativação em intervalos. Se a ativação falhar devido a uma falha na rede, é efetuada uma tentativa de ativação aquando

da nova ligação à rede, mesmo que o valor MISSTHRESHOLD não tenha sido excedido. Se um utilizador terminar sessão antes de ser alcançado o período de tempo de ativação, é atribuído um novo intervalo no início de sessão seguinte.

- [HKCU/Software/CREDANT/ActivationSlot] (dados por utilizador)

  Tempo diferido para tentar a ativação em intervalos, que é definido quando o utilizador inicia sessão na rede pela primeira vez após a ativação em intervalos ser ativada. O intervalo de ativação é novamente calculado para cada tentativa de ativação.
- [HKCU/Software/CREDANT/SlotAttemptCount] (dados por utilizador)

  Número de tentativas falhadas ou perdidas, quando o período de tempo é alcançado e há tentativa de ativação, mas esta falha. Quando este número alcança o limite definido em ACTIVATION_SLOT_MISSTHRESHOLD, o computador tenta uma ativação imediata após estabelecer ligação à rede.

- Para detetar utilizadores não geridos no computador cliente, configure o seguinte valor de registo no computador cliente:

  [HKLM\SOFTWARE\Credant\CMGShield\ManagedUsers\]

  "UnmanagedUserDetected"=valor DWORD:1

  Detetar utilizadores não geridos neste computador=1

  Não detetar utilizadores não geridos neste computador=0
- Para permitir a reativação automática silenciosa na rara eventualidade de um utilizador ficar desativado, o seguinte valor de registo deve ser definido no computador cliente.

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CMGShield]

  "AutoReactivation"=dword:00000001

  0=Desativado (predefinição),

  1=Ativado
- System Data Encryption (SDE) é imposta com base no valor da política para SDE Encryption Rules. Os diretórios adicionais são protegidos por predefinição quando a política SDE Encryption Enabled é Selecionada. Para obter mais informações, procure "SDE Encryption Rules" em AdminHelp. Quando o Encryption Client estiver a processar uma atualização de política que inclua uma política SDE ativa, o diretório do perfil de utilizador atual é encriptado por predefinição com a chave SDUser (uma chave de Utilizador) e não com a chave SDE (uma chave de Dispositivo). A chave SDUser é também utilizada para encriptar ficheiros ou pastas que são copiadas (e não movidas) para um diretório de utilizadores não encriptado com SDE.

  Para desativar a chave SDUser e utilizar a chave SDE para encriptar estes diretórios de utilizadores, crie a seguinte entrada de registo no computador:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]

  "EnableSDUserKeyUsage"=dword:00000000

  Se a chave de registo não estiver presente ou for definida para qualquer valor diferente de 0, a chave SDUser será utilizada para encriptar estes diretórios de utilizadores.

  Para obter mais informações sobre o SDUser, consulte www.dell.com/support/article/us/en/19/SLN304916
- Definir a entrada de registo, EnableNGMetadata, se ocorrerem erros relacionados com as atualizações da Microsoft em computadores com dados encriptados com chave comuns, ou com encriptação, desencriptação, ou ao descomprimir um grande número de ficheiros dentro de uma pasta.

  Defina a entrada de registo EnableNGMetadata na seguinte localização:

  [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CmgShieldFFE]

  "EnableNGMetadata" = dword:1

  0=Desativado (predefinição),

1=Ativado

- A funcionalidade de ativação dos não domínios pode ser ativada contactando o Dell ProSupport e pedindo instruções.

Definições de registo do cliente Advanced Threat Prevention

- Para que o plug-in do Advanced Threat Prevention monitorize HKLM\SOFTWARE\Dell\Dell Data Protection quanto a alterações do valor de LogVerbosity, e atualize o nível de registo do cliente em conformidade, defina o seguinte valor.

  [HKLM\SOFTWARE\Dell\Dell Data Protection]

  "LogVerbosity"=dword:<see below>

  Dump: 0

  Fatal: 1

  Erro 3

  Aviso 5

  Informações 10

  Verboso 12

  Rastreio 14

  Depuração 15

  O valor de registo é verificado quando o serviço ATP é iniciado ou sempre que o valor muda. Se o valor de registo não existir, não haverá qualquer alteração no nível de registo.

  Utilize esta definição de registo apenas para testar/depurar, uma vez que esta definição de registo controla a verbosidade do registo de outros componentes, incluindo o Encryption Client e Client Security Framework.

- O Modo de Compatibilidade permite que as aplicações sejam executadas no computador cliente enquanto as políticas de Controlo de Script e Proteção de Memória ou Proteção de Memória estão ativadas. A ativação do modo de compatibilidade requer a adição de um valor de registo no computador cliente.

  Para ativar o modo de compatibilidade, siga estes passos:

  a Na Remote Management Console, desative a política de proteção de memória ativada Se a política de Controlo de Script estiver ativada, desative-a.

  b Adicione o valor de registo Modo de Compatibilidade.

    1 Utilizando o Editor de Registo no computador cliente, aceda a HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop.

    2 Clique com o botão direito em **Desktop**, clique em**Permissões** e, em seguida, obtenha propriedade e conceda a si próprio Controlo Total.

    3 Clique com o botão direito do rato em **Ambiente de trabalho** e, em seguida, selecione **Novo** > **Valor binário**.

    4 No nome, escreva`CompatibilityMode`.

    5 Abra a definição de registo e altere o valor para `01`.

    6 Clique em **OK** e, em seguida, feche o Editor de Registo.

    Para adicionar o valor de registo com um comando, pode utilizar uma das seguintes opções de linha de comandos para execução no computador cliente:

    - (Para um computador) Psexec:

```
psexec -s reg add HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop /v CompatibilityMode /t
REG_BINARY /d 01
```

- (Para múltiplos computadores) cmdlet invocar comando:

```
$servers = "testComp1","testComp2","textComp3"

$credential = Get-Credential -Credential {UserName}\administrator

Invoke-Command -ComputerName $servers -Credential $credential -ScriptBlock {New-Item -
Path HKCU:\Software\Cylance\Desktop -Name CompatibilityMode -Type REG_BINARY -Value 01}
```

c Na Remote Management Console, ative novamente a política Proteção de Memória Ativada. Se a política de Controlo de Script tiver sido anteriormente ativada, ative-a novamente.

Definições de registo do cliente SED

- Para definir o intervalo entre tentativas quando o EE Server/VE Server não consegue comunicar com o cliente SED, adicione o seguinte valor de registo.

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "CommErrorSleepSecs"=dword:300

  Este valor corresponde ao número de segundos que o cliente SED espera para tentar contactar o EE Server/VE Server, se este estiver indisponível para comunicar com o cliente SED. A predefinição é de 300 segundos (5 minutos).
- Se for utilizado um certificado autoassinado no EE Server/VE Server para gestão SED, a validação de confiança SSL/TLS deve permanecer desativada no computador cliente (a validação de confiança SSL/TLS está *desativada* por predefinição na gestão SED). Antes de *ativar* a validação de confiança SSL/TLS no computador cliente, os requisitos seguintes devem ser cumpridos.
  - Deve ser importado um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign, para o EE Server/VE Server.
  - A cadeia de confiança completa do certificado deve ser armazenada na keystore da Microsoft no computador cliente.
  - Para *ativar* a validação de confiança SSL/TLS da gestão SED, altere o valor da seguinte entrada de registo para 0 no computador cliente.

    [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

    "DisableSSLCertTrust"=DWORD:0

    0 = Ativado

    1 = Desativado
- Para utilizar smart cards com Autenticação do Windows, o valor de registo seguinte deve ser configurado no computador cliente.

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

  "MSSmartcardSupport"=dword:1
- Para utilizar smart cards com Autenticação de pré-arranque, o valor de registo seguinte deve ser configurado no computador cliente. Além disso, configure a política de Método de autenticação para smart card na Remote Management Console e aplique a alteração.

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

  "MSSmartcardSupport"=dword:1
- Para determinar se a PBA está ativada, certifique-se de que está definido o seguinte valor:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent\Parameters]

  "PBAIsActivated"=DWORD (32 bits):1

  O valor 1 significa que a PBA está ativada. O valor 0 significa que a PBA não está ativada.

- Para definir o intervalo a que o cliente SED tenta contactar o EE Server/VE Server quando o mesmo está indisponível para comunicar com o cliente SED, defina o seguinte valor no computador cliente:

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "CommErrorSleepSecs"=Valor DWORD:300

  Este valor corresponde ao número de segundos que o cliente SED espera para tentar contactar o EE Server/VE Server, se este estiver indisponível para comunicar com o cliente SED. A predefinição é de 300 segundos (5 minutos).
- Se necessário, o anfitrião do Security Server poderá ser mudado do local de instalação original. As informações do anfitrião são lidas pelo computador cliente sempre que ocorrer uma consulta de política. Altere o seguinte valor de registo no computador cliente:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerHost"=REG_SZ:<newname>.<organization>.com
- Se necessário, a porta do Security Server poderá ser mudada do local de instalação original. Este valor é lido pelo computador cliente sempre que ocorrer uma consulta de política. Altere o seguinte valor de registo no computador cliente:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  ServerPort=REG_SZ:8888
- Se necessário, o URL do Security Server poderá ser mudado do local de instalação original. Este valor é lido pelo computador cliente sempre que ocorrer uma consulta de política. Altere o seguinte valor de registo no computador cliente:

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerUrl"=REG_SZ:https://<newname>.<organization>.com:8888/agent

Definições de registo do cliente Advanced Authentication

- Se **não** pretender que o cliente Advanced Authentication (Security Tools) altere os serviços associados a smart cards e dispositivos biométricos para um tipo de arranque "automático", desative a funcionalidade de arranque de serviços. A desativação desta funcionalidade também suprime alertas associados aos serviços necessários que não estão a ser executados.

  Quando **desativada**, o Security Tools não irá tentar iniciar estes serviços:

  - SCardSvr - Gere o acesso a smart cards lidos pelo computador. Se este serviço for interrompido, o computador deixará de poder ler smart cards. Se este serviço for desativado, não será possível iniciar quaisquer serviços que dele dependam explicitamente.
  - SCPolicySvc - Permite que o sistema seja configurado de modo a bloquear o ambiente de trabalho do utilizador aquando da remoção de smart cards.
  - WbioSrvc - O serviço de biometria do Windows permite que aplicações cliente capturem, comparem, manipulem e armazenem dados biométricos sem obter acesso direto a amostras ou hardware de biometria. O serviço é alojado num processo SVCHOST privilegiado.

    Por predefinição, se a chave de registo não existe ou o valor está definido para 0, esta funcionalidade está ativada.

    [HKLM\SOFTWARE\DELL\Dell Data Protection]

    SmartCardServiceCheck=REG_DWORD:0

    0 = Ativado

    1 = Desativado
- Para utilizar smart cards com Autenticação do Windows, o valor de registo seguinte deve ser configurado no computador cliente.

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

"MSSmartcardSupport"=dword:1

- Para utilizar smart cards com Autenticação de pré-arranque da SED, o valor de registo seguinte deve ser configurado no computador cliente equipado com SED.

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

  "MSSmartcardSupport"=dword:1

  Configure a política de Método de autenticação para smart card na Remote Management Console e aplique a alteração.

Definições de registo do cliente BitLocker Manager

- Se for utilizado um certificado autoassinado no EE Server/VE Server para o BitLocker Manager, a validação de confiança SSL/TLS deve permanecer desativada no computador cliente (a validação de confiança SSL/TLS está *desativada* por predefinição no BitLocker Manager). Antes de *ativar* a validação de confiança SSL/TLS no computador cliente, os requisitos seguintes devem ser cumpridos.
  - Deve ser importado um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign, para o EE Server/VE Server.
  - A cadeia de confiança completa do certificado deve ser armazenada na keystore da Microsoft no computador cliente.
  - Para *ativar* a validação de confiança SSL/TLS do BitLocker Manager, altere o valor da seguinte entrada de registo para 0 no computador cliente.

    [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

    "DisableSSLCertTrust"=DWORD:0

    0 = Ativado

    1 = Desativado

Instalar utilizando o instalador principal do ESS

- 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 do ESS.
- Os ficheiros de registo do instalador principal do ESS mestão localizados 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 *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 *Ajuda do EMS* para saber como utilizar as funcionalidades do External Media Shield. 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 de Advanced Authentication e Advanced Threat Prevention. Aceda à ajuda a partir de **<Install dir>:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Help**.
- Após a conclusão da instalação, os utilizadores devem atualizar as respetivas políticas clicando com o botão direito do rato no ícone do Dell Data Protection no tabuleiro do sistema e selecionando **Procurar atualizações de políticas**.
- O instalador principal do ESS instala todo o conjunto de produtos. Existem dois métodos para instalar utilizando o instalador principal do ESS. Escolha uma das seguintes opções.
  - Instalar interativamente utilizando o instalador principal do ESSE

  ou

  - Instalar por linha de comandos utilizando o instalador principal do ESSE

Instalar interativamente utilizando o instalador principal do ESSE

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

1. Localize o **DDPSuite.exe** no suporte multimédia de instalação Dell. Copie-o para o computador local.
2. Faça duplo clique em **DDPSuite.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. No campo **Nome do Enterprise Server**, introduza o nome de anfitrião totalmente qualificado do EE Server/VE Server que irá gerir o utilizador pretendido, por exemplo, server.organization.com.

   No campo **URL do Device Server**, introduza o URL do Device Server (Security 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.

Security Framework instala a framework de segurança subjacente e o Security Tools, o cliente de autenticação avançada que gere múltiplos métodos de autenticação, incluindo PBA e credenciais tais como impressões digitais e palavras-passe.

Advanced Authentication instala os ficheiros e serviços necessários para a Autenticação avançada.

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.

BitLocker Manager instala o cliente BitLocker Manager, projetado 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 Protection* instala o cliente Advanced Threat Prevention, que é uma proteção antivírus de última geração que utiliza ciência algorítmica e aprendizagem automática 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: O Threat Protection e o Advanced Threat Prevention não podem ser instalados no mesmo computador. O instalador impede automaticamente a seleção de ambos os componentes. Se pretender instalar o Threat Protection, transfira o Guia de instalação avançada do Endpoint Security Suite para obter instruções.**

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

8 Clique em **Instalar** para dar início à instalação. A instalação irá demorar 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 do ESSE

- As opções devem ser especificadas em primeiro lugar numa instalação por linha de comandos. 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 ESSE.

Opção	Descrição
-y -gm2	Pré-extração do instalador principal do ESS. As opções -y e -gm2 devem ser utilizadas em conjunto. Não separe as opções.
/S	Instalação silenciosa
/z	Passa variáveis para o .msi dentro do DDPSuite.exe

Parâmetros

- A tabela seguinte descreve os parâmetros que podem ser utilizados com o instalador principal do ESS. O instalador principal do ESSE 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 EE Server/VE 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*** num SO de servidor; Advanced Threat Prevention ***e*** Encryption num SO de estação de trabalho DE-ATP = Advanced Threat Prevention e Encryption num SO de servidor. Utilize ***apenas*** para instalação num SO de servidor. Esta é a instalação predefinida num SO de servidor, se o parâmetro FEATURES não for especificado. DE = Encriptação de unidade (Encryption Client) ***apenas*** Utilize ***apenas*** para instalação num SO de servidor. BLM = Bitlocker Management SED = Gestão de unidades de encriptação automática (controladores EMAgent/Manager, PBA/GPE) (Disponível apenas quando instalado num SO de estação de trabalho) ATP-WEBFIREWALL = Client Firewall e Web Protection num SO de estação de trabalho DE-ATP-WEBFIREWALL = Client Firewall e Web Protection num SO de servidor **NOTA: Para atualizações a partir da Enterprise Edition 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 se instalar um cliente que vai ser gerido pelo Dell Enterprise Server/VE executado 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.
- (Num SO de estação de trabalho) Este exemplo instala todos os componentes utilizando o instalador principal do ESSE nas portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\, e configura-o para utilizar o EE Server/VE Server especificado.

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

- (Num SO de estação de trabalho) Este exemplo instala o Advanced Threat Prevention e o Encryption utilizando ***apenas*** o instalador principal do ESSE nas portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\, e configura-o para utilizar o EE Server/VE Server especificado.

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

- (Num SO de estação de trabalho) Este exemplo instala o Advanced Threat Prevention, o Encryption e a gestão SED utilizando o instalador principal do ESSE nas portas padrão, de forma silenciosa, com um reinício suprimido, na localização predefinida C:\Program Files\Dell\Dell Data Protection\, e configura-o para utilizar o EE Server/VE Server especificado.

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

- (Num SO de estação de trabalho) Este exemplo instala o Advanced Threat Prevention, Encryption, Web Protection e Client Firewall utilizando o instalador principal do ESSE nas portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\, e configura-o para utilizar o EE Server/VE Server especificado.

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

- (Num SO de servidor) Este exemplo instala o Advanced Threat Prevention e o Encryption utilizando ***apenas*** o instalador principal do ESSE nas portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\, e configura-o para utilizar o EE Server/VE Server especificado.

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

- (Em SO de servidor) Este exemplo instala o Advanced Threat Prevention, Encryption, Web Protection e Client Firewall utilizando o instalador principal ESSE em portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\

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

- (Num SO de servidor) Este exemplo instala o Advanced Threat Prevention utilizando ***apenas*** o instalador principal do ESSE nas portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\, e configura-o para utilizar o EE Server/VE Server especificado.

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

- (Num SO de servidor) Este exemplo instala o Encryption utilizando ***apenas*** o instalador principal do ESSE nas portas padrão, de forma silenciosa, na localização predefinida C:\Program Files\Dell\Dell Data Protection\, e configura-o para utilizar o EE Server/VE Server especificado.

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

5

Desinstalar utilizando o instalador principal do ESS

- Cada componente deve ser desinstalado separadamente e, posteriormente, deve ser efetuada a desinstalação do instalador principal do ESS. Os clientes devem ser desinstalados numa **ordem específica para impedir falhas na desinstalação**.
- Siga as instruções apresentadas em Extrair os instaladores subordinados do instalador principal do ESSE para obter instaladores subordinados.
- Certifique-se de que é utilizada a mesma versão do instalador principal do ESSE (e respetivos clientes) para a desinstalação e instalação.
- Este capítulo direciona-o para outros capítulos que contêm instruções *detalhadas* sobre como desinstalar os instaladores subordinados. Este capítulo explica **apenas** o último passo, a desinstalação do instalador principal do ESS.
- Desinstale os clientes pela seguinte ordem.

  a Desinstalar o Encryption Client.

  b Desinstalar o Advanced Threat Prevention

  c Desinstalar os clientes SED e Advanced Authentication (desinstala o Dell Client Security Framework, que não pode ser desinstalado antes de desinstalar o Advanced Threat Prevention).

  d Desinstalar o cliente BitLocker Manager

  Não é necessário desinstalar o pacote de controladores.
- Avance para Desinstalar o instalador principal do ESSE .

Desinstalar o instalador principal do ESS

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

Desinstalação por linha de comando

- O exemplo seguinte desinstala o instalador principal do ESS de forma silenciosa.

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

  Reinicie o computador quando concluído.

Instalar utilizando instaladores subordinados

- Para instalar cada cliente individualmente, primeiro é necessário extrair os ficheiros executáveis subordinados do instalador principal do ESSE, conforme descrito em Extrair os instaladores subordinados do instalador principal do ESSE .
- Os exemplos de comandos incluídos nesta secção assumem que os comandos são executados a partir de **C:\extracted**.
- 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.
- Utilize estes instaladores para instalar os clientes utilizando uma instalação com script, ficheiros batch ou qualquer outra tecnologia push disponível na sua organização.
- Nestes exemplos de linha de comandos, o reinício foi suprimido. No entanto, é necessário um eventual reinício. A encriptação só pode ser iniciada após o reinício do computador.
- Ficheiros de registo - O Windows cria ficheiros de registo de instalação 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 .msi padrão pode ser utilizado para criar um ficheiro de registo, utilizando /l*v **C:\<any directory>\<any log file name>.log**.
- Todos os instaladores subordinados utilizam as mesmas opções .msi básicas e as mesmas opções de visualização em instalações por linha de comandos, exceto onde referido. 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 (irá copiar 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
/qb-	Caixa de diálogo de Progresso com botão **Cancelar**, reinicia-se após a conclusão do processo

Opção	Significado
/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
/norestart	Suprimir reinício

- Dê a instrução aos utilizadores para consultar o seguinte documento e ficheiros de ajuda para assistência de aplicação:
  - Consulte a *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 *Ajuda do EMS* para saber como utilizar as funcionalidades do External Media Shield. 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 de Advanced Authentication e Advanced Threat Prevention. Aceda à ajuda a partir de **<Install dir>:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Help**.

Instalar controladores

- Os controladores e firmware do ControlVault, leitores de impressão digital e smart cards não estão incluídos nos ficheiros executáveis do instalador principal ou do instalador subordinado do ESSE. Os controladores e firmware devem ser mantidos atualizados e podem ser transferidos a partir de http://www.dell.com/support e selecionando o seu modelo de computador. Transfira os controladores e firmware adequados com base no seu hardware de autenticação.
  - ControlVault
  - NEXT Biometrics Fingerprint Driver
  - Validity FingerPrint Reader 495 Driver
  - O2Micro Smart Card Driver

  Se estiver a realizar a instalação em hardware não Dell, transfira os controladores e firmware atualizados a partir do Web site do vendedor correspondente.

Instalar o Encryption Client

- Se a sua organização utilizar um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign, reveja os Requisitos do Encryption Client. É necessária uma alteração na configuração de registo no computador cliente para ativar a validação do certificado.
- Após a conclusão da instalação, os utilizadores devem atualizar as respetivas políticas clicando com o botão direito do rato no ícone do Dell Data Protection no tabuleiro do sistema e selecionando **Procurar atualizações de políticas**.
- O instalador do Encryption Client está localizado em:
  - **Na sua conta FTP Dell** - Localize o pacote de instalação em DDP-Endpoint-Security-Suite-1.x.x.xxx.zip e, em seguida, Extrair os instaladores subordinados do instalador principal do ESSE . Após a extração, localize o ficheiro em **C:\extracted\Encryption**.

Instalação com linha de comandos

- A tabela seguinte descreve os parâmetros disponíveis para a instalação.

Parâmetros
SERVERHOSTNAME=<NomedoServidor> (FQDN do Servidor Dell para reativação)
POLICYPROXYHOSTNAME=<NomeRGK> (FQDN do Proxy de política predefinido)
MANAGEDDOMAIN=<MeuDomínio> (o domínio a ser utilizado pelo dispositivo)
DEVICESERVERURL=<NomedoServidordoDispositivo/NomedoServidordeSegurança> (URL utilizado para ativação; normalmente inclui nome do servidor, porta e xapi)
GKPORT=<NovaGKPort> (Porta do Gatekeeper)
MACHINEID=<NomedaMáquina> (Nome do computador)
RECOVERYID=<IDdeRecuperação> (ID de recuperação)
REBOOT=ReallySuppress (o valor zero permite a reinicialização automática, ReallySuppress desativa a reinicialização)
HIDEOVERLAYICONS=1 (0 ativa os ícones sobrepostos, 1 desativa os ícones sobrepostos)
HIDESYSTRAYICON=1 (0 ativa o ícone de tabuleiro do sistema, 1 desativa o ícone de tabuleiro do sistema)

Para obter uma lista comutadores basic .msi e opções de visualização que podem ser utilizadas em linhas de comandos, consulte Instalar utilizando os instaladores subordinados.

- A tabela que se segue detalha os parâmetros opcionais adicionais relacionados com a ativação.

Parâmetros
SLOTTEDACTIVATON=1 (0 desativa as ativações adiadas/programadas, 1 ativa as ativações adiadas/programadas)
SLOTINTERVAL=30,300 (programa as ativações através da notação x,x, onde o primeiro valor é o limite inferior da programação e o segundo valor é o limite superior - em segundos)
CALREPEAT=300 (TEM de igualar ou exceder o limite superior definido em SLOTINTERVAL. Número de segundos que o cliente de encriptação aguarda antes de gerar uma ativação com base no SLOTINTERVAL.)

Exemplo de linha de comandos

- O exemplo seguinte instala o cliente com parâmetros predefinidos (Encryption Client, Encrypt for Sharing, sem caixas de diálogo, sem barra de progresso, reinício automático, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection).

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://
server.organization.com:8443/xapi/ /qn"
```

Comando MSI:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
```

- O exemplo seguinte instala o Encryption Client e Encrypt for Sharing, oculta o ícone do tabuleiro do sistema DDP, oculta os ícones de sobreposição, sem caixas de diálogo, sem barra de progresso, suprime o reinício, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection.

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://
server.organization.com:8443/xapi/ HIDESYSTRAYICON=1 HIDEOVERLAYICONS=1
REBOOT=ReallySuppress /qn"
```

Comando MSI:

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
```

```
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
HIDESYSTRAYICON="1" HIDEOVERLAYICONS="1"
```

NOTA:

Alguns clientes mais antigos poderão requerer caracteres de \" à volta dos valores dos parâmetros. Por exemplo:

```
DDPE_XXbit_setup.exe /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"
```

Instalar o Server Encryption Client

Existem dois métodos disponíveis para instalar o Server Encryption. Selecione um dos seguintes métodos:

- Instalar o Server Encryption interativamente

  NOTA:

  O Server Encryption apenas pode ser instalado interativamente em computadores com sistemas operativos de servidor em execução. A instalação em computadores com sistemas operativos que não sejam de servidor deve ser efetuada por linha de comandos, com o parâmetro SERVERMODE=1 especificado.

- Instalar o Server Encryption utilizando a linha de comandos

Conta de utilizador virtual

- Como parte do processo de instalação, é criada uma **conta de utilizador do servidor virtual** para utilização exclusiva do Server Encryption. A palavra-passe e a autenticação DPAPI estão desativadas, de modo a que apenas o utilizador do servidor virtual tenha acesso às chaves de encriptação no computador.

Antes de começar

- A conta de utilizador com a qual se realiza a instalação deve ser de utilizador local ou de domínio, com permissões com nível de administrador.
- Para ignorar o requisito de ativação do Server Encryption por um administrador de domínio, ou executar o Server Encryption em servidores sem domínio ou com vários domínios, defina a propriedade ssos.domainadmin.verify para falso no ficheiro application.properties. O ficheiro é guardado nos seguintes caminhos de ficheiro, com base no Servidor DDP utilizado:

  Dell Enterprise Server - *<pasta de instalação>*/Security Server/conf/application.properties

  Virtual Edition - /opt/dell/server/security-server/conf/application.properties
- O servidor terá de suportar controlo de portas.

  As políticas de Sistema de Controlo de Portas afetam os suportes de dados amovíveis em servidores protegidos, por exemplo, controlando o acesso e a utilização das portas USB do servidor por parte dos dispositivos USB. A política de portas USB aplica-se a portas USB externas. A funcionalidade das portas USB internas não é afetada pela política de portas USB. No caso de a política de portas USB ser desativada, o teclado e rato do cliente USB não irá funcionar e o utilizador não será capaz de utilizar o computador, salvo se, antes da aplicação da política, for estabelecida uma Ligação ao Ambiente de Trabalho Remoto.
- Para uma ativação bem-sucedida do Encryption Client, o computador deve estar ligado à rede.
- Quando o Trusted Platform Module (TPM) estiver disponível, é utilizado para selar a GPK no hardware Dell. Se não estiver disponível um TPM, o Server Encryption utiliza a API de Proteção de Dados (DPAPI) da Microsoft para proteger a Chave para Fins Gerais.

  NOTA:

  Quando instalar um novo sistema operativo num computador Dell com TPM e com o Server Encryption em execução, elimine o TPM do BIOS. Consulte https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2 para obter instruções.

Extrair os instaladores subordinados

- O Server Encryption requer apenas um dos instaladores contidos no instalador principal. Para instalar o Server Encryption, deve primeiro extrair o instalador subordinado do Encryption Client, **DDPE_xxbit_setup.exe**, do instalador principal. Consulte Extrair os Instaladores Subordinados do Instalador Principal.

Instalar o Server Encryption interativamente

- Utilize estas instruções para instalar o Server Encryption interactivamente. Este programa de instalação inclui os componentes de que necessita para realizar encriptação de software.

1 Localize o ficheiro **DDPE_XXbit_setup.exe** na pasta C:\extracted\Encryption. Copie-o para o computador local.

2 Se estiver a instalar o Server Encryption num servidor, clique duas vezes no ficheiro **DDPE_XXbit_setup.exe** para iniciar o instalador.

> **NOTA:**
> Quando o Server Encryption é instalado num computador com um sistema operativo de servidor, como o Windows Server 2012 R2, o instalador instala a encriptação no modo de Servidor por predefinição.

3 Na caixa de diálogo de Boas-vindas, clique em **Seguinte.**

4 No ecrã Contrato de licença, leia o contrato, aceite os termos e clique em **Seguinte**.

5 Clique em **Seguinte** para instalar o Server Encryption na localização predefinida.

> **NOTA:**
> A Dell recomenda que a instalação seja realizada na localização predefinida. A instalação numa localização diferente da predefinida, seja num diretório distinto, na unidade D ou numa unidade USB, não é recomendada.

6 Clique em **Seguinte** para ignorar a caixa de diálogo **Tipo de gestão**.

7 No campo Nome do Dell Enterprise Server, introduza o nome de anfitrião totalmente qualificado do Dell Enterprise Server ou Virtual Edition que irá gerir o utilizador pretendido (por exemplo, *server.organization.com)*.

8 Introduza o nome de domínio no campo **Domínio gerido** (exemplo, organização) e clique em **Seguinte**.

9 Clique em **Seguinte** para ignorar a caixa de diálogo **Informações do Dell Policy Proxy** automaticamente preenchida.

10 Clique em **Seguinte** para ignorar a caixa de diálogo **Informações do Dell Device Server** automaticamente preenchida.

11 Clique em **Instalar** para dar início à instalação.
A instalação poderá demorar vários minutos.

12 Na caixa de diálogo **Configuração concluída**, clique em Concluir.
A instalação está concluída.

> **NOTA:**
> O ficheiro de registo para instalação está localizado no diretório %temp% da conta, localizado em C:\Users\<user name>\AppData\Local\Temp. Para localizar o ficheiro de registo do instalador, procure um ficheiro cujo nome comece com MSI e termine com a extensão .log. O ficheiro deverá ter um carimbo de data/hora coincidente com a hora em que executou o programa de instalação.

> **NOTA:**
> Como parte do processo de instalação, é criada uma **conta de utilizador do servidor virtual** para utilização exclusiva do Server Encryption. A palavra-passe e a autenticação DPAPI estão desativadas, de modo a que apenas o utilizador do servidor virtual tenha acesso às chaves de encriptação no computador.

13 Reinicie o computador.

> **IMPORTANTE: Escolha Suspender Reinício se necessitar de tempo para guardar o seu trabalho e fechar programas que estejam abertos.**

Instalar o Server Encryption utilizando a linha de comandos

Server Encryption Client - localize o instalador em C:\extracted\Encryption

- Utilize o **DDPE_xxbit_setup.exe** para instalar ou atualizar utilizando uma instalação com script, ficheiros de batch ou qualquer outra tecnologia disponível na sua organização.

Opções

A tabela seguinte descreve as opções disponíveis para a instalação.

Opção	Significado
/v	Passa variáveis para o .msi dentro do DDPE_XXbit_setup.exe
/a	Instalação administrativa
/s	Modo silencioso

Parâmetros

A tabela seguinte descreve os parâmetros disponíveis para a instalação.

Componente	Ficheiro de registo	Parâmetros da Linha de Comandos
Todos	/l*v [fullpath][filename].log *	SERVERHOSTNAME=<Management Server Name> SERVERMODE=1 POLICYPROXYHOSTNAME=<RGK Name> MANAGEDDOMAIN=<My Domain> DEVICESERVERURL=<Activation Server Name> GKPORT=<New GK Port> MACHINEID=<Machine Name> RECOVERYID=<Recovery ID> REBOOT=ReallySuppress HIDEOVERLAYICONS=1 HIDESYSTRAYICON=1 EME=1

NOTA:
Embora seja possível suprimir o reinício, este será eventualmente necessário. A encriptação só pode ser iniciada após o reinício do computador.

Opções

A tabela seguinte descreve as opções de visualização que podem ser especificadas no final do argumento passado para a opção /v.

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
/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

NOTA:
Não utilize **/q** e **/qn** na mesma linha de comandos. Utilize apenas **!** e - após **/qb**.

- O parâmetro da linha de comandos, SERVERMODE=1, é considerado apenas durante novas instalações. O parâmetro é ignorado nas desinstalações.
- A instalação numa localização diferente da predefinida, seja num diretório distinto, numa unidade diferente de C: ou numa unidade USB, não é recomendada. A Dell recomenda que a instalação seja realizada na localização predefinida.
- Inclua um valor que contenha um ou mais caracteres especiais, como um espaço em branco, entre aspas duplas de escape.
- O URL do Dell Activation Server (DEVICESERVERURL) é sensível a maiúsculas e minúsculas.

Exemplo de instalação com Linha de Comandos

- O exemplo seguinte instala o Server Encryption Client com parâmetros predefinidos (Server Encryption Client, instalação silenciosa, Encrypt for Sharing, sem caixas de diálogo, sem barra de progresso, reinício automático, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://
  server.organization.com:8443/xapi/qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  SERVERMODE="1" SERVERHOSTNAME="server.organization.com"
  POLICYPROXYHOSTNAME="rgk.organization.com" MANAGEDDOMAIN="ORGANIZATION"
  DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  ```

- O exemplo seguinte instala o Server Encryption Client com um ficheiro de registo e parâmetros predefinidos (Server Encryption Client, instalação silenciosa, Encrypt for Sharing, sem caixas de diálogo, sem barra de progresso, sem reinício, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection\Encryption) e especifica um nome de ficheiro de registo personalizado que termina com um número (DDP_ssos-090.log), o qual deve ser incrementado se a linha de comandos for executada mais do que uma vez no mesmo servidor.

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://
  server.organization.com:8443/xapi/ /l*v DDP_ssos-090.log /norestart/qn"
  ```

  Comando MSI:

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn SERVERMODE="1"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/" /l*v
  DDP_ssos-090.log /norestart/qn"
  ```

  Para especificar uma localização de registo diferente da localização predefinida onde está localizado o executável, forneça o caminho completo no comando. Por exemplo, /l*v C:\Logs\DDP_ssos-090.log irá criar registos de instalação numa pasta C:\Logs.

Reiniciar o computador

Após a instalação, reinicie o computador. O computador terá de ser reiniciado tão cedo quanto possível.

IMPORTANTE:

Escolha **Suspender Reinício** se necessitar de tempo para guardar o seu trabalho e fechar programas que estejam abertos.

Ativar o Server Encryption

- O servidor deve estar ligado à rede da sua organização.
- Certifique-se de que o nome do computador do servidor é o nome do endpoint que pretende visualizar na Remote Management Console.
- Para a ativação inicial, um utilizador real, em modo interativo e com credenciais de administrador de domínio deve iniciar sessão no servidor, pelo menos, uma vez. O utilizador com sessão iniciada pode ser de qualquer tipo - utilizador de domínio ou sem domínio, ligado ao ambiente de trabalho remoto ou interativo, mas a ativação requer credenciais de administrador de domínio.
- No seguimento do reinício após a instalação, é apresentada a caixa de diálogo Ativação. O administrador deve introduzir as credenciais de administrador de domínio com um nome de utilizador no formato Nome Principal de Utilizador (UPN). O Server Encryption Client não é automaticamente ativado.
- Durante a ativação inicial, é criada a conta de utilizador do servidor virtual. Após a ativação inicial, o computador é reiniciado para que a ativação do dispositivo possa começar.
- Durante a fase de Autenticação e Ativação do dispositivo, é atribuída ao computador uma ID de máquina única, são criadas e agrupadas chaves de encriptação e é estabelecida uma relação entre o grupo de chaves de encriptação e o utilizador do servidor virtual. O grupo de chaves de encriptação associa as políticas e as chaves de encriptação ao novo utilizador do servidor virtual para criar uma relação inquebrável entre os dados encriptados, o computador específico e o utilizador do servidor virtual. Após a ativação do dispositivo, o utilizador do servidor virtual é apresentado na Remote Management Console como SERVER-USER@*<nome de servidor totalmente qualificado>*. Para obter mais informações sobre a ativação, consulte Ativação num sistema operativo de servidor.

NOTA:

Se mudar o nome do servidor após a ativação, o nome do mesmo não será alterado na Remote Management Console. No entanto, se o Server Encryption Client for novamente ativado depois de alterar o nome do servidor, o novo nome do servidor deve ser apresentado na Remote Management Console.

Uma vez após cada reinício, será apresentada a caixa de diálogo Ativação para solicitar ao utilizador a ativação do Server Encryption. Se a ativação não for concluída, siga estes passos:

1 Inicie sessão no servidor no próprio servidor ou através de uma Ligação ao Ambiente de Trabalho Remoto.

2 Clique com o botão direito do rato no ícone do Encryption  no tabuleiro do sistema e clique em **Acerca de**.

3 Certifique-se de que o Encryption está em execução no modo de Servidor.

4 Selecione **Ativar o Encryption** no menu.

5 Introduza o Nome de Utilizador de um Administrador de Domínio no formato UPN e a respetiva palavra-passe e clique em **Ativar**. Esta é a mesma caixa de diálogo de Ativação que surge sempre que um sistema não ativado é reiniciado.

   O Servidor DDP emite uma chave de encriptação para a ID de máquina, cria a **conta de utilizador do servidor virtual**, cria uma chave de encriptação para a conta de utilizador, agrupa as chaves de encriptação e cria a relação entre o pacote de encriptação e a conta de utilizador do servidor virtual.

6 Clique em **Fechar**.

   Após a ativação, é iniciada a encriptação.

7 Quando o varrimento de encriptação estiver concluído, reinicie o computador para processar quaisquer ficheiros anteriormente utilizados. Este passo é importante por questões de segurança.

NOTA:
Se a política *Credenciais do Windows seguras* for definida para Verdadeiro, o Server Encryption encripta os ficheiros **\Windows\system32\config**, que incluem credenciais do Windows. Os ficheiros em **\Windows\system32\config** são encriptados mesmo que a política *Encriptação SDE ativada* esteja definida para **Não selecionada**. Por predefinição, a política *Credenciais do Windows seguras* está definida para **Selecionada**.

NOTA:
Depois de reiniciar o computador, a autenticação em conformidade com o material de chave Comum requer *sempre* a chave de Computador do servidor protegido. O Servidor DDP devolverá uma chave de desbloqueio para aceder às chaves de encriptação e políticas do cofre. (As chaves e políticas são para o servidor, não para o utilizador). Sem a chave de Computador do servidor, não é possível desbloquear a chave de encriptação de ficheiros Comuns e o computador não pode receber atualizações de política.

Confirmar ativação

Na consola local, abra a caixa de diálogo **Acerca de** para se certificar de que o Server Encryption está instalado, autenticado e no modo de Servidor. Se o Shield ID apresentar cor **vermelha**, a encriptação ainda não foi ativada.

O utilizador do servidor virtual

- Na Remote Management Console, os servidores protegidos são identificados pelo nome da máquina. Além disso, cada servidor protegido tem a sua própria conta de utilizador do servidor virtual. A cada conta está associado um nome de utilizador estático exclusivo e um nome de máquina estático exclusivo.
- A conta de utilizador do servidor virtual apenas é utilizada pelo Server Encryption e é, de outra forma, transparente na operação do servidor protegido. O utilizador do servidor virtual está associado ao grupo de chaves de encriptação e a proxy de políticas.
- Após a ativação, a conta de utilizador do servidor virtual é a conta de utilizador ativada e associada ao servidor.
- Uma vez ativado o utilizador do servidor virtual, serão ignoradas todas as notificações de início/fim de sessão do servidor. Em vez disso, durante o arranque, o computador efetua automaticamente a autenticação com o utilizador do servidor virtual e, em seguida, transfere a chave de Computador do Dell Data Protection Server.

Instalar o cliente Advanced Threat Prevention

- O Threat Protection e o Advanced Threat Prevention **não podem ser instalados no mesmo computador**. Não instale estes componentes no mesmo computador, uma vez que irão ocorrer problemas de compatibilidade. Se pretender instalar o Threat Protection, transfira o Guia de instalação avançada do Endpoint Security Suite para obter instruções.
- Os instaladores devem ser executados seguindo uma ordem específica. A não instalação dos componentes seguindo a ordem correta irá resultar numa falha na instalação. Execute os instaladores pela seguinte ordem:

1 **(Apenas num SO de estação de trabalho)** \Security Tools - O Advanced Threat Prevention necessita do componente Framework de segurança do cliente Dell.

(Apenas num SO de servidor) O componente Framework de segurança do cliente Dell, conforme descrito em Instalação por linha de comandos.

2 **(Apenas num SO de estação de trabalho)** \Security Tools\Authentication - Num SO de estação de trabalho, o Security Tools e o Authentication devem ser instalados em conjunto; o Authentication não está disponível num SO de servidor e não necessita de instalação.

3 Cliente Advanced Threat Prevention, conforme descrito em Instalação por linha de comandos.

- O instalador do cliente Advanced Threat Prevention pode ser localizado em:
  - **Na sua conta FTP Dell** - Localize o pacote de instalação em DDP-Endpoint-Security-Suite-1.x.x.xxx.zip e, em seguida, Extrair os instaladores subordinados do instalador principal do ESSE . Após a extração, localize o ficheiro em **C:\extracted\Advanced Threat Protection**.

- Os instaladores do cliente SED e Advanced Authentication estão localizados em:
  - **Na sua conta FTP Dell** - Localize o pacote de instalação em DDP-Endpoint-Security-Suite-1.x.x.xxx.zip e, em seguida, Extrair os instaladores subordinados do instalador principal do ESSE . Após a extração, localize o ficheiro em **C:\extracted\Security Tools** e **C:\extracted\Security Tools\Authentication**.

    NOTA: Os clientes SED e Advanced Authentication apenas podem ser instalados num SO de estação de trabalho, e não num SO de servidor.

Instalação com linha de comandos

- Encontram-se disponíveis comandos .msi básicos para a instalação.
- A tabela seguinte descreve os parâmetros disponíveis para a instalação.

Parâmetros
CM_EDITION=1 <gestão remota>
INSTALLDIR=<alterar o destino de instalação>
SERVERHOST=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 <nenhuma entrada na lista de Programas do Painel de controlo>
REBOOT=ReallySuppress <suprime o reinício>
FEATURE=BASIC <***obrigatório*** num SO de servidor; poderá também ser utilizado (opcionalmente) num SO de estação de trabalho; impede a instalação do cliente de Gestão SED e do BitLocker Manager>

Para obter uma lista de comutadores basic .msi e opções de visualização que podem ser utilizadas em linhas de comandos, consulte Instalar utilizando os instaladores subordinados.

Exemplo de linhas de comandos

- O exemplo seguinte instala o componente Framework de segurança do cliente Dell básico, sem o cliente de Gestão SED ou o BitLocker Manager (instalação silenciosa, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalado na localização predefinida **C:\Program Files\Dell\Dell Data Protection**).

```
EMAgent_XXbit_setup.exe /s /v"FEATURE=BASIC CM_EDITION=1 SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 /norestart /qn"
```

- O exemplo seguinte instala o Advanced Threat Prevention (instalação silenciosa, sem reinício, ficheiro de registo de instalação e instalação na localização especificada)

```
MSIEXEC.EXE /I "AdvancedThreatProtectionCSFPlugins_x64.msi" /qn REBOOT="ReallySuppress"
APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Plugins"
ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer Logs
\AdvancedThreatProtectionPlugins.msi.log"
```

e

```
AdvancedThreatProtectionAgentSetup.exe /s /norestart REBOOT=ReallySuppress APPFOLDER="C:
\Program Files\Dell\Dell Data Protection\Advanced Threat Protection" ARPSYSTEMCOMPONENT=1 /l
"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\AdvancedThreatProtection.log"
```

NOTA: Estes componentes apenas devem ser instalados por linha de comandos. Clicar duas vezes para instalar este componente instala uma versão não Dell e não gerida do produto, que não é suportada. Caso o faça acidentalmente, basta aceder a Adicionar/remover programas e desinstalar essa versão.

Instalar Web Protection e Firewall

- Advanced Threat Prevention e Threat Protection **não podem coexistir no mesmo computador**. Não instale estes componentes no mesmo computador, uma vez que irão ocorrer problemas de compatibilidade. Porém, o Advanced Threat Prevention pode ser instalado com os componentes Web Protection e Firewall.
- Os instaladores devem ser executados seguindo uma ordem específica. A não instalação dos componentes seguindo a ordem correta irá resultar numa falha na instalação. Execute os instaladores pela seguinte ordem:

1 É necessário o cliente de encriptação com os componentes Web Protection e Firewall. Aceda a Exemplo de linha de comandos para obter um exemplo de instalação.

2 Web Protection e Firewall, conforme descrito em Instalação por linha de comandos.

Instalação com linha de comandos

- A tabela seguinte descreve os parâmetros disponíveis para o ficheiro **EnsMgmtSdkInstaller.exe**.

Parâmetros	Descrição
LoadCert	Carrega o certificado no diretório especificado.

- A tabela seguinte descreve os parâmetros disponíveis para o ficheiro **setupEP.exe**.

Parâmetros	Descrição
ADDLOCAL="fw,wc"	Identifica os módulos a instalar: fw=Client Firewall wc=Proteção Web
override "hips"	Não instala a Prevenção contra invasões do anfitrião
INSTALLDIR	Localização de instalação diferente da predefinida
nocontentupdate	Indica ao instalador que não deve atualizar ficheiros de conteúdo automaticamente como parte do processo de instalação. A Dell recomenda o agendamento de uma atualização o mais rapidamente possível após a conclusão da instalação.
nopreservesettings	Não guarda as definições.

- A tabela seguinte descreve os parâmetros disponíveis para o ficheiro **DellThreatProtection.msi**.

Parâmetros	Descrição
Reboot=ReallySuppress	Suprime o reinício.
ARP	0=Nenhuma entrada em Adicionar/remover programas 1=Entrada em Adicionar/remover programas

- A tabela seguinte descreve os parâmetros disponíveis para o ficheiro **EnsMgmtSdkInstaller.exe**.

Parâmetros	Descrição
ProtectProcesses	Especifica o nome do ficheiro e a localização dos processos a proteger.
InstallSDK	Instala o SDK na localização especificada.
RemoveRightClick	Remove a opção do menu de clique com o botão direito do rato para os utilizadores finais.
RemoveMcTray	Remove o tabuleiro do sistema.

Exemplo de linha de comandos

\Dell Threat Protection\SDK

- A linha de comandos seguinte carrega os parâmetros predefinidos do certificado.

```
"Dell Threat Protection\SDK\EnsMgmtSdkInstaller.exe" -LoadCert >"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\McAfeeSDKInstallerBeforeEndPoint.log"
```

NOTA:
Este instalador pode ser ignorado em caso de atualização.

Em seguida:

\Dell Threat Protection\EndPointSecurity

- O exemplo seguinte instala o cliente Web Protection e Client Firewall com parâmetros predefinidos (modo silencioso, instalação do , Client Firewall e Proteção Web; substitui a Prevenção contra invasões do anfitrião, sem atualização do conteúdo, sem definições guardadas).

```
"Dell Threat Protection\EndPointSecurity\EPsetup.exe" ADDLOCAL="fw,wc" /override"hips" /nocontentupdate /nopreservesettings /qn
```

Em seguida:

\Dell Threat Protection\ThreatProtection\WinXXR

- O exemplo seguinte instala o cliente com parâmetros predefinidos (suprime o reinício, sem caixas de diálogo, sem barra de progresso, sem entrada na lista de Programas do Painel de controlo).

```
"Dell Threat Protection\ThreatProtection\WinXXR\DellThreatProtection.msi" /qn REBOOT=ReallySuppress ARPSYSTEMCOMPONENT=1
```

\Dell Threat Protection\SDK

- O exemplo seguinte instala o SDK do Threat Protection.

```
"Dell Threat Protection\SDK\EnsMgmtSdkInstaller.exe" -ProtectProcesses "C:\Program Files\Dell\Dell Data Protection\Threat Protection\DellAVAgent.exe" -InstallSDK -RemoveRightClick -RemoveMcTray >"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\McAfeeSDKInstallerAfterEndPoint.log"
```

Instalar a gestão SED e os clientes Advanced Authentication

- Na v8.x, é necessário o cliente SED para a Advanced Authentication.
- Se a sua organização utilizar um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign, reveja os Requisitos do cliente SED. É necessária uma alteração na configuração de registo no computador cliente para ativar a validação de confiança SSL/TLS.
- Os utilizadores iniciam sessão na PBA utilizando as respetivas credenciais do Windows.

- Os instaladores do cliente SED e Advanced Authentication estão localizados em:
  - **Na sua conta FTP Dell** - Localize o pacote de instalação em DDP-Endpoint-Security-Suite-1.x.x.xxx.zip e, em seguida, Extrair os instaladores subordinados do instalador principal do ESSE . Após a extração, localize o ficheiro em **C:\extracted\Security Tools** e **C:\extracted\Security Tools\Authentication**.

Instalação com linha de comandos

- A tabela seguinte descreve os parâmetros disponíveis para a instalação.

Parâmetros
CM_EDITION=1 <gestão remota>
INSTALLDIR=<alterar o destino de instalação>
SERVERHOST=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 <nenhuma entrada na lista de Programas do Painel de controlo>

Para obter uma lista comutadores basic .msi e opções de visualização que podem ser utilizadas em linhas de comandos, consulte Instalar utilizando os instaladores subordinados.

Exemplo de linha de comandos

\Security Tools

- O exemplo seguinte instala o SED gerido remotamente (instalação silenciosa, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
norestart /qn"
```

Em seguida:

\Security Tools\Authentication

- O exemplo seguinte instala a Advanced Authentication (instalação silenciosa, sem reinício)

```
setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
```

Instalar o cliente BitLocker Manager

- Se a sua organização utilizar um certificado assinado por uma autoridade raiz, como EnTrust ou Verisign, reveja os Requisitos do cliente BitLocker Manager. É necessária uma alteração na configuração de registo no computador cliente para ativar a validação de confiança SSL/TLS.
- Os instaladores do cliente BtLocker Manager estão localizados em:
  - **Na sua conta FTP Dell** - Localize o pacote de instalação em DDP-Endpoint-Security-Suite-1.x.x.xxx.zip e, em seguida, Extrair os instaladores subordinados do instalador principal do ESSE . Após a extração, localize o ficheiro em **C:\extracted\Security Tools**.

Instalação com linha de comandos

- A tabela seguinte descreve os parâmetros disponíveis para a instalação.

Parâmetros
CM_EDITION=1 <gestão remota>
INSTALLDIR=<alterar o destino de instalação>
SERVERHOST=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
FEATURE=BLM <instalar apenas o BitLocker Manager>
FEATURE=BLM,SED <instalar o BitLocker Manager com SED>
ARPSYSTEMCOMPONENT=1 <nenhuma entrada na lista de Programas do Painel de controlo>

Para obter uma lista comutadores basic .msi e opções de visualização que podem ser utilizadas em linhas de comandos, consulte Instalar utilizando os instaladores subordinados.

Exemplo de linha de comandos

- O exemplo seguinte instala apenas o BitLocker Manager (instalação silenciosa, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalado na localização predefinida **C:\Program Files\Dell\Dell Data Protection**)

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 FEATURE=BLM /norestart /qn"
```

- O exemplo seguinte instala o BitLocker Manager com SED (instalação silenciosa, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalado na localização predefinida **C:\Program Files\Dell\Dell Data Protection**)

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 FEATURE=BLM,SED /
norestart /qn"
```

7

Desinstalar utilizando os instaladores subordinados

- Para desinstalar cada cliente individualmente, primeiro é necessário extrair os ficheiros executáveis subordinados do instalador principal do ESSE, conforme descrito em Extrair os instaladores subordinados do instalador principal do ESSE . 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 (irá copiar todos os ficheiros contidos no .msi)

NOTA:
Com /v, as opções predefinidas da Microsoft ficam disponíveis. Para ver 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 os Web Protection e Firewall

Se o Web Protection e a Firewall não estiverem instalados, avance para Desinstalar o Encryption Client.

Desinstalação por linha de comando

- Uma vez extraído do instalador principal do ESS, o instalador do cliente Web Protection e Firewall pode ser localizado em **C:\extracted \Dell Threat Protection\ThreatProtection\WinXXR\DellThreatProtection.msi.**
- Aceda a Adicionar/remover programas no Painel de controlo e desinstale os seguintes componentes por esta ordem:
  - McAfee Endpoint Security Firewall
  - McAfee Endpoint Security Web Control
  - McAfee Agent
- Em seguida:
- O exemplo que se segue desinstala o Web Protection e Firewall.

```
MSIEXEC.EXE /x "DellThreatProtection.msi"
```

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 Windows e os Shields atualizam o EE Server/VE Server para alterar o estado para *Desprotegido* no início do processo de desinstalação do Shield. No entanto, caso o cliente não consiga contactar o EE Server/VE Server, independentemente do motivo, não é possível atualizar o estado. Neste caso, terá de *Remover o endpoint* manualmente na Remote 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 Remote Management Console ou no Compliance Reporter.

Processo

- **Antes de iniciar o processo de desinstalação**, consulte (Opcional) Criar um ficheiro de registo do Encryption Removal Agent. Este ficheiro de registo é útil para resolução de problemas numa operação de desinstalação/desencriptação. Se não pretender desencriptar ficheiros durante o processo de desinstalação, não é necessário criar um ficheiro de registo do Agente de remoção de encriptação.

- O Key Server (e EE 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 EE Server para obter instruções. Não é necessária qualquer ação anterior se o cliente a ser desinstalado está ativado em um VE Server, uma vez que o VE Server 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.
- Após concluir a desinstalação, mas antes de reiniciar o computador, execute o WSScan para assegurar que todos os dados foram desencriptados. Consulte Utilizar o WSScan para obter instruções.
- Periodicamente, verifique o estado do Encryption Removal Agent. Se o serviço Encryption Removal Agent ainda se encontrar no painel de Serviços, a desencriptação de dados ainda está a ser processada.

Desinstalação por linha de comando

- Uma vez extraído do instalador principal do ESSE, 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 1 - Transferir chaves do Servidor Dell 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 EE Server anfitrião da sessão de negociação.
DA_PORT	Porta do EE Server para pedidos (a predefinição é 8050)
SVCPN	Nome de utilizador, em formato UPN, com o qual o serviço Key Server tem sessão iniciada no EE Server.
DA_RUNAS	Nome de utilizador em formato compatível com SAM, sendo o pedido de recuperação de chaves realizado neste contexto. Este utilizador deve encontrar-se na lista do Key Server no EE Server.
DA_RUNASPWD	Palavra-passe do utilizador runas.
FORENSIC_ADMIN	A conta de Administrador forense no Servidor Dell, que pode ser utilizada para pedidos forenses para desinstalações ou chaves.
FORENSIC_ADMIN_PWD	A palavra-passe da conta de Administrador forense.
Propriedades opcionais	

Parâmetro	Seleção
SVCLOGONUN	Nome de utilizador em 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 EE Server.

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

  Comando MSI:

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

  Reinicie o computador 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 quando utilizar uma palavra-passe de Administrador forense na linha de comandos:

1. Crie uma conta de Administrador forense na Remote 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 Framework de segurança do cliente Dell.

- **IMPORTANTE: Se tiver instalado os clientes SED e Advanced Authentication ou tiver ativado a Autenticação pré-arranque, siga as instruções de desinstalação apresentadas em Desinstalar os clientes SED e Advanced Authentication.**

  O exemplo seguinte apresenta a desinstalação apenas do componente Framework de segurança do cliente Dell e não os clientes SED e Advanced Authentication.

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

Desinstalar os clientes SED e Advanced Authentication

- A ligação de rede ao EE Server/VE Server é necessária para desativar a PBA.

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.
- Desinstalar o software de cliente Advanced Authentication.

Desativar a PBA

1. Como Administrador Dell, inicie sessão na Remote Management Console.
2. No painel do lado esquerdo, clique em **Proteger e gerir** > **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 ícone **Detalhes** do computador pretendido.
7. Clique em **Políticas de segurança** no menu superior.
8. Selecione **Unidades de encriptação automática** a partir do menu de lista pendente de **Categoria de política**.
9. Expanda a área **Administração SED** e altere as políticas **Permitir gestão SED** e **Ativar PBA** de `True` para ***`False`***.
10. Clique em **Guardar**.
11. No painel do lado esquerdo, clique em **Ações** > **Consolidar políticas**.
12. Clique em **Aplicar alterações**.

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

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

Desinstale o cliente SED e clientes Advanced Authentication

Desinstalação por linha de comando

- Uma vez extraído do instalador principal do ESS, o instalador do cliente SED pode ser localizado em C:\extracted\Security Tools \EMAgent_XXbit_setup.exe.
- Uma vez extraído do instalador principal do ESSE, o instalador do cliente SED pode ser localizado em C:\extracted\Security Tools \Authentication\<x64/x86>\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.

  Em seguida:

- O seguinte exemplo desinstala o cliente Advanced Authentication de forma silenciosa.

  ```
  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 ESS, o instalador do cliente BitLocker pode ser localizado em **C:\extracted\Security Tools \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.

8

Cenários normalmente utilizados

- Para instalar cada cliente individualmente, primeiro é necessário extrair os ficheiros executáveis subordinados do instalador principal do ESSE, conforme descrito em Extrair os instaladores subordinados do instalador principal do ESSE .
- É necessário o cliente SED para a Advanced Authentication na v8.x, motivo pelo qual faz parte da linha de comandos nos exemplos seguintes.
- O componente do instalador subordinado do Advanced Threat Prevention apenas deve ser instalado por linha de comandos. Clicar duas vezes para instalar este componente instala uma versão não Dell e não gerida do produto, que não é suportada. Caso o faça acidentalmente, basta aceder a Adicionar/remover programas e desinstalar essa versão.
- 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.
- Utilize estes instaladores para instalar os clientes utilizando uma instalação com script, ficheiros batch ou qualquer outra tecnologia push disponível na sua organização.
- Nestes exemplos de linha de comandos, o reinício foi suprimido. No entanto, é necessário um eventual reinício. A encriptação só pode ser iniciada após o reinício do computador.
- Ficheiros de registo - O Windows cria ficheiros de registo de instalação 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 .msi padrão pode ser utilizado para criar um ficheiro de registo, utilizando /l*v C:\<any directory>\<any log file name>.log.
- Todos os instaladores subordinados utilizam as mesmas opções .msi básicas e as mesmas opções de visualização em instalações por linha de comandos, exceto onde referido. 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 *.exe
/s	Modo silencioso
/i	Modo de instalação

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
/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

Opção	Significado
/qn	Sem interface de utilizador

- Dê a instrução aos utilizadores para consultar o seguinte documento e ficheiros de ajuda para assistência de aplicação:
  - Consulte a *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 *Ajuda do EMS* para saber como utilizar as funcionalidades do External Media Shield. 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 de Advanced Authentication e Advanced Threat Prevention. Aceda à ajuda a partir de **<Install dir>:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Help**.

Encryption Client, Advanced Threat Prevention e Advanced Authentication

- O exemplo seguinte instala o SED gerido remotamente (instalação silenciosa, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalado na localização predefinida **C:\Program Files\Dell\Dell Data Protection**). Este componente instala o Dell Client Security Framework exigido pelo Advanced Threat Prevention.

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
  norestart /qn"
  ```

  Em seguida:

- O exemplo seguinte instala o cliente Advanced Authentication (instalação silenciosa, sem reinício, instalado na localização predefinida **C:\Program Files\Dell\Dell Data Protection\Authentication**).

  ```
  setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
  ```

  Em seguida:

- O exemplo seguinte instala o Advanced Threat Prevention (instalação silenciosa, sem reinício, ficheiro de registo de instalação e instalação na localização especificada)

  ```
  MSIEXEC.EXE /I "AdvancedThreatProtectionCSFPlugins_x64.msi" /qn REBOOT="ReallySuppress"
  APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Plugins"
  ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer Logs
  \AdvancedThreatProtectionPlugins.msi.log"
  ```

  e

  ```
  AdvancedThreatProtectionAgentSetup.exe /s /norestart REBOOT=ReallySuppress APPFOLDER="C:
  \Program Files\Dell\Dell Data Protection\Advanced Threat Protection" ARPSYSTEMCOMPONENT=1 /l
  "C:\ProgramData\Dell\Dell Data Protection\Installer Logs\AdvancedThreatProtection.log"
  ```

- O exemplo seguinte instala o Encryption Client com parâmetros predefinidos (Encryption Client e Encrypt for Sharing, sem caixas de diálogo, sem barra de progresso, sem reinício, instalado na localização predefinida **C:\Program Files\Dell\Dell Data Protection**).

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION DEVICESERVERURL=https://
  server.organization.com:8443/xapi/ /norestart /qn"
  ```

- Os exemplos que se seguem instalam as funcionalidades ***opcionais***, Web Protection e Firewall.
- **\Dell Threat Protection\SDK**

  A linha de comandos seguinte carrega os parâmetros predefinidos do certificado.

  ```
  EnsMgmtSdkInstaller.exe -LoadCert >"C:\ProgramData\Dell\Dell Data Protection\Installer Logs
  \McAfeeSDKInstallerBeforeEndPoint.log"
  ```

NOTA:
Este instalador pode ser ignorado em caso de atualização.

Em seguida:

\Dell Threat Protection\EndPointSecurity

- O exemplo seguinte instala as funcionalidades*opcionais* Web Protection e Firewall com parâmetros predefinidos (modo silencioso, instalação do Threat Protection, Client Firewall e Proteção Web; substituição da Prevenção contra invasões do anfitrião, sem atualização do conteúdo, sem definições guardadas).

```
"Dell Threat Protection\EndPointSecurity\EPsetup.exe" ADDLOCAL="fw,wc" /override"hips" /
nocontentupdate /nopreservesettings /qn
```

Em seguida:

\Dell Threat Protection\ThreatProtection\WinXXR

- O exemplo seguinte instala o cliente com parâmetros predefinidos (suprime o reinício, sem caixas de diálogo, sem barra de progresso, sem entrada na lista de Programas do Painel de controlo).

```
"DellThreatProtection.msi" /qn REBOOT=ReallySuppress ARPSYSTEMCOMPONENT=1
```

\Dell Threat Protection\SDK

- O exemplo seguinte instala o SDK do Threat Protection.

```
EnsMgmtSdkInstaller.exe -ProtectProcesses "C:\Program Files\Dell\Dell Data Protection\Threat
Protection\DellAVAgent.exe" -InstallSDK -RemoveRightClick -RemoveMcTray >"C:\ProgramData\Dell
\Dell Data Protection\Installer Logs\McAfeeSDKInstallerAfterEndPoint.log"
```

Cliente SED (incluindo Advanced Authentication) e External Media Shield

- O exemplo seguinte instala o SED gerido remotamente (instalação silenciosa, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
norestart /qn"
```

Em seguida:

- O exemplo seguinte instala o cliente Advanced Authentication (instalação silenciosa, sem reinício, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection\Authentication).

```
setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
```

Em seguida:

- O exemplo seguinte instala apenas o EMS (instalação silenciosa, sem reinício, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection).

```
DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com DEVICESERVERURL=https://server.organization.com:8443/
xapi/ MANAGEDDOMAIN=ORGANIZATION /norestart /qn"
```

BitLocker Manager e External Media Shield

- O exemplo seguinte instala o BitLocker Manager (instalação silenciosa, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalado na localização predefinida C:\Program Files\Dell\Dell Data Protection).

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 FEATURE=BLM /norestart /qn"
```

Em seguida:

- O exemplo seguinte instala apenas o EMS (instalação silenciosa, sem reinício, instalado na localização predefinida **C:\Program Files\Dell\Dell Data Protection**).

```
DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com DEVICESERVERURL=https://server.organization.com:8443/
xapi/ MANAGEDDOMAIN=ORGANIZATION /norestart /qn"
```

BitLocker Manager e Advanced Threat Prevention

- O exemplo seguinte instala o BitLocker Manager (instalação silenciosa, sem reinício, sem entrada na lista de Programas do Painel de controlo, instalado na localização predefinida **C:\Program Files\Dell\Dell Data Protection**). Este componente instala o Dell Client Security Framework, que é exigido pelo Advanced Threat Prevention.

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 FEATURE=BLM /norestart /qn"
```

Em seguida:

- O exemplo seguinte instala o Advanced Threat Prevention (instalação silenciosa, sem reinício, ficheiro de registo de instalação e instalação na localização especificada)

```
MSIEXEC.EXE /I "AdvancedThreatProtection_xXX.msi" /qn REBOOT="ReallySuppress"
ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer Logs\ATP.log"
APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection"
```

Configurar um inquilino para o Advanced Threat Prevention

Se a sua organização utilizar o Advanced Threat Prevention, deve ser configurado um inquilino no Dell Server antes da ativação da aplicação de políticas do Advanced Threat Prevention.

Pré-requisitos

- Deve ser efetuado por um administrador com função de Administrador do sistema.
- Deve ter ligação à Internet para configuração no Dell Server.
- Deve ter ligação à Internet no cliente para visualizar a integração do serviço online do Advanced Threat Prevention na Remote 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 Inicie sessão na Remote Management Console e navegue até **Gestão de serviços**.

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

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

4 Leia e aceite o EULA (a caixa de verificação está **desativada** por predefinição) e clique em **Seguinte**.

5 Disponibilize credenciais de identificação no Servidor DDP para configuração do Inquilino. Clique em **Seguinte**. *A configuração de um Inquilino existente da marca Cylance não é suportada.*

6 Transfira o Certificado. Este é necessário para recuperação em caso de desastres no Servidor DDP. Não são automaticamente efetuadas cópias de segurança deste Certificado através do "upgrader" v9.2. Efetue uma cópia de segurança do Certificado numa localização segura num computador diferente. Assinale a caixa de verificação para confirmar que efetuou uma cópia de segurança do Certificado e clique em **Seguinte**.

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

Configurar a atualização automática do Advanced Threat Prevention Agent

Na Remote Management Console do Dell Server, pode subscrever a receção de autoatualizações do Advanced Threat Prevention Agent. A subscrição da receção de atualizações automáticas do agente permite aos clientes transferir e aplicar autoatualizações a partir do servidor 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 Remote Management Console, clique em **Gestão** > **Gestão de serviços**.

2 No separador **Ameaças avançadas**, sob Autoatualização do Agente, clique no botão **Ligar** e, em seguida, clique no botão **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 Remote Management Console, clique em **Gestão** > **Gestão de serviços**.

2 No separador **Ameaças avançadas**, sob Autoatualização do Agente, clique no botão **Ligar** e, em seguida, clique no botão **Guardar preferências**

Configuração da pré-instalação para Palavra-passe monouso, UEFI SED e BitLocker

Inicializar o TPM

- Tem de ser membro do grupo local de Administradores ou equivalente.
- O computador tem de estar equipado com um BIOS e um TPM compatíveis.

Esta tarefa é necessária se utilizar a Palavra-passe monouso (OTP).

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

Configuração da pré-instalação para computadores UEFI

Ativar a ligação à rede durante a Autenticação do pré-arranque UEFI

Para que a autenticação de pré-arranque seja bem-sucedida num computador com firmware UEFI, a PBA deve ter ligação à rede. Por predefinição, os computadores com firmware UEFI não têm ligação à rede até que o sistema operativo seja carregado, o que ocorre depois do modo PBA.

O procedimento seguinte ativa a ligação à rede durante a PBA em computadores com UEFI ativado. Uma vez que os passos de configuração podem variar consoante o modelo de computador UEFI, o procedimento seguinte é apenas um exemplo.

1 Inicie a configuração do firmware UEFI.
2 Prima F2 continuamente durante o arranque até ser apresentada no canto superior direito do ecrã uma mensagem como "a preparar o menu de arranque único".
3 Se solicitado, introduza a palavra-passe de administrador do BIOS.

> **NOTA:**
> Normalmente, tratando-se de um computador novo, tal não é solicitado, uma vez que a palavra-passe do BIOS ainda não foi definida.

4 Selecione **Configuração do sistema**.
5 Selecione **NIC integrado**.
6 Selecione a caixa de verificação **Ativar a pilha da rede UEFI**.
7 Selecione **Ativado** ou **Ativado c/PXE**.
8 Selecione **Aplicar**

> **NOTA:**
> Os computadores *sem* firmware UEFI não necessitam de configuração.

Desativar ROMs de opção legadas

Certifique-se de que a definição **Ativar ROMs de opção legadas** está desativada no BIOS.

1 Reinicie o computador.
2 À medida que se reinicia, prima **F12** repetidamente to para abrir as definições de arranque do computador com UEFI.
3 Prima a seta para baixo, realce a opção **Definições do BIOS** e prima **Enter**.
4 Selecione **Definições** > **Geral** > **Opções de arranque avançadas**.
5 Desmarque a caixa de verificação **Ativar ROMs de opção legadas** e clique em **Aplicar**.

Configuração da pré-instalação para configurar uma partição de PBA do BitLocker

- Deve criar a partição de PBA **antes** de instalar o BitLocker Manager.
- Ligue e ative o TPM **antes** de instalar o BitLocker Manager. O BitLocker Manager assume a propriedade do TPM (não é necessário reiniciar). No entanto, se o TPM já tiver um proprietário, o BitLocker Manager irá iniciar o processo de configuração da encriptação. O importante é que o TPM tenha um "proprietário".
- Poderá ter de realizar a partição do disco manualmente. Consulte a descrição da Microsoft para a Ferramenta de Preparação da Unidade BitLocker para obter mais informações.
- Utilize o comando BdeHdCfg.exe para criar a partição de PBA. O parâmetro predefinido indica que a ferramenta da linha de comandos segue o mesmo processo que o Assistente de configuração do BitLocker.

```
BdeHdCfg -target default
```

SUGESTÃO:
Para obter mais opções disponíveis para o comando BdeHdCfg, consulte a Referência do parâmetro BdeHdCfg.exe da Microsoft.

Definir GPO no controlador do domínio para ativar as elegibilidades

- Se os clientes forem elegíveis partir do Dell Digital Delivery (DDD), siga estas instruções para definir o GPO no controlador do domínio e ativar as elegibilidades (poderá não ser o mesmo servidor a executar o EE Server/VE Server).
- A estação de trabalho deve fazer parte da UO onde o GPO está aplicado.

> **NOTA:**
> Certifique-se de que a porta de saída 443 está disponível para comunicar com o EE Server/VE Server. Se a porta 443 estiver bloqueada (por qualquer motivo) a funcionalidade de elegibilidade não irá funcionar.

1. No Controlador do domínio para gerir os clientes, clique em **Iniciar** > **Ferramentas administrativas** > **Gestão de política de grupo**.
2. Clique com o botão direito do rato na UO onde a política deve ser aplicada e selecione **Criar um GPO neste domínio** e **Ligá-lo aqui...**.
3. Introduza um nome para o novo GPO, selecione (nenhum) para GPO de arranque de origem e clique em **OK**.
4. Clique com o botão direito no GPO que foi criado e selecione **Editar**.
5. É carregado o Editor de gestão de política de grupo. Aceda a **Configuração do computador** > **Preferências** > **Definições do Windows** > **Registo**.
6. Clique com o botão direito do rato no Registo e selecione **Novo** > **Item do registo**. Execute as seguintes ações.

   Ação: Criar

   Ramo de registo: HKEY_LOCAL_MACHINE

   Caminho da chave: SOFTWARE\Dell\Dell Data Protection

   Nome do valor: Servidor

   Tipo do valor: REG_SZ

   Dados do valor: <Endereço IP do EE Server/VE Server>
7. Clique em **OK**.
8. Termine sessão e, em seguida, inicie novamente sessão na estação de trabalho ou execute **gpupdate /force** para aplicar a política de grupo.

Extrair os instaladores subordinados do instalador principal do ESS

- Para instalar cada cliente individualmente, extraia os ficheiros executáveis subordinados do instalador.
- O instalador principal do ESS não é um *desinstalador* principal. Cada cliente deve ser desinstalado individualmente e, posteriormente, deve ser efetuada a desinstalação do instalador principal do ESS. Utilize este processo para extrair os clientes do instalador principal do ESS para que possam ser utilizados na desinstalação.

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

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

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

O caminho de extração não pode exceder os 63 caracteres.

Antes de iniciar a instalação, certifique-se de que todos os pré-requisitos foram cumpridos e de que todo o software necessário foi instalado para cada instalador subordinado que pretende instalar. Consulte os Requisitos para obter mais informações.

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

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

- Esta seção explica como configurar componentes para utilização com a autenticação/autorização Kerberos ao utilizar um EE Server. O VE Server não utiliza o Key Server.

  O Key Server consiste num serviço que verifica os clientes que se ligam a um socket. Depois de um cliente se ligar, é estabelecida, autenticada e encriptada uma ligação segura através de APIs Kerberos (se não for possível estabelecer uma ligação segura, o cliente é desligado).

  O Key Server verifica então no Security Server (anteriormente no Device Server) se o utilizador que está a executar o cliente tem permissão para aceder às chaves. Este acesso é concedido na Remote Management Console através de domínios individuais.
- Se for necessário utilizar Autenticação/Autorização Kerberos, o servidor que contém o componente Key Server necessita fazer parte do domínio afetado.
- Dado que o VE Server não utiliza o Key Server, a desinstalação típica é afetada. Quando um Encryption Client ativado num VE Server 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 EE 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:**.

   No campo *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 continuar a utilizá-lo).
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 do EE 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").

O formato "superadmin" pode incluir qualquer método que possa ser autenticado no EE Server. São aceitáveis o nome de conta SAM, UPN ou o domínio\nome de utilizador. Qualquer método que possa ser autenticado no EE Server é aceitável, uma vez que é necessária validação para essa conta de utilizador no Active Directory.

Por exemplo, num ambiente com vários domínios, a introdução apenas do nome de conta SAM, como "jdoe", irá provavelmente falhar, uma vez que o EE Server não consegue autenticar "jdoe" pois não consegue encontrar "jdoe". Num ambiente de vários domínios, é recomendada a utilização do UPN, embora também seja aceitável o formato domínio\nome de utilizador. Num ambiente de domínio único, é aceitável o nome de conta SAM.

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

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

Exemplo de ficheiro de configuração

<?xml version="1.0" encoding="utf-8" ?>

<configuration>

<appSettings>

<add key="port" value="8050" /> [porta TCP escutada pelo Key Server. A predefinição é 8050.]

<add key="maxConnections" value="2000" /> [número de ligações de socket ativas permitidas pelo Key Server]

<add key="url" value="https://keyserver.domain.com:8443/xapi/" /> [URL do Security Server (anteriormente Device Server) (o formato é 8081/xapi para um EE Server anterior à v7.7)]

<add key="verifyCertificate" value="false" /> [se verdadeiro, verifica certificados/defina como falso para não verificar ou se utilizar certificados auto-assinados]

<add key="user" value="superadmin" /> [Nome de utilizador usado para comunicar com o Security Server. Este utilizador precisa ter a função de administrador selecionada na Remote Management Console. O formato "superadmin" pode incluir qualquer método que possa ser autenticado no EE Server. São aceitáveis o nome de conta SAM, UPN ou o domínio\nome de utilizador. Qualquer método que possa ser autenticado no EE Server é aceitável, uma vez que é necessária validação para essa conta de utilizador no Active Directory. Por exemplo, num ambiente com vários domínios, a introdução apenas do nome de conta SAM, como "jdoe", irá provavelmente falhar, uma vez que o EE Server não consegue autenticar "jdoe" pois não consegue encontrar "jdoe". Num ambiente de vários domínios, é recomendada a utilização do UPN, embora também seja aceitável o formato domínio\nome de utilizador. Num ambiente de domínio único é aceitável o nome de conta SAM.]

<add key="cacheExpiration" value="30" /> [A frequência (em segundos) com que o Serviço deve verificar quem tem permissão para solicitar chaves. O serviço mantém uma cache e regista o quão antiga ela é. Quando a cache for anterior ao valor, é obtida uma nova lista. Quando um utilizador se liga, o Key Server necessita de transferir utilizadores autorizados do Security Server. Se estes utilizadores não estiverem em cache, ou se a lista não tiver sido transferida nos últimos "x" segundos, esta será transferida novamente. Não existe qualquer consulta, mas este valor configura quão obsoleta a lista se pode tornar antes de ser atualizada quando necessário.]

<add key="epw" value="encrypted value of the password" /> [Palavra-passe utilizada para comunicar com o Security Server. Se a palavra-passe de superadmin tiver sido alterada, deve ser alterada aqui.]

</appSettings>

</configuration>

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.

Remote Management Console - Adicionar administrador forense

1 Caso necessário, inicie a sessão na Remote Management Console.
2 Clique em **Populações** > **Domínios**.
3 Selecione o Domínio adequado.
4 Clique no separador **Key Server**.
5 No campo Conta, adicione o utilizador que irá realizar as atividades de administrador. O formato é DOMAIN\UserName. 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.

15

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 EE Server/VE Server.
- 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 VE Server não utiliza o Key Server, portanto o modo de Administrador não pode ser utilizado para obter um pacote de chave a partir de um VE Server. Utilize o Modo forense para obter o pacote de chaves se o cliente estiver ativado em um VE Server.

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.

Configurar o Server Encryption

Ativar o Server Encryption

NOTA:
O Server Encryption converte a encriptação de Utilizador para encriptação Comum.

1 Inicie sessão como Administrador Dell na Dell Remote Management Console.

2 Selecione **Grupo de endpoints** (ou **Endpoint**), procure o endpoint ou grupo de endpoints que pretende ativar, selecione **Políticas de segurança** e, em seguida, selecione a categoria de política **Server Encryption**.

3 Defina as seguintes políticas:

- Server Encryption - **Selecione** para ativar o Server Encryption e as políticas relacionadas.
- Encriptação SDE ativada - **Selecione** para ligar a encriptação SDE.
- Encriptação ativada - **Selecione** para ligar a encriptação Comum.
- Credenciais do Windows seguras - Esta política está **Selecionada** por predefinição.

  Quando a política *Credenciais do Windows seguras* está **Selecionada** (predefinição), todos os ficheiros da pasta de ficheiros \Windows\system32\config são encriptados, incluindo as credenciais Windows. Para evitar a encriptação das credenciais do Windows, defina a política *Credenciais do Windows seguras* para **Não selecionada**. A encriptação das credenciais Windows ocorre independentemente de qual seja a definição da política *Encriptação SDE Ativada*.

4 Guarde e consolide as políticas.

Personalizar a caixa de diálogo Início de sessão de Ativação

A caixa de diálogo Início de sessão de Ativação é exibida:

- Quando um utilizador não gerido inicia sessão.
- Quando o utilizador selecionar Ativar o Dell Encryption no menu do ícone Encriptação, localizado no tabuleiro do sistema.

Definir políticas EMS do Server Encryption

O ***computador de encriptação de origem*** é o computador no qual originalmente foi encriptado um dispositivo amovível. Quando o computador de origem é um ***servidor protegido*** - um servidor com o Server Encryption instalado e ativado - e o servidor protegido deteta a presença, pela primeira vez, de um dispositivo amovível, é solicitado ao utilizador que encripte o dispositivo amovível.

- As políticas EMS controlam, entre outros, o acesso de suportes de dados amovíveis ao servidor, autenticação e encriptação.
- As políticas de Controlo de Portas afetam os suportes de dados amovíveis em servidores protegidos, por exemplo, controlando o acesso e a utilização das portas USB do servidor pelos dispositivos USB.

As políticas para encriptação de suportes de dados amovíveis podem ser encontradas na Remote Management Console, no grupo de tecnologia *Server Encryption*.

Server Encryption e Suportes Multimédia Externos

Quando a política *Suporte de dados externo de encriptação EMS* do servidor protegido é **Selecionada**, o suporte de dados externo é encriptado. O Server Encryption associa o dispositivo ao servidor protegido com a chave de computador, e ao utilizador, com a chave de Roaming de utilizador do proprietário/utilizador do dispositivo amovível. Todos os ficheiros adicionados ao dispositivo amovível serão então encriptados com essas mesmas chaves, independentemente do computador ao qual se encontra ligado.

NOTA:
O Server Encryption converte a encriptação de Utilizador para encriptação Comum, exceto em dispositivos amovíveis. Em dispositivos amovíveis, a encriptação é realizada com a chave de Roaming de utilizador associada ao computador.

Quando o utilizador não concorda com a encriptação do dispositivo amovível, o acesso do utilizador ao dispositivo poderá ser definido para *bloqueado*, quando for utilizado no servidor protegido, *Só de leitura*, enquanto for utilizado no servidor protegido, ou *Acesso total*. As políticas do servidor protegido determinam o nível de acesso de um dispositivo amovível desprotegido.

As atualizações de política ocorrem quando o dispositivo amovível é reintroduzido no servidor protegido de origem.

Autenticação e Suportes de Dados Externos

As políticas do servidor protegido determinam a funcionalidade da autenticação.

Depois de um dispositivo amovível ter sido encriptado, apenas o respetivo proprietário/utilizador pode aceder ao dispositivo amovível no servidor protegido. Os restantes utilizadores não irão conseguir aceder aos ficheiros encriptados no suporte de dados amovível.

A autenticação local automática permite que o suporte de dados amovível protegido seja automaticamente autenticado quando inserido no servidor protegido e o proprietário desse suporte de dados tiver sessão iniciada. Quando a autenticação automática estiver desativada, o proprietário/utilizador deve efetuar a autenticação para aceder ao dispositivo amovível protegido.

Quando o computador de encriptação de origem de um dispositivo amovível for um servidor protegido, o proprietário/utilizador deve sempre iniciar sessão no dispositivo amovível quando o utilizar em computadores que não sejam de origem, independentemente das definições de política EMS definidas nos outros computadores.

Consulte AdminHelp para obter informações sobre o Controlo de Portas e políticas EMS do Server Encryption.

Suspender uma instância de servidor encriptado

A suspensão de um servidor encriptado impede o acesso aos respetivos dados encriptados após um reinício. O utilizador do servidor virtual não pode ser suspenso. Em vez disso, é suspensa a chave de computador do Server Encryption.

NOTA:
A suspensão do endpoint do servidor não suspende imediatamente o servidor. A suspensão ocorre quando a chave for novamente solicitada, tipicamente quando o servidor é reiniciado.

IMPORTANTE:

Use esta função com cautela. A suspensão de uma instância de servidor encriptado poderá originar instabilidade, dependendo das definições de política e se o servidor protegido está suspenso enquanto se encontra desligado da rede.

Pré-requisitos

- Os direitos de Administrador de suporte técnico, atribuídos na Remote Management Console, são necessários para suspender um endpoint.
- O administrador deve ter sessão iniciada na Remote Management Console.

No painel esquerdo da Remote Management Console, clique em **Populações** > **Endpoints**.

Procure ou selecione um Nome do anfitrião e, em seguida, clique no separador **Detalhes e ações**.

Em Controlo de dispositivos do servidor, clique em **Suspender** e, em seguida, em **Sim**.

NOTA:

Clique no botão **Restabelecer** para permitir que o Server Encryption aceda a dados encriptados no servidor após reiniciar.

Resolução de problemas

Todos os clientes - Resolução de problemas

- **Os ficheiros de registo do instalador principal do ESSE m** estão localizados 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\<UserName>\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\<UserName>\AppData\Local\Temp. Por exemplo, C:\Users\<UserName>\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.
- Consulte *Dell Data Protection | Security Tools Compatibility* 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.

Resolução de problemas do Encryption e do Server Encryption Client

Atualização para o Windows 10 Anniversary

Para atualizar para a versão de atualização do Windows 10 Anniversary, siga as instruções apresentadas no artigo seguinte: 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 de 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 de domínio.

As credenciais utilizadas para ativação não possuem direitos de administrador de domínio ou o nome de utilizador do administrador não está em formato UPN.

Solução possível**:** Na caixa de diálogo Ativação, introduza as credenciais de um Administrador de domínio e certifique-se de que estão em 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 DDP Security 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 Servidor DDP para garantir que é o mesmo URL que o administrador forneceu. 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 Servidor DDP deve ser a versão 9.1 ou superior. Se necessário, faça uma atualização de versão do seu Servidor DDP para a versão 9.1 ou superior.
- Verifique o URL do Servidor DDP para garantir que é o mesmo URL que o administrador forneceu. 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 sem domínio, ligado ao ambiente de trabalho remoto ou interativo, mas o utilizador deve ter acesso a credenciais de Administrador de 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 no tabuleiro do sistema 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 de 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 de domínio, consulte Antes de começar.

6 O Servidor DDP verifica as credenciais no cofre da empresa (Active Directory ou equivalente) para confirmar se as mesmas são as credenciais de Administrador de domínio.

7 Um UPN é construído utilizando as credenciais.

8 Com o UPN, o Servidor DDP cria uma nova conta de utilizador para o utilizador do servidor virtual, e guarda as credenciais no cofre do Servidor DDP.

A **conta de utilizador do servidor virtual** destina-se a utilização exclusiva do Encryption Client. Esta será utilizada para autenticação no servidor, para 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 parte da ativação, Autenticação e 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 DDP Enterprise 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.
- No caso de o Shield ID (ID de Proteção) exibir cor vermelha, a encriptação ainda não foi ativada.
- Na Remote 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 Remote Management Console, para obter detalhes sobre a política *Intervalo de tempo entre tentativas em caso de falha de rede*.

Autenticação e processo de 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 Servidor DDP:

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

- Se o computador tiver anteriormente ativado o dispositivo, o Servidor DDP verifica o certificado de confiança.

3 Depois de o Servidor DDP 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.

(Opcional) Criar um ficheiro de registo do Encryption Removal Agent

- Antes de iniciar o processo de desinstalação, é possível criar, de forma opcional, um ficheiro de registo do Agente de remoção de encriptação. Este ficheiro de registo é útil para resolução de problemas numa operação de desinstalação/desencriptação. Se não pretender desencriptar ficheiros durante o processo de desinstalação, não é necessário criar este ficheiro de registo.
- O ficheiro de registo do Encryption Removal Agent apenas é criado após a execução do Encryption Removal Agent, que ocorre somente quando o computador é reiniciado. Quando o cliente for desinstalado com êxito e o computador for totalmente desencriptado, o ficheiro de registo é eliminado definitivamente.
- O caminho do ficheiro de registo é **C:\ProgramData\Dell\Dell Data Protection\Encryption.**
- Crie a seguinte entrada de registo no computador destinado à desencriptação.

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=dword:2

  0: sem registos

  1: regista os erros que impedem a execução do Serviço

  2: regista os erros que impedem a desencriptação total dos dados (nível recomendado)

  3: regista informações acerca de todos os ficheiros e volumes de desencriptação

  5: regista as informações de depuração

Encontrar versão do TSS

- O TSS é um componente que interage com o TPM. Para encontrar a versão do TSS, aceda a (localização predefinida) **C:\Program Files \Dell\Dell Data Protection\Drivers\TSS\bin > tcsd_win32.exe**. Clique com o botão direito do rato no ficheiro e selecione **Propriedades**. Verifique a versão do ficheiro no separador **Detalhes**.

Interações com EMS e PCS

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

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

Para encriptar os dados gravados em CD/DVD

- Defina EMS: Encriptar suporte multimédia externo = Verdadeiro.

- Definir EMS: excluir encriptação de CD/DVD = Falso.
- 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 no menu pendente: *Todas as unidades, Unidades fixas*, *Unidades amovíveis* ou *CDROM/DVDROM*.
5 Selecione o Tipo de relatório de encriptação pretendido no menu pendente: *Ficheiros encriptados*, *Ficheiros desencriptados*, *Todos os ficheiros* ou *Ficheiros desencriptados 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 na caixa pendente será 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.

Utilização da linha de comandos do WSScan

```
WSScan [-ta] [-tf] [-tr] [-tc] [drive] [-s] [-o<filepath>] [-a] [-f<format specifier>] [-r] [-u[a][-|v]] [-d<delimeter>] [-q] [-e] [-x<exclusion directory>] [-y<sleep time>]
```

Opção	Significado
Unidade	Unidade a analisar. Se não for especificada, serão assumidas, por predefinição, todas as unidades de disco rígido fixas locais. Pode ser uma unidade de rede mapeada.
-ta	Analisar todas as unidades
-tf	Analisar as unidades fixas (predefinição)
-tr	Analisar as unidades amovíveis
-tc	Analisar CDROM/DVDROM
-s	Operação silenciosa
-o	Caminho do ficheiro de saída
-A	Anexar ao ficheiro de saída. O ficheiro de saída é truncado pelo comportamento predefinido.
-f	Reportar o especificador de formato (Reportar, Fixo, Delimitado)
-r	Executar o WSScan sem privilégios de administrador. **Se este modo for utilizado, alguns ficheiros poderão não ficar visíveis.**
-u	Incluir ficheiros desencriptados no ficheiro de saída. Esta opção é sensível à ordem: "u" deve ser utilizado primeiro, "a" deve ser o segundo (ou ser omitido), "-" ou "v" deve ser o último.
-u-	Incluir apenas ficheiros desencriptados no ficheiro de saída
-ua	Reportar também ficheiros desencriptados, mas utilizar todas as políticas do utilizador para apresentar o campo "should".
-ua-	Reportar apenas ficheiros desencriptados, mas utilizar todas as políticas do utilizador para apresentar o campo "should".
-uv	Reportar ficheiros desencriptados que apenas violem a política (Is=No/Should=Y)
-uav	Reportar ficheiros desencriptados que apenas violem a política (Is=No/Should=Y), utilizando todas as outras políticas de utilizador.
-d	Especificar o que é utilizado como separador de valores para uma saída delimitada
-q	Especificar os valores que devem ser colocados entre aspas para uma saída delimitada
-e	Incluir campos de encriptação alargada em saída delimitada
-x	Excluir o diretório da análise. São permitidas várias exclusões.
-y	Tempo de suspensão (em milissegundos) entre os diretórios. Esta opção resulta em análises mais lentas, mas potencialmente num CPU com maior capacidade de resposta.

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 de encriptação 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. 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

Utilizar o WSProbe

O Probing Utility pode ser utilizado com todas as versões do Encryption Client, exceto as políticas do EMS: Utilize o Probing Utility para:

- Analisar ou agendar análises de um computador encriptado. O Probing Utility verifica a sua política de Prioridade de análise da estação de trabalho.
- Desative temporariamente ou volte a ativar o Application Data Encryption List do utilizador atual.
- Adicione ou remova nomes de processos na lista de privilégios.
- Efetue a resolução de problemas de acordo com as instruções do Dell ProSupport.

Abordagens ao Data Encryption

Se especificar políticas de encriptação de dados em dispositivos Windows, pode utilizar qualquer uma das seguintes abordagens:

- A primeira abordagem é aceitar o comportamento predefinido do cliente. Se especificar pastas em Pastas encriptadas comuns ou Pastas encriptadas do utilizador, ou definir Encriptar "Meus documentos", Encriptar pastas pessoais do Outlook, Encriptar ficheiros temporários, Encriptar ficheiros temporários da Internet ou Encriptar ficheiro de paginação do Windows para selecionado, os ficheiros afetados são encriptados quando são criados, ou (depois de serem criados por um utilizador não gerido) quando um utilizador gerido

inicia sessão. O cliente também analisa as pastas especificadas ou relacionadas com estas políticas para uma possível encriptação/desencriptação, quando o nome de uma pasta é alterado ou quando o cliente recebe alterações a estas políticas.

- Também pode definir Analisar estação de trabalho no início de sessão para Verdadeiro. Se Analisar estação de trabalho no início de sessão estiver definido para Verdadeiro, quando um utilizador iniciar sessão, o cliente compara a forma como os ficheiros estão encriptados nas pastas encriptadas, anterior e atualmente, com as políticas do utilizador, e efetua as alterações necessárias.
- Para encriptar ficheiros que cumpram os critérios de encriptação, mas que foram criados antes da entrada em vigor das políticas de encriptação, sem qualquer impacto no desempenho da análise frequente, pode utilizar este utilitário para analisar ou agendar a análise do computador.

Pré-requisitos

- O dispositivo Windows em que pretende trabalhar deve estar encriptado.
- O utilizador em que pretende trabalhar deve ter sessão iniciada.

Utilizar o Probing Utility

O WSProbe.exe está localizado no suporte multimédia de instalação.

Sintaxe

```
wsprobe [path]

wsprobe [-h]

wsprobe [-f path]

wsprobe [-u n] [-x process_names] [-i process_names]
```

Parâmetros

Parâmetro	Para
caminho	Especificação opcional de um caminho específico no dispositivo que pretende analisar para uma possível encriptação/desencriptação. Se não especificar um caminho, este utilitário analisa todas as pastas relacionadas com as suas políticas de encriptação.
-h	Consulte a Ajuda da linha de comandos.
-f	Efetue a resolução de problemas de acordo com as instruções do Dell ProSupport
-u	Desative temporariamente ou volte a ativar o Application Data Encryption List do utilizador Esta lista apenas é eficaz se a opção Encriptação ativada estiver selecionada no utilizador atual. Especifique o valor 0 para desativar ou 1 para voltar a ativar. A atual política em vigor para o utilizador é restabelecida no próximo início de sessão.
-x	Adicione nomes de processos à lista de privilégios. Os nomes de processos do computador e do instalador indicados nesta lista, incluindo os adicionados utilizando este parâmetro ou HKLM \Software\CREDANT\CMGShield\EUWPrivilegedList, são ignorados se forem especificados no Application Data Encryption List. Separe os nomes de processos com vírgulas. Se a sua lista incluir um ou mais espaços, delimite a lista com aspas duplas.
-i	Elimine os nomes de processos previamente adicionados à lista de privilégios (não é possível eliminar nomes de processos codificados). Separe os nomes de processos com vírgulas. Se a sua lista incluir um ou mais espaços, delimite a lista com aspas duplas.

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 (selecione 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 resolução de problemas, defina a verbosidade do registo para 2 e reinicie o serviço de Agente de Remoção de Encriptação para forçar outro varrimento de desencriptação. Consulte (Opcional) Criar um ficheiro de registo do Encryption Removal Agent para obter instruções.
- **Concluído** - O varrimento da desencriptação está concluído. É agendada a eliminação do Serviço, do executável, do controlador e do executável do controlador no próximo reinício.

Resolução de problemas do cliente Advanced Threat Prevention

Encontrar o código do produto com o Windows PowerShell

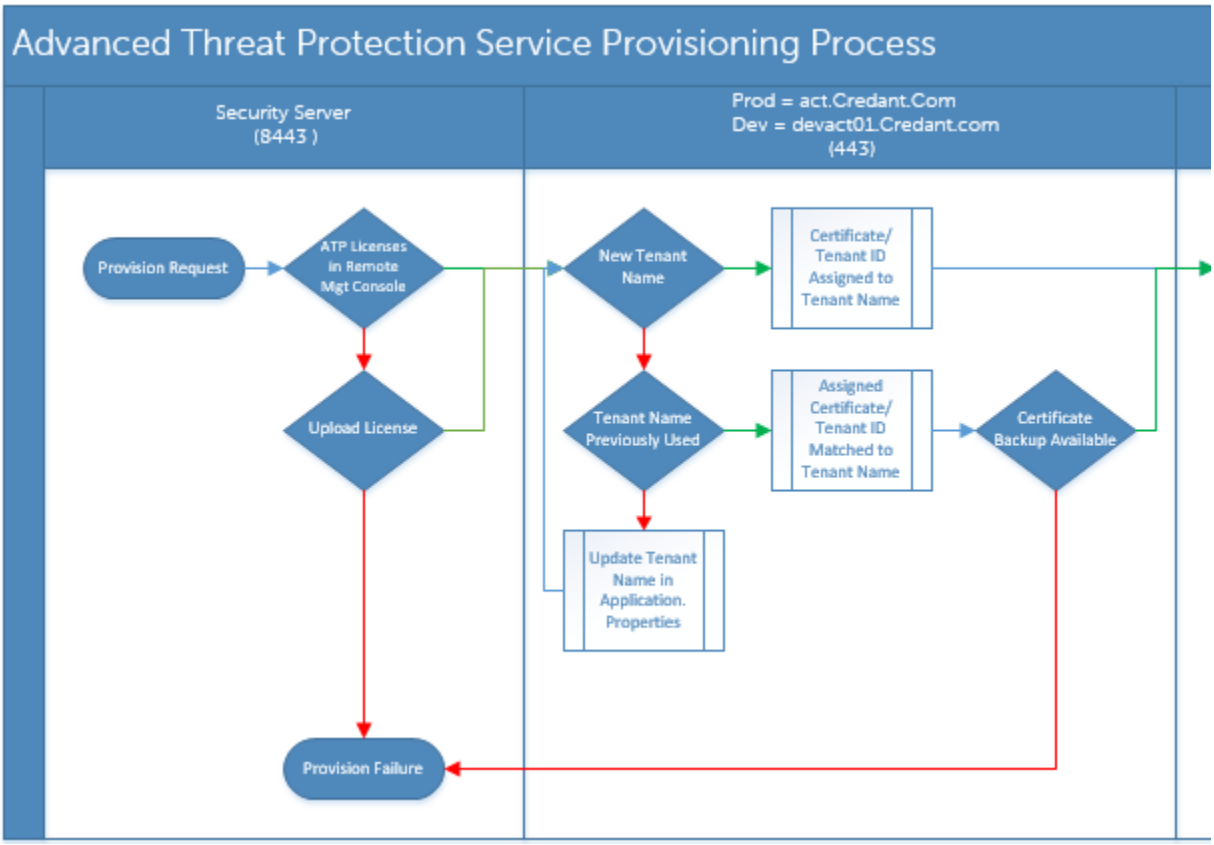
- Pode identificar facilmente o código do produto, se o código do produto mudar no futuro, utilizando este método.

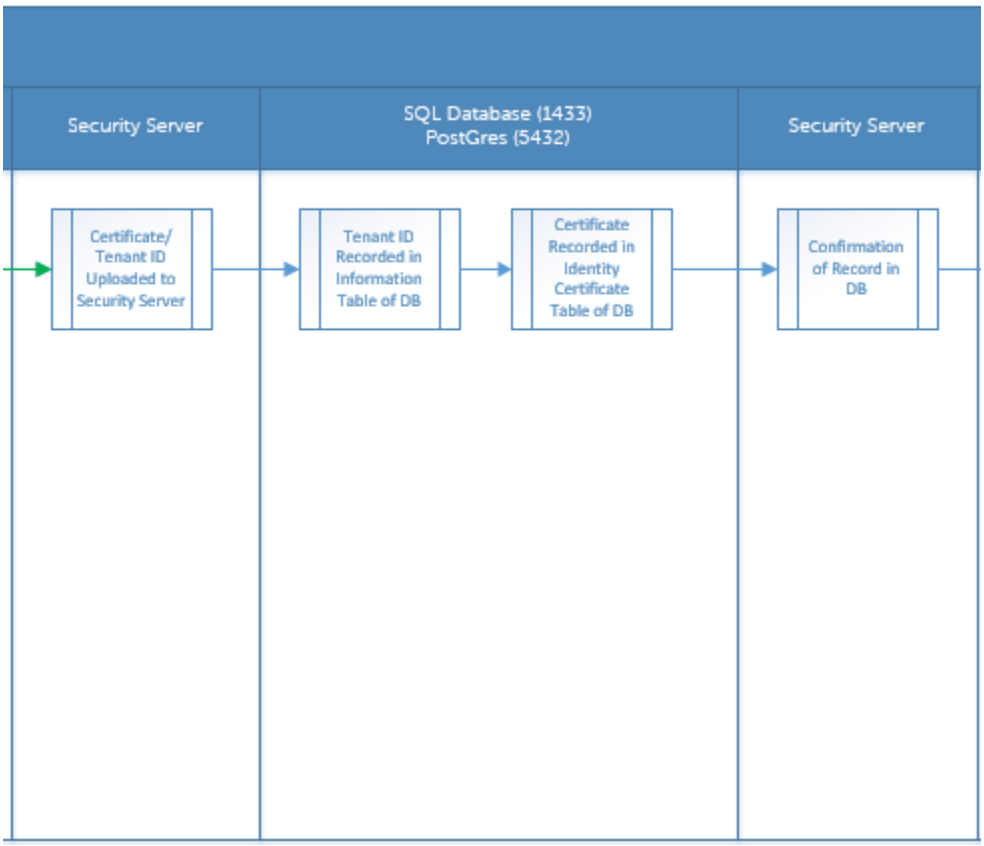
  ```
  Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT
  IdentifyingNumber, Name, LocalPackage
  ```

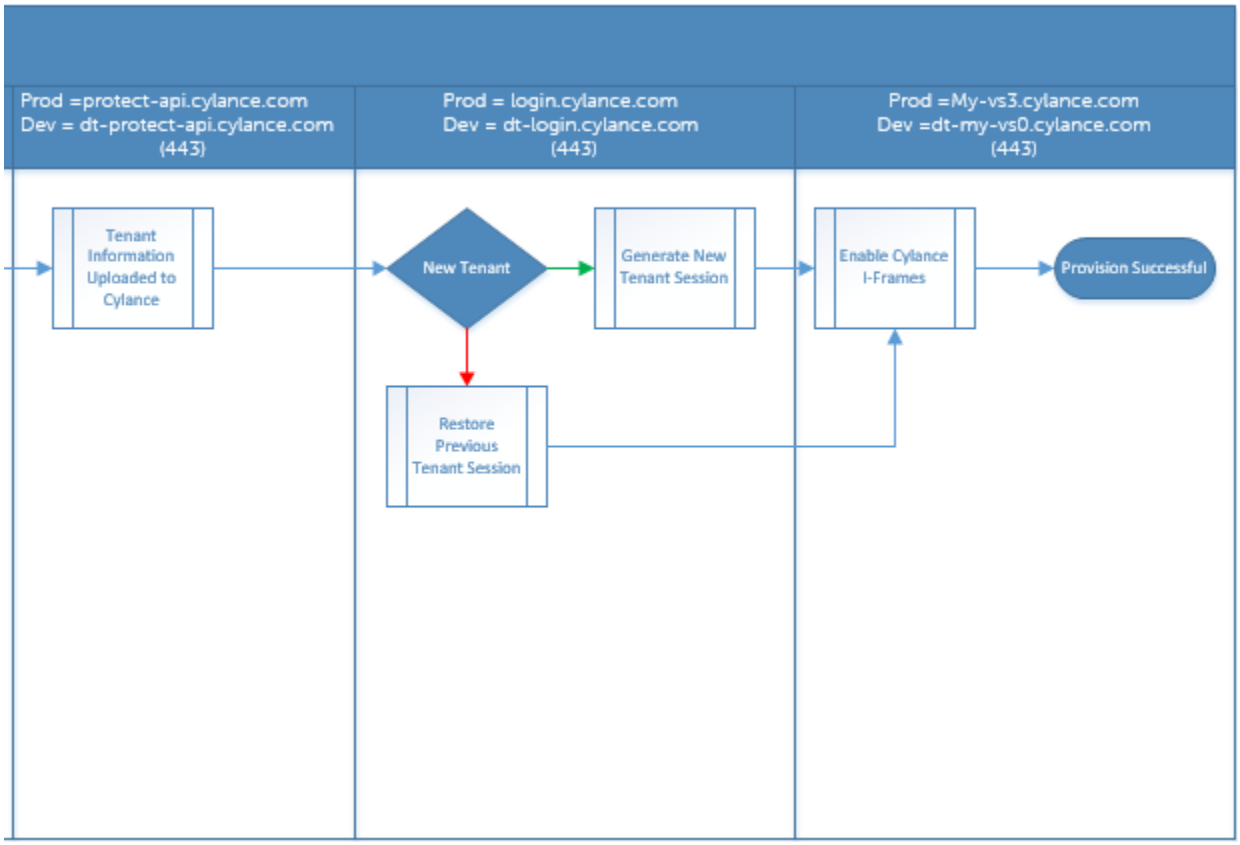
  O resultado será o caminho completo e o nome do ficheiro .msi (o nome hexadecimal convertido do ficheiro).

Aprovisionamento e comunicação do agente do Advanced Threat Prevention

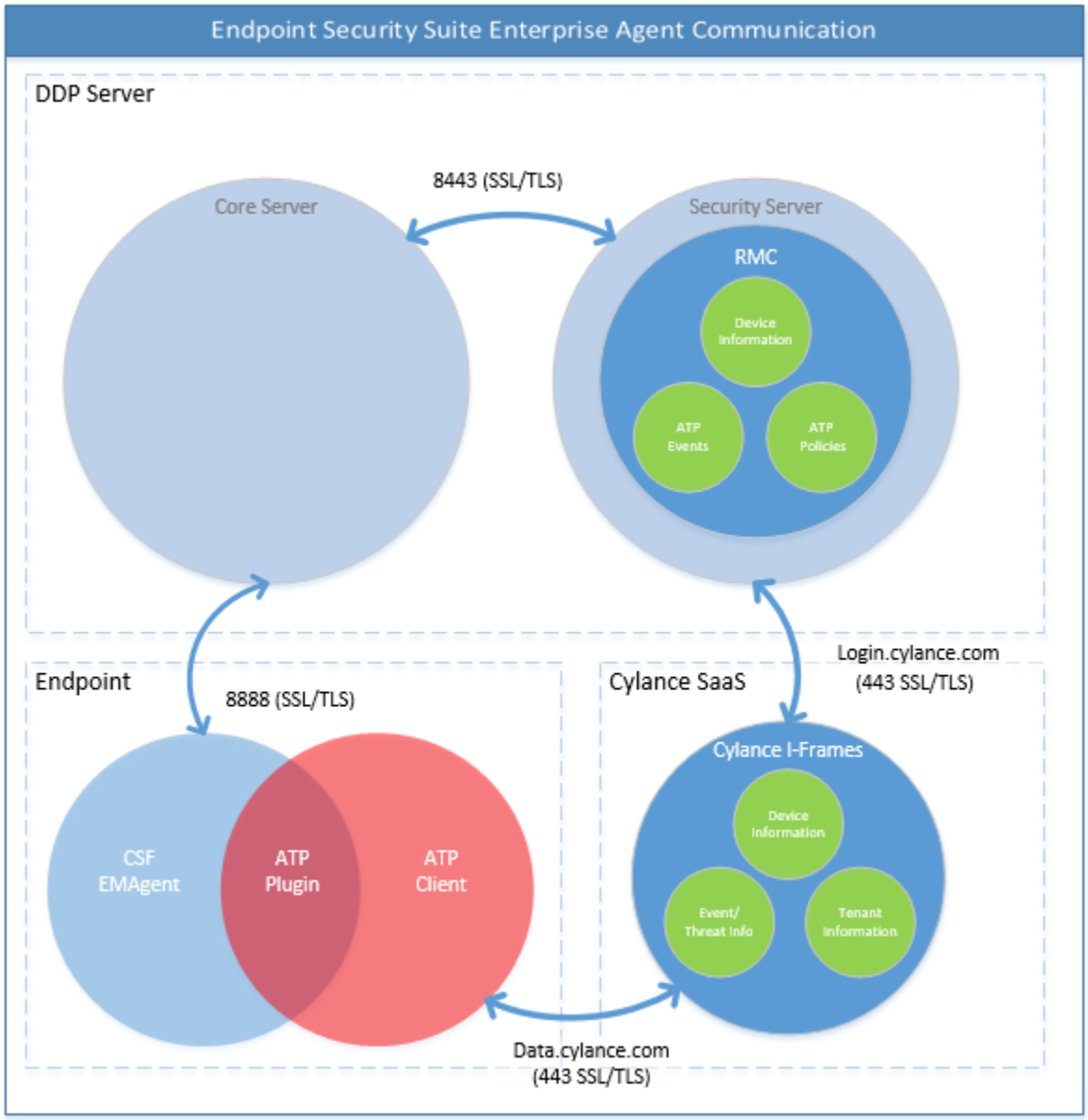
Os diagramas seguintes ilustram o processo de aprovisionamento do serviço do Advanced Threat Prevention.


Advanced Threat Protection Service Provisioning Process
Security Server
(8443)
Prod = act.Credant.Com
Dev = devact01.Credant.com
(443)
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
New Tenant Name
Certificate/ Tenant ID Assigned to Tenant Name
Tenant Name Previously Used
Assigned Certificate/ Tenant ID Matched to Tenant Name
Certificate Backup Available
Update Tenant Name in Application. Properties
Provision Failure


Security Server
SQL Database (1433)
PostGres (5432)
Security Server
Certificate/ Tenant ID Uploaded to Security Server
Tenant ID Recorded in Information Table of DB
Certificate Recorded in Identity Certificate Table of DB
Confirmation of Record in DB

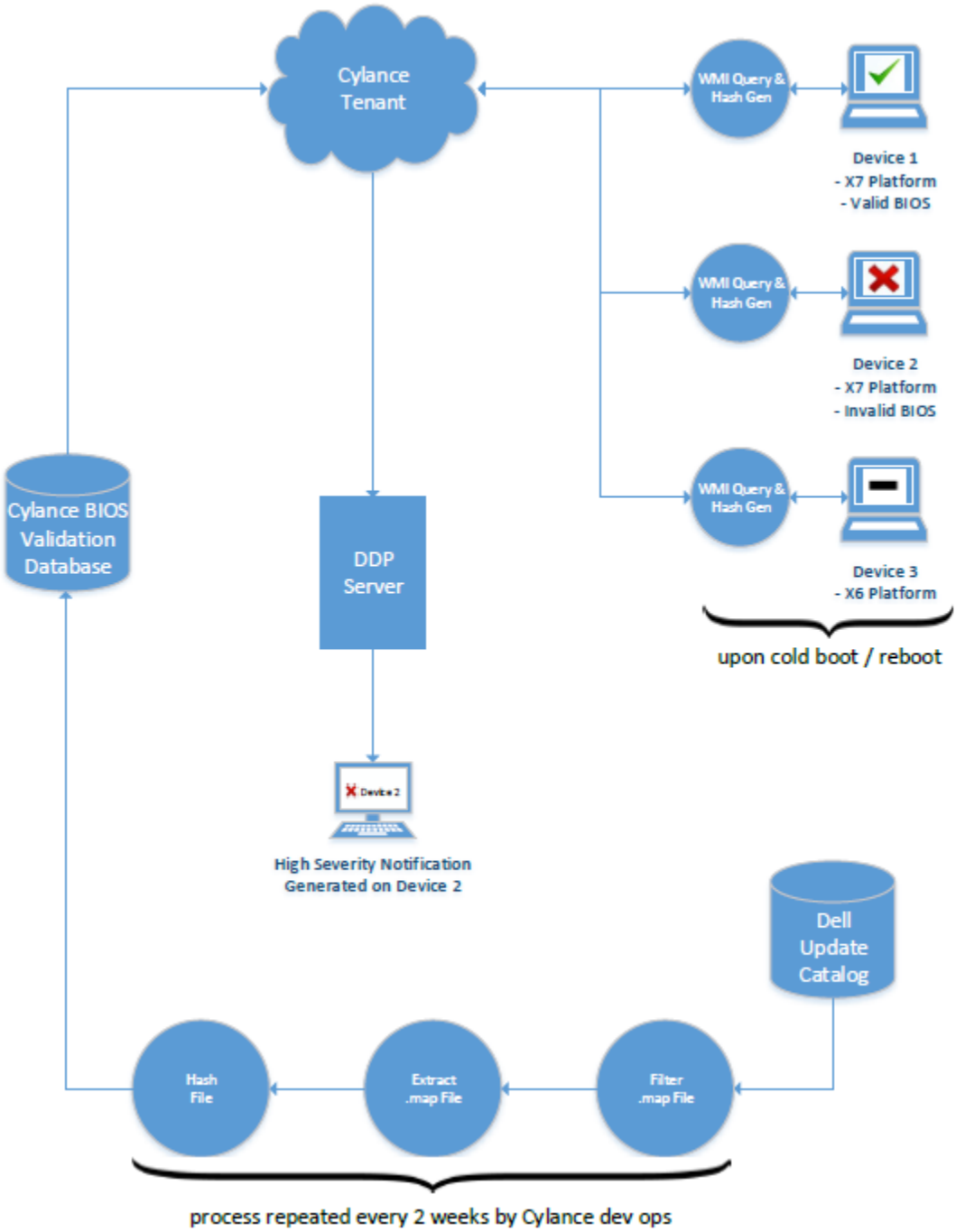


O diagrama seguinte ilustra o processo de comunicação do agente do Advanced Threat Prevention.



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.



Resolução de problemas do cliente SED

Utilizar a política de Código de acesso inicial

- Esta política é utilizada para iniciar sessão num computador quando o acesso à rede não se encontra disponível. Ou seja, o acesso ao EE Server/VE Server e AD não se encontram disponíveis. Utilize a política de *Código de acesso inicial* apenas se for absolutamente necessário. A Dell não recomenda este método para iniciar sessão. A utilização da política de *Código de acesso inicial* não proporciona o mesmo nível de segurança que o método comum de início de sessão utilizando o nome do utilizador, domínio e palavra-passe.

Além de ser um método de início de sessão menos seguro, se um utilizador final for ativado utilizando o *Código de acesso inicial*, não existe qualquer registo no EE Server/VE Server da ativação desse utilizador neste computador. Por outro lado, não há forma de gerar um Código de resposta no EE Server/VE Server para o utilizador final, caso este erre a palavra-passe e as respostas às perguntas de autoajuda.

- O *Código de acesso inicial* só pode ser utilizado **uma** vez, imediatamente após a ativação. Após o início de sessão de um utilizador final, o *Código de acesso inicial* fica indisponível. O primeiro início de sessão do domínio que ocorre depois de introduzir o *Código de acesso inicial*, será colocado em cache e o campo para introdução do *Código de acesso inicial* não será novamente apresentado.
- O *Código de acesso inicial* **apenas** é apresentado nas seguintes circunstâncias:
  - Nunca foi ativado um utilizador dentro da PBA.
  - O cliente não possui ligação à rede ou ao EE Server/VE Server.

Utilizar o Código de acesso inicial

1. Defina um valor para a política de **Código de acesso inicial** na Remote Management Console.
2. Guarde e consolide a política.
3. Inicie o computador local.
4. Introduza o **Código de acesso inicial** quando for apresentado o ecrã Código de acesso.
5. Clique na **seta azul**.
6. Clique em **OK** quando for apresentado o ecrã Aviso legal.
7. Inicie sessão no Windows com as credenciais de utilizador deste computador. Estas credenciais devem fazer parte do domínio.
8. Após iniciar sessão, abra a Security Console e verifique se o utilizador da PBA foi criado com êxito.

   Clique em **Registo** no menu superior e procure a mensagem *Criado utilizador da PBA para <domínio\nome de utilizador>*, que indica que o processo foi bem-sucedido.
9. Encerre e reinicie o computador.
10. No ecrã de início de sessão, introduza o nome do utilizador, o domínio e a palavra-passe anteriormente utilizados para iniciar sessão no Windows.

    Deve fazer corresponder o formato do nome de utilizador que foi utilizado ao criar o utilizador da PBA. Desta forma, se tiver utilizado o formato domínio/nomedeutilizador, deve introduzir domínio/nomedeutilizador no campo Nome de utilizador.
11. (Apenas Credant Manager) Responda às solicitações de pergunta e resposta.

    Clique na **seta azul**.
12. Clique em **Iniciar sessão** quando for apresentado o ecrã Aviso legal.

    O Windows é, então, iniciado e é possível utilizar o computador da forma habitual.

Criar um ficheiro de registo de PBA para resolução de problemas

- Poderão existir casos em que é necessário um ficheiro de registo de PBA para a resolução de problemas com a PBA, tais como:
  - Não consegue ver o ícone de ligação à rede, embora saiba que existe conectividade de rede. O ficheiro de registo contém informações de DHCP para resolver o problema.
  - Não consegue ver o ícone de ligação ao EE Server/VE Server. O ficheiro de registo contém informações para ajudar a diagnosticar problemas de conectividade do EE Server/VE Server.
  - A autenticação falha mesmo ao introduzir as credenciais corretas. O ficheiro de registo utilizado nos registos do EE Server/VE Server pode ajudar a diagnosticar o problema.

Captar registos aquando do arranque através da PBA (PBA legada)

1. Crie uma pasta numa unidade USB, no nível da raiz, e atribua-lhe o nome **\CredantSED**.

2 Crie um ficheiro com o nome actions.txt e coloque-o na pasta **\CredantSED**.

3 No ficheiro actions.txt, adicione a linha:

```
get environment
```

4 Guarde e feche o ficheiro.

Não introduza a unidade USB quando o computador estiver desligado. Se a unidade USB já estiver inserida durante o processo de encerramento, remova-a.

5 Ligue o computador e inicie sessão na PBA. Insira a unidade USB no computador do qual serão recolhidos os registos durante este passo.

6 Depois de introduzir a unidade USB, aguarde entre 5 e 10 segundos e, em seguida, retire a unidade.

Um ficheiro credpbaenv.tgz é criado na pasta **\CredantSED** que contém os ficheiros de registo necessários.

Captar registos aquando do arranque através da PBA (PBA UEFI)

1 Crie um ficheiro com o nome **PBAErr.log** no nível da raiz da unidade USB.

2 Introduza a unidade USB **antes** de ligar o computador.

3 Remova a unidade USB **depois** de reproduzir o problema que requer os registos.

O ficheiro PBAErr.log será atualizado e gravado em tempo real.

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\<New Folder>.

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\<New Folder>.
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, ser-lhe-á pedida 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.

Computadores UEFI

Resolução de problemas de ligação à rede

- Para que a autenticação de pré-arranque seja bem-sucedida num computador com firmware UEFI, o modo PBA deve ter ligação à rede. Por predefinição, os computadores com firmware UEFI não têm ligação à rede até que o sistema operativo seja carregado, o que ocorre

depois do modo PBA. Se o procedimento do computador descrito em Configuração da pré-instalação para computadores UEFI for concluído com sucesso e configurado corretamente, o ícone de ligação à rede é apresentado no ecrã de autenticação de pré-arranque quando o computador estiver ligado à rede.

- Verifique o cabo de rede para garantir que está ligado ao computador caso o ícone de ligação continue a não ser apresentado durante a autenticação de pré-arranque. Reinicie o computador para reiniciar o modo PBA caso o mesmo não esteja ligado ou esteja solto.

TPM e BitLocker

Códigos de erro do TPM e BitLocker

Constante/Valor	Descrição
TPM_E_ERROR_MASK 0x80280000	Trata-se de uma máscara de erro para converter erros de hardware de TPM em erros do Windows.
TPM_E_AUTHFAIL 0x80280001	A autenticação falhou.
TPM_E_BADINDEX 0x80280002	O índice para um PCR, DIR ou outro registo é incorreto.
TPM_E_BAD_PARAMETER 0x80280003	Um ou mais parâmetros estão errados.
TPM_E_AUDITFAILURE 0x80280004	Uma operação foi concluída com êxito, mas a auditoria dessa operação falhou.
TPM_E_CLEAR_DISABLED 0x80280005	O sinalizador de desativação de limpeza está definido e todas as operações de limpeza requerem agora acesso físico.
TPM_E_DEACTIVATED 0x80280006	Ativa o TPM.
TPM_E_DISABLED 0x80280007	Ativa o TPM.
TPM_E_DISABLED_CMD 0x80280008	O comando de destino foi desativado.
TPM_E_FAIL 0x80280009	Falha na operação.
TPM_E_BAD_ORDINAL	O ordinal era desconhecido ou inconsistente.

Constante/Valor	Descrição
0x8028000A	
TPM_E_INSTALL_DISABLED	A capacidade de instalar um proprietário está desativada.
0x8028000B	
TPM_E_INVALID_KEYHANDLE	Não é possível interpretar o identificador da chave.
0x8028000C	
TPM_E_KEYNOTFOUND	O identificador da chave aponta para uma chave inválida.
0x8028000D	
TPM_E_INAPPROPRIATE_ENC	Esquema de encriptação inaceitável.
0x8028000E	
TPM_E_MIGRATEFAIL	Falha na autorização de migração.
0x8028000F	
TPM_E_INVALID_PCR_INFO	Não foi possível interpretar as informações de PCR.
0x80280010	
TPM_E_NOSPACE	Não existe espaço para carregar a chave.
0x80280011	
TPM_E_NOSRK	Não existe qualquer conjunto SRK (Storage Root Key).
0x80280012	
TPM_E_NOTSEALED_BLOB	Um blob encriptado é inválido ou não foi criado por este TPM.
0x80280013	
TPM_E_OWNER_SET	O TPM já tem um proprietário.
0x80280014	
TPM_E_RESOURCES	O TPM tem recursos internos insuficientes para executar a ação pedida.
0x80280015	
TPM_E_SHORTRANDOM	Uma cadeia aleatória era demasiado curta.
0x80280016	
TPM_E_SIZE	O TPM não tem espaço para executar a operação.
0x80280017	
TPM_E_WRONGPCRVAL	O valor de PCR nomeado não corresponde ao valor de PCR atual.
0x80280018	
TPM_E_BAD_PARAM_SIZE	O argumento paramSize do comando tem um valor incorreto

Constante/Valor	Descrição
0x80280019	
TPM_E_SHA_THREAD 0x8028001A	Não existe qualquer thread SHA-1.
TPM_E_SHA_ERROR 0x8028001B	O cálculo não pode prosseguir porque o thread SHA-1 existente já encontrou um erro.
TPM_E_FAILEDSELFTEST 0x8028001C	O dispositivo de hardware de TPM reportou uma falha durante o respetivo autoteste interno. Experimente reiniciar o computador para resolver o problema. Se o problema continuar, poderá ser necessário substituir a placa principal ou o hardware de TPM.
TPM_E_AUTH2FAIL 0x8028001D	A autorização da segunda chave numa função de 2 chaves falhou.
TPM_E_BADTAG 0x8028001E	O valor da etiqueta enviado para um comando é inválido.
TPM_E_IOERROR 0x8028001F	Ocorreu um erro de ES ao transmitir informações para o TPM.
TPM_E_ENCRYPT_ERROR 0x80280020	Ocorreu um problema no processo de encriptação.
TPM_E_DECRYPT_ERROR 0x80280021	O processo de desencriptação não foi concluído.
TPM_E_INVALID_AUTHHANDLE 0x80280022	Foi utilizado um identificador inválido.
TPM_E_NO_ENDORSEMENT 0x80280023	O TPM não tem uma Chave de Endossamento (EK) instalada.
TPM_E_INVALID_KEYUSAGE 0x80280024	Não é permitida a utilização de uma chave.
TPM_E_WRONG_ENTITYTYPE 0x80280025	O tipo de entidade submetido não é permitido.
TPM_E_INVALID_POSTINIT 0x80280026	O comando foi recebido na sequência errada relativamente a TPM_Init e a um TPM_Startup subsequente.
TPM_E_INAPPROPRIATE_SIG 0x80280027	Os dados assinados não podem incluir informações de DER adicionais.

Constante/Valor	Descrição
TPM_E_BAD_KEY_PROPERTY 0x80280028	As propriedades das chaves nos TPM_KEY_PARMs não são suportadas por este TPM.
TPM_E_BAD_MIGRATION 0x80280029	As propriedades de migração desta chave estão incorretas.
TPM_E_BAD_SCHEME 0x8028002A	O esquema de encriptação ou assinatura desta chave estão incorretos ou não são permitidos nesta situação.
TPM_E_BAD_DATASIZE 0x8028002B	O parâmetro de tamanho dos dados (ou blob) está incorreto ou é inconsistente com a chave referenciada.
TPM_E_BAD_MODE 0x8028002C	Um parâmetro de modo é incorreto, tal como capArea ou subCapArea para TPM_GetCapability, o parâmetro phsicalPresence para TPM_PhysicalPresence ou migrationType para TPM_CreateMigrationBlob.
TPM_E_BAD_PRESENCE 0x8028002D	Os bits de physicalPresence ou physicalPresenceLock têm um valor incorreto.
TPM_E_BAD_VERSION 0x8028002E	O TPM não pode executar esta versão da capacidade.
TPM_E_NO_WRAP_TRANSPORT 0x8028002F	O TPM não permite sessões de transporte moldadas.
TPM_E_AUDITFAIL_UNSUCCESSFUL 0x80280030	A construção da auditoria do TPM falhou e o comando subjacente também devolveu um código de falha.
TPM_E_AUDITFAIL_SUCCESSFUL 0x80280031	A construção da auditoria do TPM falhou e o comando subjacente devolveu um código de êxito.
TPM_E_NOTRESETABLE 0x80280032	Tentativa de repor um registo PCR que não tem o atributo de reposição.
TPM_E_NOTLOCAL 0x80280033	Tentativa de repor um registo PCR que necessita da localidade e o modificador de localidade não faz parte do transporte do comando.
TPM_E_BAD_TYPE 0x80280034	Make identity blob não está escrito corretamente.
TPM_E_INVALID_RESOURCE 0x80280035	O tipo de gravação de recurso identificado pelo contexto não corresponde ao recurso propriamente dito.
TPM_E_NOTFIPS 0x80280036	O TPM está a tentar executar um comando que só está disponível no modo FIPS.

Constante/Valor	Descrição
TPM_E_INVALID_FAMILY 0x80280037	O comando está a tentar utilizar um ID de família inválido.
TPM_E_NO_NV_PERMISSION 0x80280038	A permissão para manipular a memória NV não está disponível.
TPM_E_REQUIRES_SIGN 0x80280039	A operação necessita de um comando assinado.
TPM_E_KEY_NOTSUPPORTED 0x8028003A	Operação incorreta para carregar uma chave NV.
TPM_E_AUTH_CONFLICT 0x8028003B	NV_LoadKey blob necessita da autorização do proprietário e do blob.
TPM_E_AREA_LOCKED 0x8028003C	A área NV está bloqueada e não podem ser escritos dados na mesma.
TPM_E_BAD_LOCALITY 0x8028003D	A localidade está incorreta para a operação tentada.
TPM_E_READ_ONLY 0x8028003E	A área NV é só de leitura e não é possível escrever na mesma.
TPM_E_PER_NOWRITE 0x8028003F	Não existe proteção para a escrita na área NV.
TPM_E_FAMILYCOUNT 0x80280040	O valor de contador de famílias não coincide.
TPM_E_WRITE_LOCKED 0x80280041	Já foram escritos dados na área NV.
TPM_E_BAD_ATTRIBUTES 0x80280042	Os atributos da área NV estão em conflito.
TPM_E_INVALID_STRUCTURE 0x80280043	A etiqueta de estrutura e a versão são inválidas ou inconsistentes.
TPM_E_KEY_OWNER_CONTROL 0x80280044	A chave está sob controlo do Proprietário do TPM e só pode ser expulsa pelo Proprietário do TPM.
TPM_E_BAD_COUNTER 0x80280045	O identificador de contador está incorreto.

Constante/Valor	Descrição
TPM_E_NOT_FULLWRITE 0x80280046	A ação de escrita não é uma ação de escrita completa da área.
TPM_E_CONTEXT_GAP 0x80280047	O intervalo entre as contagens de contexto guardadas é demasiado grande.
TPM_E_MAXNVWRITES 0x80280048	Foi excedido o número máximo de escritas NV sem um proprietário.
TPM_E_NOOPERATOR 0x80280049	Não existe qualquer valor AuthData de operador definido.
TPM_E_RESOURCEMISSING 0x8028004A	O recurso apontado pelo contexto não está carregado.
TPM_E_DELEGATE_LOCK 0x8028004B	A administração de delegado está bloqueada.
TPM_E_DELEGATE_FAMILY 0x8028004C	Foi efetuada uma tentativa de gerir uma família que não é a família delegada.
TPM_E_DELEGATE_ADMIN 0x8028004D	A gestão de tabelas de delegação não está ativada.
TPM_E_TRANSPORT_NOTEXCLUSIVE 0x8028004E	Foi executado um comando fora de uma sessão de transporte exclusiva.
TPM_E_OWNER_CONTROL 0x8028004F	Foi efetuada uma tentativa de guardar o contexto de uma chave com expulsão controlada pelo proprietário.
TPM_E_DAA_RESOURCES 0x80280050	O comando DAA não tem quaisquer recursos disponíveis para executar o comando.
TPM_E_DAA_INPUT_DATA0 0x80280051	A verificação de consistência do parâmetro inputData0 de DAA falhou.
TPM_E_DAA_INPUT_DATA1 0x80280052	A verificação de consistência do parâmetro inputData1 de DAA falhou.
TPM_E_DAA_ISSUER_SETTINGS 0x80280053	A verificação de consistência de DAA_issuerSettings falhou.
TPM_E_DAA_TPM_SETTINGS 0x80280054	A verificação de consistência de DAA_tpmSpecific falhou.

Constante/Valor	Descrição
TPM_E_DAA_STAGE 0x80280055	O processo atómico indicado pelo comando DAA submetido não é o processo esperado.
TPM_E_DAA_ISSUER_VALIDITY 0x80280056	A verificação de validade do emissor detetou uma inconsistência.
TPM_E_DAA_WRONG_W 0x80280057	Falha na verificação de consistência em w.
TPM_E_BAD_HANDLE 0x80280058	O identificador está incorreto.
TPM_E_BAD_DELEGATE 0x80280059	A delegação não está correta.
TPM_E_BADCONTEXT 0x8028005A	O blob de contexto é inválido.
TPM_E_TOOMANYCONTEXTS 0x8028005B	Demasiados contextos mantidos pelo TPM.
TPM_E_MA_TICKET_SIGNATURE 0x8028005C	Falha de validação da assinatura da autoridade de migração.
TPM_E_MA_DESTINATION 0x8028005D	Destino de migração não autenticado.
TPM_E_MA_SOURCE 0x8028005E	Origem de migração incorreta.
TPM_E_MA_AUTHORITY 0x8028005F	Autoridade de migração incorreta.
TPM_E_PERMANENTEK 0x80280061	Foi efetuada uma tentativa de revogar a EK e a EK não é revogável.
TPM_E_BAD_SIGNATURE 0x80280062	Assinatura incorreta da permissão de CMK.
TPM_E_NOCONTEXTSPACE 0x80280063	Não existe espaço na lista de contextos para contextos adicionais.
TPM_E_COMMAND_BLOCKED 0x80280400	O comando foi bloqueado.

Constante/Valor	Descrição
TPM_E_INVALID_HANDLE 0x80280401	O identificador especificado não foi encontrado.
TPM_E_DUPLICATE_VHANDLE 0x80280402	O TPM devolveu um identificador duplicado e o comando tem de ser submetido novamente.
TPM_E_EMBEDDED_COMMAND_BLOCKED 0x80280403	O comando contido no transporte estava bloqueado.
TPM_E_EMBEDDED_COMMAND_UNSUPPORTED 0x80280404	O comando existente no transporte não é suportado.
TPM_E_RETRY 0x80280800	O TPM está demasiado ocupado para responder ao comando imediatamente, mas o comando pode ser novamente submetido mais tarde.
TPM_E_NEEDS_SELFTEST 0x80280801	SelfTestFull não foi executado.
TPM_E_DOING_SELFTEST 0x80280802	O TPM está atualmente a executar um autoteste completo.
TPM_E_DEFEND_LOCK_RUNNING 0x80280803	O TPM está a defender-se contra ataques de dicionário e encontra-se num período de tempo limite.
TBS_E_INTERNAL_ERROR 0x80284001	Foi detetado um erro de software interno.
TBS_E_BAD_PARAMETER 0x80284002	Um ou mais parâmetros de entrada estão incorretos.
TBS_E_INVALID_OUTPUT_POINTER 0x80284003	Um apontador de saída especificado está incorreto.
TBS_E_INVALID_CONTEXT 0x80284004	O identificador de contexto especificado não se refere a um contexto válido.
TBS_E_INSUFFICIENT_BUFFER 0x80284005	Uma memória intermédia de saída especificada é demasiado pequena.
TBS_E_IOERROR 0x80284006	Ocorreu um erro ao comunicar com o TPM.
TBS_E_INVALID_CONTEXT_PARAM 0x80284007	Um ou mais parâmetros de contexto são inválidos.

Constante/Valor	Descrição
TBS_E_SERVICE_NOT_RUNNING 0x80284008	O serviço TBS não está em execução e não pode ser iniciado.
TBS_E_TOO_MANY_TBS_CONTEXTS 0x80284009	Não foi possível criar um novo contexto porque existem demasiados contextos abertos.
TBS_E_TOO_MANY_RESOURCES 0x8028400A	Não foi possível criar um novo recurso virtual porque existem demasiados recursos virtuais abertos.
TBS_E_SERVICE_START_PENDING 0x8028400B	O serviço TBS foi iniciado mas ainda não está em execução.
TBS_E_PPI_NOT_SUPPORTED 0x8028400C	A interface de presença física não é suportada.
TBS_E_COMMAND_CANCELED 0x8028400D	O comando foi cancelado.
TBS_E_BUFFER_TOO_LARGE 0x8028400E	A memória intermédia de entrada ou saída é demasiado grande.
TBS_E_TPM_NOT_FOUND 0x8028400F	Não é possível localizar um Dispositivo de Segurança de TPM compatível neste computador.
TBS_E_SERVICE_DISABLED 0x80284010	O serviço TBS foi desativado.
TBS_E_NO_EVENT_LOG 0x80284011	Não está disponível nenhum registo de eventos TCG.
TBS_E_ACCESS_DENIED 0x80284012	O emissor não tem os direitos adequados para executar a operação pedida.
TBS_E_PROVISIONING_NOT_ALLOWED 0x80284013	A ação de aprovisionamento de TPM não é permitida pelos sinalizadores especificados. Para que o aprovisionamento seja efetuado com êxito, poderá ser necessária uma de várias ações. A ação da consola de gestão de TPM (tpm.msc) para preparar o TPM para utilização poderá ajudar. Para mais informações, consulte a documentação do método WMI Win32_Tpm 'Provision'. (As ações que poderão ser necessárias incluem importar o valor de Autorização de Proprietário de TPM para o sistema, chamar o método WMI Win32_Tpm para aprovisionar o TPM e especificar TRUE para 'ForceClear_Allowed' ou para 'PhysicalPresencePrompts_Allowed' (como indicado pelo valor devolvido nas Informações Adicionais), ou ativar o TPM no BIOS do sistema.)
TBS_E_PPI_FUNCTION_UNSUPPORTED 0x80284014	A Interface de Presença Física deste firmware não suporta o método pedido.

Constante/Valor	Descrição
TBS_E_OWNERAUTH_NOT_FOUND 0x80284015	O valor OwnerAuth de TPM pedido não foi encontrado.
TBS_E_PROVISIONING_INCOMPLETE 0x80284016	O aprovisionamento de TPM não foi concluído. Para mais informações sobre a conclusão do aprovisionamento, chame o método WMI Win32_Tpm para aprovisionar o TPM ('Provision') e consulte as informações devolvidas.
TPMAPI_E_INVALID_STATE 0x80290100	A memória intermédia de comandos não está no estado correto.
TPMAPI_E_NOT_ENOUGH_DATA 0x80290101	A memória intermédia de comandos não contém dados suficientes para satisfazer o pedido.
TPMAPI_E_TOO_MUCH_DATA 0x80290102	A memória intermédia de comandos não contém mais dados.
TPMAPI_E_INVALID_OUTPUT_POINTER 0x80290103	Um ou vários parâmetros de saída eram NULL ou inválidos.
TPMAPI_E_INVALID_PARAMETER 0x80290104	Um ou mais parâmetros de entrada são inválidos.
TPMAPI_E_OUT_OF_MEMORY 0x80290105	Não existe memória suficiente disponível para satisfazer o pedido.
TPMAPI_E_BUFFER_TOO_SMALL 0x80290106	A memória intermédia especificada era demasiado pequena.
TPMAPI_E_INTERNAL_ERROR 0x80290107	Foi detetado um erro interno.
TPMAPI_E_ACCESS_DENIED 0x80290108	O emissor não tem os direitos adequados para executar a operação pedida.
TPMAPI_E_AUTHORIZATION_FAILED 0x80290109	As informações de autorização especificadas são inválidas.
TPMAPI_E_INVALID_CONTEXT_HANDLE 0x8029010A	O identificador de contexto especificado não era válido.
TPMAPI_E_TBS_COMMUNICATION_ERROR 0x8029010B	Ocorreu um erro ao comunicar com o TBS.
TPMAPI_E_TPM_COMMAND_ERROR 0x8029010C	O TPM devolveu um resultado inesperado.

Constante/Valor	Descrição
TPMAPI_E_MESSAGE_TOO_LARGE 0x8029010D	A mensagem era demasiado grande para o esquema de codificação.
TPMAPI_E_INVALID_ENCODING 0x8029010E	A codificação do blob não foi reconhecida.
TPMAPI_E_INVALID_KEY_SIZE 0x8029010F	O tamanho da chave não é válido.
TPMAPI_E_ENCRYPTION_FAILED 0x80290110	Falha na operação de encriptação.
TPMAPI_E_INVALID_KEY_PARAMS 0x80290111	A estrutura dos parâmetros chave não era válida
TPMAPI_E_INVALID_MIGRATION_AUTHORIZATION_BLOB 0x80290112	Os dados fornecidos pedidos não parecem ser um blob de autorização de migração válido.
TPMAPI_E_INVALID_PCR_INDEX 0x80290113	O índice de PCR especificado era inválido
TPMAPI_E_INVALID_DELEGATE_BLOB 0x80290114	Os dados indicados não parecem ser um blob delegado válido.
TPMAPI_E_INVALID_CONTEXT_PARAMS 0x80290115	Um ou vários parâmetros de contexto especificados não são válidos.
TPMAPI_E_INVALID_KEY_BLOB 0x80290116	Os dados indicados não parecem ser um blob de chave válido
TPMAPI_E_INVALID_PCR_DATA 0x80290117	Os dados de PCR especificados eram inválidos.
TPMAPI_E_INVALID_OWNER_AUTH 0x80290118	O formato dos dados de autenticação do proprietário era inválido.
TPMAPI_E_FIPS_RNG_CHECK_FAILED 0x80290119	O número aleatório gerado não passou na verificação FIPS RNG.
TPMAPI_E_EMPTY_TCG_LOG 0x8029011A	O Registo de Eventos TCG não contém quaisquer dados.
TPMAPI_E_INVALID_TCG_LOG_ENTRY 0x8029011B	Uma entrada no Registo de Eventos TCG era inválida.

Constante/Valor	Descrição
TPMAPI_E_TCG_SEPARATOR_ABSENT 0x8029011C	Um Separador TCG não foi encontrado.
TPMAPI_E_TCG_INVALID_DIGEST_ENTRY 0x8029011D	Um valor de resumo numa entrada do Registo TCG não correspondeu aos dados com hash.
TPMAPI_E_POLICY_DENIES_OPERATION 0x8029011E	A operação pedida foi bloqueada pela política de TPM atual. Contacte o administrador de sistema para obter assistência.
TBSIMP_E_BUFFER_TOO_SMALL 0x80290200	A memória intermédia especificada era demasiado pequena.
TBSIMP_E_CLEANUP_FAILED 0x80290201	Não foi possível limpar o contexto.
TBSIMP_E_INVALID_CONTEXT_HANDLE 0x80290202	O identificador de contexto especificado é inválido.
TBSIMP_E_INVALID_CONTEXT_PARAM 0x80290203	Foi especificado um parâmetro de contexto inválido.
TBSIMP_E_TPM_ERROR 0x80290204	Ocorreu um erro ao comunicar com o TPM
TBSIMP_E_HASH_BAD_KEY 0x80290205	Não foi encontrada qualquer entrada com a chave especificada.
TBSIMP_E_DUPLICATE_VHANDLE 0x80290206	O identificador virtual especificado corresponde a um identificador virtual que já está a ser utilizado.
TBSIMP_E_INVALID_OUTPUT_POINTER 0x80290207	O apontador para a localização do identificador devolvida era NULL ou inválido
TBSIMP_E_INVALID_PARAMETER 0x80290208	Um dos parâmetros não é válido.
TBSIMP_E_RPC_INIT_FAILED 0x80290209	Não foi possível inicializar o subsistema de RPC.
TBSIMP_E_SCHEDULER_NOT_RUNNING 0x8029020A	O programador de TBS não está em execução.
TBSIMP_E_COMMAND_CANCELED 0x8029020B	O comando foi cancelado.

Constante/Valor	Descrição
TBSIMP_E_OUT_OF_MEMORY 0x8029020C	Não existe memória suficiente disponível para satisfazer o pedido
TBSIMP_E_LIST_NO_MORE_ITEMS 0x8029020D	A lista especificada está vazia ou a iteração alcançou o final da lista.
TBSIMP_E_LIST_NOT_FOUND 0x8029020E	O item especificado não foi encontrado na lista.
TBSIMP_E_NOT_ENOUGH_SPACE 0x8029020F	O TPM não tem espaço suficiente para carregar o recurso pedido.
TBSIMP_E_NOT_ENOUGH_TPM_CONTEXTS 0x80290210	Existem demasiados contextos de TPM em utilização.
TBSIMP_E_COMMAND_FAILED 0x80290211	Falha do comando de TPM.
TBSIMP_E_UNKNOWN_ORDINAL 0x80290212	O TBS não reconhece o ordinal especificado.
TBSIMP_E_RESOURCE_EXPIRED 0x80290213	O recurso pedido já não se encontra disponível.
TBSIMP_E_INVALID_RESOURCE 0x80290214	O tipo de recurso não é igual.
TBSIMP_E_NOTHING_TO_UNLOAD 0x80290215	Não é possível descarregar recursos.
TBSIMP_E_HASH_TABLE_FULL 0x80290216	Não podem ser adicionadas novas entradas na tabela hash.
TBSIMP_E_TOO_MANY_TBS_CONTEXTS 0x80290217	Não foi possível criar um novo contexto de TBS porque existem demasiados contextos abertos.
TBSIMP_E_TOO_MANY_RESOURCES 0x80290218	Não foi possível criar um novo recurso virtual porque existem demasiados recursos virtuais abertos.
TBSIMP_E_PPI_NOT_SUPPORTED 0x80290219	A interface de presença física não é suportada.
TBSIMP_E_TPM_INCOMPATIBLE 0x8029021A	O TBS não é compatível com a versão de TPM encontrada no sistema.

Constante/Valor	Descrição
TBSIMP_E_NO_EVENT_LOG 0x8029021B	Não está disponível nenhum registo de eventos TCG.
TPM_E_PPI_ACPI_FAILURE 0x80290300	Foi detetado um erro geral ao tentar adquirir a resposta do BIOS a um comando de Presença Física.
TPM_E_PPI_USER_ABORT 0x80290301	O utilizador não conseguiu confirmar o pedido de operação do TPM.
TPM_E_PPI_BIOS_FAILURE 0x80290302	A falha do BIOS impediu a execução com êxito da operação do TPM pedida (por ex.: pedido de operação do TPM inválido, erro de comunicação do BIOS com o TPM).
TPM_E_PPI_NOT_SUPPORTED 0x80290303	O BIOS não suporta a interface de presença física.
TPM_E_PPI_BLOCKED_IN_BIOS 0x80290304	O comando de Presença Física foi bloqueado pelas definições de BIOS atuais. O proprietário do sistema poderá conseguir reconfigurar as definições de BIOS para permitir o comando.
TPM_E_PCP_ERROR_MASK 0x80290400	Trata-se de uma máscara de erro para converter erros do Fornecedor Criptográfico da Plataforma em erros do Windows.
TPM_E_PCP_DEVICE_NOT_READY 0x80290401	O Dispositivo Criptográfico da Plataforma não está preparado neste momento. O dispositivo necessita de ser totalmente aprovisionado para estar operacional.
TPM_E_PCP_INVALID_HANDLE 0x80290402	O identificador fornecido ao Fornecedor Criptográfico da Plataforma é inválido.
TPM_E_PCP_INVALID_PARAMETER 0x80290403	Um parâmetro fornecido ao Fornecedor Criptográfico da Plataforma é inválido.
TPM_E_PCP_FLAG_NOT_SUPPORTED 0x80290404	Um sinalizador fornecido ao Fornecedor Criptográfico da Plataforma não é suportado.
TPM_E_PCP_NOT_SUPPORTED 0x80290405	A operação pedida não é suportada por este Fornecedor Criptográfico da Plataforma.
TPM_E_PCP_BUFFER_TOO_SMALL 0x80290406	A memória intermédia é demasiado pequena para conter todos os dados. Não foram escritas informações na memória intermédia.
TPM_E_PCP_INTERNAL_ERROR 0x80290407	Ocorreu um erro interno inesperado no Fornecedor Criptográfico da Plataforma.
TPM_E_PCP_AUTHENTICATION_FAILED 0x80290408	Falha na autorização para utilizar um objeto de fornecedor.

Constante/Valor	Descrição
TPM_E_PCP_AUTHENTICATION_IGNORED 0x80290409	O Dispositivo Criptográfico da Plataforma ignorou a autorização para o objeto de fornecedor, para mitigar um ataque de dicionário.
TPM_E_PCP_POLICY_NOT_FOUND 0x8029040A	A política referenciada não foi encontrada.
TPM_E_PCP_PROFILE_NOT_FOUND 0x8029040B	O perfil referenciado não foi encontrado.
TPM_E_PCP_VALIDATION_FAILED 0x8029040C	A validação não foi concluída com êxito.
PLA_E_DCS_NOT_FOUND 0x80300002	O Conjunto de Recoletores de Dados não foi encontrado.
PLA_E_DCS_IN_USE 0x803000AA	O Conjunto de Recoletores de Dados ou das respetivas dependências está em utilização.
PLA_E_TOO_MANY_FOLDERS 0x80300045	Não é possível iniciar o Conjunto de Recoletores de Dados porque existem demasiadas pastas.
PLA_E_NO_MIN_DISK 0x80300070	Não existe espaço livre suficiente em disco para iniciar o Conjunto de Recoletores de Dados.
PLA_E_DCS_ALREADY_EXISTS 0x803000B7	O Conjunto de Recoletores de Dados já existe.
PLA_S_PROPERTY_IGNORED 0x00300100	O valor da propriedade será ignorado.
PLA_E_PROPERTY_CONFLICT 0x80300101	Conflito de valores da propriedade.
PLA_E_DCS_SINGLETON_REQUIRED 0x80300102	A configuração atual deste Conjunto de Recoletores de Dados necessita que este contenha exatamente um Recoletor de Dados.
PLA_E_CREDENTIALS_REQUIRED 0x80300103	É necessária uma conta de utilizador para consolidar as propriedades atuais do Conjunto de Recoletores de Dados.
PLA_E_DCS_NOT_RUNNING 0x80300104	O Conjunto de Recoletores de Dados não está em execução.
PLA_E_CONFLICT_INCL_EXCL_API 0x80300105	Foi detetado um conflito na lista de APIs de inclusão/exclusão. Não especifique a mesma API simultaneamente na lista de inclusão e na lista de exclusões.

Constante/Valor	Descrição
PLA_E_NETWORK_EXE_NOT_VALID 0x80300106	O caminho executável que especificou refere-se a uma partilha de rede ou caminho UNC.
PLA_E_EXE_ALREADY_CONFIGURED 0x80300107	O caminho executável que especificou já está configurado para rastreio de APIs.
PLA_E_EXE_PATH_NOT_VALID 0x80300108	O caminho executável que especificou não existe. Verifique se o caminho especificado está correto.
PLA_E_DC_ALREADY_EXISTS 0x80300109	O Recoletor de Dados já existe.
PLA_E_DCS_START_WAIT_TIMEOUT 0x8030010A	A espera pela notificação de início do Conjunto de Recoletores de Dados excedeu o tempo limite.
PLA_E_DC_START_WAIT_TIMEOUT 0x8030010B	A espera pelo início do Recoletor de Dados excedeu o tempo limite.
PLA_E_REPORT_WAIT_TIMEOUT 0x8030010C	A espera pela conclusão da ferramenta de geração de relatórios excedeu o tempo limite.
PLA_E_NO_DUPLICATES 0x8030010D	Não são permitidos itens duplicados.
PLA_E_EXE_FULL_PATH_REQUIRED 0x8030010E	Quando especificar o executável que pretende rastrear, tem de especificar um caminho completo para o executável e não apenas um nome de ficheiro.
PLA_E_INVALID_SESSION_NAME 0x8030010F	O nome de sessão fornecido é inválido.
PLA_E_PLA_CHANNEL_NOT_ENABLED 0x80300110	O canal do Registo de Eventos Microsoft-Windows-Diagnosis-PLA/Operacional tem de estar ativado para executar esta operação.
PLA_E_TASKSCHED_CHANNEL_NOT_ENABLED 0x80300111	O canal do Microsoft-Windows-TaskScheduler tem de estar ativado para executar esta operação.
PLA_E_RULES_MANAGER_FAILED 0x80300112	Falha na execução do Gestor de Regras.
PLA_E_CABAPI_FAILURE 0x80300113	Ocorreu um erro ao tentar comprimir ou extrair os dados.
FVE_E_LOCKED_VOLUME 0x80310000	Esta unidade está bloqueada pela Encriptação de Unidade BitLocker. Tem de desbloquear esta unidade a partir do Painel de Controlo.

Constante/Valor	Descrição
FVE_E_NOT_ENCRYPTED 0x80310001	A unidade não está encriptada.
FVE_E_NO_TPM_BIOS 0x80310002	O BIOS não comunicou corretamente com o TPM. Contacte o fabricante do computador para obter as instruções de atualização do BIOS.
FVE_E_NO_MBR_METRIC 0x80310003	O BIOS não comunicou corretamente com o registo de arranque principal (MBR). Contacte o fabricante do computador para obter as instruções de atualização do BIOS.
FVE_E_NO_BOOTSECTOR_METRIC 0x80310004	Uma medição de TPM necessária está em falta. Se existir um CD ou DVD de arranque no computador, remova-o, reinicie o computador e ative novamente o BitLocker. Se o problema persistir, certifique-se de que o registo de arranque principal está atualizado.
FVE_E_NO_BOOTMGR_METRIC 0x80310005	O setor de arranque desta unidade não é compatível com a Encriptação de Unidade BitLocker. Utilize a ferramenta Bootrec.exe no Ambiente de Recuperação do Windows para atualizar ou reparar o gestor de arranque (BOOTMGR).
FVE_E_WRONG_BOOTMGR 0x80310006	O gestor de arranque deste sistema operativo não é compatível com a Encriptação de Unidade BitLocker. Utilize a ferramenta Bootrec.exe no Ambiente de Recuperação do Windows para atualizar ou reparar o gestor de arranque (BOOTMGR).
FVE_E_SECURE_KEY_REQUIRED 0x80310007	É necessário, pelo menos, um protetor de chave seguro para que esta operação seja efetuada.
FVE_E_NOT_ACTIVATED 0x80310008	A Encriptação de Unidade BitLocker não está ativada nesta unidade. Ative o BitLocker.
FVE_E_ACTION_NOT_ALLOWED 0x80310009	A Encriptação de Unidade BitLocker não consegue efetuar a ação pedida. Esta condição pode ocorrer quando são emitidos dois pedidos ao mesmo tempo. Aguarde alguns momentos e tente a operação novamente.
FVE_E_AD_SCHEMA_NOT_INSTALLED 0x8031000A	A floresta dos Serviços de Domínio do Active Directory não contém os atributos e as classes necessários para alojar informações de Encriptação de Unidade BitLocker ou do TPM. Contacte o administrador do domínio para verificar se quaisquer extensões de esquema do Active Directory para o BitLocker necessárias foram instaladas.
FVE_E_AD_INVALID_DATATYPE 0x8031000B	O tipo de dados obtido a partir do Active Directory não era esperado. As informações de recuperação do BitLocker podem estar em falta ou danificadas.
FVE_E_AD_INVALID_DATASIZE 0x8031000C	O tamanho dos dados obtidos a partir do Active Directory não era esperado. As informações de recuperação do BitLocker podem estar em falta ou danificadas.
FVE_E_AD_NO_VALUES 0x8031000D	O atributo lido a partir do Active Directory não contém quaisquer valores. As informações de recuperação do BitLocker podem estar em falta ou danificadas.
FVE_E_AD_ATTR_NOT_SET	O atributo não foi definido. O atributo não foi definido. Verifique se tem sessão iniciada com uma conta de domínio que tenha a

Constante/Valor	Descrição
0x8031000E	capacidade de escrever informações em objetos do Active Directory.
FVE_E_AD_GUID_NOT_FOUND 0x8031000F	Não foi possível encontrar o atributo especificado nos Serviços de Domínio do Active Directory. Contacte o administrador do domínio para verificar se quaisquer extensões de esquema do Active Directory para o BitLocker necessárias foram instaladas.
FVE_E_BAD_INFORMATION 0x80310010	Os metadados do BitLocker para a unidade encriptada não são válido. Pode tentar reparar a unidade para restaurar o acesso.
FVE_E_TOO_SMALL 0x80310011	Não é possível encriptar a unidade porque esta não tem espaço livre suficiente. Elimine quaisquer dados desnecessários na unidade para criar espaço livre adicional e tente novamente.
FVE_E_SYSTEM_VOLUME 0x80310012	Não é possível encriptar a unidade porque esta contém informações de arranque do sistema Crie uma partição separada para utilizar como a unidade de sistema que contém as informações de arranque e uma segunda partição para utilizar como unidade de sistema operativo e, em seguida, encripte a unidade do sistema operativo.
FVE_E_FAILED_WRONG_FS 0x80310013	Não é possível encriptar a unidade porque o sistema de ficheiros não é suportado.
FVE_E_BAD_PARTITION_SIZE 0x80310014	O sistema de ficheiros é maior do que o tamanho da partição existente na tabela de partições. Esta unidade pode estar danificada ou ter sido adulterada. Para a utilizar com o BitLocker, tem de reformatar a partição.
FVE_E_NOT_SUPPORTED 0x80310015	Não é possível encriptar esta unidade.
FVE_E_BAD_DATA 0x80310016	Os dados não são válidos.
FVE_E_VOLUME_NOT_BOUND 0x80310017	A unidade de dados especificada não está definida para desbloquear automaticamente no computador atual e não pode ser desbloqueada automaticamente.
FVE_E_TPM_NOT_OWNED 0x80310018	É necessário inicializar o TPM antes de poder utilizar a Encriptação de Unidade BitLocker.
FVE_E_NOT_DATA_VOLUME 0x80310019	Não é possível efetuar a operação tentada numa unidade do sistema operativo.
FVE_E_AD_INSUFFICIENT_BUFFER 0x8031001A	A memória intermédia fornecida a uma função é insuficiente para conter os dados devolvidos. Aumente o tamanho da memória intermédia antes de executar a função novamente.
FVE_E_CONV_READ 0x8031001B	Uma operação de leitura falhou ao converter a unidade. A unidade não foi convertida. Ative novamente o BitLocker.
FVE_E_CONV_WRITE	Uma operação de escrita falhou ao converter a unidade. A unidade não foi convertida. Ative novamente o BitLocker.

Constante/Valor	Descrição
0x8031001C	
FVE_E_KEY_REQUIRED 0x8031001D	Este volume necessita de um ou mais protetores de chave do BitLocker. Não é possível eliminar a última chave existente nesta unidade.
FVE_E_CLUSTERING_NOT_SUPPORTED 0x8031001E	A Encriptação de Unidade BitLocker não suporta configurações de cluster.
FVE_E_VOLUME_BOUND_ALREADY 0x8031001F	A unidade especificada já está configurada para ser automaticamente desbloqueada no computador atual.
FVE_E_OS_NOT_PROTECTED 0x80310020	A unidade do sistema operativo não está a ser protegida pela Encriptação de Unidade BitLocker.
FVE_E_PROTECTION_DISABLED 0x80310021	A Encriptação de Unidade BitLocker foi suspensa nesta unidade. Todos os protetores de chave BitLocker configurados para esta unidade estão efetivamente desativados e a unidade será desbloqueada automaticamente utilizando uma chave não encriptada.
FVE_E_RECOVERY_KEY_REQUIRED 0x80310022	A unidade que está a tentar bloquear não tem protetores de chave disponíveis para encriptação porque a proteção BitLocker está atualmente suspensa. Ative novamente o BitLocker para bloquear esta unidade.
FVE_E_FOREIGN_VOLUME 0x80310023	O BitLocker não pode utilizar o TPM para proteger uma unidade de dados. Só é possível utilizar a proteção TPM na unidade do sistema operativo.
FVE_E_OVERLAPPED_UPDATE 0x80310024	Não é possível atualizar os metadados do BitLocker relativos à unidade encriptada porque esta está bloqueada para atualização por outro processo. Repita este processo.
FVE_E_TPM_SRK_AUTH_NOT_ZERO 0x80310025	Os dados da autorização para o SRK (Storage Root Key) do TPM são diferentes de zero, pelo que são incompatíveis com o BitLocker. Inicialize o TPM antes de tentar utilizá-lo com o BitLocker.
FVE_E_FAILED_SECTOR_SIZE 0x80310026	O algoritmo de encriptação da unidade não pode ser utilizado neste tamanho de setores.
FVE_E_FAILED_AUTHENTICATION 0x80310027	Não é possível desbloquear a unidade com a chave fornecida. Confirme se forneceu a chave correta e tente novamente.
FVE_E_NOT_OS_VOLUME 0x80310028	A unidade especificada não é a unidade do sistema operativo.
FVE_E_AUTOUNLOCK_ENABLED 0x80310029	Não é possível desativar a Encriptação de Unidade BitLocker na unidade do sistema operativo até que a funcionalidade de desbloqueio automático tenha sido desativada para as unidades de dados fixas e amovíveis associadas a este computador.
FVE_E_WRONG_BOOTSECTOR	O setor de arranque da partição do sistema não efetua medições do TPM. Utilize a ferramenta Bootrec.exe no Ambiente de

Constante/Valor	Descrição
0x8031002A	Recuperação do Windows para atualizar ou reparar o setor de arranque.
FVE_E_WRONG_SYSTEM_FS 0x8031002B	As unidades do sistema operativo da Encriptação de Unidade BitLocker têm de estar formatadas com o sistema de ficheiros NTFS para serem encriptadas. Converta a unidade para NTFS e ative o BitLocker.
FVE_E_POLICY_PASSWORD_REQUIRED 0x8031002C	As definições de Política de Grupo necessitam que seja especificada uma palavra-passe antes da encriptação da unidade.
FVE_E_CANNOT_SET_FVEK_ENCRYPTED 0x8031002D	Não é possível definir o algoritmo de encriptação e a chave da unidade numa unidade previamente encriptada. Para encriptar esta unidade com a Encriptação de Unidade BitLocker, remova a encriptação anterior e, em seguida, ative o BitLocker.
FVE_E_CANNOT_ENCRYPT_NO_KEY 0x8031002E	A Encriptação de Unidade BitLocker não consegue encriptar a unidade especificada, porque não está disponível uma chave de encriptação. Adicione um protetor de chave para encriptar esta unidade.
FVE_E_BOOTABLE_CDDVD 0x80310030	A Encriptação de Unidade BitLocker detetou suportes multimédia de arranque (CD ou DVD) no computador. Remova o suporte multimédia e reinicie o computador antes de configurar o BitLocker.
FVE_E_PROTECTOR_EXISTS 0x80310031	Não é possível adicionar este protetor de chave. Só é permitido um protetor de chave deste tipo para esta unidade.
FVE_E_RELATIVE_PATH 0x80310032	O ficheiro de palavra-passe de recuperação não foi encontrado porque foi especificado um caminho relativo. As palavras-chave de recuperação têm de ser guardadas num caminho totalmente qualificado. As variáveis de ambiente configuradas no computador podem ser utilizadas no caminho.
FVE_E_PROTECTOR_NOT_FOUND 0x80310033	O protetor de chave especificado não foi encontrado na unidade. O protetor de chave especificado não foi encontrado na unidade. Tente outro protetor de chave.
FVE_E_INVALID_KEY_FORMAT 0x80310034	A chave de recuperação fornecida está danificada e não pode ser utilizada para aceder à unidade. Tem de ser utilizado um método de recuperação alternativo, tal como uma palavra-passe de recuperação, um agente de recuperação de dados ou uma versão de cópia de segurança da chave de recuperação para recuperar o acesso à unidade.
FVE_E_INVALID_PASSWORD_FORMAT 0x80310035	O formato da palavra-passe de recuperação fornecida é inválido. As palavras-passe de recuperação do BitLocker têm 48 dígitos. Verifique se a palavra-passe de recuperação tem e formato correto e tente novamente.
FVE_E_FIPS_RNG_CHECK_FAILED 0x80310036	Falha no teste de verificação do gerador de números aleatórios.
FVE_E_FIPS_PREVENTS_RECOVERY_PASSWORD 0x80310037	A definição de Política de Grupo que necessita da compatibilidade com FIPS impede a geração ou a utilização pela Encriptação de Unidade BitLocker de uma palavra-passe de recuperação local. Quando trabalha no modo compatível com FIPS, as opções de recuperação do BitLocker podem ser uma chave de recuperação

Constante/Valor	Descrição
	armazenada numa unidade USB ou a recuperação através de um agente de recuperação de dados.
FVE_E_FIPS_PREVENTS_EXTERNAL_KEY_EXPORT 0x80310038	A definição de Política de Grupo que necessita da compatibilidade com FIPS impede que a palavra-passe de recuperação seja guardada no Active Directory. Quando trabalha no modo compatível com FIPS, as opções de recuperação do BitLocker podem ser uma chave de recuperação armazenada numa unidade USB ou a recuperação através de um agente de recuperação de dados. Verifique a configuração das definições de Política de Grupo.
FVE_E_NOT_DECRYPTED 0x80310039	A unidade tem de ser totalmente desencriptada para concluir esta operação.
FVE_E_INVALID_PROTECTOR_TYPE 0x8031003A	Não é possível utilizar o protetor de chave especificado para esta operação.
FVE_E_NO_PROTECTORS_TO_TEST 0x8031003B	Não existem protetores de chave na unidade para efetuar o teste de hardware.
FVE_E_KEYFILE_NOT_FOUND 0x8031003C	Não é possível localizar a chave de arranque ou a palavra-passe de recuperação do BitLocker no dispositivo USB. Verifique se tem o dispositivo USB correto, se o dispositivo USB está introduzido numa porta USB ativa no computador, reinicie o computador e tente novamente. Se o problema persistir, contacte o fabricante do computador para obter instruções de atualização do BIOS.
FVE_E_KEYFILE_INVALID 0x8031003D	A chave de arranque ou o ficheiro de palavra-passe de recuperação do BitLocker está danificado ou é inválido. Verifique se tem a chave de arranque ou o ficheiro de palavra-passe de recuperação correto e tente novamente.
FVE_E_KEYFILE_NO_VMK 0x8031003E	Não é possível obter a chave de encriptação do BitLocker a partir da chave de arranque ou da palavra-passe de recuperação. Verifique se tem a chave de arranque ou a palavra-passe de recuperação correta e tente novamente.
FVE_E_TPM_DISABLED 0x8031003F	O TPM está desativado. O TPM tem de estar ativado, inicializado e tem de ter uma propriedade válida antes de poder ser utilizado com a Encriptação de Unidade BitLocker.
FVE_E_NOT_ALLOWED_IN_SAFE_MODE 0x80310040	Não é possível gerir a configuração BitLocker da unidade especificada porque o computador está atualmente a funcionar no Modo de Segurança. Enquanto estiver no Modo de Segurança, a Encriptação de Unidade BitLocker só poderá ser utilizada para fins de recuperação.
FVE_E_TPM_INVALID_PCR 0x80310041	O TPM não conseguiu desbloquear a unidade porque as informações de arranque do sistema foram alteradas ou porque não foi fornecido um PIN correto. Confirme se a unidade não foi adulterada e se as alterações às informações de arranque do sistema foram efetuadas por uma origem fidedigna. Depois de confirmar se é seguro aceder à unidade, utilize a consola de recuperação do BitLocker para desbloquear a unidade e, em seguida, suspenda e retome o BitLocker para atualizar as informações de arranque do sistema que o BitLocker associa a esta unidade.

Constante/Valor	Descrição
FVE_E_TPM_NO_VMK 0x80310042	Não é possível obter a chave de encriptação do BitLocker a partir do TPM.
FVE_E_PIN_INVALID 0x80310043	Não é possível obter a chave de encriptação do BitLocker a partir do TPM e do PIN.
FVE_E_AUTH_INVALID_APPLICATION 0x80310044	Uma aplicação de arranque foi alterada desde a ativação de Encriptação de Unidade BitLocker.
FVE_E_AUTH_INVALID_CONFIG 0x80310045	As definições do BCD (Boot Configuration Data) foram alteradas desde a ativação da Encriptação de Unidade BitLocker.
FVE_E_FIPS_DISABLE_PROTECTION_NOT_ALLOWED 0x80310046	A definição de Política de Grupo que necessita da compatibilidade com FIPS proíbe a utilização de chaves não encriptadas, o que impede que o BitLocker seja suspenso nesta unidade. Contacte o administrador do domínio para obter mais informações.
FVE_E_FS_NOT_EXTENDED 0x80310047	Esta unidade não pode ser encriptada com a Encriptação de Unidade BitLocker porque o sistema de ficheiros não abrange até ao final da unidade. Crie partições nesta unidade e tente novamente.
FVE_E_FIRMWARE_TYPE_NOT_SUPPORTED 0x80310048	Não é possível ativar a Encriptação de Unidade BitLocker na unidade do sistema operativo. Contacte o fabricante do computador para obter as instruções de atualização do BIOS.
FVE_E_NO_LICENSE 0x80310049	Esta versão do Windows não inclui a Encriptação de Unidade BitLocker. Para utilizar a Encriptação de Unidade BitLocker, atualize o sistema operativo.
FVE_E_NOT_ON_STACK 0x8031004A	Não é possível utilizar a Encriptação de Unidade BitLocker porque ficheiros de sistema críticos do BitLocker estão em falta ou danificados. Utilize a Reparação do Arranque do Windows para restaurar estes ficheiros no computador.
FVE_E_FS_MOUNTED 0x8031004B	Não é possível bloquear a unidade enquanto esta está a ser utilizada.
FVE_E_TOKEN_NOT_IMPERSONATED 0x8031004C	O token de acesso associado ao thread atual não é um token representado.
FVE_E_DRY_RUN_FAILED 0x8031004D	Não é possível obter a chave de encriptação do BitLocker. Verifique se o TPM está ativado e se a propriedade foi obtida. Se este computador não tiver um TPM, verifique se a unidade USB está introduzida e disponível.
FVE_E_REBOOT_REQUIRED 0x8031004E	Tem de reiniciar o computador antes de continuar com a Encriptação de Unidade BitLocker.
FVE_E_DEBUGGER_ENABLED 0x8031004F	Não é possível encriptar a unidade enquanto a depuração de arranque está ativada. Utilize a ferramenta de linha de comandos bcdedit para desativar a depuração de arranque.
FVE_E_RAW_ACCESS	Não foi executada nenhuma ação porque a Encriptação de Unidade BitLocker está no modo de acesso RAW.

Constante/Valor	Descrição
0x80310050	
FVE_E_RAW_BLOCKED 0x80310051	A Encriptação de Unidade BitLocker não consegue entrar no modo de acesso RAW para esta unidade porque a unidade está atualmente a ser utilizada.
FVE_E_BCD_APPLICATIONS_PATH_INCORRECT 0x80310052	O caminho especificado nos Dados de Configuração de Arranque (BCD) para uma aplicação de integridade protegida por Encriptação de Unidade BitLocker está incorreto. Verifique e corrija as definições de BCD e tente novamente.
FVE_E_NOT_ALLOWED_IN_VERSION 0x80310053	Só é possível utilizar a Encriptação de Unidade BitLocker para aprovisionamento limitado ou efeitos de recuperação quando o computador é utilizado em ambientes de pré-instalação ou recuperação.
FVE_E_NO_AUTOUNLOCK_MASTER_KEY 0x80310054	A chave mestre de desbloqueio automático não estava disponível na unidade do sistema operativo.
FVE_E_MOR_FAILED 0x80310055	O firmware do sistema não conseguiu ativar a limpeza da memória do sistema quando o computador foi reiniciado.
FVE_E_HIDDEN_VOLUME 0x80310056	Não é possível encriptar a unidade oculta.
FVE_E_TRANSIENT_STATE 0x80310057	As chaves de encriptação do BitLocker foram ignoradas porque a unidade estava num estado transitório.
FVE_E_PUBKEY_NOT_ALLOWED 0x80310058	Os protetores baseados em chaves públicas não são permitidos nesta unidade.
FVE_E_VOLUME_HANDLE_OPEN 0x80310059	A Encriptação de Unidade BitLocker já está a efetuar uma operação nesta unidade. Conclua todas as operações antes de continuar.
FVE_E_NO_FEATURE_LICENSE 0x8031005A	Esta versão do Windows não suporta esta funcionalidade da Encriptação de Unidade BitLocker. Para utilizar esta funcionalidade, atualize o sistema operativo.
FVE_E_INVALID_STARTUP_OPTIONS 0x8031005B	As definições de Política de Grupo relativas às opções de arranque do BitLocker estão em conflito e não podem ser aplicadas. Contacte o administrador de sistema para obter mais informações.
FVE_E_POLICY_RECOVERY_PASSWORD_NOT_ALLOWED 0x8031005C	As definições de Política de Grupo não permitem a criação de uma palavra-passe de recuperação.
FVE_E_POLICY_RECOVERY_PASSWORD_REQUIRED 0x8031005D	As definições de Política de Grupo exigem a criação de uma palavra-passe de recuperação.
FVE_E_POLICY_RECOVERY_KEY_NOT_ALLOWED 0x8031005E	As definições de Política de Grupo não permitem a criação de uma chave de recuperação.

Constante/Valor	Descrição
FVE_E_POLICY_RECOVERY_KEY_REQUIRED 0x8031005F	As definições de Política de Grupo exigem a criação de uma chave de recuperação.
FVE_E_POLICY_STARTUP_PIN_NOT_ALLOWED 0x80310060	As definições de Política de Grupo não permitem a utilização de um PIN durante o arranque. Selecione outra opção de arranque do BitLocker.
FVE_E_POLICY_STARTUP_PIN_REQUIRED 0x80310061	As definições de Política de Grupo exigem a utilização de um PIN durante o arranque. Selecione esta opção de arranque do BitLocker.
FVE_E_POLICY_STARTUP_KEY_NOT_ALLOWED 0x80310062	As definições de Política de Grupo não permitem a utilização de uma chave de arranque. Selecione outra opção de arranque do BitLocker.
FVE_E_POLICY_STARTUP_KEY_REQUIRED 0x80310063	As definições de Política de Grupo exigem a utilização de uma chave de arranque. Selecione esta opção de arranque do BitLocker.
FVE_E_POLICY_STARTUP_PIN_KEY_NOT_ALLOWED0x80310064	As definições de Política de Grupo não permitem a utilização de uma chave de arranque e PIN. Selecione outra opção de arranque do BitLocker.
FVE_E_POLICY_STARTUP_PIN_KEY_REQUIRED 0x80310065	As definições de Política de Grupo necessitam da utilização de uma chave de arranque e PIN. Selecione esta opção de arranque do BitLocker.
FVE_E_POLICY_STARTUP_TPM_NOT_ALLOWED 0x80310066	A política de grupo não permite a utilização de apenas TPM durante o arranque. Selecione outra opção de arranque do BitLocker.
FVE_E_POLICY_STARTUP_TPM_REQUIRED 0x80310067	As definições de Política de Grupo necessitam da utilização de apenas TPM durante o arranque. Selecione esta opção de arranque do BitLocker.
FVE_E_POLICY_INVALID_PIN_LENGTH 0x80310068	O PIN fornecido não satisfaz as necessidades de comprimento mínimo ou máximo.
FVE_E_KEY_PROTECTOR_NOT_SUPPORTED 0x80310069	O protetor de chave não é suportado pela versão da Encriptação de Unidade BitLocker existente atualmente na unidade. Atualize a unidade para adicionar o protetor de chave.
FVE_E_POLICY_PASSPHRASE_NOT_ALLOWED 0x8031006A	As definições de Política de Grupo não permitem a criação de uma palavra-passe.
FVE_E_POLICY_PASSPHRASE_REQUIRED 0x8031006B	As definições de Política de Grupo necessitam da criação de uma palavra-passe.
FVE_E_FIPS_PREVENTS_PASSPHRASE 0x8031006C	A definição de política de grupo que necessita da compatibilidade com FIPS impediu a geração ou a utilização da palavra-passe. Contacte o administrador do domínio para obter mais informações.
FVE_E_OS_VOLUME_PASSPHRASE_NOT_ALLOWED 0x8031006D	Não é possível adicionar uma palavra-passe à unidade do sistema operativo.

Constante/Valor	Descrição
FVE_E_INVALID_BITLOCKER_OID 0x8031006E	O identificador de objeto (OID) do BitLocker existente na unidade parece ser inválido ou estar danificado. Utilize manage-BDE para repor o OID nesta unidade.
FVE_E_VOLUME_TOO_SMALL 0x8031006F	A unidade é demasiado pequena para ser protegida utilizando a Encriptação de Unidade BitLocker.
FVE_E_DV_NOT_SUPPORTED_ON_FS 0x80310070	O tipo de unidade de deteção selecionada é incompatível com o sistema de ficheiros existente na unidade. As unidades de deteção BitLocker To Go têm de ser criadas em unidades formatadas com FAT.
FVE_E_DV_NOT_ALLOWED_BY_GP 0x80310071	O tipo de unidade de deteção selecionado não é permitido pelas definições de Política de Grupo do computador. Verifique se as definições de Política de Grupo permitem a criação de unidades de deteção para utilização com o BitLocker To Go.
FVE_E_POLICY_USER_CERTIFICATE_NOT_ALLOWED 0x80310072	As definições de Política de Grupo não permitem a utilização de certificados de utilizador, tais como smart cards, com a Encriptação de Unidade BitLocker.
FVE_E_POLICY_USER_CERTIFICATE_REQUIRED 0x80310073	As definições de Política de Grupo necessitam que tenha um certificado de utilizador válido, tal como um smart card, para utilização com a Encriptação de Unidade BitLocker.
FVE_E_POLICY_USER_CERT_MUST_BE_HW 0x80310074	As definições de Política de Grupo exigem a utilização de um protetor de chave baseado em smart card com Encriptação de Unidade BitLocker.
FVE_E_POLICY_USER_CONFIGURE_FDV_AUTOUNLOCK_NOT_ALLOWED 0x80310075	As definições de Política de Grupo não permitem que unidades de dados fixas protegidas pelo BitLocker sejam automaticamente desbloqueadas.
FVE_E_POLICY_USER_CONFIGURE_RDV_AUTOUNLOCK_NOT_ALLOWED 0x80310076	As definições de Política de Grupo não permitem que unidades de dados amovíveis protegidas pelo BitLocker sejam automaticamente desbloqueadas.
FVE_E_POLICY_USER_CONFIGURE_RDV_NOT_ALLOWED 0x80310077	As definições de Política de Grupo não permitem que configure a Encriptação de Unidade BitLocker em unidades de dados amovíveis.
FVE_E_POLICY_USER_ENABLE_RDV_NOT_ALLOWED 0x80310078	As definições de Política de Grupo não permitem que ative a Encriptação de Unidade BitLocker em unidades de dados amovíveis. Contacte o administrador de sistema se necessitar de ativar o BitLocker.
FVE_E_POLICY_USER_DISABLE_RDV_NOT_ALLOWED 0x80310079	As definições de Política de Grupo não permitem que desative a Encriptação de Unidade BitLocker em unidades de dados amovíveis. Contacte o administrador de sistema se necessitar de desativar o BitLocker.
FVE_E_POLICY_INVALID_PASSPHRASE_LENGTH 0x80310080	A sua palavra-passe não satisfaz as necessidades de comprimento mínimo. Por predefinição, as palavras-passe têm de ter um comprimento mínimo de 8 caracteres. Contacte o administrador de sistema para obter as necessidades de comprimento de palavras-passe da organização.

Constante/Valor	Descrição
FVE_E_POLICY_PASSPHRASE_TOO_SIMPLE 0x80310081	A palavra-passe não satisfaz as necessidades de complexidade definidas pelo administrador de sistema. Tente adicionar caracteres maiúsculos e minúsculos, números e símbolos
FVE_E_RECOVERY_PARTITION 0x80310082	Não é possível encriptar esta unidade porque esta está reservada para as Opções de Recuperação do Sistema do Windows.
FVE_E_POLICY_CONFLICT_FDV_RK_OFF_AUK_ON 0x80310083	Não é possível aplicar a Encriptação de Unidade BitLocker a esta unidade devido à existência de definições de Política de Grupo em conflito. Não é possível configurar o BitLocker para desbloquear automaticamente unidades de dados fixas quando as opções de recuperação do utilizador estão desativadas. Se pretender que as unidades de dados fixas protegidas pelo BitLocker sejam automaticamente desbloqueadas após a validação da chave, peça ao administrador de sistema para resolver o conflito das definições antes de ativar o BitLocker.
FVE_E_POLICY_CONFLICT_RDV_RK_OFF_AUK_ON 0x80310084	Não é possível aplicar a Encriptação de Unidade BitLocker a esta unidade devido à existência de definições de Política de Grupo em conflito. Não é possível configurar o BitLocker para desbloquear automaticamente unidades de dados amovíveis quando as opções de recuperação do utilizador estão desativadas. Se pretender que as unidades de dados amovíveis protegidas pelo BitLocker sejam automaticamente desbloqueadas após a validação da chave, peça ao administrador de sistema para resolver o conflito das definições antes de ativar o BitLocker.
FVE_E_NON_BITLOCKER_OID 0x80310085	O atributo EKU (Utilização de Chave Avançada) do certificado especificado não permite que este seja utilizado para a Encriptação de Unidade BitLocker. O BitLocker não necessita que o certificado tenha um atributo EKU, mas se existir um configurado, tem de ser definido para um OID (identificador de objeto) que corresponda ao OID configurado para o BitLocker.
FVE_E_POLICY_PROHIBITS_SELFSIGNED 0x80310086	Não é possível aplicar a Encriptação de Unidade BitLocker a esta unidade conforme atualmente configurada devido às definições de Política de Grupo. O certificado que forneceu para encriptação da unidade é autoassinado. As definições atuais de Política de Grupo não permitem a utilização de certificados autoassinados. Obtenha um novo certificado junto da autoridade de certificação antes de tentar ativar o BitLocker.
FVE_E_POLICY_CONFLICT_RO_AND_STARTUP_KEY_REQUIRED 0x80310087	Não é possível aplicar a Encriptação BitLocker a esta unidade devido à existência de definições de Política de Grupo em conflito. Quando o acesso de escrita a unidade não protegidas pelo BitLocker é negado, não é possível exigir a utilização de uma chave de arranque USB. Peça ao administrador de sistema para resolver os conflitos de política antes de tentar ativar o BitLocker.
FVE_E_CONV_RECOVERY_FAILED 0x80310088	Não é possível aplicar a Encriptação de Unidade BitLocker a esta unidade porque existem definições de Política de Grupo em conflito relativamente às opções de recuperação em unidades do sistema operativo. O armazenamento de informações de recuperação nos Serviços de Domínio do Active Directory não pode ser exigido quando a geração de palavras-passe de recuperação não é permitida. Peça ao administrador de sistema para resolver os conflitos de política antes de tentar ativar o BitLocker.
FVE_E_VIRTUALIZED_SPACE_TOO_BIG 0x80310089	O tamanho de virtualização pedido é demasiado grande.

Constante/Valor	Descrição
FVE_E_POLICY_CONFLICT_OSV_RP_OFF_ADB_ON 0x80310090	Não é possível aplicar a Encriptação de Unidade BitLocker a esta unidade porque existem definições de Política de Grupo em conflito relativamente às opções de recuperação em unidades do sistema operativo. O armazenamento de informações de recuperação nos Serviços de Domínio do Active Directory não pode ser exigido quando a geração de palavras-passe de recuperação não é permitida. Peça ao administrador de sistema para resolver os conflitos de política antes de tentar ativar o BitLocker.
FVE_E_POLICY_CONFLICT_FDV_RP_OFF_ADB_ON 0x80310091	A Encriptação de Unidade BitLocker não pode ser aplicada a esta unidade, uma vez que existem definições da Política de grupo em conflito relativamente às opções de recuperação em unidades de dados fixas. O armazenamento de informações de recuperação nos Serviços de Domínio do Active Directory não pode ser exigido quando a geração de palavras-passe de recuperação não é permitida. Peça ao administrador de sistema para resolver os conflitos de política antes de tentar ativar o BitLocker.
FVE_E_POLICY_CONFLICT_RDV_RP_OFF_ADB_ON 0x80310092	Não é possível aplicar a Encriptação de Unidade BitLocker a esta unidade porque existem definições de Política de Grupo em conflito relativamente às opções de recuperação em unidades de dados amovíveis. O armazenamento de informações de recuperação nos Serviços de Domínio do Active Directory não pode ser exigido quando a geração de palavras-passe de recuperação não é permitida. Peça ao administrador de sistema para resolver os conflitos de política antes de tentar ativar o BitLocker.
FVE_E_NON_BITLOCKER_KU 0x80310093	O atributo KU (Key Usage) do certificado especificado não permite que este seja utilizado para a Encriptação de Unidade BitLocker. O BitLocker não necessita que um certificado tenha um atributo KU, mas se existir um configurado, tem de ser definido para Cifragem de Chaves ou Correspondência de Chaves.
FVE_E_PRIVATEKEY_AUTH_FAILED 0x80310094	Não foi possível autorizar a chave privada associada ao certificado especificado. A autorização da chave privada não foi fornecida ou a autorização fornecida era inválida.
FVE_E_REMOVAL_OF_DRA_FAILED 0x80310095	A remoção do certificado do agente de recuperação de dados tem de ser efetuada utilizando o snap-in Certificados.
FVE_E_OPERATION_NOT_SUPPORTED_ON_VISTA_VOLUME 0x80310096	Esta unidade foi encriptada utilizando a versão da Encriptação de Unidade BitLocker incluída com o Windows Vista e o Windows Server 2008, que não suporta identificadores organizacionais. Para especificar identificadores organizacionais para esta unidade, atualize a encriptação da unidade para a versão mais recente utilizando o comando "manage-bde -upgrade".
FVE_E_CANT_LOCK_AUTOUNLOCK_ENABLED_VOLUME 0x80310097	Não é possível bloquear a unidade, porque esta é desbloqueada automaticamente neste computador. Remova o protetor de desbloqueio automático para bloquear esta unidade.
FVE_E_FIPS_HASH_KDF_NOT_ALLOWED 0x80310098	A Função de Derivação de Chaves SP800-56A para smart cards ECC predefinida do BitLocker não é suportada pelo seu smart card. A definição de Política de Grupo que exige a conformidade com o FIPS impede que o BitLocker utilize qualquer outra função de derivação de chaves para encriptação. Tem de utilizar um smart card compatível com FIPS em ambientes FIPS restritos.
FVE_E_ENH_PIN_INVALID 0x80310099	Não foi possível obter a chave de encriptação do BitLocker a partir do TPM e do PIN avançado. Experimente utilizar um PIN que contenha apenas numerais.

Constante/Valor	Descrição
FVE_E_INVALID_PIN_CHARS 0x8031009A	O PIN do TPM pedido contém caracteres inválidos.
FVE_E_INVALID_DATUM_TYPE 0x8031009B	As informações de gestão armazenadas na unidade contêm um tipo desconhecido. Se estiver a utilizar uma versão antiga do Windows, tente aceder à unidade a partir da versão mais recente.
FVE_E_EFI_ONLY 0x8031009C	A funcionalidade só é suportada em sistemas EFI.
FVE_E_MULTIPLE_NKP_CERTS 0x8031009D	Foi encontrado mais de um certificado de Protetor de Chave de Rede no sistema.
FVE_E_REMOVAL_OF_NKP_FAILED 0x8031009E	O certificado de Protetor de Chave de Rede tem de ser removido utilizando o snap-in Certificados.
FVE_E_INVALID_NKP_CERT 0x8031009F	Foi encontrado um certificado inválido no arquivo de certificados de Protetor de Chave de Rede.
FVE_E_NO_EXISTING_PIN 0x803100A0	Esta unidade não está protegida com PIN.
FVE_E_PROTECTOR_CHANGE_PIN_MISMATCH 0x803100A1	Introduza o PIN atual correto.
FVE_E_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED 0x803100A2	Tem de ter sessão iniciada com a conta de administrador para alterar o PIN ou a palavra-passe. Clique na hiperligação para repor o PIN ou a palavra-passe como administrador.
FVE_E_PROTECTOR_CHANGE_MAX_PIN_CHANGE_ATTEMPTS_REACHED 0x803100A3	O BitLocker desativou alterações de PIN e palavra-passe na sequência de demasiados pedidos falhados. Clique na hiperligação para repor o PIN ou a palavra-passe como administrador.
FVE_E_POLICY_PASSPHRASE_REQUIRES_ASCII 0x803100A4	O administrador de sistema exige que as palavras-passe contenham apenas caracteres ASCII imprimíveis. Isto inclui letras não acentuadas (A-Z, a-z), números (0-9), espaço, sinais aritméticos, pontuação comum, separadores e os símbolos seguintes: # $ & @ ^ _ ~ .
FVE_E_FULL_ENCRYPTION_NOT_ALLOWED_ON_TP_STORAGE 0x803100A5	A Encriptação de Unidade BitLocker só suporta a encriptação Apenas do Espaço Utilizado em armazenamento com aprovisionamento dinâmico.
FVE_E_WIPE_NOT_ALLOWED_ON_TP_STORAGE 0x803100A6	A Encriptação de Unidade BitLocker não suporta a limpeza do espaço livre em armazenamento com aprovisionamento dinâmico.
FVE_E_KEY_LENGTH_NOT_SUPPORTED_BY_EDRIVE 0x803100A7	O comprimento de chave de autenticação necessário não é suportado pela unidade.
FVE_E_NO_EXISTING_PASSPHRASE	A unidade não está protegida com palavra-passe.

Constante/Valor	Descrição
0x803100A8	
FVE_E_PROTECTOR_CHANGE_PASSPHRASE_MISMATCH 0x803100A9	Introduza a palavra-passe atual correta.
FVE_E_PASSPHRASE_TOO_LONG 0x803100AA	A palavra-passe não pode exceder 256 caracteres.
FVE_E_NO_PASSPHRASE_WITH_TPM 0x803100AB	Não é possível adicionar um protetor de chave de palavra-passe, porque existe um protetor de TPM na unidade.
FVE_E_NO_TPM_WITH_PASSPHRASE 0x803100AC	Não é possível adicionar um protetor de chave de TPM, porque existe um protetor de palavra-passe na unidade.
FVE_E_NOT_ALLOWED_ON_CSV_STACK 0x803100AD	Este comando só pode ser efetuado a partir do nó coordenador do volume CSV especificado.
FVE_E_NOT_ALLOWED_ON_CLUSTER 0x803100AE	Não é possível efetuar este comando num volume quando este faz parte de um cluster.
FVE_E_EDRIVE_NO_FAILOVER_TO_SW 0x803100AF	O BitLocker não reverteu para a utilização de encriptação de software BitLocker devido à configuração de política de grupo.
FVE_E_EDRIVE_BAND_IN_USE 0x803100B0	A unidade não pode ser gerida pelo BitLocker, porque a funcionalidade de encriptação de hardware da unidade já está a ser utilizada.
FVE_E_EDRIVE_DISALLOWED_BY_GP 0x803100B1	As definições de Política de Grupo não permitem utilizar encriptação baseada em hardware.
FVE_E_EDRIVE_INCOMPATIBLE_VOLUME 0x803100B2	A unidade especificada não suporta encriptação baseada em hardware.
FVE_E_NOT_ALLOWED_TO_UPGRADE_WHILE_CONVERTING 0x803100B3	Não é possível atualizar o BitLocker durante a encriptação ou desencriptação de um disco.
FVE_E_EDRIVE_DV_NOT_SUPPORTED 0x803100B4	Não são suportados Volumes de Deteção para volumes que utilizem encriptação de hardware.
FVE_E_NO_PREBOOT_KEYBOARD_DETECTED 0x803100B5	Não foi detetado qualquer teclado de pré-arranque. O utilizador poderá não conseguir introduzir os dados necessários para desbloquear o volume.
FVE_E_NO_PREBOOT_KEYBOARD_OR_WINRE_DETECTED 0x803100B6	Não foi detetado qualquer teclado de pré-arranque ou Ambiente de Recuperação do Windows. O utilizador poderá não conseguir introduzir os dados necessários para desbloquear o volume.
FVE_E_POLICY_REQUIRES_STARTUP_PIN_ON_TOUCH_DEVICE	As definições de Política de Grupo exigem a criação de um PIN de arranque, mas este dispositivo não tem nenhum teclado de pré-

Constante/Valor	Descrição
0x803100B7	arranque disponível. O utilizador poderá não conseguir introduzir os dados necessários para desbloquear o volume.
FVE_E_POLICY_REQUIRES_RECOVERY_PASSWORD_ON_TOUCH_DEVICE 0x803100B8	As definições de Política de Grupo exigem a criação de uma palavra-passe de recuperação, mas este dispositivo não tem um teclado de pré-arranque nem o Ambiente de Recuperação do Windows disponível. O utilizador poderá não conseguir introduzir os dados necessários para desbloquear o volume.
FVE_E_WIPE_CANCEL_NOT_APPLICABLE 0x803100B9	A limpeza do espaço livre não está a ser efetuada neste momento.
FVE_E_SECUREBOOT_DISABLED 0x803100BA	O BitLocker não pode utilizar o Arranque Seguro para integridade da plataforma, porque o Arranque Seguro foi desativado.
FVE_E_SECUREBOOT_CONFIGURATION_INVALID 0x803100BB	O BitLocker não pode utilizar o Arranque Seguro para integridade da plataforma, porque a configuração de Arranque Seguro não preenche os requisitos do BitLocker.
FVE_E_EDRIVE_DRY_RUN_FAILED 0x803100BC	O computador não suporta encriptação BitLocker baseada em hardware. Contacte o fabricante do computador para obter atualizações de firmware.
FVE_E_SHADOW_COPY_PRESENT 0x803100BD	Não é possível ativar o BitLocker no volume, porque este contém uma Cópia Sombra de Volumes. Remova todas as Cópias Sombra de Volumes antes de encriptar o volume.
FVE_E_POLICY_INVALID_ENHANCED_BCD_SETTINGS 0x803100BE	Não é possível aplicar a Encriptação de Unidade BitLocker a esta unidade, porque a definição de Política de Grupo para Dados de Configuração de Arranque Avançada contém dados inválidos. Peça ao administrador de sistema que resolva esta configuração inválida antes de tentar ativar o BitLocker.
FVE_E_EDRIVE_INCOMPATIBLE_FIRMWARE 0x803100BF	O firmware do PC não é capaz de suportar a encriptação de hardware.
FVE_E_PROTECTOR_CHANGE_MAX_PASSPHRASE_CHANGE_ATTEMPTS_REACHED 0x803100C0	O BitLocker desativou alterações de palavra-passe na sequência de demasiados pedidos falhados. Clique na hiperligação para repor a palavra-passe como administrador.
FVE_E_PASSPHRASE_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED 0x803100C1	Tem de ter sessão iniciada com a conta de administrador para alterar a palavra-passe. Clique na hiperligação para repor a palavra-passe como administrador.
FVE_E_LIVEID_ACCOUNT_SUSPENDED 0x803100C2	O BitLocker não consegue guardar a palavra-passe de recuperação, porque a conta Microsoft especificada está Suspensa.
FVE_E_LIVEID_ACCOUNT_BLOCKED 0x803100C3	O BitLocker não consegue guardar a palavra-passe de recuperação, porque a conta Microsoft especificada está Bloqueada.
FVE_E_NOT_PROVISIONED_ON_ALL_VOLUMES 0x803100C4	Este PC não está aprovisionado para suportar a encriptação do dispositivo. Ative o BitLocker em todos os volumes para estar em conformidade com a política de encriptação do dispositivo.

Constante/Valor	Descrição
FVE_E_DE_FIXED_DATA_NOT_SUPPORTED 0x803100C5	Este PC não pode suportar a encriptação do dispositivo, porque os volumes de dados fixos não encriptados estão presentes.
FVE_E_DE_HARDWARE_NOT_COMPLIANT 0x803100C6	Este PC não cumpre os requisitos de hardware para suportar a encriptação do dispositivo.
FVE_E_DE_WINRE_NOT_CONFIGURED 0x803100C7	Este PC não pode suportar a encriptação do dispositivo, porque o WinRE não está configurado corretamente.
FVE_E_DE_PROTECTION_SUSPENDED 0x803100C8	A proteção está ativada no volume, mas foi suspensa. É provável que esta situação tenha ocorrido por ter sido aplicada uma atualização ao sistema. Volte a tentar depois de reiniciar.
FVE_E_DE_OS_VOLUME_NOT_PROTECTED 0x803100C9	Este PC não está aprovisionado para suportar a encriptação do dispositivo.
FVE_E_DE_DEVICE_LOCKEDOUT 0x803100CA	O Bloqueio do Dispositivo foi acionado devido a demasiadas tentativas de palavras-passe incorretas.
FVE_E_DE_PROTECTION_NOT_YET_ENABLED 0x803100CB	A proteção não foi ativada no volume. A ativação da proteção necessita de uma conta ligada. Se já tiver uma conta ligada e estiver a visualizar este erro, consulte o registo de eventos para obter mais informações.
FVE_E_INVALID_PIN_CHARS_DETAILED 0x803100CC	O PIN só pode conter números entre 0 e 9.
FVE_E_DEVICE_LOCKOUT_COUNTER_UNAVAILABLE 0x803100CD	O BitLocker não consegue utilizar proteção de repetição de hardware, porque o PC não tem nenhum contador disponível.
FVE_E_DEVICELOCKOUT_COUNTER_MISMATCH 0x803100CE	Falha na validação do estado de bloqueio de dispositivo devido a um erro de correspondência de contador.
FVE_E_BUFFER_TOO_LARGE 0x803100CF	A memória intermédia de entrada é demasiado grande.

Glossário

Ativar - A ativação ocorre quando o computador tiver sido registado no Dell Enterprise Server/VE e tiver recebido, pelo menos, um conjunto inicial de políticas.

Active Directory (AD) - Um serviço de directório criado pela Microsoft para as redes de domínio Windows.

Advanced Authentication - O produto Advanced Authentication fornece opções de impressão digital, smart card e leitor de smart card sem contacto totalmente integradas. O Advanced Authentication ajuda a gerir estes múltiplos métodos de autenticação de hardware, suporta o início de sessão com unidades de encriptação automática, SSO e gere as credenciais e palavras-passe do utilizador. Adicionalmente, o Advanced Authentication pode ser utilizado para aceder não apenas a PCs, mas também a qualquer Web site, SaaS ou aplicação. Uma vez que os utilizadores inscrevem as suas credenciais, o Advanced Authentication permite a utilização dessas credenciais para iniciar sessão no dispositivo e realizar a substituição da palavra-passe.

Advanced Threat Prevention - O produto Advanced Threat Prevention é uma proteção antivírus de última geração que utiliza ciência algorítmica e aprendizagem automática para identificar, classificar e evitar que as ameaças virtuais, conhecidas e desconhecidas, sejam executadas ou danifiquem os pontos finais. 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.

Application Data Encryption - O Application Data Encryption encripta qualquer ficheiro gravado por uma aplicação protegida, utilizando uma substituição de categoria 2. Isto significa que qualquer diretório que tenha uma proteção de categoria 2 ou superior, ou qualquer localização que tenha extensões específicas protegidas com categoria 2 ou superior, fará com que a ADE não encripte esses ficheiros.

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.

Credenciais em cache - As credenciais em cache são credenciais adicionadas à base de dados da PBA quando um utilizador é autenticado com êxito no Active Directory. Estas informações sobre o utilizador são mantidas para que o utilizador possa iniciar sessão quando não tem ligação ao Active Directory (por exemplo, quando leva o portátil para casa).

Encriptação comum – A chave Comum torna os ficheiros encriptados acessíveis a todos os utilizadores geridos no dispositivo onde foram criados.

Desativar - A desativação ocorre quando a gestão SED é definida para DESLIGADA na Consola de Gestão Remota. Após a desativação do computador, a base de dados da PBA é eliminada e deixa de existir registo dos utilizadores em cache.

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

Código de acesso EMS - Este serviço do Dell Enterprise Server/VE permite a recuperação de dispositivos protegidos pelo External Media Shield, caso o utilizador se esqueça da palavra-passe e não consiga iniciar a sessão. Concluir este processo permite ao utilizador repor a palavra-passe definida no suporte de dados amovível ou no dispositivo de armazenamento externo.

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.

Ponto final - Um computador portátil ou dispositivo de hardware móvel gerido pelo Dell Enterprise Server/VE.

Chaves de encriptação - Na maioria dos casos, o Encryption Client utiliza a chave de Utilizador em conjunto com duas chaves de encriptação adicionais. No entanto, existem exceções: Todas as políticas de SDE e a política de Credenciais Seguras do Windows utilizam a chave de SDE. A política de Encriptar ficheiro de paginação do Windows e a política de Ficheiro de hibernação seguro do Windows utilizam a sua própria chave, a General Purpose Key (GPK). A chave Comum torna os ficheiros acessíveis a todos os utilizadores geridos no dispositivo em que foram criados. A chave de Utilizador torna os ficheiros acessíveis apenas ao utilizador que os criou, e apenas no dispositivo em que foram criados. A chave de Roaming de utilizador torna os ficheiros acessíveis apenas ao utilizador que os criou, em qualquer dispositivo Windows (ou Mac) protegido.

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, como se segue: - Um varrimento de encriptação irá ocorrer 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 Estação de trabalho de análise na Política de início de sessão está ativada, as pastas especificadas para a encriptação serão 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 (como vs. utilizador), acionará um varrimento. Adicionalmente, a alternância entre a encriptação ativada e desativada irá acionar um varrimento de encriptação.

Palavra-Passe monouso (OTP) - Uma palavra-passe monouso é uma palavra-passe que apenas pode ser utilizada uma vez e que é válida por um período de tempo limitado. A OTP requer que o TPM esteja presente, ativado e tenha proprietário. Para ativar a palavra-passe monouso (OTP), um dispositivo móvel é emparelhado com o computador que está a utilizar a Consola de segurança e a aplicação Security Tools Mobile. A aplicação Security Tools Mobile gera a palavra-passe no dispositivo móvel que é utilizado para iniciar sessão no computador no ecrã de início de sessão do Windows. Com base na politica, a funcionalidade OTP pode ser utilizada para recuperar o acesso ao computador se uma palavra-passe expirou ou foi esquecida, se a OTP não foi utilizada para iniciar sessão no computador. A funcionalidade OTP pode ser utilizada para autenticação ou recuperação, mas não para ambas. A segurança da OTP excede a de outros métodos de autenticação, uma vez que a palavra-passe gerada apenas pode ser utilizada uma vez e expira num curto período de tempo.

Autenticação de pré-arranque (PBA) - A Autenticação de pré-arranque funciona como uma extensão do BIOS ou do firmware de arranque e garante um ambiente seguro, à prova de adulteração e exterior ao sistema operativo como camada de autenticação fidedigna. A PBA impede a leitura de quaisquer informações a partir do disco rígido, como o sistema operativo, até que o utilizador confirme ter as credenciais corretas.

Controlo de script - O Controlo de script protege os dispositivos bloqueando a execução de scripts maliciosos.

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. A Gestão de SED assegura que será capaz de 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 nome de utilizador ou palavra-passe que possa ser fisicamente utilizada. É atribuído à conta um valor UCID exclusivo na Consola de Gestão Remota do Dell Enterprise Server/VE.

System Data Encryption (SDE) - A SDE foi concebida para encriptar o sistema operativo e ficheiros de programas. Para concretizar este objetivo, é necessário que a SDE consiga abrir a respetiva chave durante o arranque do sistema operativo. O seu objetivo é impedir alterações ou ataques offline ao sistema operativo por um atacante. A SDE não se destina à encriptação de dados do utilizador. A encriptação de chave Comum e de Utilizador destina-se a dados confidenciais do utilizador, uma vez que estes requerem uma palavra-passe de utilizador para desbloquear as chaves de encriptação. As políticas de SDE não encriptam os ficheiros de que o sistema operativo

necessita para iniciar o processo de arranque. As políticas de SDE não requerem uma autenticação de pré-arranque, nem interferem, de modo algum, com o Registo de Arranque Principal. Quando o computador arranca, os ficheiros encriptados estão disponíveis antes de qualquer utilizador iniciar sessão (para ativar as ferramentas de cópia de segurança e recuperação, SMS e gestão de patches). Ao desativar a encriptação SDE, é iniciada a desencriptação automática de todos os diretórios e ficheiros encriptados pela SDE para os utilizadores aplicáveis, independentemente de outras políticas de SDE, tais como as Regras de encriptação SDE.

TPM (Trusted Platform Module) – O TPM é um chip de segurança com três funções principais: armazenamento seguro, medição e atestados. O cliente Encryption utiliza o TPM para a sua função de armazenamento seguro. O TPM pode também fornecer contentores encriptados para o cofre do software. O TPM é ainda necessário para utilização com o BitLocker Manager e a funcionalidade de Palavra-passe monouso.

Encriptação de utilizador – A chave de Utilizador torna os ficheiros acessíveis apenas ao utilizador que os criou, e apenas no dispositivo onde foram criados. Quando executar o Dell Server Encryption, a Encriptação de utilizador é convertida para Encriptação comum. É aberta uma exceção aos dispositivos de suporte multimédia externos; ao serem inseridos num servidor que tenha o Encryption instalado, os ficheiros são encriptados com a chave de Roaming de utilizador.