

Dell Data Security

Guia de integração do EnCase



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

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

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

© 2012-2018 Dell Inc. Todos os direitos reservados. Dell, EMC e outras marcas comerciais são marcas comerciais da Dell Inc. ou suas subsidiárias. Todas as outras marcas comerciais são marcas comerciais de seus respectivos proprietários.

Marcas registradas e marcas comerciais usadas no conjunto de documentos do Dell Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise e Data Guardian: Dell™ e o logotipo da Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® e KACE™ são marcas comerciais da Dell Inc. Cylance®, CylancePROTECT e o logotipo da Cylance são marcas comerciais ou marcas registradas da Cylance, Inc. nos Estados Unidos e em outros países. McAfee® e o logotipo da McAfee são marcas comerciais ou marcas registradas da McAfee, Inc. nos Estados Unidos e em outros países. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® e Xeon® são marcas registradas da Intel Corporation nos Estados Unidos e em outros países. Adobe®, Acrobat®, e Flash® são marcas registradas da Adobe Systems Incorporated. Authen Tec® e Eikon® são marcas registradas da Authen Tec. AMD® é marca registrada da Advanced Micro Devices, Inc. Microsoft®, Windows® and Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, e Visual C++® são marcas comerciais ou marcas registradas da Microsoft Corporation nos Estados Unidos e/ou em outros países. VMware® é marca registrada ou marca comercial da VMware, Inc. nos Estados Unidos ou em outros países. Box® é marca comercial registrada da Box. DropboxSM é marca de serviço da Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® e Google™ Play são marcas comerciais ou marcas registradas da Google Inc. nos Estados Unidos e em outros países. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari®, e Siri® são marcas de serviço, marcas comerciais ou marcas registradas da Apple, Inc. nos Estados Unidos e/ou em outros países. GO ID®, RSA®, e SecurID® são marcas registradas da Dell EMC. EnCase™ e Guidance Software® são marcas comerciais ou marcas registradas da Guidance Software. Entrust® é marca registrada da Entrust®, Inc. nos Estados Unidos e em outros países. InstallShield® é marca registrada da Flexera Software nos Estados Unidos, China, Comunidade Europeia, Hong Kong, Japão, Taiwan, e Reino Unido. Micron® e RealSSD® são marcas registradas da Micron Technology, Inc. nos Estados Unidos e em outros países. Mozilla® Firefox® é marca registrada da Mozilla Foundation nos Estados Unidos e/ou em outros países. iOS® é marca comercial ou marca registrada da Cisco Systems, Inc. nos Estados Unidos e em determinados países e é usada sob licença. Oracle® e Java® são marcas registradas da Oracle e/ou seus afiliados. Outros nomes podem ser marcas comerciais de seus respectivos proprietários. SAMSUNG™ é marca comercial da SAMSUNG nos Estados Unidos ou em outros países. Seagate® é marca registrada da Seagate Technology LLC nos Estados Unidos e/ou em outros países. Travelstar® é marca registrada da HGST, Inc. nos Estados Unidos e em outros países. UNIX® é marca registrada da The Open Group. VALIDITY™ é marca comercial da Validity Sensors, Inc. nos Estados Unidos e em outros países. VeriSign® e outras marcas relacionadas são marcas comerciais ou marcas registradas da VeriSign, Inc. ou de suas afiliadas ou subsidiárias nos Estados Unidos e em outros países e licenciadas para a Symantec Corporation. KVM on IP® é marca comercial da Video Products. Yahoo!® é marca comercial da Yahoo! Inc. Este produto usa partes do programa 7-Zip. O código-fonte pode ser encontrado em 7-zip.org. O licenciamento é feito sob a licença GNU LGPL + restrições unRAR (7-zip.org/license.txt).

Guia de integração do EnCase

2018 - 03

Rev. A01

1 Introdução.....	4
Entre em contato com o Dell ProSupport.....	4
2 Integrar ao EnCase.....	5
Habilitar o API do EnCase.....	5
Instalar o adaptador de integração do EnCase.....	5
3 Usar Dell Data Security com EnCase.....	6
4 Usar EnCase com Dell Data Security.....	8
CEGetBundle.....	8



Introdução

O Dell Data Security se integra aos produtos forenses digitais EnCase v6.15 da Guidance Software, Inc. para suportar investigações on-line de arquivos criptografados pela Dell. Com essa integração, os investigadores forenses podem ver, exportar ou pesquisar dados protegidos pela Dell. Com as devidas credenciais de Administrador forense, todos os dados protegidos pela Dell, independentemente das chaves usadas para criptografá-los, são decodificados e apresentados ao investigador sem interação adicional. O Armazenamento seguro do EnCase salva e armazena credenciais de Administrador forense com o caso, eliminando a necessidade de digitá-las novamente.

A integração forense do EnCase v6.15 (32 bits) suporta:

- Dell Data Security Encryption Enterprise para Windows v7.0.x ou posterior
- Dell Security Management Server v7.0.1 ou posterior

ⓘ | NOTA: O Dell Data Security Encryption Enterprise para Mac não suporta investigação forense do EnCase.

Entre em contato com o Dell ProSupport

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

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

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

Para obter os números de telefone fora dos Estados Unidos, consulte [Números de telefone internacionais do Dell ProSupport](#).

Integrar ao EnCase

Habilitar o API do EnCase

NOTA: Não use esse API com servidores de dispositivo da Dell implementados em um DMZ. Use um servidor de dispositivo interno da Dell com acesso restrito à integração do EnCase para manter a segurança.

Security Management Server anterior à versão v7.7

- 1 Abra <Diretório de instalação da Dell>\Enterprise Edition\Servidor de dispositivo\conf\context.properties.
- 2 Habilite a API de integração forense.

```
service.forensic.enable=true
```

- 3 Interromper e reiniciar o servidor de dispositivo da Dell pelo menu Iniciar.

Para desativar a integração forense, defina `service.forensic.enable=false`.

Security Management Server v7.7 e posterior

- Esse serviço está ativado no servidor Dell por padrão.
- Para desativar a integração forense, defina `xapi.service.forensic.enable=false`.

Interromper e reiniciar o servidor de dispositivo da Dell pelo menu Iniciar.

Instalar o adaptador de integração do EnCase

- 1 Em um computador que esteja executando o EnCase, clique duas vezes em **CMGEnCaseIntegration.exe**.
- 2 Quando for exibida a caixa de diálogo Instalador da biblioteca, verifique se a pasta de destino do EnCase está correta.
- 3 Clique em **Concluir** para extrair o CEGetBundle e os arquivos do Adaptador de integração para `\Program Files\EnCase6\Lib\Credant Technologies\CMG`



Usar Dell Data Security com EnCase

Obter chaves de criptografia

Use a interface do usuário do EnCase Enterprise para obter chaves de criptografia do Console de gerenciamento remoto da Dell e descriptografar todos os dados criptografados pela Dell para esse computador ou arquivo de evidência.

- 1 Marque a caixa de seleção **On-line**.
- 2 Digite o **Nome de usuário** do Administrador forense.
- 3 Digite a **Senha** do Administrador forense.
- 4 Digite o URL para o servidor Dell com a API EnCase ativada. Por exemplo:

`https://cred01.somedomain.com:8443/xapi/` (se o Security Management Server for v7.7 ou posterior)

`https://cred01.somedomain.com:8081/xapi` (se o Security Management Server for anterior à versão v7.7)

Localize o URI do servidor Dell em HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet

NOTA: O servidor Dell precisa ter o API EnCase ativado para exportar chaves. Como opção, implemente um servidor de dispositivo Dell alternativo exclusivamente para integração do EnCase.

- 5 Digite o ID de máquina (também chamado de MCID e ID exclusivo) para o computador de destino ou arquivo de evidência.

Localize o MCID no registro do computador de destino em HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield

do Console de gerenciamento remoto da Dell, no painel esquerdo, clique em **Populações > Endpoints**

- Clique no ícone Detalhes do dispositivo apropriado.
- No menu superior, clique em **Detalhes e ações**.
- Localize o ID exclusivo na área *Detalhe do endpoint*.

- 6 Digite o ID do Shield (também chamado de ID de dispositivo, DCID, ID de recuperação ou SCID) para o computador de destino ou arquivo de evidência.

Localize o DCID no registro do computador de destino em HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield

do Console de gerenciamento remoto da Dell, no painel esquerdo, clique em **Populações > Endpoints**

- Clique no ícone **Detalhes** do dispositivo apropriado.
- No menu superior, clique em **Detalhes e ações**.
- Localize o ID de recuperação na área *Shield*.

NOTA: Especifique o MCID, o DCID ou ambos os IDs. O caso importado contém todos os materiais de chave para o ID de máquina especificado, ID do Shield ou ambos os IDs.

- 7 Clique em **OK**.

A descriptografia está agora em andamento.

Uma vez que a descriptografia estiver concluída, os arquivos estarão acessíveis para exame forense. Os arquivos descriptografados serão visíveis somente pelo módulo EnCase, os arquivos da fonte original permanecem inalterados e criptografados.



Usar EnCase com Dell Data Security

CEGetBundle

CEGetBundle é um utilitário que permite aos administradores forenses para extrair materiais de chaves de um servidor Dell. Esse utilitário está disponível pelo Dell ProSupport.

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

Parâmetros

-L = modo legado para exportação de chaves de um servidor CMG 5.3.x

URL = URL do servidor de dispositivo (<securityserver.organization.com>)

AdminName = nome de usuário do administrador

AdminPwd = senha do administrador

AdminDomain = domínio do administrador

MCID = ID de máquina do dispositivo de destino (também chamado de ID exclusivo ou nome de host)

SCID = ID do Shield Credant do Shield de destino (também chamado de DCID ou ID de recuperação)

Nome de usuário = usuário destinatário da exportação do material de chave (somente modo legado)

OutputFile = nome de arquivo do pacote de chaves exportado

OutputPwd = senha do pacote de chaves exportado

-R = usar modo de arquivo de backup

BackupFile = o executável contendo as chaves de backup

BackupPwd = a senha de administrador usado para o arquivo de backup

- ⓘ** **NOTA:** O parâmetro **AdminDomain** só deve ser fornecido para exportar as chaves de servidores CMG Enterprise Edition 6.0 e posteriores configurados para suportar múltiplos domínios.
- ⓘ** **NOTA:** No modo legado, o **MCID**, o **SCID** e o nome de usuário devem ser especificados. O material de chave apenas para o usuário especificado será anexado ao arquivo de saída. É necessário executar essa ferramenta com o mesmo nome de arquivo de saída para cada usuário no dispositivo destinado à descryptografia, se a criptografia de usuário ou de roaming de usuário estiver ativada. O material de chave de cada usuário será anexado ao arquivo de saída.

Exemplo de linha de comando

- O exemplo a seguir usa o MCID, o SCID ou ambos. Todos os materiais de chaves associados à máquina especificada (MCID), SCID ou ambos serão salvos no arquivo de saída, o qual será substituído, se existir.

```
CEGetBundle [-L] -XURL -aAdminName -AAdminPwd [-DAdminDomain] [-dMCID] [-sSCID] [-uUsername] -  
oOutputFile -iOutputPwd
```

- O exemplo a seguir extrai material de chave do arquivo de backup exportado pelo instalador.

```
CEGetBundle -R -bBackupFile -ABackupPwd -oOutputFile -iOutputPwd
```

