

Dell Encryption

Utilitários de administrador



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

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

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

© 2018 Dell Inc. Todos os direitos reservados. Dell, EMC e outras marcas registradas são marcas registradas da Dell Inc. ou das suas subsidiárias. Outras marcas registradas podem ser marcas registradas dos seus respetivos proprietários.

Marcas comerciais e marcas comerciais registadas utilizadas no Dell Encryption, Endpoint Security Suite Pro, Endpoint Security Suite Enterprise, e conjunto de aplicações de documentos Data Guardian: Dell™ e o logótipo Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® e KACE™ são marcas comerciais da Dell Inc. Cylance®, CylancePROTECT e o logótipo Cylance são marcas registradas da Cylance, Inc. nos EUA e noutros países. McAfee® e o logótipo da McAfee são marcas comerciais ou marcas comerciais registradas da McAfee, Inc. nos Estados Unidos e noutros países. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® e Xeon® são marcas comerciais registradas da Intel Corporation nos EUA e noutros 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 registada 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 noutros países. VMware® é marca registada ou marca comercial da VMware, Inc. nos Estados Unidos ou noutros países. Box® é marca registada da Box. DropboxSM é uma marca de serviço da Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® e Google™ Play são marcas comerciais ou marcas comerciais registradas da Google Inc. nos Estados Unidos e noutros 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 comerciais registradas da Apple, Inc. nos Estados Unidos e/ou noutros países. GO ID®, RSA® e SecurID® são marcas registradas da Dell EMC. EnCase™ e Guidance Software® são marcas comerciais ou marcas comerciais registradas da Guidance Software. Entrust® é marca registada da Entrust®, Inc. nos Estados Unidos e noutros países. InstallShield® é marca registada 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 noutros países. Mozilla® Firefox® é uma marca comercial registada da Mozilla Foundation nos Estados Unidos e/ou noutros países. iOS® é uma marca comercial ou marca comercial registada da Cisco Systems, Inc. nos Estados Unidos e outros países e é utilizada sob licença. Oracle® e Java® são marcas registradas da Oracle e/ou suas afiliadas. Os outros nomes podem ser marcas comerciais dos respetivos proprietários. SAMSUNG™ é uma marca comercial da SAMSUNG nos Estados Unidos ou noutros países. Seagate® é marca registada da Seagate Technology LLC nos Estados Unidos e/ou noutros países. Travelstar® é marca registada da HGST, Inc. nos Estados Unidos e noutros países. UNIX® é marca registada da The Open Group. VALIDITY™ é uma marca comercial da Validity Sensors, Inc. nos Estados Unidos e noutros países. VeriSign® e outras marcas similares são marcas comerciais ou marcas comerciais registradas da VeriSign, Inc. ou respetivas filiais ou subsidiárias nos Estados Unidos e noutros países e licenciadas à Symantec Corporation. KVM on IP® é marca registada da Video Products. Yahoo!® é marca registada da Yahoo! Inc. Este produto utiliza partes do programa 7-Zip. O código-fonte encontra-se disponível em 7-zip.org. O licenciamento é efetuado ao abrigo da licença GNU LGPL + restrições unRAR (7-zip.org/license.txt).

Utilitários de administrador

2017 - 08

Rev. A01

1 Introdução.....	4
Contacte o Dell ProSupport.....	4
2 Administrative Download Utility (CMGAd).....	5
Utilizar o Modo forense.....	5
Utilizar o Modo de administrador.....	6
3 Administrative Launch Utility (CMGAlu).....	7
Utilizar o Modo forense.....	7
Sintaxe do Modo forense.....	7
Utilizar o Modo de administrador.....	8
Sintaxe do Modo de administrador.....	8
Utilizar o Modo de ficheiro de cópia de segurança.....	8
Sintaxe do Modo de ficheiro de cópia de segurança.....	8
4 Administrative Unlock Utility (CMGAu).....	10
Trabalhar offline com um ficheiro previamente transferido.....	10
Realizar uma transferência agora no Modo forense.....	10
Realizar uma transferência agora no Modo de administrador.....	11

Introdução

Este documento descreve os utilitários destinados à recuperação da chave de encriptação e ao acesso aos ficheiros. Os utilitários oferecem as seguintes funções:

Transferir chaves - O comando **CMGAd** permite aos administradores transferir um pacote de material de chave para utilização num computador que não está ligado a um Dell Server.

Iniciar Tarefas - O comando **CMGAlu** permite aos administradores desbloquear ficheiros encriptados de utilizador ou comuns num computador enquanto o processo está a ser executado.

Desbloquear Ficheiros - O comando **CMGAu** permite aos administradores aceder a ficheiros de utilizador, comuns ou com encriptação SDE numa unidade subordinada, num computador arrancado num ambiente pré-instalado, ou num computador em que um utilizador ativado não tem sessão iniciada.

Contacte o Dell ProSupport

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

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

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

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

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 Dell Server. O Administrador pode utilizar estes pacotes offline.

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 estar localizados em C:\ProgramData\CmgAdmin.log

Utilizar o 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).

Parâmetros de Modo forense Descrição

URL do Device Server	URL do Security Server (Device Server) totalmente qualificado. O formato é https://securityserver.domain.com:8443/xapi/. Se o seu Dell Server é pré-v7.7, o formato é https://deviceserver.domain.com:8081/xapi (diferente número de porta, sem a barra no final).
Dell Admin	Nome do administrador com credenciais de administrador forense, como "jdoe" (ativado na Management Console)
Palavra-passe	Palavra-passe de administrador forense
MCID	ID do computador, tal como machineID.domain.com
DCID	Primeiros oito dígitos do ID do 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 informações diferentes utilizadas por este utilitário.

Clique em **Seguinte**.

- 3 Em *Frase de acesso*, introduza 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 seleccionar outra localização.

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.

Utilizar o Modo de administrador

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

- 1 Abra uma linha de comandos onde o CMGAd está localizado e introduza **cmgad.exe -a**.
- 2 Introduza a seguinte informação (alguns campos podem ser pré-preenchidos).

Parâmetros de Modo administrador	Descrição
Servidor:	Nome de anfitrião totalmente qualificado do Key Server, tal como keyserver.domain.com.
Número da porta	A porta predefinida é 8050
Conta do servidor	O utilizador do domínio como o qual o Key Server está a ser executado. O formato é DOMÍNIO \Nome de utilizador. 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, tal como machineID.domain.com
DCID	Primeiros oito dígitos do ID do 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 informações diferentes utilizadas por este utilitário.

Clique em **Seguinte**.

- 3 Em *Frase de acesso*, introduza 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 seleccionar outra localização.

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.

Administrative Launch Utility (CMGAlu)

Este utilitário permite aos administradores desbloquear ficheiros encriptados de utilizador ou comuns num computador enquanto o processo está a ser executado.

Este utilitário é utilizado para iniciar tarefas a partir de uma gestão de consola. O utilitário tem de ser copiado para o computador de destino e qualquer tarefa que requeira acesso a ficheiros encriptados de utilizador ou comuns é alterada para executar este utilitário, passando a linha de comandos para a tarefa de gestão para o utilitário. Assim que o processo sair, o utilitário termina.

Este utilitário utiliza um dos seguintes métodos para desbloquear ficheiros, 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 **-k** é passado na linha de comandos.
- **Modo de ficheiro de cópia de segurança** - Utilizado se **-b** é passado na linha de comandos.

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

Utilizar o Modo forense

Sintaxe do Modo forense

```
CmgAlu -f -vX -aAdminName -AAdminPwd [-r] [-XURL [-dMCID] [-sSCID]] "command"
```

Parâmetros de Modo forense	Descrição
-f	Indica que o Modo forense está a ser utilizado.
-vX	X indica o nível de registo. Os níveis de registo são 0 - 5 (0 sem registos/5 nível de depuração).
AdminPwd	Palavra-passe de administrador forense
AdminName	Nome de utilizador do administrador com credenciais de administrador forense
-r	Instrui o utilitário para carregar o URL e MCID (ou SCID) do Device Server do computador do registo. Se -r não for especificado, o URL/MCID (ou SCID) do Servidor tem de ser fornecido.
URL	URL do Device Server totalmente qualificado Se o seu Dell Server for anterior a v7.7, o formato é https://deviceserver.domain.com:8081/xapi Se o seu Dell Server for anterior a v7.7, o formato é https://deviceserver.domain.com:8443/xapi
MCID	ID do Dispositivo para o dispositivo a desbloquear.

Parâmetros de Modo forense	Descrição
SCID	MCID também é conhecido como ID exclusivo ou nome de anfitrião do dispositivo. ID de Proteção do dispositivo a desbloquear. SCID também é conhecido como DCID ou ID de Recuperação.
-?	Ajuda de linha de comandos.

Utilizar o Modo de administrador

Sintaxe do Modo de administrador

```
CmdGAlu -k -vX -aServerPrincipal -pPort [-r] [-XServer [-dMCID] [-sSCID]] "command"
```

Parâmetros de Modo administrador	Descrição
k	Indica que Kerberos (Modo de administrador) deve ser utilizado. O CmdGAlu requer que o sinalizador -k funcione no Modo de administrador.
-vX	X indica o nível de registo. Os níveis de registo são 0 - 5 (0 sem registos/5 nível de depuração).
ServerPrincipal	Conta AD (Conta Domínio) em que o Key Server está a ser executado.
Porta	Porta TCP para ligar ao Key Server ligado.
Servidor	Nome/endereço IP de Key Server.
-r	Instrui o utilitário para carregar o Nome e MCID (ou SCID) do Key Server do computador do registo. Se -r não for especificado, o nome e MCID (ou SCID) do Key Server têm de ser fornecidos.
MCID	ID do Dispositivo para o dispositivo a desbloquear. MCID também é conhecido como ID exclusivo ou nome de anfitrião do dispositivo.
SCID	ID de Proteção do dispositivo a desbloquear. SCID também é conhecido como DCID ou ID de Recuperação.
-?	Ajuda de linha de comandos.

Utilizar o Modo de ficheiro de cópia de segurança

Sintaxe do Modo de ficheiro de cópia de segurança

```
CmdGAlu -vX -b"FilePath" -ABackupPwd "command"
```

Parâmetros do Modo de ficheiro de cópia de segurança**Descrição**

-vX	X indica o nível de registo. Os níveis de registo são 0 - 5 (0 sem registos/5 nível de depuração).
-b"FilePath"	O caminho do sistema de ficheiro para o ficheiro de cópia de segurança, normalmente um ficheiro de recuperação LSA ou um ficheiro de exportação transferido do CMGAd.
-BackupPwd	A palavra-passe utilizada para criar o ficheiro de cópia de segurança.
-?	Ajuda de linha de comandos.

Administrative Unlock Utility (CMGAu)

Este utilitário permite acesso a ficheiros de Utilizador, Comuns ou com encriptação SDE numa unidade subordinada, num computador arrancado num ambiente pré-instalado, ou num computador em que um utilizador ativado não tem sessão iniciada.

Este utilitário utiliza o seguinte método para transferir um pacote de material de chave:

- **Modo forense** - Utilizado se **-f** é passado na linha de comandos ou se não é utilizado qualquer parâmetro de linha de comando.
- **Modo de administrador** - Utilizado se **-a** é passado na linha de comandos.

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

Trabalhar offline com um ficheiro previamente transferido

Se escolher trabalhar offline com um ficheiro previamente transferido, CMGAu funciona da mesma forma, independentemente de como foi iniciado, significando que a operação é igual quer faça duplo clique em .exe para iniciar o utilitário, o inicie sem qualquer mudança numa linha de comandos ou o inicie utilizando a opção **-f** na linha de comandos.

- 1 Abra uma linha de comandos onde o CMGAu está localizado e introduza **cmgau.exe**.
- 2 Selecione **Sim, trabalhar offline com um ficheiro previamente transferido**. Clique em **Seguinte** >.
- 3 Em *Ficheiro transferido*, navegue até à localização do material de chave guardado. Este ficheiro foi guardado aquando da utilização de Administrative Download Utility.

Em *Frase de acesso*, introduza a frase de acesso que foi utilizada para proteger o ficheiro do material de chave. Esta frase de acesso foi definida quando da utilização de Administrative Download Utility.

Clique em **Seguinte** >.

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

- 4 **Assim que tiver terminado de trabalhar com os ficheiros encriptados**, clique em **Concluir**. *Após clicar em Concluir, os ficheiros encriptados deixam de estar disponíveis.*

Realizar uma transferência agora no Modo forense

- 1 Abra uma linha de comandos onde o CMGAu está localizado e introduza **cmgau.exe**.
- 2 Selecione **Não, realizar uma transferência a partir de um servidor agora**. Clique em **Seguinte** >.
- 3 Introduza a seguinte informação (alguns campos podem ser pré-preenchidos).

Opção	Descrição
URL do Device Server:	URL do Device Server totalmente qualificado. Se o seu Dell Server for anterior a v7.7, o formato é https://deviceserver.domain.com:8081/xapi Se o seu Dell Server for anterior a v7.7, o formato é https://deviceserver.domain.com:8443/xapi

Opção	Descrição
Dell Admin :	Nome do administrador com credenciais de administrador forense, como "jdoe" (ativado na Management Console)
Palavra-passe:	Palavra-passe de administrador forense
MCID:	ID do computador, tal como machineID.domain.com
DCID:	Primeiros oito dígitos do ID do Shield de 16 dígitos

Clique em **Seguinte >**.

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

- 4 **Assim que tiver terminado de trabalhar com os ficheiros encriptados**, clique em **Concluir**. Após clicar em **Concluir**, os ficheiros encriptados já não estão disponíveis.

Realizar uma transferência agora no Modo de administrador

- 1 Abra uma linha de comandos onde o CMGAu está localizado e introduza **cmgau.exe -a**.
- 2 Selecione **Não, realizar uma transferência a partir de um servidor agora**. Clique em **Seguinte >**.
- 3 Introduza a seguinte informação (alguns campos podem ser pré-preenchidos).

Parâmetros de Modo administrador	Descrição
Servidor:	Nome de anfitrião totalmente qualificado do Key Server, tal como keyserver.domain.com
Número da porta:	A porta predefinida é 8050
Conta do servidor:	O utilizador do domínio como o qual o Key Server está a ser executado. O formato é DOMÍNIO\Nome de utilizador. 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, tal como machineID.domain.com
DCID:	Primeiros oito dígitos do ID do Shield de 16 dígitos

Clique em **Seguinte >**.

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

- 4 **Assim que tiver terminado de trabalhar com os ficheiros encriptados**, clique em **Concluir**. Após clicar em **Concluir**, os ficheiros encriptados já não estão disponíveis.