Dell Data Protection Encryption

Utilitários de administrador

© 2014 Dell Inc.

Marcas comerciais e marcas comerciais registradas usadas no DDP|E, DDP|ST, e no pacote de documentos DDP|CE: Dell™ e o logotipo da Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, e KACE™ são marcas comerciais da Dell Inc. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, e Xeon® são marcas comerciais registradas da Intel Corporation nos Estados Unidos da América e em outros países. Adobe®, Acrobat®, e Flash® são marcas comerciais registradas da Adobe Systems Incorporated. Authen Tec® e Eikon® são marcas comerciais registradas da Authen Tec. AMD® é uma marca comercial registrada da Advanced Micro Devices, Inc. Microsoft®, Windows®, e 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 comerciais registradas da Microsoft Corporation nos Estados Unidos da América e/ou em outros países. VMware® é marca comercial ou marca comercial registrada da VMware, Inc. nos Estados Unidos da América ou em outros países. Box® é marca comercial registrada da Box. Dropbox℠ 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 da América ou em outros países. Apple®, Aperture®, App Store℠, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®℠, 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 da América e/ou em outros países. GO ID®, RSA®, e SecurID® são marcas comerciais registradas da EMC Corporation. EnCase™ e Guidance Software® são marcas comerciais ou marcas comerciais registradas da Guidance Software. Entrust® é uma marca comercial registrada da Entrust®, Inc. nos Estados Unidos da América e em outros países. InstallShield® é uma marca comercial registrada da Flexera Software nos Estados Unidos da América, na China, na Comunidade Europeia, em Hong Kong, no Japão, em Taiwan e no Reino Unido. Micron® e RealSSD® são marcas comerciais registradas da Micron Technology, Inc. nos Estados Unidos da América e em outros países. Mozilla® Firefox® é uma marca comercial registrada da Mozilla Foundation nos Estados Unidos da América e/ou em outros países. iOS® é uma marca comercial ou marca comercial registrada da Cisco Systems, Inc. nos Estados Unidos da América e em determinados outros países e é usada sob licença. Oracle® e Java® são marcas comerciais registradas da Oracle e/ou suas afiliadas. Outros nomes podem ser marcas comerciais de seus respectivos proprietários. SAMSUNG™ é uma marca comercial da SAMSUNG nos Estados Unidos da América ou em outros países. Seagate® é uma marca comercial registrada da Seagate Technology LLC nos Estados Unidos da América e/ou em outros países. Travelstar® é uma marca comercial registrada da HGST, Inc. nos Estados Unidos da América e em outros países. UNIX® é uma marca comercial registrada da The Open Group. VALIDITY™ é uma marca comercial da Validity Sensors, Inc. nos Estados Unidos da América e em outros países. VeriSign® e outras marcas relacionadas são marcas comerciais ou marcas comerciais registradas da VeriSign, Inc. ou suas afiliadas ou subsidiárias nos Estados Unidos da América e em outros países e licenciadas à Symantec Corporation. KVM on IP® é uma marca comercial registrada da Video Products. Yahoo!® é uma marca comercial registrada da Yahoo! Inc.

Este produto usa partes do programa 7-Zip. O código-fonte pode ser encontrado em www.7-zip.org. Licenciamento sob a licença GNU LGPL + restrições unRAR (www.7-zip.org/license.txt).

2014-05

Protegido por uma ou mais patentes dos EUA, incluindo: Nº 7665125; Nº 7437752; e Nº 7665118.
As informações neste documento estão sujeitas a alterações sem aviso.

Sumário

1

Utilitário de download administrativo

Este utilitário permite o download de um grupo de materiais de chaves para uso em um computador que não esteja conectado a um Enterprise Server. Os Utilitários de administrador podem usar esses grupos off-line.

Este utilitário usa um dos seguintes métodos para baixar um grupo de materiais de chaves, dependendo do parâmetro de linha de comando enviado ao aplicativo:

- **Modo admim** - Usado se **-a** for enviado à linha de comando ou se nenhum parâmetro de linha de comando for usado.
- **Modo forense** - Usado se **-f** for enviado à linha de comando.

Os arquivos de log podem estar localizados em:

Windows XP - C:\Documents and Settings\All Users\Application Data\CmgAdmin.log

Windows 7, Windows 8, e Windows 8.1 - C:\ProgramData\CmgAdmin.log

Use o Utilitário de download administrativo no Modo admin

1. Clique duas vezes em **cmgad.exe** para iniciar o utilitário.

   ou

   No local onde se encontra o Utilitário de download administrativo, abra um prompt de comando e digite **cmgad.exe -a** (ou cmgad.exe).

2. Insira as seguintes informações (alguns campos podem estar preenchidos previamente).

Servidor:	Nome de host totalmente qualificado do Servidor de chaves, como keyserver.domain.com
Número de porta:	A porta padrão é 8050
Conta de servidor:	O usuário de domínio com o qual o Servidor de chaves está em execução. O formato é domínio\nome de usuário. O usuário de domínio que executa o utilitário deve ter autorização para realizar o download a partir do Servidor de chaves
MCID:	ID da máquina, como machineID.domain.com
DCID:	Os primeiros oito dígitos do ID do Shield de 16 dígitos

   Clique em **Avançar >**.

3. No campo **Frase secreta:**, digite uma frase secreta para proteger o arquivo de download. A frase secreta deve ter pelo menos oito caracteres e conter pelo menos um caractere alfabético e um caractere numérico.

   Confirme a frase secreta.

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

   Uma mensagem é exibida, indicando que um material de chaves foi desbloqueado com êxito. Os arquivos estão acessíveis agora.

4. Quando terminar, clique em **Concluir**.

Use o Utilitário de download administrativo no Modo forense

1 No local onde se encontra o Utilitário de download administrativo, abra um prompt de comando e digite **cmgad.exe -f**.

2 Insira as seguintes informações (alguns campos podem estar preenchidos previamente).

URL do Device Server:	URL do Device Server totalmente qualificada Caso o seu Enterprise Server seja pré-v7.7, o formato será https://deviceserver.domain.com:8081/xapi Caso o seu Enterprise Server seja v7.7 ou mais recente, o formato será https://deviceserver.domain.com:8443/xapi/
Dell Admin:	Nome do administrador com credenciais administrativas forenses (ativado no Enterprise Server), como jdoe
Senha:	Senha administrativa forense
MCID:	ID da máquina, como machineID.domain.com
DCID:	Os primeiros oito dígitos do ID do Shield de 16 dígitos

Clique em **Avançar >**.

3 No campo **Frase secreta:**, digite uma frase secreta para proteger o arquivo de download. A frase secreta deve ter pelo menos oito caracteres e conter pelo menos um caractere alfabético e um caractere numérico.

Confirme a frase secreta.

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

Uma mensagem é exibida, indicando que um material de chaves foi desbloqueado com êxito. Os arquivos estão acessíveis agora.

4 Quando terminar, clique em **Concluir**.

2

Utilitário de inicialização administrativo

Este utilitário de linha de comando permite aos administradores desbloquear arquivos criptografados de usuário ou comuns em um computador enquanto um processo está em execução.

Este utilitário é usado para iniciar tarefas a partir de um console de gerenciamento. O utilitário deve ser copiado para o computador cliente e qualquer tarefa que precise de acesso aos arquivos criptografados de usuário ou comuns é alterada para executar o utilitário, por meio do envio da linha de comando da tarefa de gerenciamento ao utilitário. Quando o processo terminar, o utilitário será encerrado.

Este utilitário usa um dos seguintes métodos para desbloquear arquivos, dependendo do parâmetro de linha de comando enviado ao aplicativo:

- Modo admin - Nenhuma opção necessária.
- Modo forense - Usado se **-f** for enviado à linha de comando.
- Modo arquivo de backup - Usado se **-b** for enviado à linha de comando.

Os arquivos de log podem estar localizados em:

Windows XP - C:\Documents and Settings\All Users\Application Data\CmgAdmin.log

Windows 7, Windows 8, e Windows 8.1 - C:\ProgramData\CmgAdmin.log

Use o Utilitário de inicialização administrativo no Modo admin

Sintaxe do Modo admin

CmgAlu -k -vX -aServerPrincipal -pPort [-r] [-XServer [-dMCID] [-sSCID]] “comando”

Parâmetros do Modo admin	Descrição
-k	Indica que Kerberos (Modo admin) precisa ser usado. CmgAlu requer a opção-k trabalhar em Modo admin.
X	Nível de log. Os níveis de log são de 0 a 5 (0 é nenhum log/5 é nível de depuração).
ServerPrincipal	Conta AD (conta de domínio) com a qual o Servidor de chaves está em execução.
Porta	Porta TCP para conectar ao Servidor de chaves.
Servidor	Nome do Servidor de chaves/endereço IP.
-r	Instrui o utilitário a carregar o nome do Servidor de chaves e MCID (ou SCID) do computador a partir do registro. Se –r não for especificado, o Nome do servidor de chaves e MCID (ou SCID) deverão ser fornecidos.
MCID	ID de dispositivo para o dispositivo desbloquear. MCID é também conhecido como ID exclusivo de dispositivo.

Parâmetros do Modo admin	Descrição
SCID	ID do Shield de dispositivo para o dispositivo desbloquear. SCID é também conhecido como DCID ou ID de recuperação.
-?	Ajuda da linha de comando.

Use o Utilitário de inicialização administrativo no Modo forense

Sintaxe do Modo forense

CmgAlu -f -vX -aAdminName -AAdminPwd [-r] [-XURL [-dMCID] [-sSCID]] “comando”

Parâmetros do Modo forense	Descrição
-f	Indica que o Modo forense precisa ser usado.
AdminName	Nome de usuário do administrador com credenciais administrativas forenses.
AdminPwd	Senha administrativa forense.
URL	URL do Device Server totalmente qualificada. Caso o seu Enterprise Server seja pré-v7.7, o formato será https://deviceserver.domain.com:8081/xapi Caso o seu Enterprise Server seja v7.7 ou mais recente, o formato será https://deviceserver.domain.com:8443/xapi/
-r	Instrui o utilitário a carregar a URL do Device Server e MCID (ou SCID) do computador a partir do registro. Se –r não for especificado, a URL/o servidor e MCID (ou SCID) deverão ser fornecidos.
X	Nível de log. Os níveis de log são de 0 a 5 (0 é nenhum log/5 é nível de depuração).
MCID	ID de dispositivo para o dispositivo desbloquear. MCID é também conhecido como ID exclusivo de dispositivo.
SCID	ID do Shield de dispositivo para o dispositivo desbloquear. SCID é também conhecido como DCID ou ID de recuperação.
-?	Ajuda da linha de comando.

Use o Utilitário de inicialização administrativo no Modo arquivo de backup

Sintaxe do Modo arquivo de backup

CmgAlu -vX -b"FilePath" -ABackupPwd "command"

Parâmetros do Modo arquivo de backup	Descrição
X	Nível de log. Os níveis de log são de 0 a 5 (0 é nenhum log/5 é nível de depuração).
-b"FilePath"	O arquivo sistema caminho à arquivo de segurança, tipicamente quer um LSA recuperação arquivo ou um arquivo de saída baixado de CmgAd.
BackupPwd	A senha usado para criar os arquivo de backup.
-?	Ajuda da linha de comando.

3

Utilitário de desbloqueio administrativo

Este utilitário permite o acesso aos arquivos criptografados de usuário, comuns ou SDE em uma unidade escrava, um computador inicializado em um ambiente pré-instalado ou em um computador ao qual um usuário ativado não está conectado.

Este utilitário usa o seguinte método para baixar um grupo de materiais de chaves:

- Modo admin - Nenhuma opção necessária. Este é o modo padrão.
- Modo forense - Usado se **-f** for enviado à linha de comando.

Os arquivos de log podem estar localizados em:

Windows XP - C:\Documents and Settings\All Users\Application Data\CmgAdmin.log

Windows 7, Windows 8, e Windows 8.1 - C:\ProgramData\CmgAdmin.log

Use o Utilitário de desbloqueio administrativo para trabalhar off-line com um arquivo baixado anteriormente

Se você optar por trabalhar off-line com um arquivo baixado anteriormente, o CMGAu funcionará da mesma forma, não tendo diferença na forma como você o inicia, significando que a operação será a mesma se você clicar duas vezes em .exe para iniciar o utilitário, iniciá-lo sem nenhuma opção em uma linha de comando ou iniciá-lo usando a opção -f na linha de comando.

1. Clique duas vezes em **cmgau.exe** para iniciar o utilitário.
2. Selecione **Sim, trabalhar off-line com um arquivo cujo download foi realizado antes**. Clique em **Avançar >**.
3. No campo **Arquivo baixado:**, navegue até o local do material de chaves salvo. Esse arquivo foi salvo com o uso do Utilitário de download administrativo.

   No campo **Frase secreta:**, insira a frase secreta que foi usada para proteger o arquivo de material de chaves. Essa frase secreta foi salva com o uso do Utilitário de download administrativo.

   Clique em **Avançar >**.

   Uma mensagem é exibida, indicando que um material de chaves foi desbloqueado com êxito. Os arquivos estão acessíveis agora.
4. Quando tiver terminado de trabalhar com os arquivos criptografados, clique em **Concluir**. *Depois que você clicar em Concluir, os arquivos criptografados não ficarão mais disponíveis.*

Use o Utilitário de desbloqueio administrativo para realizar um download de um servidor agora no Modo admin

1. Clique duas vezes em **cmgau.exe** para iniciar o utilitário.

   ou

   No local onde se encontra o Utilitário de desbloqueio administrativo, abra um prompt de comando e digite **cmgau.exe**.
2. Selecione **Não, executar um download de um servidor agora**. Clique em **Avançar >**.

3 Insira as seguintes informações (alguns campos podem estar preenchidos previamente).

Servidor:	Nome de host totalmente qualificado do Servidor de chaves, como keyserver.domain.com
Número de porta:	A porta padrão é 8050
Conta de servidor:	O usuário de domínio com o qual o Servidor de chaves está em execução. O formato é domínio\nome de usuário. O usuário de domínio que executa o utilitário deve ter autorização para realizar o download a partir do Servidor de chaves
MCID:	ID da máquina, como machineID.domain.com
DCID:	Os primeiros oito dígitos do ID do Shield de 16 dígitos

Clique em **Avançar >**.

Uma mensagem é exibida, indicando que um material de chaves foi desbloqueado com êxito. Os arquivos estão acessíveis agora

4 Quando tiver terminado de trabalhar com os arquivos criptografados, clique em **Concluir**. *Depois que você clicar em Concluir, os arquivos criptografados não ficarão mais disponíveis.*

Use o Utilitário de desbloqueio administrativo para realizar um download de um servidor agora no Modo forense

1 No local onde se encontra o Utilitário de desbloqueio administrativo, abra um prompt de comando e digite **cmgau.exe -f**.

2 Selecione **Não, executar um download de um servidor agora**. Clique em **Avançar >**.

3 Insira as seguintes informações (alguns campos podem estar preenchidos previamente).

URL do Device Server:	URL do Device Server totalmente qualificada. Caso o seu Enterprise Server seja pré-v7.7, o formato será https://deviceserver.domain.com:8081/xapi Caso o seu Enterprise Server seja v7.7 ou mais recente, o formato será https://deviceserver.domain.com:8443/xapi/
Dell Admin:	Nome do administrador com credenciais administrativas forenses (ativado no Enterprise Server), como jdoe
Senha:	Senha administrativa forense
MCID:	ID da máquina, como machineID.dell.com
DCID:	Os primeiros oito dígitos do ID do Shield de 16 dígitos

Clique em **Avançar >**.

Uma mensagem é exibida, indicando que um material de chaves foi desbloqueado com êxito. Os arquivos estão acessíveis agora

4 Quando tiver terminado de trabalhar com os arquivos criptografados, clique em **Concluir**. *Depois que você clicar em Concluir, os arquivos criptografados não ficarão mais disponíveis.*


0 XXXXXA0 X