Dell Encryption

Utilitários de administrador

Notas, avisos e advertências

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.

Utilitários de administrador

2017 - 08

Rev. A01

Índice

1

Introdução

Este documento descreve utilitários para recuperação de chaves de criptografia e acesso aos arquivos. Os utilitários oferecem as seguintes funções:

Fazer download de chaves - CMGAd permite aos administradores fazer download de um pacote de materiais de chaves para uso em um computador não conectado a um Dell Server.

Abrir trabalhos - O comando **CMGAlu** permite aos administradores desbloquear arquivos criptografados do usuário ou comuns em um computador enquanto um processo está em execução.

Desbloquear arquivos - CMGau permite aos administradores acessar arquivos do usuário, comuns ou criptografados por SDE em uma unidade escrava, um computador iniciado em um ambiente pré-instalado, ou em um computador onde um usuário ativado não está conectado.

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 o código de serviço, 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.

Utilitário Administrativo de Download (CMGAd)

Este utilitário possibilita fazer download de um pacote de materiais de chaves para uso em um computador não conectado a um Dell Server. Os utilitários de administração podem então usar esses pacotes offline.

O utilitário usa um dos métodos a seguir para fazer download de um pacote de chaves, dependendo do parâmetro de linha de comando passado ao aplicativo:

- **Modo forense** - Usado se **-f** for incluído na linha de comando ou se nenhum parâmetro de linha de comando for usado.
- **Modo administrativo** - Usado se **-a** for incluído na linha de comando.

Os arquivos de log podem ser encontrados em C:\ProgramData\CmgAdmin.log

Uso do modo forense

1 Clique duas vezes em **cmgad.exe** para abrir o utilitário ou abra um prompt de comando onde o CMGAd está localizado e digite **cmgad.exe -f** (ou **cmgad.exe**).

2 Digite as informações a seguir (alguns campos podem já estar preenchidos).

Parâmetros do modo forense	Descrição
URL do Device Server	URL do Security Server totalmente qualificado (Device Server). O formato é https://securityserver.domain.com:8443/xapi/. Caso o seu Dell Server seja pré-v7.7, o formato é https://deviceserver.domain.com:8081/xapi (número de porta diferente, sem a barra).
Dell Admin	Nome do administrador com credenciais de administrador forense, como, por exemplo, jdoe (Ativado no Management Console)
Senha	Senha do administrador forense
MCID	ID da máquina, por exemplo, IDdemaquina.dominio.com
DCID	Oito primeiros dígitos da ID Shield de 16 dígitos

DICA:
Normalmente, especificar o MCID ou o DCID é suficiente. No entanto, se você souber ambos, é útil digitar os dois. Cada parâmetro contém diferentes informações usadas por este utilitário.

Clique em **Avançar**.

3 Em *Senha*, digite uma senha para proteger o arquivo de download. A senha deve ter no mínimo oito caracteres e conter pelo menos um caractere alfabético e um numérico. Confirme a senha.

Aceite o nome e o local padrão onde o arquivo será salvo ou clique em ... para selecionar outro local.

Clique em **Avançar**.

Uma mensagem indicando que o material de chave foi desbloqueado corretamente é mostrada. Os arquivos estão acessíveis agora.

4 Clique em **Concluir** quando terminar.

Uso do modo administrativo

O Servidor de gerenciamento de segurança virtual não usa o Key Server. Portanto, o modo administrativo não pode ser usado para obter um pacote de chaves de um Servidor de gerenciamento de segurança virtual. Use o modo forense para obter um pacote de chaves se o cliente estiver ativado em um Servidor de gerenciamento de segurança virtual.

1 Abra um prompt de comando onde o CMGAd está localizado e digite **cmgad.exe -a**.

2 Digite as informações a seguir (alguns campos podem já estar preenchidos).

Parâmetros do modo administrativo	Descrição
Servidor:	Nome de host totalmente qualificado do Key Server, por exemplo keyserver.dominio.com.
Número da porta	A porta padrão é 8050
Conta do servidor	O usuário de domínio em que o Key Server está executando. O formato é DOMÍNIO\Nome de usuário. O usuário de domínio executando o utilitário precisa estar autorizado a fazer download do Key Server.
MCID	ID da máquina, por exemplo, IDdemaquina.dominio.com
DCID	Oito primeiros dígitos da ID Shield de 16 dígitos

DICA:

Normalmente, especificar o MCID *ou* o DCID é suficiente. No entanto, se você souber ambos, é útil digitar os dois. Cada parâmetro contém diferentes informações usadas por este utilitário.

Clique em **Avançar**.

3 Em *Senha*, digite uma senha para proteger o arquivo de download. A senha deve ter no mínimo oito caracteres e conter pelo menos um caractere alfabético e um numérico.

Confirme a senha.

Aceite o nome e o local padrão onde o arquivo será salvo ou clique em ... para selecionar outro local.

Clique em **Avançar**.

Uma mensagem indicando que o material de chave foi desbloqueado corretamente é mostrada. Os arquivos estão acessíveis agora.

4 Clique em **Concluir** quando terminar.

3

Utilitário Administrativo de Inicialização (CMGAlu)

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

Este utilitário é usado para iniciar trabalhos a partir de um console de gerenciamento. O utilitário deve ser copiado para o computador alvo e qualquer trabalho que exija acesso a arquivos criptografados do usuário ou comuns é alterado para executar este utilitário, passando a linha de comando do trabalho de gerenciamento para o utilitário. Após a saída do processo, o utilitário é encerrado.

O utilitário usa um dos métodos a seguir para desbloquear arquivos, dependendo do parâmetro de linha de comando passado ao aplicativo:

- **Modo forense** - Usado se **-f** for incluído na linha de comando ou se nenhum parâmetro for incluído na linha de comando.
- **Modo administrativo** - Usado se **-k** for incluído na linha de comando.
- **Modo de arquivo de backup** - Usado se **-b** for incluído na linha de comando.

Os arquivos de log podem ser encontrados em C:\ProgramData\CmgAdmin.log

Uso do 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 deve ser usado.
-vX	X indica o nível de log. Os níveis de log são de 0 a 5 (0 significa sem log/5 significa nível de depurador).
SenhaAdmin	Senha do administrador forense
NomeAdmin	Nome de usuário do administrador com credenciais de administrador forense
-r	Instrui o utilitário a carregar o URL do Device Server e MCID (ou SCID) do computador a partir do registro. Se -r não for especificado, o URL/servidor e MCID (ou SCID) precisam ser fornecidos.
URL	URL de servidor de dispositivo totalmente qualificado Caso o seu Dell Server seja anterior à v7.7, o formato será https://deviceserver.domain.com:8081/xapi Caso o seu Dell Server seja v7.7 ou mais recente, o formato será https://deviceserver.domain.com:8443/xapi/

Parâmetros do modo forense	Descrição
MCID	ID de Dispositivo do dispositivo a ser desbloqueado. O MCID também é conhecido como o nome de host ou ID Exclusivo do Dispositivo.
SCID	ID Shield do dispositivo a ser desbloqueado. O SCID também é conhecido como DCID ou ID de Recuperação.
-?	Ajuda da linha de comando.

Uso do modo administrativo

Sintaxe do modo administrativo

```
CmgAlu -k -vX -aServidorPrincipal -pPorta [-r] [-XServidor [-dMCID] [-sSCID]] "comando"
```

Parâmetros do modo administrativo	Descrição
-k	Indica que o Kerberos (modo administrativo) deve ser usado. CmgAlu exige o indicador -k para funcionar no modo administrativo.
-vX	X indica o nível de log. Os níveis de log são de 0 a 5 (0 significa sem log/5 significa nível de depurador).
ServidorPrincipal	Conta do AD (conta de domínio) em que o Key Server está sendo executado.
Porta	Porta TCP para conectar ao Key Server.
Server	Endereço IP/nome do Key Server.
-r	Instrui o utilitário a carregar o nome do Key Server e MCID (ou SCID) do computador a partir do registro. Se -r não for especificado, o nome do Key Server e MCID (ou SCID) precisam ser fornecidos.
MCID	ID de Dispositivo do dispositivo a ser desbloqueado. O MCID também é conhecido como o nome de host ou ID Exclusivo do Dispositivo.
SCID	ID Shield do dispositivo a ser desbloqueado. O SCID também é conhecido como DCID ou ID de Recuperação.
-?	Ajuda da linha de comando.

Uso do modo de arquivo de backup

Sintaxe do modo de arquivo de backup

```
CmgAlu -vX -b"CaminhoArq" -ASenhaBackup "comando"
```

Parâmetros de modo de arquivo de backup	Descrição
-vX	X indica o nível de log. Os níveis de log são de 0 a 5 (0 significa sem log/5 significa nível de depurador).
-b"CaminhoArq"	O caminho do sistema de arquivos para o arquivo de backup, normalmente um arquivo de recuperação do LSA ou um arquivo de saída obtido por download do CmgAd.
-BackupPwd	A senha usada para criar o arquivo de backup.
-?	Ajuda da linha de comando.

Utilitário Administrativo de Desbloqueio (CMGAu)

Este utilitário permite acesso a arquivos do usuário, comuns ou criptografados por SDE em uma unidade escrava, um computador iniciado em um ambiente pré-instalado, ou em um computador onde um usuário ativado não está conectado.

Este utilitário usa o seguinte método para fazer o download de um pacote de material de chave:

- **Modo forense** - Usado se **-f** for incluído na linha de comando ou se nenhum parâmetro de linha de comando for usado.
- **Modo administrativo** - Usado se **-a** for incluído na linha de comando.

Os arquivos de log podem ser encontrados em C:\ProgramData\CmgAdmin.log

Trabalhar off-line com um Arquivo baixado anteriormente

Se você optar por trabalhar offline com um arquivo obtido por download anteriormente, o CMGAu funciona da mesma forma, independentemente de como você o inicia, o que significa que a operação é a mesma quer você clique duas vezes no .exe para iniciar o utilitário, inicie o utilitário sem qualquer opção em uma linha de comando ou inicie o utilitário usando a opção -f na linha de comando.

1. Abra um prompt de comando onde o CMGAu está localizado e digite **cmgau.exe**.
2. Selecione **Sim**, **trabalhar offline com um arquivo obtido por download anteriormente**. Clique em **Avançar >**.
3. Em *Arquivo baixado*, navegue até o local do material de chave salvo. Este arquivo foi salvo ao usar o Utilitário Administrativo de Download.

   Em *Senha*, digite a senha usada para proteger o arquivo do material de chave. Esta senha foi definida ao usar o Utilitário Administrativo de Download.

   Clique em **Avançar >**.

   Uma mensagem indicando que o material de chave foi desbloqueado corretamente é mostrada. Os arquivos estão acessíveis agora.
4. **Após terminar de trabalhar com os arquivos criptografados**, clique em **Concluir**. *Após clicar em Concluir, os arquivos criptografados não estarão mais disponíveis.*

Executar o Fazer download agora no modo forense

1. Abra um prompt de comando onde o CMGAu está localizado e digite **cmgau.exe**.
2. Selecione **Não, fazer um download a partir de um servidor agora**. Clique em **Avançar >**.
3. Digite as informações a seguir (alguns campos podem já estar preenchidos).

Opção	Descrição
URL de servidor de dispositivo:	URL de servidor de dispositivo totalmente qualificado. Caso o seu Dell Server seja anterior à v7.7, o formato será https://deviceserver.domain.com:8081/xapi Caso o seu Dell Server seja v7.7 ou mais recente, o formato será https://deviceserver.domain.com:8443/xapi/
Admin Dell:	Nome do administrador com credenciais de administrador forense, como, por exemplo, jdoe (Ativado no Management Console)

Opção	Descrição
Senha:	Senha do administrador forense
MCID:	ID da máquina, por exemplo, IDdemaquina.dominio.com
DCID:	Oito primeiros dígitos da ID Shield de 16 dígitos

Clique em **Avançar >.**

Uma mensagem indicando que o material de chave foi desbloqueado corretamente é mostrada. Os arquivos estão acessíveis agora.

4 **Após terminar de trabalhar com os arquivos criptografados**, clique em **Concluir**. *Após clicar em **Concluir**, os arquivos criptografados não estarão mais disponíveis.*

Executar o Fazer download agora no modo administrativo

1 Abra um prompt de comando onde o CMGAu está localizado e digite **cmgau.exe -a**.

2 Selecione **Não, fazer um download a partir de um servidor agora**. Clique em **Avançar >**.

3 Digite as informações a seguir (alguns campos podem já estar preenchidos).

Parâmetros do modo administrativo	Descrição
Servidor:	Nome de Host totalmente qualificado do Key Server, por exemplo, keyserver.domonio.com
Número da porta:	A porta padrão é 8050
Conta do servidor:	O usuário de domínio em que o Key Server está executando. O formato é DOMÍNIO\Nome de usuário. O usuário de domínio executando o utilitário precisa estar autorizado a fazer download do Key Server.
MCID:	ID da máquina, por exemplo, IDdemaquina.dominio.com
DCID:	Oito primeiros dígitos da ID Shield de 16 dígitos

Clique em **Avançar >**.

Uma mensagem indicando que o material de chave foi desbloqueado corretamente é mostrada. Os arquivos estão acessíveis agora.

4 **Após terminar de trabalhar com os arquivos criptografados**, clique em **Concluir**. *Após clicar em **Concluir**, os arquivos criptografados não estarão mais disponíveis.*