Dell Data Protection | Encryption

Utilidades administrativas

© 2014 Dell, Inc.

Marcas comerciales utilizadas en el conjunto de documentos de DDP|E, DDP|ST y DDP|CE: Dell™ y su logotipo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® y KACE™ son marcas de Dell, Inc. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® y Xeon® son marcas de Intel Corporation en Estados Unidos y otros países. Adobe®, Acrobat® y Flash® son marcas de Adobe Systems Incorporated. Authen Tec® y Eikon® son marcas de Authen Tec. AMD® es marca de Advanced Micro Devices, Inc. Microsoft®, Windows®, y 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® y Visual C++® son marcas de Microsoft Corporation en Estados Unidos u otros países. VMware® es marca de VMware, Inc. en Estados Unidos u otros países. Box® es marca de Box. Dropbox℠ es marca de servicios de Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® y Google™ Play son marcas de Google, Inc. en Estados Unidos y otros países. Apple®, Aperture®, App Store℠, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®℠, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® y Siri® son marcas, algunas de ellas de servicios, de Apple, Inc. en Estados Unidos u otros países. GO ID®, RSA® y SecurID® son marcas de EMC Corporation. EnCase™ y Guidance Software® son marcas de Guidance Software. Entrust® es marca de Entrust®, Inc. en Estados Unidos y otros países. InstallShield® es marca de Flexera Software en Estados Unidos, China, Unión Europea, Hong Kong, Japón, Taiwán y Reino Unido. Micron® y RealSSD® son marcas de Micron Technology, Inc. en Estados Unidos y otros países. Mozilla® Firefox® es marca de Mozilla Foundation en Estados Unidos u otros países. iOS® se utiliza con licencia y es marca de Cisco Systems, Inc. en Estados Unidos y otros países. Oracle® y Java® son marcas de Oracle o sus filiales. Los demás nombres utilizados pueden ser marcas de sus respectivos titulares. SAMSUNG™ es marca de SAMSUNG en Estados Unidos u otros países. Seagate® es marca de Seagate Technology, LLC en Estados Unidos u otros países. Travelstar® es marca de HGST, Inc. en Estados Unidos y otros países. UNIX® es marca de The Open Group. VALIDITY™ es marca de Validity Sensors, Inc. en Estados Unidos y otros países. VeriSign® y los nombres relacionados son marcas de VeriSign, Inc. o sus filiales o compañías controladas, en Estados Unidos y otros países, y cuentan con licencia a favor de Symantec Corporation. KVM on IP® es marca de Video Products. Yahoo!® es marca de Yahoo! Inc.

Este producto utiliza partes del programa 7-Zip. El código fuente puede consultarse en www.7-zip.org.
La licencia se encuentra sujeta a las restricciones de licencia GNU LGPL y unRAR (www.7-zip.org/license.txt).

2014-05

Protegido por una o varias patentes de Estados Unidos, entre otras: Número 7665125; Número 7437752; y Número 7665118.

La información en este documento está sujeta a cambios sin aviso previo.

Contenido

1

Utilidad administrativa para descargas

Esta utilidad permite la descarga de un paquete de material de clave para usarse en computadoras que no estén conectadas a un Enterprise Server. Las utilidades Admin pueden usar entonces, sin conexión, estos paquetes.

Esta utilidad emplea uno de los siguientes métodos para descargar el paquete de material de clave, dependiendo del parámetro utilizado en la línea de comandos:

- Modo admin: Se usa si se coloca **-a** en la línea de comandos o si no se usa otro parámetro de línea de comandos.
- Modo forense: Se usa si se coloca **-f** en la línea de comandos.

Los archivos de registro pueden ubicarse en:

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

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

Uso de la utilidad administrativa para descargas en modo Admin

1. Haga doble clic en **cmgad.exe** para iniciar la utilidad.

   o bien

   En la ubicación donde se encuentra la utilidad administrativa para descargas, abra una ventana de comandos y escriba **cmgad.exe -a** (o cmgad.exe).

2. Introduzca la información siguiente (es posible que algunos campos ya estén completos).

Servidor:	Nombre de host completo de Key Server; por ejemplo, keyserver.domain.com
N.º de puerto:	El puerto predeterminado es 8050
Cuenta del servidor:	El usuario del dominio que Key Server está usando. El formato es dominio\nombre de usuario. El usuario del dominio que ejecuta la utilidad debe estar autorizado para realizar la descarga desde el servidor de claves
MCID:	ID del equipo; por ejemplo, machineID.domain.com
DCID:	Los primeros ocho dígitos de la ID de Shield de 16 dígitos

   Haga clic en **Siguiente >**.

3. En el campo **Frase de contraseña:**, indique una frase de contraseña para proteger el archivo de descarga. La frase debe tener al menos ocho caracteres, con al menos uno alfabético y otro numérico.

   Confirme la frase de contraseña.

   Puede aceptar el nombre predeterminado y la ubicación donde se guardará el archivo o hacer clic en **...** para seleccionar una ubicación distinta.

   Se mostrará un mensaje que indica que el material de clave se ha desbloqueado con éxito. Ahora puede acceder a los archivos.

4. Una vez que finalice, haga clic en **Finalizar**.

Uso de la utilidad administrativa para descargas en modo forense

1. En la ubicación donde se encuentra la utilidad administrativa para descargas, abra una ventana de comandos y escriba **cmgad.exe -f**.
2. Introduzca la información siguiente (es posible que algunos campos ya estén completos).

   URL del Device Server: URL completo del Device Server

   Si su Enterprise Server es pre-v7.7, el formato es https://deviceserver.domain.com:8081/xapi

   Si su Enterprise Server es v7.7 o posterior, el formato es https://deviceserver.domain.com:8443/xapi/

   Dell Admin: Nombre del administrador con derechos de administrador forense (se configura en Enterprise Server); por ejemplo, jdoe

   Contraseña: Contraseña del administrador forense

   MCID: ID del equipo; por ejemplo, machineID.domain.com

   DCID: Los primeros ocho dígitos de la ID de Shield de 16 dígitos

   Haga clic en **Siguiente >**.
3. En el campo **Frase de contraseña:**, indique una frase de contraseña para proteger el archivo de descarga. La frase debe tener al menos ocho caracteres, con al menos uno alfabético y otro numérico.

   Confirme la frase de contraseña.

   Puede aceptar el nombre predeterminado y la ubicación donde se guardará el archivo o hacer clic en **...** para seleccionar una ubicación distinta.

   Se mostrará un mensaje que indica que el material de clave se ha desbloqueado con éxito. Ahora puede acceder a los archivos.
4. Una vez que finalice, haga clic en **Finalizar**.

2

Utilidad administrativa para iniciar tareas

Esta utilidad de línea de comandos permite a los administradores desbloquear archivos encriptados tanto por clave común como de usuario, aun cuando se esté ejecutando un proceso.

La utilidad se emplea para ejecutar tareas desde la consola de administración. Además, debe copiarse a la computadora cliente. Para ejecutar la utilidad, cualquier tarea que necesite acceder a los archivos encriptados se modifica direccionando la línea de comandos de la tarea a la utilidad. Una vez que el proceso finalice, la utilidad se cierra.

Esta utilidad emplea uno de los siguientes métodos para desbloquear archivos, dependiendo del parámetro utilizado en la línea de comandos:

- Modo Admin - No se requiere interruptor.
- Modo forense: Se usa si se coloca **-f** en la línea de comandos.
- Modo archivo de copia de seguridad: Se usa si se coloca **-b** en la línea de comandos.

Los archivos de registro pueden ubicarse en:

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

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

Uso de la utilidad administrativa para iniciar tareas en modo Admin

Sintaxis del modo Admin

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

Parámetros del modo Admin	Descripción
-k	Indica que debe usarse Kerberos (Modo Admin). CmgAlu requiere la opción -k para trabajar en Modo Admin.
X	Nivel de registro. Los niveles de registro van del 0 al 5 (el cero no incluirá registros y el cinco es el nivel de depuración).
ServerPrincipal	Cuenta AD (cuenta de dominio) que el servidor de claves está usando.
Port	Puerto TCP para conectarse al servidor de claves.
Server	Nombre o dirección IP del servidor de claves.
-r	Ordena a la utilidad la carga del nombre del servidor de claves y la MCID (o SCID) del equipo desde el registro. Si no se especifica el parámetro –r, deben indicarse el nombre del servidor de claves y la MCID (o SCID).
MCID	ID del dispositivo para desbloquear. MCID también se conoce como la ID única del dispositivo o nombre de host.

Parámetros del modo Admin	Descripción
SCID	ID de Shield del dispositivo para desbloquear. SCID también se conoce como DCID o ID de recuperación.
-?	Ayuda para el uso de la línea de comandos.

Uso de la utilidad administrativa para iniciar tareas en modo forense

Sintaxis del modo forense

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

Parámetros del modo forense	Descripción
-f	Indica que debe usarse el modo forense.
AdminName	Nombre de usuario del administrador con derechos de administrador forense.
AdminPwd	Contraseña del administrador forense.
URL	URL de Device Server totalmente calificada. Si su Enterprise Server es pre-v7.7, el formato es https://deviceserver.domain.com:8081/xapi Si su Enterprise Server es v7.7 o posterior, el formato es https://deviceserver.domain.com:8443/xapi/
-r	Ordena a la utilidad la carga del URL del Device Server y la MCID (o SCID) del equipo desde el registro. Si no se especifica el parámetro –r, deben indicarse el URL/Servidor y la MCID (o SCID).
X	Nivel de registro. Los niveles de registro van del 0 al 5 (el cero no incluirá registros y el cinco es el nivel de depuración).
MCID	ID del dispositivo para desbloquear. MCID también se conoce como la ID única del dispositivo o nombre de host.
SCID	ID de Shield del dispositivo para desbloquear. SCID también se conoce como DCID o ID de recuperación.
-?	Ayuda para el uso de la línea de comandos.

Uso de la utilidad administrativa para iniciar tareas en modo archivo de copia de seguridad

Sintaxis del modo archivo de copia de seguridad

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

Parámetros del modo archivo de copia de seguridad	Descripción
X	Nivel de registro. Los niveles de registro van del 0 al 5 (el cero no incluirá registros y el cinco es el nivel de depuración).
-b"FilePath"	La ruta del sistema de archivos en el archivo de copia de seguridad, por lo general, ya sea un LSA archivo de recuperación o un archivo de salida descargado de CmgAd.
BackupPwd	La contraseña utilizado para crear archivo de copia de seguridad.
-?	Ayuda para el uso de la línea de comandos.

3

Utilidad administrativa de desbloqueo

Esta utilidad le permite acceder a los archivos encriptados por clave SDE, común o de usuario en una unidad esclava, una computadora en un entorno preinstalado o donde un usuario activado no haya iniciado sesión.

Esta utilidad usa el siguiente método para descargar un paquete de material de clave:

- Modo Admin - No se requiere interruptor. Este es el modo predeterminado.
- Modo forense: Se usa si se coloca **-f** en la línea de comandos.

Los archivos de registro pueden ubicarse en:

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

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

Utilice la utilidad administrativa de desbloqueo para trabajar sin conexión con un archivo previamente descargado

Si elige trabajar sin conexión con un archivo previamente descargado, CMGAu funciona de la misma manera, sin importar cómo lo inicie, lo que significa que el funcionamiento es el mismo sin importar si hace doble clic en el archivo ejecutable (.exe) para iniciar la utilidad, si lo inicia sin ningún interruptor en una línea de comandos o si lo hace usando el interruptor -f en la línea de comandos.

1. Haga doble clic en **cmgau.exe** para iniciar la utilidad.
2. Seleccione la opción **Sí, trabajar sin conexión con un archivo descargado previamente**. Haga clic en **Siguiente >**.
3. En el campo **Archivo descargado:**, busque la ubicación del archivo de material de claves. Este archivo se guardó con la utilidad administrativa para descargas.

   En el campo **Frase de contraseña:**, indique la frase de contraseña usada para proteger el archivo de material de claves. La contraseña se estableció con la utilidad administrativa para descargas.

   Haga clic en **Siguiente >**.

   Se mostrará un mensaje que indica que el material de clave se ha desbloqueado con éxito. Ahora puede acceder a los archivos.
4. Una vez que termine de trabajar con los archivos encriptados, haga clic en **Terminar**. *Una vez que haya hecho clic en Terminar, los archivos encriptados ya no estarán disponibles.*

Utilice la utilidad administrativa de desbloqueo para llevar a cabo una descarga de un servidor que se encuentre en ese momento en modo Admin

1. Haga doble clic en **cmgau.exe** para iniciar la utilidad.

   o bien

   En la ubicación donde se encuentra la utilidad administrativa de desbloqueo, abra una ventana de comandos y escriba **cmgau.exe**.
2. Seleccione la opción **No, descargar del servidor ahora**. Haga clic en **Siguiente >**.

3 Introduzca la información siguiente (es posible que algunos campos ya estén completos).

Servidor:	Nombre de host completo de Key Server; por ejemplo, keyserver.domain.com
N.º de puerto:	El puerto predeterminado es 8050
Cuenta del servidor:	El usuario del dominio que Key Server está usando. El formato es dominio\nombre de usuario. El usuario del dominio que ejecuta la utilidad debe estar autorizado para realizar la descarga desde el servidor de claves
MCID:	ID del equipo; por ejemplo, machineID.domain.com
DCID:	Los primeros ocho dígitos de la ID de Shield de 16 dígitos

Haga clic en Siguiente >.

Se mostrará un mensaje que indica que el material de clave se ha desbloqueado con éxito. Ahora puede acceder a los archivos

4 Una vez que termine de trabajar con los archivos encriptados, haga clic en Terminar. *Una vez que haya hecho clic en Terminar, los archivos encriptados ya no estarán disponibles.*

Utilice la utilidad administrativa de desbloqueo para llevar a cabo una descarga de un servidor que se encuentre en ese momento en modo forense

1 En la ubicación donde se encuentra la utilidad administrativa de desbloqueo, abra una ventana de comandos y escriba cmgau.exe -f.

2 Seleccione la opción No, descargar del servidor ahora. Haga clic en Siguiente >.

3 Introduzca la información siguiente (es posible que algunos campos ya estén completos).

URL del Device Server:URL completo del Device Server.

Si su Enterprise Server es pre-v7.7, el formato es https://deviceserver.domain.com:8081/xapi

Si su Enterprise Server es v7.7 o posterior, el formato es https://deviceserver.domain.com:8443/xapi/

Dell Admin:	Nombre del administrador con derechos de administrador forense (se configura en Enterprise Server); por ejemplo, jdoe
Contraseña:	Contraseña del administrador forense
MCID:	ID del equipo; por ejemplo, machineID.dell.com
DCID:	Los primeros ocho dígitos de la ID de Shield de 16 dígitos

Haga clic en Siguiente >.

Se mostrará un mensaje que indica que el material de clave se ha desbloqueado con éxito. Ahora puede acceder a los archivos

4 Una vez que termine de trabajar con los archivos encriptados, haga clic en Terminar. *Una vez que haya hecho clic en Terminar, los archivos encriptados ya no estarán disponibles.*


0 XXXXXA0 X