

Dell Encryption

Admin Utilities



Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

© 2018 Dell Inc. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Registered trademarks and trademarks used in the Dell Encryption, Endpoint Security Suite Pro, Endpoint Security Suite Enterprise, and Data Guardian suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Cylance®, CylancePROTECT, and the Cylance logo are registered trademarks of Cylance, Inc. in the U.S. and other countries. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen Tec® and Eikon® are registered trademarks of Authen Tec. AMD® is a registered trademark of 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®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. DropboxSM is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari®, and Siri® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. GO ID®, RSA®, and SecurID® are registered trademarks of Dell EMC. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. InstallShield® is a registered trademark of Flexera Software in the United States, China, European Community, Hong Kong, Japan, Taiwan, and United Kingdom. Micron® and RealSSD® are registered trademarks of Micron Technology, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. SAMSUNG™ is a trademark of SAMSUNG in the United States or other countries. Seagate® is a registered trademark of Seagate Technology LLC in the United States and/or other countries. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc. This product uses parts of the 7-Zip program. The source code can be found at 7-zip.org. Licensing is under the GNU LGPL license + unRAR restrictions (7-zip.org/license.txt).

Admin Utilities

2017 - 08

Rev. A01

Contents

1 Introduction.....	4
Contact Dell ProSupport.....	4
2 Administrative Download Utility (CMGAd).....	5
Use Forensic Mode.....	5
Use Admin Mode.....	7
3 Administrative Launch Utility (CMGAlu).....	9
Use Forensic Mode.....	9
Forensic Mode Syntax.....	9
Use Admin Mode.....	10
Admin Mode Syntax.....	10
Use Backup File Mode.....	10
Backup File Mode Syntax.....	10
4 Administrative Unlock Utility (CMGAu).....	12
Work Offline With a Previously Downloaded File.....	12
Perform a Download Now in Forensic Mode.....	12
Perform a Download Now in Admin Mode.....	13

Introduction

This document describes utilities for encryption key retrieval and file access. The utilities offer the following functions:

Download Keys - CMGAd allows administrators to download a key material bundle for use on a computer that is not connected to a Dell Server.

Launch Jobs - The CMGAlu command allows administrators to unlock User or Common encrypted files on a computer while a process is running.

Unlock Files - CMGAu allows administrator to access User, Common, or SDE-encrypted files on a slaved drive, a computer booted in a pre-installed environment, or on a computer where an activated user is not logged in.

Contact Dell ProSupport

Call 877-459-7304, extension 4310039 for 24x7 phone support for your Dell product.

Additionally, online support for Dell products is available at dell.com/support. Online support includes drivers, manuals, technical advisories, FAQs, and emerging issues.

Be sure to help us quickly connect you to the right technical expert by having your Service Code available when you call.

For phone numbers outside of the United States, check [Dell ProSupport International Phone Numbers](#).

Administrative Download Utility (CMGAd)

This utility allows the download of a key material bundle for use on a computer that is not connected to a Dell Server. The Admin utilities can then use these offline bundles.

This utility uses one of the following methods to download a key bundle, depending on the command line parameter passed to the application:

- **Forensic Mode** - Used if **-f** is passed on the command line or if no command line parameter is used.
- **Admin Mode** - Used if **-a** is passed on the command line.

Log files can be located at C:\ProgramData\CmgAdmin.log

Use Forensic Mode

- 1 Double-click **cmgad.exe** to launch the utility or open a command prompt where CMGAd is located and type **cmgad.exe -f** (or **cmgad.exe**).
- 2 Enter the following information (some fields may be pre-populated).

Forensic Mode Parameters Description

Device Server URL	Fully qualified Security Server (Device Server) URL. The format is https://securityserver.domain.com:8443/xapi/. If your Dell Server is pre-v7.7, the format is https://deviceserver.domain.com:8081/xapi (different port number, without the trailing slash).
Dell Admin	Name of the administrator with forensic administrator credentials, such as jdoe (Enabled in the Management Console)
Password	Forensic administrator password
MCID	Machine ID, such as machineID.domain.com
DCID	First eight digits of the 16-digit Shield ID

TIP:

Specifying either the MCID or DCID is usually sufficient. However, if both are known, it is helpful to enter both. Each parameter contains different information used by this utility.

Click **Next**.

Dell Administrative Download

 Encryption

Device Server:

Dell Admin:

Password:

MCID:

DCID:


< Back Next > Cancel

- 3 In *Passphrase*, enter a passphrase to protect the download file. The passphrase must be at least eight characters long, and contain at least one alphabetic and one numeric character. Confirm the passphrase.

Either accept the default name and location of where the file will be saved to or click ... to select another location.

Click **Next**.

Dell Administrative Download

 Encryption

The download will be saved to a file, protected by a passphrase. Please enter the passphrase below.

Passphrase:

Confirm:

Download To: ...

< Back Next > Cancel

A message displays, indicating that the key material was successfully unlocked. Files are now accessible.


- 4 Click **Finish** when complete.

Use Admin Mode

The Security Management Server Virtual does not use the Key Server, so Admin mode cannot be used to obtain a key bundle from a Security Management Server Virtual. Use Forensic mode to obtain the key bundle if the client is activated against a Security Management Server Virtual.

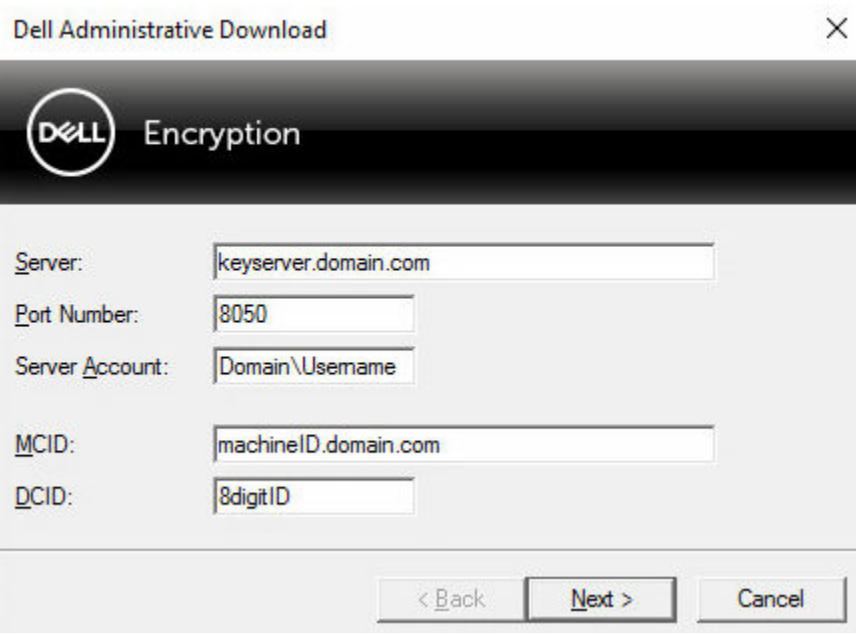
- 1 Open a command prompt where CMGAd is located and type **cmgad.exe -a**.
- 2 Enter the following information (some fields may be pre-populated).

Admin Mode Parameters Description	
Server:	Fully qualified hostname of the Key Server, such as keyserver.domain.com.
Port Number	The default port is 8050
Server Account	The domain user the Key Server is running as. The format is DOMAIN\Username. The domain user running the utility must be authorized to perform the download from the Key Server.
MCID	Machine ID, such as machineID.domain.com
DCID	First eight digits of the 16-digit Shield ID



TIP:
Specifying either the MCID or DCID is usually sufficient. However, if both are known, it is helpful to enter both. Each parameter contains different information used by this utility.

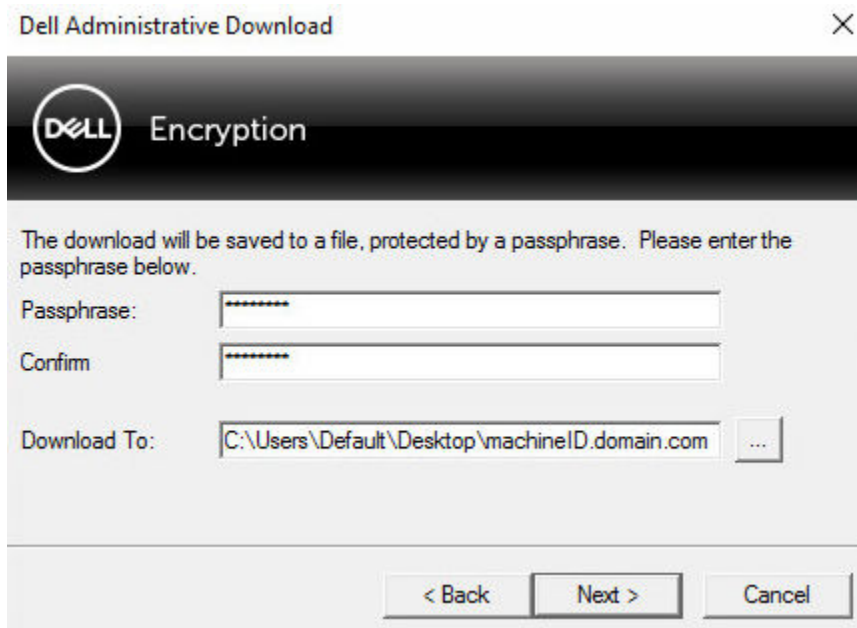
Click **Next**.



- 3 In *Passphrase*, enter a passphrase to protect the download file. The passphrase must be at least eight characters long, and contain at least one alphabetic and one numeric character.
Confirm the passphrase.

Either accept the default name and location of where the file will be saved or click ... to select another location.

Click **Next**.



A message displays, indicating that the key material was successfully unlocked. Files are now accessible.

- 4 Click **Finish** when complete.

Administrative Launch Utility (CMGAlu)

This utility enables administrators to unlock User or Common encrypted files on a computer while a process is running.

This utility is used to launch jobs from a management console. The utility must be copied to the target computer and any job that requires access to User or Common encrypted files is changed to run this utility, by passing the command line for the management job, to the utility. Once the process exits, the utility terminates.

This utility uses one of the following methods to unlock files, depending on the command line parameter passed to the application:

- **Forensic Mode** - Used if **-f** is passed on the command line, or if no parameter is passed on the command line.
- **Admin Mode** - Used if **-k** is passed on the command line.
- **Backup File Mode** - Used if **-b** is passed on the command line.

Log files can be located at C:\ProgramData\CmgAdmin.log

Use Forensic Mode

Forensic Mode Syntax

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

Forensic Mode Parameters	Description
-f	Indicates that Forensic mode is to be used.
-vX	X indicates the log level. Log levels are 0-5 (0 is no logs/5 is debug level).
AdminPwd	Forensic administrator password
AdminName	User name of the administrator with forensic administrator credentials
-r	Instructs the utility to load the Device Server URL and MCID (or SCID) of the computer from the registry. If -r is not specified, the URL/Server and MCID (or SCID) must be supplied.
URL	Fully qualified Device Server URL If your Dell Server is pre-v7.7, the format is https://deviceserver.domain.com:8081/xapi If your Dell Server is v7.7 or later, the format is https://deviceserver.domain.com:8443/xapi/
MCID	Device ID for the device to unlock. MCID is also known as the Device Unique ID or hostname.
SCID	Shield ID for the device to unlock.

Forensic Mode Parameters	Description
	SCID is also known as DCID or Recovery ID.
-?	Command line help.

Use Admin Mode

Admin Mode Syntax

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

Admin Mode Parameters	Description
-k	Indicates that Kerberos (Admin mode) is to be used. CmgAlu requires the -k flag to operate in Admin mode.
-vX	X indicates the log level. Log levels are 0-5 (0 is no logs/5 is debug level).
ServerPrincipal	AD Account (Domain Account) the Key Server is running under.
Port	TCP Port to connect to the Key Server on.
Server	Key Server Name/IP Address.
-r	Instructs the utility to load the Key Server Name and MCID (or SCID) of the computer from the registry. If -r is not specified, the Key Server Name and MCID (or SCID) must be supplied.
MCID	Device ID for the device to unlock. MCID is also known as the Device Unique ID or hostname.
SCID	Shield ID for the device to unlock. SCID is also known as DCID or Recovery ID.
-?	Command line help.

Use Backup File Mode

Backup File Mode Syntax

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

Backup File Mode Parameters	Description
-vX	X indicates the log level. Log levels are 0-5 (0 is no logs/5 is debug level).
-b"FilePath"	The file system path to the backup file, typically either an LSA recovery file or an output file downloaded from CMGAd.
-BackupPwd	The password used to create the backup file.

Backup File Mode Parameters**Description**

-?

Command line help.

Administrative Unlock Utility (CMGAu)

This utility allows access to User, Common, or SDE encrypted files on a slaved drive, a computer booted in a pre-installed environment, or on a computer where an activated user is not logged in.

This utility uses the following method to download a key material bundle:

- **Forensic Mode** - Used if **-f** is passed on the command line, or if no command line parameter is used.
- **Admin Mode** - Used if **-a** is passed on the command line.

Log files can be located at C:\ProgramData\CmgAdmin.log

Work Offline With a Previously Downloaded File

If you choose to work offline with a previously downloaded file, CMGAu works the same way, no matter how you launch it, meaning the operation is the same whether you double-click the .exe to launch the utility, launch it without any switch in a command line or launch it using the -f switch in the command line.

- 1 Open a command prompt where CMGAu is located and type **cmgau.exe**.
- 2 Select **Yes, work offline with a previously downloaded file**. Click **Next >**.
- 3 In *Downloaded file*, browse to the location of the saved key material. This file was saved when using the Administrative Download Utility.

In *Passphrase*, enter the passphrase that was used to protect the key material file. This passphrase was set when using the Administrative Download Utility.

Click **Next >**.

A message displays, indicating that the key material was successfully unlocked. Files are now accessible.

- 4 **Once you are finished working with the encrypted files**, click **Finish**. *After you click Finish, the encrypted files are no longer available.*

Perform a Download Now in Forensic Mode

- 1 Open a command prompt where CMGAu is located and type **cmgau.exe**.
- 2 Select **No, perform a download from a server now**. Click **Next >**.
- 3 Enter the following information (some fields may be pre-populated).

Option	Description
Device Server URL:	Fully qualified Device Server URL. If your Dell Server is pre-v7.7, the format is https://deviceserver.domain.com:8081/xapi If your Dell Server is v7.7 or later, the format is https://deviceserver.domain.com:8443/xapi/
Dell Admin:	Name of the administrator with forensic administrator credentials, such as jdoe (Enabled in the Management Console)
Password:	Forensic administrator password

Option	Description
MCID:	Machine ID, such as machineID.domain.com
DCID:	First eight digits of the 16-digit Shield ID

Click **Next >**.

A message displays, indicating that the key material was successfully unlocked. Files are now accessible.

- 4 **Once you are finished working with the encrypted files**, click **Finish**. *After you click **Finish**, the encrypted files are no longer available.*

Perform a Download Now in Admin Mode

- 1 Open a command prompt where CMGAu is located and type **cmgau.exe -a**.
- 2 Select **No, perform a download from a server now**. Click **Next >**.
- 3 Enter the following information (some fields may be pre-populated).

Admin Mode Parameters Description

Server:	Fully qualified hostname of the Key Server, such as keyserver.domain.com
Port Number:	The default port is 8050
Server Account:	The domain user the Key Server is running as. The format is DOMAIN\Username. The domain user running the utility must be authorized to perform the download from the Key Server.
MCID:	Machine ID, such as machineID.domain.com
DCID:	First eight digits of the 16-digit Shield ID

Click **Next >**.

A message displays, indicating that the key material was successfully unlocked. Files are now accessible.

- 4 **Once you are finished working with the encrypted files**, click **Finish**. *After you click **Finish**, the encrypted files are no longer available.*