

Dell Data Security

EnCase Integration Guide



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.

© 2012-2018 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).

EnCase Integration Guide

2018 - 03

Rev. A01

Contents

1 Introduction.....	4
Contact Dell ProSupport.....	4
2 Integrate with EnCase.....	5
Enable the EnCase API.....	5
Install EnCase Integration Adapter.....	5
3 Use Dell Data Security with EnCase.....	6
4 Use EnCase with Dell Data Security.....	7
CEGetBundle.....	7



Introduction

Dell Data Security integrates with EnCase v6.15 digital forensic products from Guidance Software, Inc. to support online investigations of Dell-encrypted files. With this integration, forensic investigators can view, export, or search within Dell-secured data. With proper Forensic Administrator credentials, all Dell-secured data, regardless of the keys used to encrypt it, are decrypted and presented to the investigator without additional interaction. EnCase's Secure Storage saves and stores the Forensic Administrator credentials with the case, eliminating the need to re-enter them.

EnCase v6.15 (32-bit) forensic integration supports:

- Dell Data Security Encryption Enterprise for Windows v7.0.x or later
- Dell Security Management Server v7.0.1 or later

NOTE: Dell Data Security Encryption Enterprise for Mac does not support EnCase forensic investigation.

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 Tag or Express Service Code available when you call.

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

Integrate with EnCase

Enable the EnCase API

NOTE: Do not use this API with Dell Device Servers deployed in a DMZ. Use an internal Dell Device Server with restricted access for EnCase integration to maintain security.

Pre v7.7 Security Management Server

- 1 Open **<Dell install dir>\Enterprise Edition\Device Server\conf\context.properties**.
- 2 Enable the forensic integration API.

`service.forensic.enable=true`
- 3 Stop and restart the Dell Device Server from the Start Menu.

To disable forensic integration, set `service.forensic.enable=false`.

v7.7 Security Management Server and Later

- This service is enabled in the Dell Server by default.
- To disable forensic integration, set `xapi.service.forensic.enable=false`.

Stop and restart the Dell Device Server from the Start Menu.

Install EnCase Integration Adapter

- 1 On a computer running EnCase, double-click **CMGEnCaseIntegration.exe**.
- 2 When the Library Installer dialog displays, ensure that the target EnCase folder is correct.
- 3 Click **Finish** to extract CEGetBundle and Integration Adapter files to `\Program Files\EnCase6\Lib\Credant Technologies\CMG`



Use Dell Data Security with EnCase

Get Encryption Keys

Use the EnCase Enterprise user interface to get encryption keys from the Dell Remote Management Console and decrypt all Dell-encrypted data for this computer or evidence file.

- 1 Select the **Online** check box.
- 2 Type the **Username** of the Forensic Administrator.
- 3 Type the **Password** of the Forensic Administrator.
- 4 Type the URL to the Del Server with the EnCase API enabled. For example:

`https://cred01.somedomain.com:8443/xapi/` (if your Security Management Server is v7.7 or later)

`https://cred01.somedomain.com:8081/xapi` (if your Security Management Server is pre-v7.7)

Locate the Dell Server URI at HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet

NOTE: The Dell Server must have the EnCase API enabled to export keys. You may optionally deploy an alternate Dell Device Server exclusively for EnCase integration.

- 5 Type the Machine ID (also known as MCID and Unique ID) for the target computer or evidence file.

Locate the MCID in the registry of the target computer at HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield

from the Dell Remote Management Console, in the left pane, click **Populations > Endpoints**

- Click the Details icon of the appropriate device.
- From the top menu, click **Details & Actions**.
- Locate the Unique ID in the *Endpoint Detail* area.

- 6 Type the Shield ID (also known as Device ID, DCID, Recovery ID, or SCID) for the target computer or evidence file.

Locate the DCID in the registry of the target computer at HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield

from the Dell Remote Management Console, in the left pane, click **Populations > Endpoints**

- Click the **Details** icon of the appropriate device.
- From the top menu, click **Details & Actions**.
- Locate the Recovery ID in the *Shield* area.

NOTE: Specify the MCID, DCID, or both IDs. The imported case contains all key material for the specified Machine ID, Shield ID, or both IDs.

- 7 Click **OK**.

Decryption is now in-progress.

Once decryption is complete, the files are accessible for forensic examination. Decrypted files are only viewable through the EnCase module, the original source files remain unaltered and encrypted.

Use EnCase with Dell Data Security

CEGetBundle

CEGetBundle is a utility which allows forensic administrators to pull key material from a Dell Server. This utility is available through Dell ProSupport.

The following table details the parameters available for the installation.

Parameters

-L=Legacy mode for exporting keys from a CMG 5.3.x Server

URL =Device Server URL (<securityserver.organization.com>)

AdminName=Administrator username

AdminPwd=Administrator password

AdminDomain=Administrator domain

MCID=Machine ID for the target device (also known as the Unique ID or hostname)

SCID=Shield Credant ID for the target Shield (also known as DCID or Recovery ID)

Username=User targeted for key material export (legacy mode only)

OutputFile=Filename for the exported key bundle

OutputPwd = Password for the exported key bundle

-R=Use backup file mode

BackupFile=The executable containing backup keys

BackupPwd=The administrator password used for the backup file

NOTE: The AdminDomain parameter should be supplied only for exporting keys from CMG Enterprise Edition 6.0 and later servers configured to support multiple domains.

NOTE: In legacy mode, the MCID, SCID, and Username must be specified. The key material for only the specified user will be appended to the output file. You must run this tool with the same output filename for each user on the device targeted for decryption if user or user-roaming encryption is enabled. Each user's key material will be appended to the output file.

Example Command Line

- The following example uses the MCID, SCID, or both. All key material associated with the specified machine (MCID), or SCID, or both will be saved to the output file which will be overwritten if it exists.

```
CEGetBundle [-L] -XURL -aAdminName -AAdminPwd [-DAdminDomain] [-dMCID] [-sSCID] [-uUsername] -oOutputFile -iOutputPwd
```



- The following example extracts key material from the backup file exported by the installer.

```
CEGetBundle -R -bBackupFile -ABackupPwd -oOutputFile -iOutputPwd
```

