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.

EnCase Integration Guide

2018 - 03

Rev. A01

Contents

1

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.

2

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
```