Dell Encryption

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.

2019 - 08

Rev. A01

Contents

1

Introduction

Dell Encryption integrates with EnCase v6.15 digital forensic products from Guidance Software, Inc. to support online investigations of encrypted files. With this integration, forensic investigators can view, export, or search within Dell Encryption-secured data. With proper forensic administrator credentials, all Dell Encryption-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:

- Encryption Enterprise for Windows v7.0.x or later
- Security Management Server and Security Management Server Virtual v7.0.1 or later

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

Topics:

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, see Dell ProSupport International Phone Numbers.

2

Integrate with EnCase

Enable the EnCase API

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

Security Management Server pre-v7.7

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 Security Server.

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

Security Management Server v7.7 and Later

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

  Stop and restart the Security 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

3

Use Dell Encryption 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 Dell 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 URl 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 Security Server exclusively for EnCase integration.
5. Enter the Machine ID (also known as MCID and Unique ID) for the target computer or evidence file.

   Locate the MCID at either:

   - The registry of the target computer at:
     - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield

   Or

   - Management Console
     a. In the left pane, click **Populations > Endpoints**.
     b. Click the Details icon of the appropriate device.
     c. From the top menu, click **Details & Actions**.
     d. Locate the Unique ID in the *Endpoint Detail* area.
6. Enter the Shield ID (also known as Device ID, DCID, Recovery ID, or SCID) for the target computer or evidence file.

   Locate the DCID at either:

   - The registry of the target computer at:
     - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield

   Or

   - Management Console
     a. In the left pane, click **Populations > Endpoints**.
     b. Click the Details icon of the appropriate device.
     c. From the top menu, click **Details & Actions**.
     d. 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.

4

Use EnCase with Dell Encryption

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 (Parameters are case sensitive)
-L = Legacy mode for exporting keys from a CMG 5.3.x Server
-X = URL for the Security Server (Default Security Server for a server at “SecurityServer.Organization.Com would be: https://securityserver.organization.com:8443/xapi/)
-a = AdminName, an account defined within the Security Management Server with forensic administrator rights, account user name
-A = AdminPwd, an account defined within the Security Management Server with forensic administrator rights, account password
-D = AdminDomain, the domain for the username that is defined within the Security Management Server with Forensic Administrator rights
-d = MCID, Machine ID for the target device (also known as the Unique ID or FQDN of the device)
-s = SCID, Shield ID for the target device (also known as DCID or Recovery ID, can be found by using WSScan to find a “Common” key encrypted file)
-u = Username, User targeted for key material export (legacy mode only)
-o = OutputFile, File name for the exported key bundle
-i = OutputPwd, Password for the exported key bundle
-R = Use backup file mode
-b = BackupFile, The previously downloaded keybundle containing the encryption keys
-A = 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 are saved to the output file which is overwritten if it exists.

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

  The following details the previous example command with example parameter values: `CEGetBundle.exe -L -Xhttps://cred01.domain.com:8081/xapi -ajsmith -Achangeit -dmachine774.somedomain.com -sALD25WL7 -ucstevens -o"C:\temp\KeyBundle.bin" -iKeyP@ssw0rd`

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

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

The following details the previous example command with example parameter values: `CEGetBundle.exe -b"C:\temp\BackupFile.exe" -Aabc123456 -o"C:\temp2\KeyBundle.bin" -iKeyP@ssw0rd`

- The following example downloads the KeyBundle for the device Test1.domain.com with RecoveryID 1A2S3D4F using the forensic administrator A-Admin1@Dom-ain.com:

```
CEGetBundle -Xhttps://server.domain.com:8443/xapi/ -a"A-Admin@Dom-ain.com" -AP@ssw0rd!123 -dTest1.domain.com -s1A2S3D4F -o"C:\OutputFolder\File Name.bin" -i3ncryp73d
```