Dell Data Security

EnCase 統合ガイド

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示しています。

EnCase 統合ガイド

2018 - 03

Rev. A01

目次

1

はじめに

Dell Data Security は、デル暗号化ファイルのオンライン調査に対応できるように、Guidance Software, Inc. の EnCase v6.15 デジタルフォレンジック製品と統合されます。この統合により、フォレンジック調査担当者は、デルで保護されたデータの表示、エクスポート、検索ができるようになります。適切なフォレンジック管理者資格情報を有していれば、暗号化の際に使用したキーにかかわらず、デルで保護されたすべてのデータが復号化されて調査担当者に表示されます。余分な操作は一切必要ありません。EnCase の Secure Storage にフォレンジック管理者の資格情報が大文字小文字を区別して格納保存されるため、再入力の必要はありません。

EnCase v6.15（32 ビット）フォレンジック統合のサポート対象は次のとおりです。

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

メモ: Dell Data Security Encryption Enterprise for Mac は EnCase フォレンジック調査をサポートしません。

Dell ProSupport へのお問い合わせ

デル製品向けの 24 時間 365 日対応電話サポート（877-459-7304、内線 4310039）にご連絡ください。

さらに、デル製品のオンラインサポートも dell.com/support からご利用いただけます。オンラインサポートでは、ドライバ、マニュアル、テクニカルアドバイザリー、よくあるご質問（FAQ）、および緊急の問題を取り扱っています。

適切なサポート担当者に迅速におつなぎするためにも、お電話の際はお客様のサービスタグまたはエクスプレスサービスコードをご用意ください。

米国外の電話番号については、Dell ProSupport の国際電話番号をチェックしてください。

2

EnCase との統合

EnCase API の有効化

メモ: DMZ に展開している Dell デバイスサーバには、この API を使用しないでください。セキュリティ維持のため、内部で使用する Dell デバイスサーバでは、統合した EnCase へのアクセスを制限してください。

v7.7 より前の Security Management Server の場合

1 **<Dell install dir>\Enterprise Edition\Device Server\conf\context.properties** を開きます。

2 フォレンジック統合 API を有効化します。

service.forensic.enable=true

3 スタート メニューから、Dell デバイスサーバを停止して再起動します。

フォレンジック統合を無効化するには、次のように指定します：set service.forensic.enable=false。

v7.7 以降の Security Management Server の場合

- このサービスは、Dell サーバでデフォルトで有効になっています。
- フォレンジック統合を無効化するには、次のように指定します：set xapi.service.forensic.enable=false。

スタート メニューから、Dell デバイスサーバを停止して再起動します。

EnCase 統合アダプタのインストール

1 EnCase を実行しているコンピュータで、**CMGEnCaseIntegration.exe** をダブルクリックします。

2 ライブラリインストーラのダイアログが表示されたら、ターゲットの EnCase フォルダが正しいことを確認します。

3 **終了** をクリックして、CEGetBundle ファイルと統合アダプタファイルを \Program Files\EnCase6\Lib\Credant Technologies\CMG に解凍します。

3

EnCase が統合された Dell Data Security の使用方法

暗号化キーの取得

EnCase Enterprise ユーザーインタフェースを使用して Dell リモート管理コンソールから暗号化キーを取得し、このコンピュータまたはエビデンスファイルのためにデル暗号化データを復号化します。

1 **オンライン** チェックボックスを選択します。
2 フォレンジック管理者の **ユーザー名** を入力します。
3 フォレンジック管理者の **パスワード** を入力します。
4 EnCase API が有効化されている Dell サーバの URL を入力します。次に例を示します。

https://cred01.somedomain.com:8443/xapi/（Security Management Server が v7.7 以降の場合）

https://cred01.somedomain.com:8081/xapi（Security Management Server が v7.7 より前の場合）

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet で、Dell サーバ URI を見つけます。

メモ: キーをエクスポートするため、Dell サーバでは EnCase API が有効化されている必要があります。オプションとして、EnCase 統合専用に使用する Dell デバイスサーバを別にもう 1 台用意する方法もあります。

5 ターゲットコンピュータまたはエビデンスファイルのマシン ID（MCID またはユニーク ID とも呼ぶ）を入力します。

Dell リモート管理コンソールで、HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield のターゲットコンピュータのレジストリにある MCID を見つけます。

左のペインで、**ポピュレーション** > **エンドポイント** をクリックします。

- 適切なデバイスの 詳細 アイコンをクリックします。
- 上部のメニューで、**詳細およびアクション** をクリックします。
- エンドポイントの詳細 エリアでユニーク ID を見つけます。

6 ターゲットコンピュータまたはエビデンスファイルのシールド ID（デバイス ID、DCID、リカバリ ID、SCID とも呼ぶ）を入力します。

Dell リモート管理コンソールで、HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield のターゲットコンピュータのレジストリにある DCID を見つけます。

左のペインで、**ポピュレーション** > **エンドポイント** をクリックします。

- 適切なデバイスの **詳細** アイコンをクリックします。
- 上部のメニューで、**詳細およびアクション** をクリックします。
- シールド エリアでリカバリ ID を見つけます。

メモ: MCID、DCID、または両方の ID を指定します。インポートしたケースには、指定したマシン ID、シールド ID、またはその両方の ID のすべてのキーマテリアルが含まれています。

7 **OK** をクリックします。

復号化が進行します。

復号化が完了すると、ファイルのフォレンジック調査が可能になります。復号化されたファイルは、EnCase モジュールを介してのみ表示できます。元のソースファイルは変更されず、暗号化されたままです。

4

Dell Data Security に統合された EnCase の使用方法

CEGetBundle

CEGetBundle は、フォレンジック管理者が Dell サーバからキーマテリアルを取得するためのユーティリティです。このユーティリティは Dell ProSupport から入手できます。

次の表は、インストールで使用できるパラメータの詳細です。

パラメータ
-L = レガシーモード（CMG 5.3.x サーバからキーをエクスポートするときに使用）
URL = デバイスサーバの URL（<securityserver.organization.com>）
AdminName = 管理者ユーザー名
AdminPwd = 管理者パスワード
AdminDomain = 管理者ドメイン
MCID = ターゲットデバイスのマシン ID（ユニーク ID またはホスト名とも呼ぶ）
SCID = ターゲットシールドのシールド Credant ID（DCID またはリカバリ ID とも呼ぶ）
Username = キーマテリアルをエクスポートするユーザー（レガシーモードのみ）
OutputFile = エクスポートしたキーバンドルのファイル名
OutputPwd = エクスポートしたキーバンドルのパスワード
-R = ユーザーバックアップファイルモード
BackupFile = バックアップキーを含む実行可能ファイル
BackupPwd = バックアップファイルに使用する管理者パスワード

メモ: AdminDomain パラメータは、複数ドメインをサポートするように設定された CMG Enterprise Edition 6.0 以降のサーバからキーをエクスポートする場合にのみ指定します。

メモ: レガシーモードでは、MCID、SCID、Username の指定は必須です。出力ファイルに追加されるキーマテリアルは、指定したユーザーのものに限られます。ユーザーまたはユーザーローミング暗号化が有効になっている場合、復号化対象デバイスでユーザーごとに同じ出力ファイル名でこのツールを実行する必要があります。各ユーザーのキーマテリアルは出力ファイルに追加されます。

コマンドラインの例

- 次の例では、MCID、SCID、またはその両方を使用しています。指定したマシン(MCID)、SCID、またはその両方に関連付けられたすべてのキーマテリアルが出力ファイルに保存されます。すでに出力ファイルが存在している場合は上書きされます。

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

- 次の例では、インストーラによってエクスポートされたバックアップファイルからキーマテリアルが抽出されます。

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