Dell Encryption

管理ユーティリティ

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。

Dell Encryption、Endpoint Security Suite Pro、Endpoint Security Suite Enterprise、および Data Guardian スイートのドキュメントに使用されている登録商標および商標（Dell™、Dell のロゴ、Dell Precision™、OptiPlex™、ControlVault™、Latitude™、XPS®、および KACE™）は、Dell Inc. の商標です。Cylance®、CylancePROTECT、および Cylance のロゴは、米国およびその他の国における Cylance, Inc. の登録商標です。McAfee® および McAfee のロゴは、米国およびその他の国における McAfee, Inc. の商標または登録商標です。Intel ®、Pentium ®、Intel Core Inside Duo®、Itanium®、および Xeon ® は米国およびその他の国における Intel Corporation の登録商標です。Adobe®、Acrobat®、および Flash® は、Adobe Systems Incorporated の登録商標です。Authen Tec® および Eikon® は、Authen Tec の登録商標です。AMD® は、詳細設定 Micro Devices, Inc. の登録商標です。Microsoft®、Windows®、および Windows Server®、Internet Explorer®、MS-DOS®、Windows Vista®、MSN®、ActiveX®、Active Directory®、Access®、ActiveSync®、BitLocker®、BitLocker To Go®、Excel®、Hyper-V®、Silverlight®、Outlook®、PowerPoint®、Skydrive®、SQL Serve®、および Visual C++® は、米国および / またはその他の国における Microsoft Corporation の商標または登録商標です。VMware® は、米国およびその他の国における VMware, Inc. の登録商標または商標です。Box® は、Box の登録商標です。DropboxSM は、Dropbox, Inc. のサービスマークです。Google™、Android™、Google™ Chrome™、Gmail™、YouTube®、および Google™ Play は、米国およびその他の国における Google Inc. の商標または登録商標のいずれかです。Apple®、Aperture®、App StoreSM、Apple Remote Desktop™、Apple TV®、Boot Camp™、FileVault™、iCloud®SM、iPad®、iPhone®、iPhoto®、iTunes Music Store®、Macintosh®、Safari®、および Siri® は、米国またはその他の国あるいはその両方における Apple, Inc. のサービスマーク、商標、または登録商標です。GO ID®、RSA®、および SecurID® は Dell EMC の登録商標です。EnCaseTM™ および Guidance Software® は、Guidance Software の商標または登録商標です。Entrust® は、米国およびその他の国における Entrust®, Inc. の登録商標です。InstallShield® は、米国、中国、欧州共同体、香港、日本、台湾、および英国における Flexera Software の登録商標です。Micron® および RealSSD® は、米国およびその他の国における Micron Technology, Inc. の登録商標です。Mozilla® Firefox® は、米国およびその他の国における Mozilla Foundation の登録商標です。IOS ® は同社の商標または米国およびその他の特定の国で Cisco Systems, Inc. の登録商標であり、ライセンスに使用されます。Oracle® および Java® は、Oracle および / またはその関連会社の登録商標です。その他の名称は、それぞれの所有者の商標である場合があります。SAMSUNG™ は、米国およびその他の国における SAMSUNG の商標です。Seagate® は、米国および / またはその他の国における Seagate Technology LLC の登録商標です。Travelstar® は、米国およびその他の国における HGST, Inc. の登録商標です。UNIX® は、The Open Group の登録商標です。VALIDITYTM™ は、米国およびその他の国における Validity Sensors, Inc. の商標です。VeriSign® およびその他の関連標章は、米国およびその他の国における VeriSign, Inc. またはその関連会社あるいは子会社の商標または登録商標であり、Symantec Corporation にライセンス供与されています。KVM on IP® は、Video Products の登録商標です。Yahoo!® は、Yahoo! Inc. の登録商標ですこの製品は、7-Zip プログラムの一部を使用しています。このソースコードは、7-zip.org に掲載されています。ライセンス供与は、GNU LGPL ライセンス + unRAR 制限（7-zip.org/license.txt）の対象です。

管理ユーティリティ

2017 - 08

Rev. A01

目次

1 はじめに 4
Dell ProSupport へのお問い合わせ 4

2 Administrative Download Utility（CMGAd） 5
フォレンジックモードの使用 5
管理者モードの使用 6

3 Administrative Launch Utility（CMGAlu） 7
フォレンジックモードの使用 7
フォレンジックモードの構文 7
管理者モードの使用 8
管理者モードの構文 8
バックアップファイルモードの使用 8
バックアップファイルモードの構文 8

4 Administrative Unlock Utility（CMGAu） 10
以前にダウンロードしたファイルに対するオフライン作業 10
フォレンジックモードでの 今すぐダウンロード の実行 10
管理者モードでの 今すぐダウンロード の実行 11

1

はじめに

本書では、暗号化キーの入手とファイルへのアクセスを行うユーティリティについて説明します。ユーティリティは次の機能を提供します。

キーのダウンロード - CMGAd を使用して、管理者はデルサーバに接続されていないコンピュータで使用するためのキーマテリアルのバンドルをダウンロードできます。

ジョブの起動 - CMGAlu コマンドを使用して、管理者はプロセスの実行中にコンピュータ上にあるユーザーによるまたは共通の暗号化済みファイルのロックを解除できます。

ファイルのロック解除 - CMGAu を使用して、管理者はスレーブドライブ、インストール前の環境で起動されたコンピュータ、またはアクティブ化されたユーザーがログインしていないコンピュータの、ユーザー、共通、SDE 暗号化済みファイルにアクセスできます。

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

Administrative Download Utility (CMGAd)

このユーティリティを使用して、デルサーバに接続していないコンピュータで使用するキーマテリアルのバンドルをダウンロードできます。Admin ユーティリティはその後これらのオフラインバンドルを使用できるようになります。

このユーティリティは、アプリケーションに渡されるコマンドラインパラメータに応じて、次のいずれかの方法を使用してキーバンドルをダウンロードします。

- **フォレンジックモード** - コマンドラインで **-f** が渡された場合、またはコマンドラインパラメータが使用されていない場合に使用されます。
- **管理者モード** - コマンドラインで **-a** が渡された場合に使用されます。

ログファイルは、C:\ProgramData\CmgAdmin.log にあります。

フォレンジックモードの使用

1 **cmgad.exe** をダブルクリックして、ユーティリティを起動するか、CMGAd が置かれている場所でコマンドプロンプトを開いて **cmgad.exe -f** (または **cmgad.exe**) と入力します。

2 次の情報を入力します (一部のフィールドは事前に入力されている場合があります)。

フォレンジックモードのパラメータ	説明
デバイスサーバの URL	セキュリティサーバ (デバイスサーバ) の完全修飾 URL。書式は、https://securityserver.domain.com:8443/xapi/ です。 お使いのデルサーバが v7.7 より前の場合は、書式は https://deviceserver.domain.com:8081/xapi (ポート番号が違う、末尾のスラッシュなし) です。
Dell Admin	JDOE など、フォレンジック管理者の資格情報を持つ管理者の名前 (管理コンソールで有効にする)
パスワード	フォレンジック管理者パスワード
MCID	マシン ID (machineID.domain.com など)
DCID	16 桁の Shield ID のうち最初の 8 桁

ヒント:
通常は MCID または DCID のどちらかを指定すれば十分です。ただし、どちらもわかっている場合は、両方を入力すると役立ちます。各パラメータに、このユーティリティが使用する情報が別々に含まれています。

次へ をクリックします。

3 パスフレーズ には、ダウンロードファイルを保護するためのパスフレーズを入力します。パスフレーズは 8 文字以上の長さにし、少なくとも 1 つのアルファベットと 1 つの数字を含む必要があります。パスフレーズを確認します。
ファイルの保存先のデフォルトの名前と場所を使用するか、... をクリックして別の場所を選択します。

次へ をクリックします。

キーマテリアルが正しくロック解除されたことを示すメッセージが表示されます。ファイルはこれでアクセス可能になります。

4 完了したら、**終了** をクリックします。

管理者モードの使用

Security Management Server Virtual は Key Server を使用しないので、管理者モードを使用して Security Management Server Virtual からキーバンドルを取得することはできません。Security Management Server Virtual に対してクライアントがアクティブ化されている場合は、フォレンジックモードを使用してキーバンドルを取得してください。

1 CMGAd が置かれている場所でコマンドプロンプトを開き、**cmgad.exe -a** と入力します。

2 次の情報を入力します (一部のフィールドは事前に入力されている場合があります)。

管理者モードのパラメータ	説明
サーバー :	Key Server の完全修飾ホスト名 (keyserver.domain.com など)。
ポート番号	デフォルトのポートは 8050 です。
サーバーアカウント	Key Server を実行するときのドメインユーザー。形式はドメイン\ユーザー名です。ユーティリティを実行するドメインユーザーには、Key Server からダウンロードを実行する権限が与えられている必要があります。
MCID	マシン ID (machineID.domain.com など)
DCID	16 桁の Shield ID のうち最初の 8 桁

ヒント:
通常は MCID または DCID のどちらかを指定すれば十分です。ただし、どちらもわかっている場合は、両方を入力すると役立ちます。各パラメータに、このユーティリティが使用する情報が別々に含まれています。

次へ をクリックします。

3 パスフレーズ には、ダウンロードファイルを保護するためのパスフレーズを入力します。パスフレーズは 8 文字以上の長さにし、少なくとも 1 つのアルファベットと 1 つの数字を含む必要があります。

パスフレーズを確認します。

ファイルの保存先のデフォルトの名前と場所を使用するか、... をクリックして別の場所を選択します。

次へ をクリックします。

キーマテリアルが正しくロック解除されたことを示すメッセージが表示されます。ファイルはこれでアクセス可能になります。

4 完了したら、**終了** をクリックします。

3

Administrative Launch Utility (CMGAlu)

このユーティリティを使用すると、管理者はコンピュータでプロセスの実行中に、ユーザーによるまたは共通の暗号化済みファイルのロックを解除することができます。

このユーティリティは、管理コンソールからジョブを起動するときに使用します。このユーティリティは対象コンピュータにコピーする必要があります。ユーザーによるまたは共通の暗号化済みファイルにアクセスする必要があるジョブは、管理ジョブのコマンドラインをユーティリティに渡して、このユーティリティを実行するように変更します。プロセスが終了すると、ユーティリティも終了します。

このユーティリティは、アプリケーションに渡されるコマンドラインパラメータに応じて、次のいずれかの方法を使用してファイルのロック解除を行います。

- **フォレンジックモード** - コマンドラインで **-f** が渡された場合、またはコマンドラインでパラメータが渡されていない場合に使用されます。
- **管理者モード** - コマンドラインで **-k** が渡された場合に使用されます。
- **バックアップファイルモード** - コマンドラインで **-b** が渡された場合に使用されます。

ログファイルは、C:\ProgramData\CmgAdmin.log にあります。

フォレンジックモードの使用

フォレンジックモードの構文

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

フォレンジックモードのパラメータ	説明
-f	フォレンジックモードが使用されることを示します。
-vX	X は、ログレベルを示します。ログレベルは、0 ~ 5 です (0 はログなし / 5 はデバッグレベル)。
AdminPwd	フォレンジック管理者パスワード
AdminName	フォレンジック管理者の資格情報を持つ管理者のユーザー名
-r	レジストリからデバイスサーバの URL とコンピュータの MCID (または SCID) をロードするようユーティリティに指示します。 –r が指定されていない場合には、URL/Server と MCID (または SCID) を入力する必要があります。
URL	デバイスサーバの完全修飾 URL お使いの Dell Server のバージョンが v7.7 よりも前の場合、形式は https://deviceserver.domain.com:8081/xapi です。 お使いの Dell Server のバージョンが v7.7 以降の場合、形式は https://deviceserver.domain.com:8443/xapi/ です。
MCID	デバイスがロック解除するためのデバイス ID です。

フォレンジックモードのパラメータ	説明
	MCID は、Device Unique ID またはホスト名と呼ばれることもあります。
SCID	デバイスがロック解除するためのシールド ID です。 SCID は、DCID またはリカバリ ID と呼ばれることもあります。
-?	コマンドラインのヘルプです。

管理者モードの使用

管理者モードの構文

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

管理者モードのパラメータ	説明
-k	Kerberos (管理者モード) が使用されることを示します。管理者モードで作業するには、CmgAlu に -k フラグが必要です。
-vX	X は、ログレベルを示します。ログレベルは、0 ~ 5 です (0 はログなし / 5 はデバッグレベル) 。
ServerPrincipal	Key Server を実行するときの AD アカウント (ドメインアカウント) です。
ポート	Key Server に接続する TCP ポートです。
サーバー	キーサーバー名 / IP アドレスです。
-r	レジストリから Key Server 名とコンピュータの MCID (または SCID) をロードするようユーティリティに指示します。 –r が指定されていない場合には、Key Server 名と MCID (または SCID) を入力する必要があります。
MCID	デバイスがロック解除するためのデバイス ID です。 MCID は、Device Unique ID またはホスト名と呼ばれることもあります。
SCID	デバイスがロック解除するためのシールド ID です。 SCID は、DCID またはリカバリ ID と呼ばれることもあります。
-?	コマンドラインのヘルプです。

バックアップファイルモードの使用

バックアップファイルモードの構文

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

バックアップファイルモードのパラメータ	説明
-vX	X は、ログレベルを示します。ログレベルは、0 ~ 5 です（0 はログなし / 5 はデバッグレベル）。
-b"FilePath"	バックアップファイルのファイルシステムパスです（通常は LSA リカバリファイルまたは CMGAd からダウンロードされた出力ファイルのどちらか）。
-BackupPwd	バックアップファイルの作成に使用されるパスワードです。
-?	コマンドラインのヘルプです。

4

Administrative Unlock Utility（CMGAu）

このユーティリティでは、スレーブドライブ上、インストール前の環境で起動されたコンピューター上、アクティブ化されたユーザーがログインしていないコンピュータ上のユーザー、共通、SDE 暗号化済みファイルへアクセスできます。

このユーティリティはキーマテリアルバンドルをダウンロードするのに次のメソッドを使用します。

- **フォレンジックモード** - コマンドラインで **-f** が渡された場合、またはコマンドラインパラメータが使用されていない場合に使用されます。
- **管理者モード** - コマンドラインで **-a** が渡された場合に使用されます。

ログファイルは、C:\ProgramData\CmgAdmin.log にあります。

以前にダウンロードしたファイルに対するオフライン作業

以前にダウンロードしたファイルでオフライン作業をする場合、CMGAu は起動方法に関係なく同様に機能します。これは、.exe ファイルをダブルクリックしてユーティリティを起動する場合、コマンドラインでスイッチなしで起動する場合、コマンドラインで -f スイッチを使用して起動する場合でも動作は同じであることを意味します。

1 CMGAu が存在する場所でコマンドプロンプトを開き、**cmgau.exe** と入力します。
2 **はい。以前にダウンロードしたファイルでオフライン作業をします。** を選択します。**次へ>** をクリックします。
3 ダウンロードしたファイル で、キーマテリアルを保存した場所に移動します。このファイルは、Administrative Download Utility を使用した際に保存されたファイルです。
パスフレーズ に、キーマテリアルファイルの保護に使用するパスフレーズを入力します。このパスフレーズは、Administrative Download Utility を使用した際に設定されたパスフレーズです。

次へ> をクリックします。

キーマテリアルが正しくロック解除されたことを示すメッセージが表示されます。ファイルはこれでアクセス可能になります。
4 **暗号化済みファイルの作業が終了したら、終了** をクリックします。終了 をクリックすると、暗号化済みのファイルにアクセスできなくなります。

フォレンジックモードでの 今すぐダウンロード の実行

1 CMGAu が存在する場所でコマンドプロンプトを開き、**cmgau.exe** と入力します。
2 **いいえ、今すぐサーバーからのダウンロードを実行します** を選択します。**次へ>** をクリックします。
3 次の情報を入力します（一部のフィールドは事前に入力されている場合があります）。

オプション	説明
デバイスサーバの URL：	デバイスサーバの完全修飾 URL です。 お使いの Dell Server のバージョンが v7.7 よりも前の場合、形式は https://deviceserver.domain.com:8081/xapi です。 お使いの Dell Server のバージョンが v7.7 以降の場合、形式は https://deviceserver.domain.com:8443/xapi/ です。
Dell Admin:	JDOE など、フォレンジック管理者の資格情報を持つ管理者の名前（管理コンソールで有効にする）
パスワード：	フォレンジック管理者パスワード

オプション	説明
MCID:	マシン ID (machineID.domain.com など)
DCID:	16 桁の Shield ID のうち最初の 8 桁

次へ> をクリックします。

キーマテリアルが正しくロック解除されたことを示すメッセージが表示されます。ファイルはこれでアクセス可能になります。

4 **暗号化済みファイルの作業が終了したら、終了** をクリックします。**終了** のクリック後、暗号化済みファイルは使用不可となります。

管理者モードでの 今すぐダウンロード の実行

1 CMGAu が存在する場所でコマンドプロンプトを開き、**cmgau.exe -a** と入力します。

2 **いいえ。今すぐサーバーからのダウンロードを実行する。**を選択します。**次へ>** をクリックします。

3 次の情報を入力します (一部のフィールドは事前に入力されている場合があります)。

管理者モードのパラメータ	説明
サーバー：	Key Server の完全修飾ホスト名 (keyserver.domain.com など)
ポート番号：	デフォルトのポートは 8050 です。
サーバーアカウント：	Key Server を実行するときのドメインユーザー。形式はドメイン\ユーザー名です。ユーティリティを実行するドメインユーザーには、Key Server からダウンロードを実行する権限が与えられている必要があります。
MCID:	マシン ID (machineID.domain.com など)
DCID:	16 桁の Shield ID のうち最初の 8 桁

次へ> をクリックします。

キーマテリアルが正しくロック解除されたことを示すメッセージが表示されます。ファイルはこれでアクセス可能になります。

4 **暗号化済みファイルの作業が終了したら、終了** をクリックします。**終了** のクリック後、暗号化済みファイルは使用不可となります。