




Dell Encryption Enterprise for Mac

管理者ガイド v10.9

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、その危険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。

© 2012-2021 Dell Inc. All rights reserved. Registered trademarks and trademarks used in the Dell Encryption and Endpoint Security Suite Enterprise 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®, Windows Vista®, Windows 7®, Windows 10®, Active Directory®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, 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™, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, App StoreSM, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle®, and iPod nano®, Macintosh®, and Safari® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. 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. 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. 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. Bing® is a registered trademark of Microsoft Inc. Ask® is a registered trademark of IAC Publishing, LLC. Other names may be trademarks of their respective owners.

章 1: はじめに	5
概要.....	5
FileVault 暗号化.....	5
Dell ProSupport へのお問い合わせ.....	5
章 2: 要件	6
Encryption クライアントハードウェア.....	6
Encryption クライアントソフトウェア.....	6
章 3: Encryption クライアントのタスク	8
Encryption Enterprise for Mac のインストールとアップグレード.....	8
対話型インストールまたはアップグレード.....	9
コマンドラインでのインストール/アップグレード.....	10
リムーバブルメディアのフルディスク アクセスの有効化.....	12
Encryption Enterprise for Mac のアクティブ化.....	13
Encryption Enterprise ログファイルの収集.....	13
暗号化のポリシーとステータスの表示.....	14
管理コンソールのポリシーとステータスの表示.....	17
システムボリューム.....	18
暗号化の有効化.....	18
暗号化プロセス.....	18
FileVault リカバリキーの再利用.....	21
ユーザーエクスペリエンス.....	21
リカバリ.....	23
FileVault リカバリ.....	23
リムーバブルメディア.....	27
サポートされるフォーマット.....	27
Encryption External Media とポリシーの更新.....	27
暗号化例外.....	27
リムーバブルメディア タブ上のエラー.....	27
監査メッセージ.....	28
Encryption Enterprise for Mac のアンインストール.....	28
Encryption External Media のアンインストール.....	28
章 4: 管理者としてのアクティブ化	29
アクティブ化.....	29
一時的なアクティブ化.....	29
章 5: Boot Camp の使用	30
Mac OS X Boot Camp のサポート.....	30
Boot Camp 上の Encryption Enterprise for Windows の回復.....	30
章 6: クライアントツール	32

章 7: 用語集.....	35
---------------	----

はじめに

Encryption Enterprise for Mac 管理者ガイドは、クライアントソフトウェアの導入とインストールに必要な情報を提供します。

トピック：

- [概要](#)
- [FileVault 暗号化](#)
- [Dell ProSupport へのお問い合わせ](#)

概要

Encryption Enterprise for Mac で、FileVault フル ディスク暗号化を管理できます。

- Encryption Enterprise for Mac - すべてのデータを暗号化し、アクセス制御を実施するクライアント暗号化ソフトウェアです
- [ポリシープロキシ](#) - ポリシーの配布に使用します
- [セキュリティサーバ](#) - クライアント暗号化ソフトウェアのアクティベーションに使用されます
- Security Management Server または Security Management Server Virtual - 一元化されたセキュリティポリシー管理を提供し、既存のエンタープライズディレクトリを統合し、レポートを作成します。ここでは、特定のバージョンに言及する必要 (Dell Security Management Server Virtual を使用する場合は手順が異なる場合など) がない限り、両方のサーバとも Dell Server と呼びます。

これらのデルコンポーネントはシームレスに相互動作し、ユーザーエクスペリエンスを損なうことなく、安全なモバイル環境を提供します。

FileVault 暗号化

Dell Encryption では、Mac FileVault フル ディスク暗号化を管理することができます。暗号化を行い、その他のポリシー設定が機能するようにするには、[*Dell Volume Encryption*] ポリシーが [**オン**] に設定されている必要があります。他のポリシーの詳細については、[AdminHelp](#) を参照してください。

サポートされるのは FileVault 暗号化のみで、Encryption Enterprise で管理します。コンピュータで *Dell Volume Encryption* ポリシーが **オン** に設定され、*FileVault for Mac* を使用して暗号化が **オフ** に設定されている場合、Encryption クライアントにポリシーの競合を示すメッセージが表示されます。管理者は、両方のポリシーを **オン** に設定する必要があります。

Dell ProSupport へのお問い合わせ

Dell 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、Dell 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。

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。

要件

本章では、クライアントのハードウェアとソフトウェアの要件を説明します。導入タスクを続行する前に、導入環境が要件を満たしていることを確認してください。

トピック：

- Encryption クライアントハードウェア
- Encryption クライアントソフトウェア

Encryption クライアントハードウェア

最小限のハードウェア要件は、オペレーティングシステムの最小要件を満たしている必要があります。

ハードウェア
<ul style="list-style-type: none"> • 30 MB の空きディスク容量
<ul style="list-style-type: none"> • 10/100/1000 または Wi-Fi ネットワークインターフェースカード
<ul style="list-style-type: none"> • システム ディスクは GUID Partition Table (GPT) パーティション スキームでパーティショニングされている必要があり、次のいずれかでフォーマットできます。 <ul style="list-style-type: none"> ○ Mac OS X Extended Journaled (HFS+) : FileVault に適用するためコアストレージに変換されます。 ○ Apple File System (APFS)

Encryption クライアントソフトウェア

次の表では、サポートされているソフトウェアの詳細を説明します。

オペレーティングシステム (64 ビットカーネル)
<ul style="list-style-type: none"> • macOS High Sierra 10.13.6
<ul style="list-style-type: none"> • macOS Mojave 10.14.5 ~ 10.14.6
<ul style="list-style-type: none"> • macOS Catalina 10.15.5 ~ 10.15.6

メモ: Dell Encryption は、macOS Big Sur をサポートしていません。

メモ:

認証にネットワークユーザーアカウントを使用している場合、FileVault 2 管理を完全に設定するためには、このアカウントがモバイルアカウントとして設定されている必要があります。

[暗号化メディア]

次の表では、Dell の暗号化された外部メディアへのアクセス時にサポートされるオペレーティングシステムを詳しく説明しています。

メモ:

Encryption External Media は以下をサポートします。

- FAT32
- exFAT

- マスター ブート レコード (MBR) または GUID パーティション テーブル (GPT) スキームを採用した HFS Plus (Mac OS 拡張) フォーマットのメディア [[HFS Plus の有効化](#)] を参照してください。

メモ:

Encryption External Media をホストするには、外部メディア上の 55 MB の空き容量に加えて、メディア上に暗号化対象の最大ファイルに等しい空き容量が必要です。

[暗号化されたメディアへのアクセス用にサポートされる Windows オペレーティングシステム (32 ビットおよび 64 ビット)]

- Microsoft Windows 7 SP1
 - Enterprise
 - Professional
 - Ultimate
- Microsoft Windows 8.1 - Windows 8.1 Update 1
 - Enterprise
 - Pro
- Microsoft Windows 10
 - Education
 - Enterprise
 - Pro v1607 (Anniversary Update/Redstone 1) ~ v1909 (November 2019 Update/19H2)

[暗号化されたメディアへのアクセス用にサポートされる Mac オペレーティングシステム (64 ビットカーネル)]

- macOS High Sierra 10.13.6
 - メモ:**
macOS High Sierra 10.14.x で Encryption External Media を使用するには、Encryption Enterprise v8.16 以降が必要です。
- macOS Mojave 10.14.5 ~ 10.14.6
- macOS Catalina 10.15.5 ~ 10.15.6

Encryption クライアントのタスク

トピック：

- Encryption Enterprise for Mac のインストールとアップグレード
- Encryption Enterprise for Mac のアクティブ化
- Encryption Enterprise ログファイルの収集
- 暗号化のポリシーとステータスの表示
- システムボリューム
- リカバリ
- リムーバブルメディア
- Encryption Enterprise for Mac のアンインストール
- Encryption External Media のアンインストール

Encryption Enterprise for Mac のインストールとアップグレード

このセクションでは、Encryption Enterprise for Mac のインストール/アップグレードおよびアクティブ化のプロセスについて説明します。

Encryption Enterprise for Mac には 2 つのインストール/アップグレード方法があります。次の**いずれか**を選択してください。

- **インタラクティブなインストール/アップグレードおよびアクティブ化** - この方法は、クライアントのソフトウェアパッケージをインストールまたはアップグレードする最も簡単な方法です。ただし、この方法ではカスタマイズが一切できません。Boot Camp またはデルがまだ完全にサポートしていないオペレーティングシステムのバージョン（.plist の変更により）に使用する予定の場合は、コマンドラインインストール/アップグレードの方法を使用する必要があります。Boot Camp の使用については、「[Boot Camp の使用](#)」を参照してください。
- **コマンドラインインストール/アップグレード** - これはコマンドラインの構文を熟知している管理者によってのみ使用される高度なインストール/アップグレード方法です。Boot Camp またはデルがまだ完全にサポートしていないオペレーティングシステムのバージョン（.plist の変更により）に使用する予定の場合は、この方法を使用してクライアントソフトウェアパッケージをインストールまたはアップグレードする必要があります。Boot Camp の使用については、「[Boot Camp の使用](#)」を参照してください。

インストーラコマンドオプションに関する詳細については、<http://developer.apple.com> にある『Mac OS X Reference Library』を参照してください。<http://developer.apple.com> デルでは、クライアントインストールパッケージの配布に Apple Remote Desktop などのリモート導入ツールを使用することをお勧めしています。

① メモ:

Apple は、Encryption Enterprise for Mac のリリースの間に頻繁にオペレーティングシステムの新しいバージョンをリリースします。できるだけ多くのお客様をサポートするため、com.dell.ddp.plist ファイルの修正により、これらのケースをサポートすることができます。これらのバージョンのテストは、Apple が Encryption Enterprise for Mac と互換性があることを確認するため、新しいバージョンをリリースするとすぐに開始されます。

前提条件

デルでは、クライアントソフトウェアの導入時は IT のベストプラクティスに従うことをお勧めします。これには初期テストのための制御されたテスト環境、およびユーザーへのスタッガ化された導入が含まれますが、これらに限定されるものではありません。

このプロセスを開始する前に、次の前提条件が満たされていることを確認してください。

- Dell Server およびそのコンポーネントがすでにインストールされていることを確認します。
Dell Server をまだインストールしていない場合は、以下の該当するガイドの指示に従います。
Security Management Server インストールおよびマイグレーション ガイド

- セキュリティサーバとポリシープロキシの URL が手元にあることを確認します。どちらもクライアントソフトウェアのインストールおよびアクティブ化に必要です。
- 導入時にデフォルト以外の設定を使用する場合は、セキュリティサーバのポート番号を把握しておいてください。これは、クライアントソフトウェアのインストールおよびアクティブ化に必要です。
- ターゲットコンピュータがセキュリティサーバおよびポリシープロキシにネットワーク接続されていることを確認します。
- Active Directory にドメインユーザーアカウントがあり、Dell Server で使用するためにインストールが設定されていることを確認します。ドメインユーザーアカウントは、クライアントソフトウェアのアクティブ化に使用されます。ドメイン（ネットワーク）認証用に Mac エンドポイントを設定することは必須ではありません。

暗号化ポリシーを設定する前に、[Dell Volume Encryption] ポリシーを [オン] にしてください。[FileVault for Mac を使用して暗号化] ポリシーと [暗号化のターゲットとなるボリューム] ポリシーを確認しておくようにしてください。

暗号化ポリシーの詳細については、[Mac 暗号化 > Dell Volume Encryption](#) を参照してください。

対話型インストールまたはアップグレード

クライアントソフトウェアをインストールまたはアップグレードしてアクティブ化するには、次の手順に従います。これらの手順を実行するには、管理者アカウントが必要です。

対話型インストール

メモ:

開始する前に、ユーザーの作業を保存し、その他のアプリケーションを閉じます。インストールが完了した後すぐにコンピュータを再起動する必要があります。

1. デルのインストールメディアから、Dell-Encryption-Enterprise-<version>.dmg ファイルをマウントします。
2. パッケージインストーラをダブルクリックします。次のようなメッセージが表示されます：
このパッケージは、ソフトウェアをインストールできるかどうかを判定するプログラムを実行します。
3. [続行] をクリックして進めます。
4. ようこそ画面のテキストを読み、[[続行]] をクリックします。
5. ライセンス契約を読み、[続行] をクリックし、次に [同意する] をクリックしてライセンス契約の条項に同意します。
6. ドメインアドレスフィールドに、department.organization.com のようなターゲットユーザーの完全修飾ドメインを入力します。
7. 表示名 (オプション) フィールドで、表示名をドメインの NetBIOS (Windows 2000 より前) 名に設定することを考慮します。通常は大文字で設定します。
設定すると、ドメインアドレスの代わりにこのフィールドが **アクティブ化ダイアログ** に表示されます。この名前は、ドメイン管理下の Windows コンピューターの [認証] ダイアログに表示されるドメイン名と一致します。
8. セキュリティサーバフィールドに、セキュリティサーバのホスト名を入力します。
導入時にデフォルト以外の設定を使用した場合は、ポートと [SSL を使用する] チェック ボックスをアップデートします。
接続が確立されると、セキュリティサーバ接続インジケータが赤から緑に変化します。
9. [ポリシー プロキシ] フィールドに、セキュリティ サーバーのホストと同じホストを含むポリシー プロキシのホスト名が自動入力されます。ポリシーの設定でホストが指定されていない場合は、このホストがポリシープロキシとして使用されます。
接続の確立後に、ポリシープロキシ接続インジケータは赤から緑に変化します。
10. デル設定 ダイアログボックスが完了し、セキュリティサーバおよびポリシープロキシへの接続が確立されたら、**続行** をクリックしてインストールの種類を表示します。
11. 特定のコンピュータの一部のインストールでは **インストールの種類** ダイアログが表示される前に **宛先の選択** ダイアログが表示されます。この場合、表示されるディスクのリストから現在のシステムディスクを選択します。現在のシステム ディスクのアイコンは、緑色の矢印でディスクを指し示しています。**続行** をクリックします。
12. インストールの種類が表示されたら、[**インストール**] をクリックしてインストールを続行します。
13. プロンプトが表示されたら、管理者アカウントの認証情報を入力します (MacOS X インストーラー アプリケーションを使用するには、認証情報が必要です) 。
14. [OK] をクリックします。

メモ:

コンピュータは、インストールの完了直後に再起動する必要があります。他のアプリケーションで開いているファイルがあり、再起動する準備ができていない場合は、**キャンセル** をクリックして作業を保存し、そのアプリケーションを閉じます。

15. **インストールの続行** をクリックします。インストールが開始されます。
16. インストールが完了したら、[**再起動**] をクリックします。
17. Encryption Enterprise の新規インストールの場合、[**機能拡張がブロックされました**] ダイアログが表示されます。

kext-consent では、これらのダイアログのいずれかまたは両方が表示されます。

システム拡張がブロックされました	システム拡張がブロックされました
<ol style="list-style-type: none"> a. [OK] をクリックします。 b. [OK] をクリックします。 c. 機能拡張を承認するには、システム環境設定 > セキュリティとプライバシー を選択します。 d. 開発元である <i>Credant Technologies (Dell, Inc.、旧称 Credant Technologies)</i> のシステム ソフトウェアの横にある [[許可]] をクリックします。 e. [OK] をクリックします。 	<ol style="list-style-type: none"> FDEEM ボリュームをマウントするシステム拡張機能をロードできなかった場合は、次の手順を実行します。 a. "システム環境設定"を開く をクリックします。 b. [OK] をクリックします。 c. [[全般]] タブで、開発元である <i>Credant Technologies (Dell, Inc.、旧称 Credant Technologies)</i> のシステム ソフトウェアの横にある [[許可]] をクリックします。 d. [OK] をクリックします。

[許可] ボタンを使用できるのは、インストールしてから 30 分以内です。この手順をスキップした場合、手順を完了するまで、このダイアログが 25 分ごとに表示され続けます。

18. Encryption Enterprise for Mac の**アクティブ化**を続行します。

リムーバブルメディアを使用する macOS 10.15 以降

企業が macOS 10.15 以降でリムーバブルメディアを使用している場合、ユーザーは外部メディアに対してフル ディスク アクセスを有効にする必要があります。詳細については、「[リムーバブルメディアのフル ディスク アクセスの有効化](#)」を参照してください。

コマンドラインでのインストール/アップグレード

コマンドラインを使用してクライアントソフトウェアをインストールするには、次の手順に従います。

コマンドラインでのインストール

1. デルのインストールメディアから、Dell-Encryption-Enterprise-<version>.dmg ファイルをマウントします。
2. **Install Dell Encryption Enterprise** パッケージと **com.dell.ddp.plist** ファイルをローカル ドライブにコピーします。
3. 管理コンソールで、必要に応じて次のポリシーを変更します。ポリシーの設定によって .plist ファイルの設定が上書きされます。管理コンソールにポリシーが存在しない場合は、.plist 設定を使用します。
 - **認証ユーザーリストなし** - 場合によっては、指定されたユーザーまたはユーザーのクラスが Dell Server に対してアクティブ化する必要がないように、このポリシーを編集できます。たとえば、教育施設で、教師には Dell Server に対して自分のコンピュータをアクティブ化する事を求めるメッセージが表示されますが、ラボのコンピュータを使用している個々の学生には表示されません。ラボの管理者は、このポリシーとクライアントツールを実行するアカウントを使用して、学生のユーザーがアクティブ化を求められなくてもログインできるようにします。クライアントツールに関する情報は、「[クライアントツール](#)」を参照してください。企業はどのユーザーアカウントがエンタープライズの各 Mac コンピュータに関連付けられているかを知っている必要があります、すべてのユーザーは企業がこのプロパティを編集しないように Dell Server に対してアクティブ化されている必要があります。ただし、Encryption External Media のプロビジョニングを希望するユーザーは、Dell Server に対して認証されていなければなりません。
4. .plist ファイルを開き、すべての追加のプレースホルダについて値を編集します。

メモ:

Apple は、Encryption Enterprise for Mac のリリースの間に頻繁にオペレーティングシステムの新しいバージョンをリリースします。できる限り多くのお客様をサポートするために、デルは .plist ファイルを変更可能にして、これらのケースに対応しています。Apple が新しいバージョンをリリースするとすぐに、デルはこれらのバージョンと Encryption Enterprise for Mac との互換性を確認するためのテストを開始します。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
```

```

PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>NoAuthenticateUsers</key> [In this sample code, after one user activates the
computer against the Dell Server, other users can log in without being prompted to
activate.]
  <dict>
    <key>dsAttrTypeStandard:AuthenticationAuthority</key>
    <array>
      <string>*</string>
    </array>
  </dict>
  <key>NoAuthenticateUsers</key> [In this sample code, users from a specific domain name
can log in without being prompted to activate against the Dell Server.]
  <dict>
    <key>dsAttrTypeStandard:AuthenticationAuthority</key>
    <array>
      <string>;Kerberosv5;;*@domainName.com;domainName.com*</string>
    </array>
  </dict>
  <key>NoAuthenticateUsers</key> [In this sample code, specific users can log in without
being prompted to authenticate against the Dell Server.]
  <dict>
    <key>dsAttrTypeStandard:AuthenticationAuthority</key>
    <array>
      <string>;Kerberosv5;;username1@domainName.com;domainName.com*</string>
      <string>;Kerberosv5;;username2@domainName.com;domainName.com*</string>
    </array>
  </dict>
  <key>AllowedOSVersions</key> [AllowedOSVersions is not present in the default .plist
file, it must be added to the file. Add from <key> through </array> to allow a newer
version of operating system to be used. See Note above.]
  <array>
    <string>10.<x.x></string> [Operating system version]
  </array>
  <key>UseRecoveryKey</key>
  <false/> [This value is obsolete since current versions can use both personal and
institutional recovery keys for FileVault encryption.]
  <key>SecurityServers</key>
  <array>
    <dict>
      <key>Host</key>
      <string>securityserver.organization.com</string> [Replace this value with your
Security Server URL]
      <key>Port</key>
      <integer>8443</integer> [Beginning in v8.0, the default port number is 8443. However,
port number 8081 will still allow activations. In general, if your Dell Server is v8.0 or
later, use port 8443. If your Dell Server is pre-v8.0, use port 8081.]
      <key>UseSSL</key>
      <true/> [Dell recommends a true value]
    </dict>
  </array>
  <key>ReuseUniqueIdentifier</key>
  <false/> [When this value is set to true, the computer identifies itself to the Dell
Server by the same hostname it was activated with, regardless of changes to the computer
hostname.]
  <key>Domains</key>
  <array>
    <dict>
      <key>DisplayName</key>
      <string>COMPANY</string>
      <key>Domain</key>
      <string>department.organization.com</string> [Replace this value with the Domain URL
that users will activate against]
    </dict>
  </array>
  <key>PolicyProxies</key>
  <array>
    <dict>
      <key>Host</key>
      <string>policyproxy.organization.com</string> [Replace this value with your Policy
Proxy URL]
      <key>Port</key>

```

```

    <integer>8000</integer> [Leave as-is unless there is a conflict with an existing
port]
  </dict>
</array>
<key>Version</key>
<integer>2</integer> [Do not modify]
<key>MaxPasswordDelay</key>
<integer>xxxx</integer> [Number of seconds to apply to the security policy, "Require
password XXXX after sleep or screen saver begins." The acceptable range is 0-32400.]
<key>EMSTreatsUnsupportedFileSystemAs</key>
<string>ignore</string> [For handling Mac OS Extended media. Possible values are ignore,
provisioningRejected, or unshieldable. ignore - the media is usable (default).
provisioningRejected - retains the value in the Dell Server policy, EMS Access to
unShielded Media. unshieldable - If the EMS Access to unShielded Media policy is set to
Block, the media is ejected. If the EMS Access to unShielded Media policy is not set to
Block, it is usable as provisioningRejected. The key and value are case sensitive.]
<key>ClientActivationTimeout</key>
<integer>120</integer> [Range: 5 to 300, inclusive. The default value is 30. The time in
seconds to give the Security Server time to respond to an activation attempt before giving
up. This plist value is valid for clients running v8.6.0.6627 or later.]
</dict>
</plist>

```

- .plist ファイルを保存して閉じます。
- 各ターゲットコンピュータに対して、パッケージを一時フォルダにコピーし、com.dell.ddp.plist ファイルを **/Library/Preferences** にコピーします。
- 次の **installer** コマンドを使用して、パッケージのコマンドラインでのインストールを実行します。
sudo installer -pkg "Install Dell Encryption Enterprise.pkg" -target /
- 次のコマンドラインを使用してコンピュータを再起動します。**sudo shutdown -r now**

メモ:

macOS High Sierra (10.13) では System Integrity Protection (SIP) が強化されているため、ユーザーによる新規サードパーティ製カーネル拡張の承認が必要です。macOS High Sierra でのカーネル拡張の承認の詳細については、[KB 記事 SLN307814](#) を参照してください。

- Enterprise Edition for Mac のアクティブ化 を続行します。

リムーバブル メディアを使用する macOS 10.15 以降

企業が macOS 10.15 以降でリムーバブル メディアを使用している場合、ユーザーは外部メディアに対してフル ディスク アクセスを有効にする必要があります。詳細については、「[リムーバブル メディアのフル ディスク アクセスの有効化](#)」を参照してください。

リムーバブル メディアのフル ディスク アクセスの有効化

企業が macOS 10.15 以降でリムーバブル メディアを使用している場合、ユーザーは外部メディアに対してフル ディスク アクセスを有効にする必要があります。ユーザーには、次のいずれかのプロンプトが表示されます。

- クライアント ソフトウェアをインストールすると、外部メディアに対するフル ディスク アクセスに同意する必要があることを示すプロンプトが表示されます。[[**セキュリティとプライバシー**] **へ移動**] ボタンをクリックして、次の手順を続行します。
- インストール後にプロンプトが表示されない場合は、リムーバブル メディアを初めてマウントしたときに、フル ディスク アクセスを有効にすることを求めるプロンプトが表示されます。Dell Encryption External Media または EMS Explorer がリムーバブルボリューム上のファイルへのアクセスを求めていることを示すメッセージが表示されます。[**OK**] をクリックして、次の手順を続行します。

詳細については、[KB 記事 SLN319972](#) を参照してください。

- [**システム環境設定**] > [**セキュリティとプライバシー**] で、[**プライバシー**] タブをクリックします。
- 左ペインで、[**フル ディスク アクセス**] を選択します。
Dell Encryption External Media アプリは表示されません。
- 画面下部のロック アイコンをクリックして、ローカル管理者アカウントの認証情報を入力します。
左ペイン > [**ファイルとフォルダー**] で、ユーザーは外部メディア (EMS) コンポーネントをチェックして必要な許可を設定できます。
- 左ペインで、[**フル ディスク アクセス**] を選択します。

これで *Dell Encryption External Media* アプリが表示されます。ただし、承認リクエストが保留中の場合、そのアプリのチェックボックスはオンになっていません。

5. チェック ボックスを選択して許可を付与します。
Dell Encryption External Media アプリが表示されない場合は、次の手順に従います。
 - a. 右ペインで、プラス アイコン (+) をクリックします。
 - b. /Library/Dell/EMS に移動し、**Dell Encryption External Media** を選択します。
 - c. [開く] をクリックします。
 - d. [**フル ディスク アクセス**] で、Dell Encryption External Media のチェックボックスを選択します。
6. [**セキュリティとプライバシー**] を閉じます。

Encryption Enterprise for Mac のアクティブ化

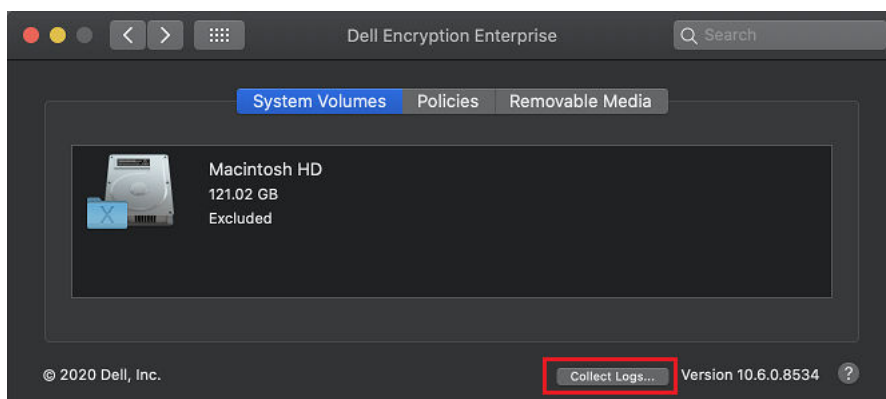
アクティブ化プロセスは Dell Server のネットワークユーザーアカウントを Mac コンピュータと関連付け、各アカウントのセキュリティポリシーを取得してインベントリとステータスの更新を送信し、リカバリのワークフローを有効化して包括的なコンプライアンスレポートを提供します。クライアントソフトウェアは、各ユーザーがユーザーアカウントにログインするときに、コンピュータ上で見つけた各ユーザーアカウントに対してアクティブ化プロセスを実行します。

ユーザーは、クライアントソフトウェアがインストールされ、Mac が再起動された後でログインします。

1. Active Directory によって管理されるユーザー名およびパスワードを入力します。
パスワードダイアログボックスがタイムアウトした場合は、ポリシー タブの **更新** をクリックします。[**ローカルコンピュータでのポリシーとステータスの表示**] の **手順 1** を参照してください。
 2. ログオン先のドメインを選択します。
Dell Server が複数ドメインサポートに対して設定され、アクティブ化に別のドメインを使用する必要がある場合は、<username>@<domain> 形式のユーザープリンシプル名 (UPN) を使用します。
 3. オプションには次のものがあります。
 - **アクティブ化** をクリックします。
 - アクティブ化が成功すると、アクティブ化の成功を示すメッセージが表示されます。Encryption Enterprise for Mac は現在完全に動作可能で Dell Server によって管理されています。
- メモ:**
Encryption External Media の必須リソースに関するアラートが表示される場合は、[**セキュリティとプライバシーへ移動**] ボタンをクリックし、[**許可**] をクリックして、組織が必要とするシステム拡張を行います。Encryption External Media を適切に機能させるには、この拡張を許可する必要があります。
- アクティブ化に失敗すると、クライアントソフトウェアは、3 回まで正しいドメイン資格情報の入力を許可します。3 回とも失敗すると、ドメイン資格情報に対するプロンプトは次のユーザーログイン時に再度表示されます。
- **今はしない** をクリックしてダイアログを閉じると、次のユーザーログインで再度を表示されます。
- メモ:**
管理者が Mac コンピュータ上のドライブの復号化を必要とする場合、それがリモートの場所からか、スクリプトの実行によるものか、または本人が直接行うかにかかわらず、クライアントソフトウェアはユーザーに管理者によるアクセスを許可するためのプロンプトを表示し、パスワードの入力を要求します。
- メモ:**
FileVault 暗号化向けにコンピュータを設定し、ファイルが暗号化されている場合は、後ほどシステムを起動できるアカウントにログインするようにしてください。
4. 以下のいずれかを行います。
 - アクティブ化の前に暗号化が有効化**されなかった**場合は、**暗号化プロセス**を続行します。
 - アクティブ化の前に暗号化が有効化**された**場合は、**暗号化ポリシーおよびステータスの表示**を続行します。

Encryption Enterprise ログファイルの収集

[システム プリファランス] > [Dell Encryption Enterprise] > [システム ボリューム] で、右下にある [ログの収集] ボタンを使用すると、管理者はサポートのためにログを事前に生成することができます。このアクションでは、ログの収集中にパフォーマンスに影響を与える可能性があります。



DellLogs.zip には、Mac Encryption Enterprise のログが含まれています。ログを収集する方法については、<http://www.dell.com/support/article/us/en/19/SLN303924> を参照してください。

暗号化のポリシーとステータスの表示

暗号化ポリシーとステータスは、暗号化されたコンピュータまたは [管理コンソール](#) で表示できます。

ローカルコンピュータでのポリシーとステータスの表示

ローカルコンピュータ上で暗号化ポリシーと暗号化ステータスを表示するには、次の手順を実行します。

1. システムプリファレンスを起動して、[Dell Encryption Enterprise] をクリックします。
2. [ポリシー] タブをクリックして、このコンピュータに設定されている現在のポリシーを表示します。この表示を参照して、このコンピュータに対して有効になっている個別の暗号化ポリシーを確認します。

i メモ:

更新 をクリックしてポリシーのアップデートを確認します。

管理コンソールは、下記の技術グループ内で Mac ポリシーを一覧表示します。

- **Mac 暗号化**
- **リムーバブルメディア暗号化**

設定するポリシーは企業の暗号化要件によって異なります。

次の表にポリシーオプションの一覧を示します。

Mac 暗号化 > Dell Volume Encryption	
High Sierra 以降の場合は、両方のポリシーを有効にする必要があります。Sierra 以前の場合は、旧バージョンのマニュアルを参照してください。	
Dell Volume Encryption	<p>オンまたは オフ</p> <p>これは、その他のすべての Dell Volume Encryption ポリシーの「マスターポリシー」です。他のすべての Dell Volume Encryption ポリシーを適用するためには、このポリシーを オン に設定する必要があります。</p> <p>オンの場合は、暗号化が有効になり、暗号化の対象となるボリュームポリシーまたは FileVault for Mac を使用して暗号化ポリシーに従って、暗号化されていないボリュームの暗号化が開始されます。デフォルトの設定は オン です。</p> <p>オフの場合は、暗号化が無効になり、完全にまたは部分的に暗号化されているボリュームの復号化スイープが開始されます。</p>
FileVault for Mac を使用した暗号化	FileVault 暗号化を使用する予定の場合は、まず始めに Dell Volume Encryption を オン にします。

	<p>管理コンソールで <i>FileVault for Mac</i> を使用して暗号化ポリシーが設定されていることを確認します。</p> <p>有効にすると、暗号化の対象となるボリュームポリシー設定に基づいて、Fusion Drive を含めたシステムボリュームを暗号化するために FileVault が使用されます。</p>
Mac 暗号化 > Mac グローバル設定	
暗号化のターゲットとなるボリューム	<p>システムボリュームのみまたは すべての固定ドライブ</p> <p>システムボリュームのみでは、現在実行中のシステムボリュームのみがセキュア化されます。</p> <p>すべての固定ドライブ 設定は、現在実行中のシステムボリュームのほかに、すべての固定ディスク上のすべての Mac OS 拡張ボリュームをセキュア化します。</p>

3. すべてのポリシーの説明については、管理コンソールから利用できる *AdminHelp* を参照してください。 *AdminHelp* で特定のポリシーを見つける方法。
 - a. 検索アイコンをクリックします。
 - b. 検索で、引用符を使ってポリシー名を入力します。
 - c. 表示されるトピックのリンクをクリックします。引用符で囲んで入力したポリシー名がトピックでハイライト表示されません。
4. [システムボリューム] タブをクリックして、暗号化のターゲットとなるボリュームのステータスを表示します。

状態	説明
除外	ボリュームは暗号化から除外されます。これは、暗号化が無効化されているときの未暗号化ボリューム、外部ボリューム、Mac OS X 拡張 (ジャーナリング) 以外のフォーマットのボリューム、および暗号化のターゲットとなるボリュームがシステムボリュームのみに設定されているときの非システムボリュームに適用されます。
暗号化のためにボリュームを準備しています	クライアントソフトウェアは、現在ボリュームの暗号化プロセスを開始していますが、暗号化スイープは開始していません。
ボリュームのサイズを変更できません	ボリュームを適切なサイズに変更できないため、クライアントソフトウェアが暗号化を開始できません。このメッセージを受け取ったら、Dell ProSupport に連絡してログファイルを提供してください。
暗号化の開始前に修復が必要です	ボリュームは、ディスクユーティリティ検証に失敗しました。 ボリュームを修復するには、Apple サポート記事 HT1782 (http://support.apple.com/kb/HT1782) の手順に従ってください。
暗号化の準備が完了しました。再起動を保留しています	暗号化は再起動後に開始されます。
暗号化ポリシーの拮抗	ディスクが不適切な設定で暗号化されているため、このディスクにポリシーを適用できません。「 <i>FileVault for Mac を使用して暗号化</i> 」を参照してください。
Dell Server でキーが預託されるのを待っています	すべての暗号化データがリカバリ可能であることを確実にするため、クライアントは、すべての暗号化キーが正常に Dell Server に預託されるまで暗号化プロセスを開始しません。キーが預託されるまで、この状態でクライアントはセキュリティサーバ接続をポーリングします。
暗号化	暗号化スイープが進行中です。
暗号化済み	暗号化スイープが完了しました。
復号化	復号化スイープが進行中です。





状態	説明
元の状態に復元しています	クライアントソフトウェアは、復号化プロセスの最後においてパーティションスキームを元の状態に復元しています。これは、暗号化用にボリュームを準備している状態に相当する復号化スイープです。
復号化済み	復号化スイープが完了しました。

色	説明
緑	暗号化された部分
赤	暗号化されていない部分
黄	再暗号化されている部分 たとえば、暗号化アルゴリズムの変更によるものなどです。データは引き続きセキュアです。これは、別のタイプの暗号化に移行しているだけです。

システムボリューム タブには、GUID パーティションテーブル (GPT) フォーマットのディスクに存在するコンピュータに接続されたすべてのボリュームが表示されます。次の表では、内部ドライブのためのボリューム設定の例をリストします。




① メモ:

お使いのオペレーティングシステムに応じて、バッジおよびアイコンが多少異なる場合があります。

バッジ	ボリュームタイプとステータス
	現在起動している Mac OS X システムボリュームです。X フォルダバッジは、現在の起動パーティションを示します。
	暗号化のために設定されたボリュームです。セキュリティとプライバシーバッジは、FileVault によって保護されたパーティションを示します。
	暗号化のために設定された非起動ボリュームです。セキュリティとプライバシーバッジは、FileVault によって保護されたパーティションを示します。
	マルチドライブで、暗号化されていません。 ① メモ: バッジのないボリュームアイコンは、ディスクに対して何も行われていないことを示します。これは起動ディスクではありません。

5. [リムーバブルメディア] タブをクリックして、暗号化のターゲットとなるボリュームのステータスを表示します。次の表では、リムーバブルメディアのためのボリューム設定の例をリストします。

お使いのオペレーティングシステムに応じて、バッジおよびアイコンが多少異なる場合があります。

バッジ	ステータス
	<p>淡色表示されたボリュームアイコンは、マウントされていないデバイスを示します。これには次の理由が挙げられます。</p> <ul style="list-style-type: none"> • ユーザーがこのデバイスをプロビジョニングしないことを選択した。 • メディアがブロックされている。 <p>メモ: このアイコンの赤丸/スラッシュバッジは、サポートされていないために保護から除外されるパーティションを示します。これには、FAT32 フォーマットのボリュームが含まれます。</p>
	<p>明色表示のボリュームアイコンは、マウントされたデバイスを示します。書き込み禁止バッジは、読み取り専用を示します。暗号化は有効になっていますが、メディアはプロビジョニングされておらず、非暗号化メディアに対する Encryption External Media アクセスが読み取り専用を設定されています。</p>
	<p>メディアは Encryption External Media で暗号化され、Dell バッジで示されます。</p>

管理コンソールのポリシーとステータスの表示

管理コンソールで暗号化ポリシーと暗号化ステータスを表示するには、次の手順を実行します。

1. 管理コンソールに Dell 管理者としてログインします。
2. 左ペインで [ポピュレーション > エンドポイント] の順にクリックします。
3. ワークステーションでは、**ホスト名** フィールドのオプションをクリックするか、エンドポイントのホスト名がわかる場合は、検索フィールドにその名前を入力します。フィルタを入力してエンドポイントを検索することもできます。

メモ:

ワイルドカード文字 (*) を使用できますが、テキストの文頭や文末には必要ありません。共通名、UPN (Universal Principal Name)、または sAMAccountName を入力します。

4. 適切なエンドポイントをクリックします。
5. [詳細とアクション] タブをクリックします。
エンドポイント詳細 エリアに、Mac コンピュータに関する情報が表示されます。
Shield の詳細 エリアに暗号化スリープ開始時刻と終了時刻を含むクライアントソフトウェアについての情報が表示されます。
有効なポリシーを表示するには、アクション エリアで **有効なポリシーの表示** をクリックします。
6. [セキュリティポリシー] タブをクリックします。このタブから、ポリシーの種類を展開して個々のポリシーを変更することができます。
 - a. 終了したら、**保存** をクリックします。
 - b. 左側のペインで、[管理] > **コミット** をクリックします。

メモ:

保留中のポリシーの変更の隣りに表示される数字は累積的なものです。これには、他のエンドポイントでの変更、または同じアカウントを使用しているその他の管理者によって行われた変更が含まれる場合があります。

- c. コメントボックスに変更内容を入力し、[ポリシーのコミット] をクリックします。
7. [ユーザー] タブをクリックします。このエリアには、この Mac コンピュータ上でアクティブ化されたユーザーのリストが表示されます。ユーザーの名前をクリックして、このユーザーがアクティブ化されたすべてのコンピュータの情報を表示します。
 8. [エンドポイントグループ] タブをクリックします。このエリアには、この Mac コンピュータが属するすべてのエンドポイントグループが表示されます。

システムボリューム

暗号化の有効化

暗号化対象として以下がサポートされます。

- 起動ボリュームで物理メディアを共有する Apple File System (APFS) ボリューム。
- GUID パーティションテーブル (GPT) パーティションスキームを使用して分割された Mac OS X 拡張 (ジャーナリング) ボリュームおよびシステムディスク。

アクティブ化する前に暗号化が有効になっていない場合は、このプロセスを使用して、クライアントコンピュータで暗号化を有効にします。このプロセスは、1台のコンピュータに対してのみ暗号化を有効にします。必要に応じて、企業レベルですべての Mac コンピュータの暗号化を有効にすることを選択できます。エンタープライズレベルで暗号化を有効化する方法のさらなる詳細については、AdminHelp を参照してください。

1. 管理コンソールに Dell 管理者としてログインします。
2. 左ペインで、[ポピュレーション] > [エンドポイント] の順にクリックします。
3. ワークステーションでは、ホスト名列でのオプションをクリックするか、またはエンドポイントのホスト名を知っている場合は、検索フィールドに入力します。フィルタを入力してエンドポイントを検索することもできます。

① メモ:

ワイルドカード文字 (*) を使用できますが、テキストの文頭や文末には必要ありません。共通名、UPN (Universal Principal Name)、または sAMAccountName を入力します。

4. 適切なエンドポイントをクリックします。
5. セキュリティポリシーページで、**Mac 暗号化** テクノロジグループをクリックします。
デフォルトでは、*Dell Volume Encryption* マスターポリシーは、オンに切り替わります。
6. Mac に Fusion Drive がある場合、*FileVault for Mac* を使用して暗号化ポリシーのチェックボックスを選択します。

① メモ:

このポリシーでは、*Dell Volume Encryption* ポリシーも オンに設定する必要があります。ただし、FileVault 暗号化が有効の場合、グループ内の他のポリシーは無効です。[Mac 暗号化 > Dell Volume Encryption](#) を参照してください。

7. FileVault の選択を解除する場合は (macOS Sierra 以前)、必要に応じて他のポリシーを変更します。
すべてのポリシーの説明については、管理コンソールから利用できる *AdminHelp* を参照してください。
8. 終了したら、**保存** をクリックします。
9. 左側のペインで、[管理] > **コミット** をクリックします。
保留中のポリシーの変更の隣りに表示される数字は累積的なものです。これには、他のエンドポイントでの変更、または同じアカウントを使用しているその他の管理者によって行われた変更が含まれる場合があります。
10. コメントボックスに変更の説明を入力して、[ポリシーのコミット] をクリックします。
11. Dell Server のポリシー送信後にローカルコンピュータでポリシー設定を表示するには、Dell Encryption Enterprise プリファレンスのポリシー ペインで、**更新** をクリックします。

暗号化プロセス

暗号化が有効になっている場合の暗号化プロセスは、起動ボリュームの状態によって異なります。

① メモ:

ユーザーデータの整合性を維持するため、クライアントソフトウェアは、対象ボリュームでの検証プロセスが成功するまで暗号化を開始しません。ボリュームが検証を失敗すると、クライアントソフトウェアがユーザーに通知し、Dell Data Protection プリファレンスに失敗が報告されます。ボリュームの修復を必要とする場合、Apple サポート記事 HT1782 (<http://support.apple.com/kb/HT1782>) の手順に従ってください。クライアントソフトウェアは、コンピュータの次回再起動時に検証を再試行します。

以下のいずれかを選択します。

- 暗号化されていないボリュームの FileVault 暗号化
- 既存の FileVault 暗号化ボリュームの管理の引き継ぎ

暗号化されていないボリュームの FileVault 暗号化

FileVault 暗号化では、PBA に無名ユーザーが 1 件追加で表示されます。デルサーバはこのユーザーを使用してデバイスにポリシーを適用するため、このユーザーを削除しないでください。この PBA ユーザーが削除されると、ポリシーが強制する復号化を開始する必要があります。

1. インストールとアクティブ化の後、FileVault 暗号化がアクティブになったら起動元にするアカウントにログインする必要があります。
2. ドライブの検証、およびボリュームの検証の完了を待ちます。
3. アカウントのパスワードを入力します。

メモ:

このダイアログがタイムアウトになった場合は、再起動する、またはログインしてこのパスワードダイアログを再表示させる必要があります。

4. [OK] をクリックします。
5. ユーザーごとに安全なトークンを持つようにしてください。 <https://www.dell.com/support/article/us/en/19/sln309192/mobile-users-unable-to-activate-dell-encryption-enterprise-for-mac-on-macos-high-sierra?lang=en> を参照してください。

ユーザーがログインしているアカウントが非モバイルアカウントの場合は、ダイアログが表示されます。起動ドライブが暗号化されると、このドライブは、FileVault 初期化中にログインしていたユーザーしか起動できません。

このアカウントは、ローカルアカウントまたはネットワークモバイルアカウントである必要があります。非モバイルネットワークアカウントをモバイルアカウントに変更するには、**システム環境設定 > ユーザーとグループ** の順に移動します。次のいずれかを実行します。

- アカウントをモバイルアカウントにします。
または
- ローカルアカウントにログインし、そこから FileVault を初期化します。

6. [OK] をクリックします。
7. 暗号化準備の完了後、コンピュータを再起動します。

メモ:

管理コンソールのユーザーエクスペリエンスポリシーに応じて、クライアントソフトウェアはユーザーに、コンピュータの再起動を求めるプロンプトを表示する場合があります。

8. コンピュータの再起動後、ネットワークに接続し、クライアントソフトウェアがリカバリ情報を Dell Server にエクスポートする必要があります。

クライアントソフトウェアは、暗号化プロセスの開始と完了、および Dell リモート管理コンソールへの暗号化ステータスの報告のすべてをユーザーログイン前に実行できます。これにより、ユーザーの操作を必要とすることなく、すべての Mac コンピュータにコンプライアンスを施行することができます。

FileVault ユーザーを追加するためのポリシーの変更

FileVault はディスク上のデータを自動的に暗号化することによって、その安全性を確保します。管理下にある FileVault ブートボリュームでは、管理コンソールでポリシーを変更し、OpenDirectory のレコード名と値の辞書を使用して、ユーザーが FileVault ディスクに自分自身を追加できるようにすることにより、複数のユーザーにディスクのロック解除を許可することができます。

1. 管理コンソールの詳細な *Mac グローバル設定* ポリシーで、*FileVault 2 PBA ユーザーリスト* ポリシーまでスクロールします。
2. *FileVault 2 PBA ユーザーリスト* ポリシーのフィールドに、指定する予定のユーザーと一致するルールを入力します。たとえば、任意のキーに対して `<string>*</string>` を一致させると、バインドされた OpenDirectory サーバーのすべてのユーザーと一致します。

タグの大文字と小文字は区別され、全体の値がプロパティリストの辞書およびアレイ要素として適切に形成されている必要があります。辞書のキーは「AND'd together」です。アレイの値は「OR'd together」なので、アレイの中の任意の要素を一致させると、そのアレイ全体に対して一致します。

メモ:

ルールが正しく形成されていない場合は、*Dell Encryption Enterprise* > *環境設定* の順に開いたタブにエラーメッセージが表示されます。

次の <dict> は 2 つのキーの例を示しています。

```
<dict>
  <key>dsAttrTypeStandard:AuthenticationAuthority</key>
  <array>
    <string>;Kerberosv5;;user1@LKDC:*</string>
    <string>;Kerberosv5;;user2@LKDC:*</string>
    <string>;Kerberosv5;;user3@LKDC:*</string>
    <string>;Kerberosv5;;z*@LKDC:*</string>
  </array>
  <key>dsAttrTypeStandard:NFSHomeDirectory</key>
  <string>/Users/*</string>
</dict>
```

- サンプルの *AuthenticationAuthority* キーエントリは、*user1*、*user2*、および *user3*、または *z* で始まる任意のユーザー id のパターンを指定します。各ユーザーの正しい構文を提供するダイアログを表示するには、クライアントで **Control-Option-Command** キーを押します。ユーザーの構文をコピーし、管理コンソールに貼り付けます。

メモ:

この例では、末尾のアスタリスクは、認証局レコードの後半部分を表します。通常、曖昧さを回避するために、末尾のアスタリスクの代わりに完全なレコードを含めます。これは、OpenDirectory レコードではアスタリスクがコロンの後の任意の情報に一致するからです。

- NFSHomeDirectory キーでは、最初のキーを渡す任意のユーザーは */Users/* にもホームディレクトリを持っていないかもしれません。

メモ:

あるユーザーに対してホームフォルダが存在しない場合は、ホームフォルダを作成する必要があります。

3. コンピュータを再起動します。
4. ユーザーアカウントに対する FileVault 起動を有効にするようユーザーに通知します。ユーザーがローカルまたはモバイルアカウントを持っている必要があります。ネットワークアカウントがモバイルアカウントに自動的に変換されます。

ユーザーが FileVault アカウントを有効にするには、次の操作を実行します。

1. システムプリファレンスを起動して、**Dell Encryption Enterprise** をクリックします。
2. システムボリューム タブをクリックします。
3. システム ボリューム ドライブを Ctrl を押しながらクリックして、[**FileVault ユーザーを FileVault 起動に追加**] を選択します。
4. 検索で、ユーザーの名前を入力するか、スクロールダウンします。ユーザーアカウントは、ポリシーで設定した基準に適合する場合にのみ表示されます。

ローカルおよびモバイルユーザーには、**ユーザーを有効にする** ボタンが表示されます。

ネットワークユーザーには、**変換 & ユーザーを有効にする** ボタンが表示されます。

メモ:

緑色のインジケータが FileVault を起動可能なユーザーアカウントの横で表示されます。

5. **ユーザーを有効にする** または **変換 & ユーザーを有効にする** をクリックします。
6. 選択したアカウントのパスワードを入力し、**OK** をクリックします。プログレスインジケータが表示されます。
7. 成功ダイアログの後で、**完了** をクリックします。

既存の FileVault 暗号化ボリュームの管理の引き継ぎ

コンピュータにすでに FileVault 暗号化ボリュームが組み込まれており、管理コンソール上で FileVault 暗号化が有効になっている場合、Dell Encryption はそのボリュームの管理を引き継ぐことができます。

起動ボリュームがすでに暗号化されていることを Dell Encryption が検知した場合は、Dell Encryption Enterprise ダイアログが表示されます。Dell Encryption によるボリュームの管理の引き継ぎを許可するには、次の手順を実行します。

1. [個人のリカバリキー] **または起動可能アカウントの資格情報** を選択します。

メモ:

macOS High Sierra および Apple File System (APFS) では、**起動可能なアカウント情報** を選択する必要があります。

- 個人のリカバリキー - ドライブが FileVault で暗号化されたときに受け取った個人のリカバリキーがある場合。
 - a. キーを入力します。
ユーザーが既存のキーを持っていない場合は、管理者から取得することができます。
 - b. **OK** をクリックします。

① メモ:

引き継ぎプロセスが完了したら、新しい個人リカバリキーが生成および預託されます。以前のリカバリキーは無効化されて削除されます。

- 起動可能アカウントの資格情報 - このボリュームからの起動が現在許可されているアカウントのユーザー名とパスワードを所持している場合。
 - a. ユーザー名とパスワードを入力します。
 - b. **OK** をクリックします。

2. デルがこのボリュームの暗号化を現在管理していることを示すダイアログが表示されたら、**OK** をクリックします。

非起動ボリュームがすでに暗号化されていることを Dell Encryption が検知した場合は、パスフレーズのプロンプトが表示されません。

3. (FileVault で暗号化されている非起動ボリュームのみ) ボリュームの管理を引き継ぐために Dell Encryption を許容するには、パスフレーズを入力してボリュームにアクセスします。これは、もともと FileVault で暗号化されたときにボリュームに割り当てられたパスワードです。

デルがボリュームの暗号化の管理を始めると、以前のパスワードは無効となります。リカバリの必要がある場合は、担当のデル管理者がボリュームのリカバリキーを回復できます。

パスワードを入力しないことを選択した場合、ボリュームの内容にはアクセス可能で FileVault によって暗号化できますが、その暗号化はデルによって管理されません。

① メモ:

管理者は管理コンソールで、現在 Dell Server がエンドポイントを管理していることを確認できます。

FileVault リカバリキーの再利用

リカバリバンドルにセキュリティ上の問題がある、またはボリュームまたはキーのセキュリティが侵害された場合、そのボリュームのキー材料を再利用できます。

Mac OS X で起動および非起動ドライブにリサイクルキーを使用できます。

キー材料を再利用するには、次の手順を実行します。

1. 管理コンソールからリカバリバンドルをダウンロードし、コンピュータのデスクトップにコピーします。
2. システムプリファレンスを起動して、[Dell Encryption Enterprise] をクリックします。
3. [システムボリューム] タブをクリックします。
4. 手順 1 のリカバリバンドルを適切なパーティションにドラッグします。
ダイアログが FileVault キーを再利用するためのプロンプトを表示します。
5. [OK] をクリックします。
ダイアログがキーの循環の成功を確認します。
6. [OK] をクリックします。

① メモ:

これで、このドライブのリカバリバンドルのキーは廃止されました。管理コンソールから新しいリカバリバンドルをダウンロードする必要があります。

ユーザーエクスペリエンス

最大セキュリティのために、クライアントソフトウェアは、Mac OS X コンピュータの自動ログイン機能を無効化します。

また、クライアントソフトウェアは、Mac OS X 機能の **スリープ後またはスクリーンセーバーの開始後にパスワードを必要とする** を自動的に実施します。また、スリープ/スクリーンセーバーモードでは、認証を実施する前に設定可能な時間が与えられます。クライアントソフトウェアでは、認証を実施するまでに最長 5 分の値を設定できます。

暗号化スリープの進行中、ユーザーはコンピュータを通常どおりに使用できます。オペレーティングシステムを含む現在起動されているシステムボリューム上のすべてのデータが暗号化される間、オペレーティングシステムは動作を続行します。

コンピュータが再起動する、またはシステムスリープ状態になると、暗号化スリープは一時停止し、再起動またはスリープ解除後に自動的に再開します。

クライアントソフトウェアは、ハイバネーションイメージの使用をサポートしていません。ハイバネーションイメージは、バッテリーがスリープ中に完全に放電されている場合に、コンピュータをウェイクアップするために Mac OS X のセーフスリープ機能によって使用されます。

ユーザーへの影響を軽減するため、クライアントソフトウェアはシステムスリープモードをハイバネーション無効に自動でアップデートし、この設定を実施します。コンピュータは引き続きスリープ状態になることができますが、現在のシステム状態はメモリにのみ維持されます。このため、コンピュータは、スリープ中に完全シャットダウン（バッテリーが切れた、または交換されると発生し得る）されると完全に再起動されます。

許可リスト ルールのコピー

非表示のメニュー項目を使用して、ユーザーはリムーバブルメディアの許可リスト ルールをコピーできます。

1. **システムプリファレンス** を起動して、[Dell Encryption Enterprise] をクリックします。
2. [リムーバブルメディア] タブを選択します。
3. ドライブ行を右クリックして、同時にコマンドキーを押します。
非表示メニューアイテムが表示されます。
4. 現在のリムーバブルメディアに対応する [許可リスト ルールのコピー] をクリックします。許可リスト ルールがクリップボードにコピーされます。
5. クリップボードにアクセスし、許可リスト ルールをコピーして管理者に送信します。

Mac Media Encryption ポリシーを **オン** に切り替えると、Thunderbolt ドライブなどのデータが暗号化されます。

個別のデバイスまたはデバイスグループを除外対象にして、暗号化されたデータが Thunderbolt ドライブまたは Encryption External Media に書き込まれないようにする場合、許可リスト ルールを使用して値を変更します。

許可リストに登録するために特定のドライブを指定するには、完全な構文を使用します。以下に例を示します。

```
bus=USB;fstype=HFS+;tbolt=0;size=4006608896;USBPRODUCTNUM=5669;USBPRODNAME=DT101  
ll;USBVENDORNAME=Kingston;USBVENDORNUM=2385;USBSENUM=001CC0EC3447AA308699119F
```

📌 メモ:

サンプル値をお使いのドライブの情報に差し替えるようにしてください。

📌 メモ:

HFS Plus を有効にする必要があります。[[HFS Plus の有効化](#)] を参照してください。

Thunderbolt を介して接続されているときに Mac Media Encryption ポリシー施行から SATA ドライブを除外する：

```
tbolt=1;bus=SATA
```

また、下記の条件に基づいて、Encryption External Media からメディアを許可リストに登録または除外することができます。

● メディアのサイズ

Encryption External Media の保護から大容量メディアを除外するための許可リスト ルール：

```
size <op> <size specifier>
```

<op> には =、<=、>=、<、> を使用することが可

<size specifier> は 10 進整数であり、{K, M, G, T} の任意のサフィックスが 1024 ではなく 1000 に整列されます。例えば、Encryption External Media から 5000000000 バイト以上のドライブまたはメディアを除外するには、次のいずれかのコマンドを使用します。

```
size >= 5000000000
```

```
size >= 5000000K
```

size >= 500M

- **ファイルシステムの種類**

許可リスト ルール :

fstype=<fstype>

<fstype> は ExFAT、FAT、または HFS+ です。

両方の除外を行うには、1TB 以上の HFS+ メディアの例を下の示します。

size>=1T;fstype=HFS+

リカバリ

時折、暗号化されたディスク上のデータへのアクセスが必要になることがあります。デルの管理者として、データを復号化せずに暗号化されたディスクにアクセスすることが可能で、時間を節約できます。

ユーザーの暗号化データへのアクセスが必要な理由は多岐にわたりますが、一般的な使用事例は次のとおりです。

- ユーザーが転職/退職したが、そのパスワードを知っている人がいない。
- ユーザーが自分のパスワードを思い出せなくなった。

このセクションでは、FileVault 暗号化がリカバリ対象のエンドポイント上にある場合の [FileVault リカバリー](#) の使用手順について説明します。FileVault は、macOS Sierra 10.12.6 で実行されている Encryption Enterprise for Mac v8.11 以降で使用できます。FileVault リカバリは、Fusion Drive でも使用されます。

FileVault リカバリ

管理対象の FileVault 暗号化ボリュームのリカバリーは Apple によって規定されており、可能な部分は自動化されていますが、さらにいくつかの手順が必要です。

Dell Recovery Utility は、ボリュームのマウントや復号化を支援するスクリプトを使用して Apple のリカバリツールの操作を簡素化します。FileVault リカバリ機能は、Recovery HD にインストールされているオペレーティングシステムおよびペアリングされている対象パーティションによって決定されます。

FileVault 暗号化ボリュームは、Mac OS X 10.9.5 以降が実行されているすべてのディスクドライブに書き込まれた Recovery HD パーティションからのみリカバリできます。この要件によって、リカバリ操作が Dell Recovery Utility から直接実行される可能性がなくなります。

FileVault リカバリキーが個人リカバリキーなのか組織リカバリキーなのかに基づいて、2通りのリカバリ方法が存在します。1つの有効なリカバリキーが常に存在します。個人リカバリキーが存在する場合は、そのキーの最新のエントリーを使用することをお勧めします。そのキーが機能しない場合は、組織リカバリキーチェーンを使用します。

- **個人リカバリキー** - 既存の FileVault 暗号化は、Dell Server が管理します。リカバリバンドル内の最新のエントリーに、RecoveryKey エントリーが含まれている場合は、「[個人のリカバリキー](#)」の手順に従います。RecoveryKey の例は次のとおりです。

```
RecoveryKey</key><string>C73W-CX2B-ANFY-HH3K-RLRE-LVAK</string>
```

- **リカバリー キーチェーン** (まれに使用される手順) - このリカバリー方法は、FileVault の組織リカバリー キーの使用に基づいています。

リカバリバンドル内の最新エントリーに KeychainKey エントリーが含まれている場合は、「[リカバリキーチェーン](#)」の手順に従います。KeychainKey の例は次のとおりです。

```
KeychainKey</key><data>a3ljaAABAAAAA...
```

個人のリカバリキー

一般的には、起動ボリュームをリカバリーした後に、暗号化された他のボリュームをマウントしている非起動ボリュームをリカバリーするのがベストプラクティスです。起動ボリュームを回復すると、通常非起動ボリュームの問題も修正されます。

[前提条件]

- 外部の起動可能ドライブ

- リカバリ対象のコンピュータのデバイス ID / 固有 ID。ほとんどの場合、所有者の名前を検索して、そのユーザー向けに暗号化されたデバイスを表示することによって、管理コンソールでのリカバリ対象のコンピュータを見つけることができます。デバイス ID または固有 ID のフォーマットは、「John Doe's MacBook.Z4291LK58RH」です。
- Dell インストールメディア

管理コンソール - リカバリバンドルの保存

1. 管理コンソールを開きます。
2. 左ペインで [ポピュレーション > エンドポイント] の順にクリックします。
3. 復元したいデバイスを検索します。
4. デバイス名をクリックしてエンドポイントの詳細ページを開きます。
5. [詳細とアクション] タブをクリックします。
6. *Shield* の詳細で、[デバイスのリカバリキー] リンクをクリックします。
7. 外付けリカバリボリューム、または Recovery Utility を実行してリカバリ操作を実行するコンピュータにリカバリバンドルを保存するには、**ダウンロード** をクリックし、[保存] をクリックします。
8. リカバリバンドルの場所を入力して、[保存] をクリックします。

プロセス - .dmg のマウント

1. リカバリバンドルおよび **Dell-Encryption-Enterprise-<version>.dmg** ファイルを起動可能 USB ドライブにコピーします。
2. ターゲットコンピュータを再起動中に、起動前 Startup Manager のオペレーティングシステムが完全にインストールされている外部ボリュームを選択して、**オプション** キーを押して事前に作成されたオペレーティングシステムが完全にインストールされている外部ボリュームからこのコンピュータを起動します。ブート可能なボリュームを作成するには、<https://support.apple.com/en-us/HT202796> を参照してください。
3. **Dell-Encryption-Enterprise-<version>.dmg** をマウントします。

プロセス - Dell Recovery Utility の起動と FileVault ボリュームの回復

1. Dell インストールメディアにある Utilities フォルダで Dell Recovery Utility を起動します。

Dell Recovery Utility > ボリュームの選択 ダイアログが表示されます。

メモ:

Recovery Utility は、リカバリ対象のコンピュータにインストールされているクライアントソフトウェアのバージョンと同じ、またはそれ以上のバージョンである必要があります。

2. *Dell Recovery Utility > ボリュームの選択* で、FileVault ボリュームを選択します。
 - オペレーティングシステムを回復する場合のベストプラクティスは、同一またはそれ以降のバージョンのオペレーティングシステムでコンピュータを起動することです。
 - 非起動ボリュームを暗号化する必要がある場合、通常は起動パーティションを最初に回復します。
3. [続行] をクリックします。
4. リカバリバンドル (先ほど保存したもの) を検索して選択し、[開く] をクリックします。
5. *リカバリレコードの選択* ダイアログが表示される場合、*預託日* 列で個人リカバリキータイプの最新の日付を選択して、[続行] をクリックします。

メモ:

これより古い預託日の場合は、キーは無効になっている可能性があります。

リカバリ操作の結果 が表示されます。

- 起動ドライブの場合は、リカバリツールから標準の Apple FileVault リカバリを使用した起動を可能にする、個人のリカバリキーが提供されます。対象パーティションで起動して、起動前認証のためにこの個人リカバリキーを入力できます (この認証はオペレーティングシステムに応じて異なる可能性があります)。
 - 非起動ドライブの場合は、個人のリカバリキーのみが表示されます。ボリュームのロックを解除してマウントするためのロック解除ボタンが用意されています。
6. 以下のいずれかを行います。
 - 起動ボリュームをリカバリする (最も一般的な手順)
 - 非起動ボリュームをリカバリする (まれに使用される手順)

起動ボリュームをリカバリする (最も一般的な手順)

ほとんどのリカバリでは、起動ボリュームをリカバリするこのオプションが使用されます。

1. キーを書き留めるか、**リカバリキーの印刷** をクリックします。

2. **閉じる** をクリックします。
3. 必要に応じて起動前 Startup Manager を使用し、リカバリーするボリュームを起動します。
複数のユーザーのアイコンがコンピューターに表示されるか、パスワードが要求されます。
4. 該当する場合はユーザーを選択し、ログイン画面で [?] をクリックします。
5. 表示される矢印をクリックします。
6. リカバリキーを入力して、[Enter] を押します。
7. ダイアログにそのユーザーの新しいパスワードを入力します。

非起動ボリュームのリカバリー オプション (まれに使用される手順) - 次のいずれかを実行します。

非起動ボリュームをリカバリーする

起動ボリュームが破損または消去されている場合、セカンダリー ボリュームが存在するのであれば、その非起動ボリュームをマウントすることができます。

1. [**ロック解除**] をクリックします。ボリュームがマウントされます。
2. **閉じる** をクリックします。

ボリュームを復号化する - ボタンをクリックする

1. **復号化** をクリックしますダイアログと進行状況バーに復号化プロセスが表示されます。
2. 復号化が完了したら、**閉じる** をクリックします。
3. 使用するために、復号化したボリュームから起動します。

ボリュームを復号化する - ターミナルからコマンドを実行する

1. *ボリュームを復号化する* エリアにコマンドをコピーします。
2. **閉じる** をクリックします。
3. ターミナルでコマンドを実行します。

リカバリキーチェーン

Recovery Utility は、暗号化されていないリカバリボリュームから起動されているときに実行する必要があります。

[前提条件]

- Recovery Utility を実行する外部リカバリボリュームまたはコンピューター
- USB ドライブ
- Firewire ケーブル
- Dell インストールメディア

管理コンソール - リカバリバンドルの保存

1. 管理コンソールを開きます。
2. 左ペインで [ポピュレーション > エンドポイント] の順にクリックします。
3. 復元したいデバイスを検索します。
4. デバイス名をクリックしてエンドポイントの詳細ページを開きます。
5. [詳細とアクション] タブをクリックします。
6. *Shield の詳細* で、[デバイスのリカバリキー] リンクをクリックします。
7. 外付けリカバリボリューム、または Recovery Utility を実行してリカバリ操作を実行するコンピューターにリカバリバンドルを保存するには、**ダウンロード** をクリックし、[保存] をクリックします。
8. リカバリバンドルの場所を入力して、[保存] をクリックします。

[プロセス]

1. 外部ドライブをリカバリ対象のシステムに接続します。
この外部ドライブには、Mac OS 起動ボリュームが含まれている必要があります。
2. **オプション** キーを長押しして外部ドライブから起動し、起動ピッカーを使用してこのボリュームを選択し、このボリュームから起動します。
3. 管理コンソールからリカバリー バンドルをコピーします。
4. インストール.dmg ファイルをマウントします。

5. Utilities フォルダで、Dell Recovery Utility を実行します。
Dell Recovery Utility > ボリュームの選択 ダイアログが表示されます。
6. 回復する FileVault ボリュームを選択して、[続行] をクリックします。
リカバリバンドルの選択 ダイアログが表示されます。
7. リカバリバンドルを選択して、[開く] をクリックします。
そのディスクに複数のリカバリキーが存在する場合は、リカバリレコードの選択 画面が表示されます。
8. 預託日 列で、キーチェーンリカバリタイプの最新日付を選択して、[続行] をクリックします。

i **メモ:**

これより古い預託日の場合は、キーは無効になっている可能性があります。

FileVault リカバリ手順 ダイアログが表示されます。

9. 手順を読んで、[続行] をクリックします。
リカバリ操作の確認 ダイアログが表示されます。
10. 回復する FileVault ボリュームをハイライト表示して、[続行] をクリックします。
リカバリファイルを格納する場所を選択するよう指示する、リカバリファイルの場所の選択 ダイアログが表示されます。
スクリプトにはデータファイルの絶対パスが記述されているため、この場所は、復元のために使用する場所である必要があります。これらのファイルを Recovery HD にコピーしないでください。
これらのファイルは、USB ドライブなどのリムーバブルドライブのルートに保存することをお勧めします。

i **メモ:**

すべてのユーザーがリカバリキーを保管する USB または他のディスクへの読み取り / 書き込みアクセス権を持っていること、およびそのディスクに十分な空き容量があることを確認してください。選択されたディスクに対するアクセス権がない場合、またはそのディスクの空き容量がない場合は、リカバリキーが保管されなかったことを示すエラーメッセージが表示されます。

11. 場所を選択して、[保存] をクリックします。
ファイルが作成されたことを示す、リカバリ操作の結果 ダイアログが表示されます。
12. [閉じる] をクリックします。
13. Recovery HD ボリュームの起動後に、スクリプトの名前とパスを入力します。

i **メモ:**

ボリュームのルート近くにファイルを保管すると、入力するパスが短くて済みます。

[リカバリ操作の結果] ダイアログにキーが表示されます。

Recovery Utility は、選択された場所にファイルを出力してから、FileVault ボリュームをマウントまたは復号化するために Recovery HD ボリュームから実行する必要がある具体的なコマンドを表示します。

14. これらのファイルが生成された後に、最後の *リカバリ操作の結果* ダイアログに表示されるコマンド文字列をコピーします。
15. 次の方法のひとつで Recovery HD から再起動します。
 - 電源オン/セルフ テストのチャイムが鳴る前、コンピューターの起動中に、**Command-R** キーを同時に長く押します。
または
 - Apple の旧バージョンの場合は、**オプション** キーを押し、起動ピッカーで [Recovery HD] を選択します。
Mac OS X Utilities ダイアログが表示されます。
16. ツール メニューで、[ユーティリティ、ターミナル] の順に選択します。
17. ターミナルからファイルをコピー、またはディスクユーティリティからディスクのイメージを取得することができるようにボリュームをマウントするには、ターミナルで完全なパスとスクリプト名 **fv2mount.sh** を入力します。例：

```
/Volumes/recoveryFOB/fv2mount.sh
```

18. コンピュータを再起動します。

リムーバブルメディア

サポートされるフォーマット

マスターブートレコード (MBR) または GUID パーティションテーブル (GPT) スキームを採用した FAT32 または exFAT、または HFS Plus (Mac OS 拡張) フォーマットのメディアがサポートされます。HFS Plus を有効にする必要があります。

メモ:

現在 Mac では、Encryption External Media の CD/DVD の書き込みはサポートしていません。ただし、Shield 対象外メディアに対する EMS アクセスのブロックポリシーが選択されている場合でも、CD/DVD ドライブへのアクセスはブロックされません。

HFS Plus の有効化

HFS Plus を有効にするには、次を .plist ファイル に追加します。

```
<key>EMSHFSPPlusOptIn</key>
```

```
<true/>
```

メモ:

Dell では、本番環境に導入する前にこの構成をテストすることを推奨します。

HFS Plus は次のものをサポートしていません。

- バージョン管理 - 既存のバージョン管理のデータはディスクから削除されます。
- ハードリンク - リムーバブルメディアの暗号化スweep中は、ファイルは暗号化されません。メディアを取り出すことを推奨するダイアログが表示されます。
- Time Machine のバックアップを含むメディア。
 - Time Machine のバックアップ先としてコンピューターが認識して使用するメディアは、自動的に許可リストに登録され、バックアップの続行を許可されます。
 - Time Machine のバックアップを使用する他のすべてのリムーバブルメディアは、プロビジョニングされていないメディアと非保護メディアを規定するポリシーに基づきます。Shield 対象外メディアに対する EMS アクセス および Shield 対象外メディアに対する EMS ブロックアクセス ポリシーを参照してください。

メモ:

バックアップ先としてまだ使用されていない新しいドライブの場合、ユーザーが許可リスト ルールをコピーし、そのルールを送信して Time Machine ドライブが許可リストに登録されるよう指定する必要があります。「[許可リスト ルールのコピー](#)」を参照してください。

Encryption External Media とポリシーの更新

リムーバブルメディアがプロビジョニングされた (または回復された) システムでは、マウント時にリムーバブルメディア上でポリシーがアップデートされます。

暗号化例外

リムーバブルメディアでは、拡張属性は暗号化されません。

リムーバブルメディア タブ上のエラー

- Shield 対象外コンピュータでは、暗号化されたファイルを、そのファイルの復号化バージョンに置き換えないでください。これは、後ほど復号化を妨げる場合があります。また、リムーバブルメディア タブでエラーとして表示されることもあります。
- ファイル終端マーカが無効になっていると (たとえば、ファイルが Encryption External Media 制御外の新しいコンテンツで上書きされ、その後 Encryption External Media にマウントした場合など)、リムーバブルメディア タブにファイル終端エラーが表示されます。

- ファイル変換時、メディアには変換される最大ファイルのサイズよりも大きい空き容量が必要です。リムーバブルメディアステータスエリアに黄色の警告三角形が表示されたら、それをクリックしてください。容量が不足していますというメッセージが表示された場合は、次の操作を行います。
 1. そのデバイス上で解放する必要がある領域サイズをメモします。レポートにはファイルのリストとそれらのサイズが表示されます。
 2. ゴミ箱を空にします。領域を解放するたびに、Encryption External Media によって自動的に新たなファイルが暗号化されます。
 3. ファイルまたはフォルダを削除する場合は、再度ゴミ箱を空にしてください。

監査メッセージ

監査メッセージは Dell Server に送信されます。

Encryption Enterprise for Mac のアンインストール

クライアントソフトウェアは、**Dell Encryption Enterprise のアンインストール** アプリケーションを実行してアンインストールする場合があります。クライアントソフトウェアをアンインストールするには、次の手順に従います。

メモ:

アンインストールアプリケーションを実行する前に、ディスクを完全に復号化する必要があります。

1. ディスクが暗号化済みの場合は、管理コンソールでコンピュータの *Dell Volume Encryption* ポリシーを **オフ** に設定して、ポリシーをコミットします。

クライアントソフトウェアがディスクを復号化できるように、システム環境設定にアクセスしてコンピュータを制御することを求めるダイアログが表示されます。

- a. ["システム環境設定" を開く] をクリックします。

拒否 を選択すると、アンインストールおよび復号化を続行できません。

- b. 管理者パスワードを入力します。

2. ディスクが完全に復号化されたら、コンピュータを再起動します (プロンプトが表示されたとき)。
3. コンピュータの再起動後に、**Dell Encryption Enterprise のアンインストール** アプリケーション (デルインストールメディアの *Dell-Encryption-Enterprise-<version>.dmg* の Utilities フォルダにあります) を起動します。

メッセージがアンインストールのステータスを表示します。

Encryption Enterprise for Mac がアンインストールされました。コンピュータを正常に使用できます。

Encryption External Media のアンインストール

Encryption External Media をアンインストールするには :

1. **ライブラリ > Dell > EMS** に移動し、**EMS のアンインストール** アプリケーションを選択します。
2. Dell EMS のアンインストール ページで、**アンインストール** をクリックします。
3. ユーザー名とパスワードを入力して **OK** をクリックします。
4. アンインストールの確認画面で、**OK** をクリックします。

管理者としてのアクティブ化

クライアントツールは、Mac コンピュータ上でクライアントソフトウェアをアクティブ化し、クライアントソフトウェアを調べるための新たな方法を管理者に提供します。次の2つのアクティブ化方法を使用できます。

- 管理者資格情報を使用したアクティブ化
- コンピュータにフットプリントを残すことなくユーザーをエミュレートする一時的なアクティブ化

どちらの方法も、シェル経由、またはスクリプト内で直接使用できます。

① メモ:

クライアントソフトウェアは、6 台以上の同一ネットワークアカウントを持つコンピュータでアクティブ化しないでください。お使いの Dell Server で深刻なセキュリティ上の脆弱性やパフォーマンスの劣化が生じる場合があります。

前提条件

- Encryption Enterprise for Mac v8.1.3 以降 をリモートコンピュータにインストールする必要があります。
- リモートの場所からのアクティブ化を試みる前に、クライアントユーザーインターフェースからアクティブ化しないでください。

トピック：

- [アクティブ化](#)
- [一時的なアクティブ化](#)

アクティブ化

このコマンドを使用して、クライアントを管理者としてアクティブ化します。

例：

```
client -a username@domain.com password admin admin
```

一時的なアクティブ化

このコマンドを使用して、コンピュータにフットプリントを残すことなくクライアントをアクティブ化します。

1. シェルを開く、またはスクリプトを使用してクライアントソフトウェアをアクティブ化します。

```
client -at username@domain.com password
```

2. クライアントソフトウェア、そのポリシー、ディスクステータス、ユーザーアカウントなどに関する情報は、クライアントツールを使用して取得します。クライアントツールに関する詳細については、「[クライアントツール](#)」を参照してください。

① メモ:

アクティブ化した後は、Dell Encryption Enterprise プリファレンスのシステムプリファレンスでもポリシー、ディスクステータス、およびユーザー情報含むクライアントソフトウェアに関する情報を入手できます。

Boot Camp の使用

トピック：

- [Mac OS X Boot Camp のサポート](#)
- [Boot Camp 上の Encryption Enterprise for Windows の回復](#)

Mac OS X Boot Camp のサポート

① メモ:

Boot Camp の使用時には、Dell Encryption Enterprise は Windows オペレーティング システムを暗号化しません。また、デバイスに 2 つ以上の起動可能な macOS パーティションが存在する場合、Encryption Enterprise はプライマリー ボリュームのみを暗号化します。

Boot Camp は Mac OS X に含まれるユーティリティであり、デュアルブート構成での Windows の Mac コンピュータへのインストールを支援します。Boot Camp は次の Windows オペレーティングシステムでサポートされています。

- Windows 7 および 7 Home Premium、Professional、Ultimate (64 ビット)
- Windows 8.1 および 8.1 Pro (64 ビット)

① メモ:

Windows 7 は Boot Camp 4 または 5.1 です。Windows 8.1 以降は Boot Camp 5.1 のみです。

Encryption Enterprise for Mac がインストールされたコンピューターの Boot Camp で Encryption Enterprise for Windows を使用するには、FileVault2 で Encryption Enterprise を使用してシステム ボリュームを暗号化する必要があります。手順については、「[コマン ドラインインストール / アップグレード](#)」を参照してください。

① メモ:

Windows パーティションが Encryption External Media の候補である場合、これを許可リストに登録するようにしてください。登録しなければ、このパーティションは暗号化されます。「[許可リスト ルールのコピー](#)」を参照してください。

① メモ:

暗号化を有効にするクライアントポリシーを導入する前に、Windows がインストールされていることを確認する必要があります。クライアントが暗号化プロセスを開始すると、Boot Camp が必要とするディスクパーティション操作が許可されなくなります。

Boot Camp 上の Encryption Enterprise for Windows の回復

Boot Camp ボリュームで動作している Encryption Enterprise for Windows を回復させるには、外付けドライブにも Boot Camp ボリュームを作成する必要があります。

前提条件

- 外部の起動可能ドライブ
- リカバリ対象のコンピュータのデバイス ID / 固有 ID。ほとんどの場合、所有者の名前を検索して、そのユーザー向けに暗号化されたデバイスを表示することによって、管理コンソールでのリカバリ対象のコンピュータを見つけることができます。デバイス ID または固有 ID のフォーマットは、「John Doe's MacBook.Z4291LK58RH」です。

プロセス

1. 外付けドライブの場合に、Boot Camp ボリュームを作成します。

手順は、ローカルシステムでの Boot Camp ボリュームの作成に似ています。<http://www.apple.com/support/bootcamp/> を参照してください。

2. 管理コンソールから、リカバリバンドルをこれらのいずれかにコピーします。
 - 起動可能な USB ドライブまたは
 - 外部 Boot Camp ボリューム上の FAT パーティション
 3. 回復される Boot Camp ボリュームがあるコンピュータをシャットダウンします。
 4. コンピュータに外付けドライブを接続します。

このドライブには、[手順 1](#) で作成した Boot Camp ボリュームが含まれています。
 5. 外付けの Boot Camp ドライブからコンピューターを起動するには、次のいずれかの操作を行います。
 - 電源オン/セルフ テストのチャイムが鳴る前、コンピューターの起動中に、**Command-R** キーを同時に長く押します。または
 - Apple の旧バージョンの場合は、コンピューターの電源をオンするときに**オプション** キーを押します。

Mac OS X Utilities ダイアログが表示されます。
 6. 外付けドライブにある Boot Camp ボリューム (Windows) を選択します。
 7. USB ドライブまたは FAT パーティションで、リカバリバンドル ([手順 2](#) から) を右クリックし、[管理者として実行] を選択します。
 8. **はい** をクリックします。
 9. Dell Encryption Enterprise ダイアログで、次のオプションを選択します。
 - システムが起動しません - ユーザーがシステムから起動できない場合は、この最初のオプションを選択します。または
 - システムが暗号化データにアクセスできません - ユーザーが暗号化されたファイルの一部にアクセスできない場合、システムにログインするとき、2 番目のオプションを選択します。
 10. [次へ] をクリックします。

バックアップとリカバリ情報 画面が表示されます。
 11. **次へ** をクリックします。
 12. 回復させる Boot Camp ボリュームを選択します。
- i** **メモ:**
これは外部 Boot Camp ボリュームではありません。
13. **次へ** をクリックします。
 14. このファイルに関連付けられているパスワードを入力します。
 15. **次へ** をクリックします。
 16. **復元** をクリックします。
 17. **終了** をクリックします。
 18. 再起動するプロンプトが表示されたら、**はい** をクリックします。
 19. システムが再起動し、Windows にログインできるようになります。

クライアントツール

クライアントツールは、Mac エンドポイントで動作するシェルコマンドです。リモートの場所からのクライアントのアクティブ化、またはリモート管理ユーティリティ経由のスクリプトの実行に使用されます。管理者として、クライアントをアクティブ化し、次の操作を実行できます。

- 管理者としてアクティブ化
- 一時的なアクティブ化
- Mac クライアントからの情報の取得

手動でクライアントツールを使用するには、ssh セッションを開き、コマンドラインに希望のコマンドを入力します。

例：

```
/Library/PreferencePanes/Dell\ Encryption\ Enterprise.prefPane/Contents/Helpers/client -at domainAccount domainPassword
```

クライアント のみを入力して使用手順を表示します。

```
/Library/PreferencePanes/Dell\ Encryption\ Enterprise.prefPane/Contents/Helpers/client
```

表 1. クライアントツールのコマンド

コマンド	目的	構文	結果
アクティブ化	<p>ユーザーインタフェースを介さずに Dell Server で Mac クライアントをアクティベーションします。有効にするには、有効なドメインユーザー名とパスワードを入力する必要があります。</p> <p>クライアントツールでは、ログインされているユーザーとは別のローカルユーザーをアクティベーションし、そのユーザーに対してドメインの資格情報を関連付けることができます。</p>	<pre>-a domainAccount domainPassword</pre> <pre>-a localAccount* domainAccount domainPassword</pre> <p>domainAccount は、クライアントツールを使用してアクティベーションに使用するアカウントです。</p> <p>localAccount はオプションで、他に指定されていない場合の現在のユーザーです。</p> <p>アクティベーションのコマンドの形式は以下の通りです。</p> <pre>client -a <user to activate*> <domainUser> <domainPassword></pre> <p>認証ユーザーリストなし ポリシーを使用して Dell Server に対してアクティブ化されていないユーザーのクラスを作成する場合は、オプションで、クライアントツールを使用してログインしているアカウントとは別のローカルアカウントを指定することができます。「手順 3 の 認証ユーザーリストなし ポリシー」を参照してください。</p>	<p>0 = 成功</p> <p>2 = アクティブ化の失敗、および失敗の理由</p> <p>6 = ユーザーが見つかりませんでした</p>
一時的なアクティブ化	<p>フットプリントを残さずに Mac クライアントをアクティブ化します。</p>	<pre>-at domainAccount domainPassword</pre> <pre>-at localAccount* domainAccount domainPassword</pre>	
ディスク	<p>ディスクのステータスを要求します。</p>	<pre>-d</pre>	<p>ディスクの ID、暗号化ステータス、およびポリシーを含むディスクステータスが表示されます。</p>

表 1. クライアントツールのコマンド (続き)

コマンド	目的	構文	結果
			空のブレースが返される場合、暗号化されているディスクがないことを意味します。
FileVault の変更リカバリ	FileVault ボリュームのリカバリキーを循環させます。	-fc deviceId recoveryPassphrase -fc deviceId personalRecoveryKey -fc deviceId pathToKeychain keychainPassword -fc deviceId recoveryFile メモ: deviceId は論理ボリューム UUID、または 1 つの LVUUID のみに解決される必要があります。多くの場合、マウントポイントまたは Devnode が機能します。	0 = 成功 7 = LVUUID が見つかりませんでした 10 = 資格情報エラー 11 = 預託に失敗しました
ポリシー	Mac クライアントのポリシーを要求します。	-p	ポリシーが表示されます。
サーバー	Mac クライアントの代わりにアップデートされたポリシーに対して Dell Server のポーリングを行います。 メモ: ポーリングの完了には数分かかる場合があります。	-s	0 = 成功 他の値はいずれも、Dell Server または Mac クライアントソフトウェアがビジー状態であった、または応答していなかったことを示します。
テスト	Mac クライアントのアクティブ化ステータスをテストします。	-t localAccount*	0 (ドメインアカウント) = 成功 1 = アクティブ化されていません 6 = ユーザーが見つかりませんでした
ユーザー	ユーザー情報を要求します。	-u localAccount*	ユーザーのアカウント情報が表示されます。 0 (アカウント情報) = 成功 6 = ユーザーが見つかりませんでした
バージョン	Mac クライアントのバージョンを要求します。	-v	Mac クライアントのバージョンが表示されます。例： 8.x.x.xxxx

* クライアントツールを実行するアカウントは別のアカウントが指定されない限りは、localAccount に使用されます。

plist オプション

-plist オプションは、それが組み合わされるコマンドの結果を印刷します。plist として結果を印刷するには、このオプションがコマンドの後ろに続き、その引数よりも前に置かれる必要があります。

例

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -p -plist**

クライアントからポリシーを取得し、これらを印刷します。

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -at -plist** *localAccount domainAccount domainPassword*

クライアントを一時的にアクティブ化し、結果を印刷します。

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -s ; echo\$?**

クライアントの代わりにアップデートされたポリシーに対して Dell Server のポーリングを行い、画面に表示します。

Library/PreferencePanes/Dell\ Encryption\Enterprise.prefPane/Contents/Helpers/**client -d -plist**

クライアントのディスクステータスを取得し、それを印刷します。

グローバルリターンコード

エラー無し 0

パラメーターエラー 4

認識されないコマンド 5

ソケットのタイムアウト 8

内部エラー 9

用語集

[Security Server] - Dell Encryption のアクティベーションに使用されます。

[Policy Proxy] - クライアントソフトウェアのポリシーの配布に使用されます。

[管理コンソール] - 企業全体の導入環境を対象としたデルサーバの管理用コンソール。

[Shield] - 時折、説明書およびユーザーインターフェースでこの名称が見られる場合があります。「Shield」は Dell Encryption を表すのに使用される名前です。