Dell Data Protection | Endpoint Security Suite Enterprise for Mac

Administrator Guide v1.1

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。

Administrator Guide

2017 - 05

Rev. A02

Contents

1

はじめに

『Endpoint Security Suite 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

Endpoint Security Suite Enterprise for Mac は、Dell Data Protection サーバからの集中管理によって、オペレーティングシステムおよびメモリのレイヤーと暗号化に高度な脅威阻止を提供します。集中管理を使用すると、統合されたコンプライアンスレポート、およびコンソールの脅威のアラートを使用して、ビジネスですべてのエンドポイントにコンプライアンスを容易に実施して証明することができます。セキュリティの専門知識は事前に定義されたポリシーおよびレポートテンプレートなどの機能に組み込まれており、ビジネスの IT 管理コストと複雑性の低減に役立ちます。

- Endpoint Security Suite Enterprise for Mac - データのクライアント暗号化および高度な脅威阻止のためのソフトウェアのスイートです。
- 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
- Enterprise Server または Dell Enterprise Server - VE - 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がない限り（たとえば、Dell Enterprise Server - VE を使用する場合は手順が異なります）、両方のサーバともデルサーバと呼びます。

  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。

Endpoint Security Suite Enterprise for Mac には、2 つの.dmg ファイルがあります - 1 つは Encryption クライアント用で 1 つは Advanced Threat Prevention 用です。両方またはいずれかをインストールできます。

Dell Encryption クライアントおよび FileVault 暗号化

Dell Encryption クライアントおよび FileVault 暗号化を管理するオプションは、Endpoint Security Suite Enterprise for Mac で利用できます。適切なオプションは、企業の暗号化要件に応じて異なります。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。

Dell ProSupport へのお問い合わせ

Dell Data Protection 製品向けの 24 時間 365 日対応電話サポート（877-459-7304、内線 431003）に電話をかけてください。

さらに、dell.com/support で Dell Data Protection 製品のオンラインサポートも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。

2

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 Client

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。

メモ: システムディスクは、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、Mac OS X 拡張（ジャーナリング）フォーマットである必要があります。

ハードウェア

- 30 MB の空きディスク容量
- 10/100/1000 または Wi-Fi ネットワークインタフェースカード

Encryption Client Software

The following table details supported software.

NOTE: If you intend to perform a major operating system upgrade when using the Dell Encryption client (not FileVault encryption), a decrypt and uninstall operation will be needed followed by regular installation of the Encryption client for Mac on the new operating system.

Operating Systems (64-bit kernels)

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.4 and 10.12.5

  NOTE: macOS Sierra is supported with the Advanced Threat Prevention Agent 1412 or later.

With Mac OS X El Capitan and higher, when using Dell Encryption Client (not FileVault encryption), you must disable Apple's System Integrity Protection (SIP).

NOTE: For information on disabling, see Interactive Installation/Upgrade and Activation, step 4. Before disabling, see Apple's help for how this impacts security.

NOTE: If you are using a network user account to authenticate, that account must be set up as a mobile account in order to fully configure FileVault 2 management.

The following table details the operating systems supported when accessing Dell-encrypted external media.

NOTE: External Media Shield supports FAT32, exFAT, or HFS Plus (Mac OS Extended) formatted media with Master Boot Record (MBR) or GUID Partition Table (GPT) partition schemes. See Enable HFS Plus.

NOTE: External media must have 55 MB available, plus open space on the media that is equal to the largest file to be encrypted, to host External Media Shield.

Encrypted Media

Windows Operating Systems (32- and 64-bit) Supported to Access Encrypted Media

- Microsoft Windows 7 SP0-SP1
  - Enterprise
  - Professional
  - Ultimate
  - Home Premium
- Microsoft Windows 8
  - Enterprise
  - Pro
  - Windows 8 (Consumer)
- Microsoft Windows 8.1 - Windows 8.1 Update 1
  - Enterprise
  - Pro
- Microsoft Windows 10
  - Enterprise
  - Pro

Mac Operating Systems (64-bit kernels) Supported to Access Encrypted Media

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.4 and 10.12.5

  NOTE: macOS Sierra is supported with the Advanced Threat Prevention Agent 1412 or later.

With Mac OS X El Capitan and higher, when using Dell Encryption client (not FileVault encryption), you must disable Apple's System Integrity Protection (SIP).

NOTE: For information on disabling, see Interactive Installation/Upgrade and Activation, step 4. Before disabling, see Apple's help for how this impacts security.

Advanced Threat Prevention

- Advanced Threat Prevention クライアントをインストールする前に、インストールが失敗しないよう、他のベンダーのアンチウイルス、アンチマルウェア、アンチスパイウェアのアプリケーションをアンインストールします。

Advanced Threat Prevention 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

- 500 MB の空きディスク容量（オペレーティングシステムに応じて異なります）
- 2 GB RAM
- 10/100/1000 または Wi-Fi ネットワークインタフェースカード

Advanced Threat Prevention 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）

- Mac OS X Mavericks 10.9.5

メモ: このバージョンは Advanced Threat Prevention のみに適用され、暗号化クライアントには適用されません。

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6

メモ: 大文字と小文字が区別されるファイルシステムはサポートされません。

Advanced Threat Prevention のポート

- Advanced Threat Prevention エージェントは、管理コンソール SaaS プラットフォームによって管理され、管理コンソール SaaS プラットフォームにレポートされます。ポート 443（https）は通信用に使用され、エージェントがコンソールと通信するために、ファイアウォールで開く必要があります。このコンソールは、Amazon Web サービスによってホストされ、固定 IP がありません。ポート 443 が何らかの理由でブロックされている場合、アンチウイルス署名アップデート（DAT ファイル）をダウンロードできないので、コンピュータに最新の保護が装備されないことがあります。次に示すとおり、クライアントコンピュータが URL にアクセスできることを確認してください。

使用	アプリケーションプロトコル	トランスポートプロトコル	ポート番号	宛先	方向
すべての通信	HTTPS	TCP	443	すべての https トラフィックを *.cylance.com に許可	アウトバウンド

3

Encryption クライアントのタスク

インストール / アップグレードの the Encryption Client

このセクションでは、the Encryption client 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。

the Encryption client 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。

> **メモ: Apple は、Endpoint Security Suite Enterprise for Mac のリリースの間にしばしば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 com.dell.ddp.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 the Encryption client for Mac との互換性を確認するためのテストを開始します。**

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。

- デルサーバ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。

  デルサーバ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。

  『*Enterprise Server* インストールおよびマイグレーションガイド 』

  『*Enterprise Server - Virtual Edition Quick Start Guide and Installation Guide*』（*Enterprise Server - Virtual Edition* クイックスタートガイドおよびインストールガイド）
- 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、デルサーバ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。

- クライアントコンピュータで暗号化を実施するには、最初に組織に適した暗号化オプションを選択してください。

Dell Encryption	FileVault 暗号化
このオプションを選択して、次の操作を実行します。 • 起動ドライブ上のすべてのパーティションの暗号化 • 起動前認証の省略 • 256 ビット暗号化の使用	このオプションを選択して、次の操作を実行します。 • Fusion Drive の暗号化 • 起動前認証の使用 • Apple 対応ソリューションの導入
メモ: Dell Encryption を使用する場合は、System Integrity Protection（SIP）を無効にする必要があります。「Interactive Installation/Upgrade and Activation」の手順 4 を参照してください。	**メモ: Mac に Fusion Drive が含まれる場合、ドライブを暗号化するには FileVault を有効にする必要があります。**

暗号化ポリシー設定は、選択する暗号化オプションを反映する必要があります。暗号化ポリシーを設定する前に、*FileVault for Mac* を使用して暗号化 および 暗号化のターゲットとなるボリューム ポリシーについて把握しておいてください。Dell Encryption または FileVault 暗号化を使用するには、*Dell Volume Encryption* ポリシーを オン に設定する必要があります。

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。

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

クライアントソフトウェアをインストール / アップグレードおよび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。

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-Data-Protection-<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。「
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 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。
Mac OS X v10.11 以降で Dell Encryption を使用すると、*Mac OS System Integrity Protection* が有効にされています というタイトルのダイアログが表示されます。System Integrity Protection（SIP）を無効にする必要があります。

次の手順に従います。

a SIP を無効にするには、http://www.dell.com/support/Article/us/en/19/SLN299063 を参照してください。
b ウィザードで、**OK** をクリックし、*Dell Data Protection Configuration* を使用して続行します。

6 ドメインアドレス： フィールドに、*department.organization.com* などの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（pre-Windows 2000）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。これは Windows コンピュータ管理下のドメインの 認証 ダイアログに表示されるドメイン名との整合性を提供します。

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する場合は、ポートフィールドおよび **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、ポリシープロキシホストがセキュリティサーバホストと一致するポリシープロキシ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に、ディスクの方向を指す緑色の矢印が表示されます。**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、Mac OS X インストーラアプリケーションによって必要とされる管理者アカウントの資格情報を入力して、**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。**

14 **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。

15 インストールが完了したら、**再起動** をクリックします。

16 Encryption Client for Mac のアクティブ化 を続行します。

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。

> **メモ: Mac OS X v10.11.x で Dell Encryption を使用する場合、SIP を無効にする必要があります。http://www.dell.com/support/Article/us/en/19/SLN299063 を参照してください。**

1 デルのインストールメディアから、Dell-Data-Protection-<version>.dmg ファイルをマウントします。

2 **Install Dell Data Protection** 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 リモート管理コンソールで、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。リモート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。

- **ファームウェアパスワードモード** - 暗号化された Mac コンピュータでブートキャンプを使用する場合、またはデルによってまだ完全にはサポートされていないバージョンのオペレーティングシステムを使用する場合は、ファームウェアパスワード保護を使用**しない**ように、このポリシーを オプション に設定する**必要があります**。詳細については、「オプションのファームウェアパスワード保護について」を参照してください。

  > **メモ:**
  > FirmwarePasswordMode ポリシーが **オプション** に設定されていると、ファームウェアパスワード保護のクライアントソフトウェアの強化だけが無効になります。既存のファームウェアパスワード保護は削除**されません**。これらの手順が完了すると、インストールが終了してコンピュータが再起動します。既存のパスワードは、Mac OS X ファームウェアパスワードユーティリティを使用して削除できます。

- **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デルサーバ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、教師にはデルサーバ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、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デルサーバ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、EMS メディアのプロビジョニングを希望するユーザーは、デルサーバ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、Endpoint Security Suite Enterprise for Mac のリリースの間にしばしば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 the Encryption client 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/> [We recommend 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>FirmwarePasswordMode</key>
```

```
  <string>Required</string> [If using Boot Camp, this value must be Optional. For more
information, see About Optional Firmware Password Protection.]
  <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>
```

5 .plist ファイルを保存して閉じます。

6 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。

7 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 Data Protection.pkg" -target /
```

8 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`

9 Encryption Client for Mac のアクティブ化 を続行します。

the Encryption Client のアクティブ化

アクティブ化プロセスはデルサーバのネットワークユーザーアカウントを Mac コンピュータへ関連付け、各アカウントのセキュリティポリシーを取得し、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、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。

メモ: 非ドメインの Mac を活性化する手順については、KB 記事 SLN302497 を参照してください。

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** を押します。「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。
デルサーバが複数ドメインサポート用に設定され、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。Enterprise Edition for Mac は現在完全に動作可能でデルサーバによって管理されています。
  - 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回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ってください。

- 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。

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 リモート管理コンソール 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 システム環境設定 を起動して、**Dell Data Protection** 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。

  ヒント: 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。

  リモート管理コンソールは、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**

  企業の暗号化要件に応じて、Dell Encryption または FileVault の暗号化に対してポリシーを設定することができます。この表は、それぞれのポリシーオプションを一覧表示します。

  Mac 暗号化 > Dell Volume Encryption

Dell Volume Encryption	オン または オフ 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。 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。 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。
Mac では FileVault を使用して暗号化	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。 デルサーバで *FileVault for Mac* 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。 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。

メモ:（FileVault ではなく）Dell Encryption を使用している場合、このポリシーを有効にすると、ポリシーの拮抗が発生します。

メモ:
Dell Encryption から FileVault 暗号化に移行する予定の場合は、「Dell Volume Encryption から FileVault 暗号化への移行」を参照してください。

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	システムボリュームのみ または すべての固定ドライブ 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。 **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。

3 すべてのポリシーの説明については、リモート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 検索フィールドで、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す。

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。「FileVault for Mac を使用した暗号化」を参照してください。
デルサーバへのキー預託を待機しています...	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、クライアントソフトウェアは、すべての暗号化キーが正常にデルサーバへキー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ソフトウェアはセキュリティサーバ接続をポーリングします。
暗号化しています...	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。
復号化しています...	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、「復号化しています...」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ます」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。

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。 Dell Encryption は、System Integrity Protection（SIP）でサポートされていません。この非互換状態がポリシーで指定されており、SIP が有効の場合、システムボリューム タブのこのドライブの隣にエラーが表示されます。SIP を無効にするには、「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」の手順 4 を参照してください。
	暗号化のために設定されたボリュームです。このバッジはデルの暗号化パーティションを表します。
	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チは、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チは、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。 **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。**

バッジ	ボリュームタイプとステータス
	システムボリュームのみが暗号化されているマルチドライブです。これはデルの暗号化パーティションの例です。

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
	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。 • 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。 **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。**
	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、Shield 対象外メディアに対する EMS アクセスが読み取り専用に設定されています。
	EMS によって暗号化されたメディアで、デルバッジで示されます。

リモート管理コンソールのポリシーとステータスの表示

リモート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 リモート管理コンソールに 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。

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 を入力できます。

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 エリアに暗号化スイ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。

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

メモ: 暗号化に対してサポートされるのは、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のみです。

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、企業ポリシーレベルですべての 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 ポリシー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 リモート管理コンソールに 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。

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 を入力できます。

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。

メモ: このポリシーでは、*Dell Volume Encryption* ポリシーも オン に設定することが必要です。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 の選択が解除されている場合は、希望に沿ってその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、リモート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 Enterprise Server による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 Data Protection 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

暗号化プロセスは、次の要因に応じて異なります。

- 暗号化が有効化されているときの起動ボリュームの起動。
- Dell Encryption または FileVault の暗号化の選択の有無。

> **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ドライブの Dell Encryption
- 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ドライブの Dell Encryption

クライアントソフトウェアが暗号化ポリシーを受信すると、暗号化の対象となるボリュームのディスクユーティリティ検証を実行してから、これらのボリュームを暗号化用に設定します。

1 プログレスバーは、検証のステータスを示します。検証が完了すると、ターゲットボリュームが暗号化用に設定されます。

このプロセスにより、コンピュータの応答が数分間遅くなることがあります。暗号化を保留中の各ボリュームについて、操作が開始中であることを示すダイアログがユーザーに表示されます。

2 暗号化準備の完了後、コンピュータを再起動します。

> **メモ: リモート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。**

3 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デルサーバに預託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。

暗号化されていないボリュームの FileVault 暗号化

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。

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。

5 **OK** をクリックします。

6 暗号化準備の完了後、コンピュータを再起動します。

メモ: リモート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。

7 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デルサーバに預託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、リモート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 リモート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る場合は、*Dell* データ保護、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、サーバに貼り付けます。

  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ければなりません。

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エンド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 **システム環境設定** を起動して、**Dell Data Protection** 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 ドライブのオプションをクリックし、**FileVault ユーザーを FileVault 起動に追加** を選択します。

4 検索 フィールドで、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、リモート管理コンソール上で FileVault 暗号化が有効になっている場合は、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 Data Protection 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。

- **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。**

  1 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。

  2 **OK** をクリックします。

  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。**

  1 ユーザー名とパスワードを入力します。

  2 **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す。

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。

メモ: 管理者はリモート管理コンソールで、現在デルサーバ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マテリアルを再利用できます。

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。

キーマテリアルを再利用するには、次の手順を実行します。

1 リモート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 システム環境設定 を起動して、**Dell Data Protection** 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。

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。リモート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。

暗号化スイープの進行中、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、暗号化スイープは一時停止し、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、Mac OS X がセーフスリープ 機能を使用して、バッテリ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、休止イメージの使用をサポートしません。

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はできますが、現在のシステム状態はメモリのみに保持されます。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。

ホワイトリストルールのコピー

非表示メニューアイテムでは、ユーザーによる外部メディアのホワイトリストルールのコピーが可能です。

1 **システム環境設定** を起動して、**Dell Data Protection** 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 現在の外部メディアの **ホワイトリストルールのコピー** をクリックします。ホワイト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、ホワイト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。

Thunderbolt ドライブまたは EMS メディアに暗号化データが書き込まれないようデバイスまたはデバイスグループを除外する場合、ホワイトリストルールを使用して値を変更できます。

ホワイトリストに対して特定のドライブを指定するためには、完全なルールを使用します。以下が例です。

bus=USB;fstype=HFS+;tbolt=0;size=4006608896;USBPRODUCTNUM=5669;USBPRODNAME=DT101 II;USBVENDORNAME=Kingston;USBVENDORNUM=2385;USBSERNUM=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 EMS ポリシー施行から SATA ドライブを除外する：

tbolt=1;bus=SATA

さらに下記の条件に基づいて EMS からメディアをホワイトリストまたは除外することができます。

- **メディアのサイズ**

  EMS 保護から大容量のメディアを除外するためのホワイトリストルール：

  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、EMS から 500000000 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 >= 500000000

  size >= 500000K

  size >= 500M

- **ファイルシステムの種類**

  ホワイトリストのルール：

  fstype=<fstype>

  <fstype> は ExFAT、FAT、または HFS+ です。

両方の除外を行うには、1 TB 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。

- ハードウェア更新の一環として、ユーザーの暗号化されたデータを別の Mac に移動させる必要があります。
- システムボリュームが起動しなくなるオペレーティングシステム障害が発生し、オペレーティングシステムの修復にさまざまなユーティリティを実行しなければならないため、暗号化されたディスクにアクセスする必要がある。
- ユーザーが無許可の設定変更を行い、この状況を是正しなければならないため、暗号化されたデータにアクセスする必要があります。

このセクションでは、利用できる 3 つの回復操作のうちの **1 つ**を使用するプロセスについて説明します。

以下からオプションを **1 つ**選択します。

- ボリュームをマウントする
- 新しいシステム設定を受け入れる
- FileVault のリカバリ - リカバリするエンドポイントの FileVault 暗号化を使用している場合にのみ使用します。FileVault は、Mac OS X 10.10.5 以降を実行している the Encryption client で使用できます。FileVault リカバリは、Fusion Drive でも使用されます。

ボリュームをマウントする

前提条件

- 復元ユーティリティを実行する暗号化されていない外部復元ボリュームまたはコンピュータ
- お使いのハードウェアに応じて FireWire または Thunderbolt ケーブル
- 復元対象のコンピュータのデバイス ID / 固有 ID。ほとんどの場合は、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で、リモート管理コンソールで復元対象のコンピュータを見つけることができます。固有 ID またはデバイス 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

プロセス

1 リモート管理コンソールに Dell 管理者としてログインします。

2 左のペインで、**管理 > エンドポイントの回復** の順にクリックします。

3 検索フィールドに、復元したいエンドポイントの完全修飾のドメイン名を入力し、検索アイコンをクリックします。

4 デバイスの **復元** リンクをクリックします。

5 エンドポイントに拡張リカバリが必要である場合は、パスワードのプロンプトが表示されます。ダウンロードしようとしているキーバンドルに新しいパスワードを割り当てます。

メモ: このパスワードは、リカバリキーへのアクセスのために覚えておかなければなりません。

6 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。

<Machine_name.domain>.csv のリカバリファイルがダウンロードされます。

メモ: このコンピュータでファームウェアパスワード保護が有効化されている場合、起動前 Startup Manager にアクセスするためのファームウェアパスワードのプロンプトが表示されます。このコンピュータのファームウェアパスワードは、リカバリバンドルの保存でダウンロードしたリカバリバンドルにあります。詳細については、「Enable Mac OS X Boot Camp を有効にする方法」を参照してください。

7 事前に作成された外部リカバリボリュームからターゲットコンピュータを起動します。システム環境設定の 起動ディスク ペインを起動し、リカバリボリュームを選択するか、またはこのコンピュータの再起動中に **オプション** キーを押して、起動前 Startup Manager でリカバリボリュームを選択することによってこれを実行できます。

または

リカバリ対象のコンピュータをターゲットディスクモードで起動します。システム環境設定の 起動ディスク ペインを起動し、**ターゲットディスクモード** をクリックするか、またはこのコンピュータの再起動中に **T** キーを押してこれを実行できます。

メモ: ファームウェアパスワード保護は、起動時に T キーを使用してターゲットディスクモードに入ることができないようにします。ターゲットディスクモードの詳細については、Apple の http://support.apple.com/kb/HT1661 を参照してください。

ここで、お使いのハードウェアに応じて FireWire ケーブルまたは Thunderbolt ケーブルを使用し、リカバリ操作を実行するホストコンピュータにこのコンピュータを接続します。

8 Dell-Data-Protection-<version>.dmg をマウントします。

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。

9 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。
次のような意味のメッセージが表示されます。「暗号化されたディスクを変更するには、DDP kext [kernel text] をロードする必要があります。これを許可するには、パスワードを入力してください。」

10 管理者またはユーザーのパスワードを入力します。
「インストールが必要です。Recovery をインストールする必要があります」というメッセージが表示されます。

11 **インストール** をクリックします。

12 リカバリが必要なボリュームまたはドライブを選択して、**続行** をクリックします。
ドライブを選択すると、ドライブ上のすべてのボリュームが同時に復元されます。

13 （手順 6 で保存された）リカバリバンドルを選択して、**開く** をクリックします。

14 **ボリュームをマウントする** オプションを選択します。

15 **続行** をクリックして ボリュームをマウントする ことを確認します。成功メッセージが表示されます。

16 **閉じる** をクリックします。

これで、Finder ウィンドウを開いて、通常のボリュームと同じように暗号化されたボリューム上のデータにアクセスできます。ファイルがボリューム間で転送される際に、すべてのデータは透過的に暗号化および復号化されます。

新しいシステム設定を受け入れる

ファームウェアパスワードまたは他のシステム設定の変更によって暗号化されたコンピュータの暗号化キーが無効になった場合、このオプションを選択して次回再起動時にアップデートされたシステム設定を受け入れ、コンピュータへのアクセスを復元します。

暗号化は特定のデバイス設定に関係しているため、設定への変更はクライアントソフトウェアの暗号化キーを無効化します。新しいシステム設定の受け入れの選択は、単に新しいシステム設定に基づいてそのセキュリティをリセットするようクライアントソフトウェアに指示しているだけです。たとえば、ユーザーがスクリーンを壊してしまったために別の Mac にドライブを移動させる必要がある場合などです。この方法を使用して、この「新しい」設定を有効な設定として受け入れるようにクライアントソフトウェアに指示します。

前提条件

- 復元ユーティリティを実行する暗号化されていない外部復元ボリュームまたはコンピュータ
- お使いのハードウェアに応じて FireWire または Thunderbolt ケーブル
- 復元対象のコンピュータのデバイス ID / 固有 ID。ほとんどの場合は、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で、リモート管理コンソールで復元対象のコンピュータを見つけることができます。固有 ID またはデバイス 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

プロセス

1 リモート管理コンソールに 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 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。

メモ: このコンピュータでファームウェアパスワード保護が有効化されている場合、起動前 Startup Manager にアクセスするためのファームウェアパスワードのプロンプトが表示されます。このコンピュータのファームウェアパスワードは、手順 7 でダウンロードしたリカバリバンドルにあります。詳細については、「Enable Mac OS X Boot Camp を有効にする方法」を参照してください。

8 事前に作成された、OS が完全にインストールされている外部ボリュームからターゲットコンピュータを起動します。これを実行するには、システム環境設定で 起動ディスク ペインを起動し、OS が完全にインストールされているボリュームを選択します。または、コンピュータの再起動中に**オプション**キーを押して、起動前 Startup Manager の OS 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。

または

リカバリ対象のコンピュータをターゲットディスクモードで起動します。システム環境設定の 起動ディスク ペインを起動し、**ターゲットディスクモード** をクリックするか、またはこのコンピュータの再起動中に **T** キーを押してこれを実行できます。

メモ: ファームウェアパスワード保護は、起動時に T キーを使用してターゲットディスクモードに入ることができないようにします。ターゲットディスクモードの詳細については、Apple の http://support.apple.com/kb/HT1661 を参照してください。

9 以下のいずれかを行ってください。

- お使いのハードウェアに応じて FireWire ケーブルまたは Thunderbolt ケーブルを使用し、リカバリ操作を実行するホストコンピュータにこのコンピュータを接続します。

  または

- OS が完全にインストールされている、いずれかのディスクからの起動に変更します。

10 Dell-Data-Protection-<version>.dmg をマウントします。

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。

11 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。

次のような意味のメッセージが表示されます。「暗号化されたディスクを変更するには、DDP kext [kernel text] をロードする必要があります。これを許可するには、パスワードを入力してください。」

12 管理者またはユーザーのパスワードを入力します。

「インストールが必要です。Recovery をインストールする必要があります」というメッセージが表示されます。

13 **インストール** をクリックします。

14 リカバリが必要なボリュームまたはドライブを選択して、**続行** をクリックします。

ドライブを選択すると、ドライブ上のすべてのボリュームが同時に復元されます。

ファイル選択ウィンドウが表示されます。

15 （手順 7 で保存された）リカバリバンドルを選択して、**開く** をクリックします。

リカバリ操作の選択 ダイアログが表示されます。

16 **新しいシステム設定を受け入れる** オプションを選択します。

17 **続行** をクリックして、新しいシステム設定を受け入れる を確認します。

18 パスワードを入力して所有権をリセットし、新しいシステム設定を受け入れます。

19 **OK** をクリックします。

元の内部システムボリュームを起動すると、リカバリ完了 メッセージが表示されます。このメッセージは、コンピュータをもう一度再起動することを求めます。これで、クライアントソフトウェアはアップデートされたシステム設定を受け入れました。コンピュータには通常どおりアクセスできます。

FileVault リカバリ

管理された FileVault 暗号化ボリュームのリカバリは、Dell 暗号化ボリュームのリカバリとは大きく異なります。リカバリプロセスは 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、いくつかの追加手順が必要です。

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。一般に、最新の個人リカバリキーを最初に使用します。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、デルサーバによって管理されます。これは推奨の方法です。

  リカバリバンドル内の最新のエントリに、RecoveryKey エントリ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>
  ```

- リカバリキーチェーン - このリカバリ方法は、FileVault の組織リカバリ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に KeychainKey エントリ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

一般に、非起動ボリュームを回復する前に起動ボリュームを回復すること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、リモート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。固有 ID またはデバイス 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

プロセス

1 リモート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。

9 リカバリバンドルおよび **Dell-Data-Protection-<version>.dmg** ファイルを起動可能 USB ドライブにコピーします。

10 ターゲットコンピュータを再起動中に、起動前 Startup Manager の OS 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 OS 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。

11 Dell-Data-Protection-<version>.dmg をマウントします。

> **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。

12 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。

13 FileVault ボリュームを選択します。

- ドライブを復号化してマウントするには、バージョン 10.9.5 以上の起動パーティションが必要です。この起動パーティションがない場合は、個人リカバリキーのみを取得できます。
- 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。

14 **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。

15 （手順 9 で保存された）リカバリバンドルを選択し、**開く** をクリックします。

リカバリレコードの選択 ダイアログが表示されます。

16 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。

復元操作の結果 ダイアログにキーが表示されます。

- 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 OS 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。非起動ボリュームをマウントするには、リカバリキーをオペレーティングシステムのパスワードプロンプトダイアログに入力します。このダイアログを以前に閉じた場合は、この時点でディスクユーティリティを通じて ロック解除 を選択して、暗号化されたパーティションをマウントできます。

17 キーを印刷するか書き留めます。

18 **閉じる** をクリックします。

19 起動時に **オプション** を押し続けることで、外部起動ボリュームから起動します。

20 必要に応じて、ファームウェアパスワードを入力します。外部起動ボリュームを選択します。

21 システムの再起動後に、ログイン画面で **?** をクリックします。

22 表示される矢印をクリックします。

23 リカバリキーを入力して、**Enter** を押します。

24 ダイアログで、新しいパスワードを入力します。

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。Recovery Utility は、暗号化された外部起動ボリュームから実行しないでください。

前提条件

- 復元ユーティリティを実行する外部復元ボリュームまたはコンピュータ
- USB ドライブ
- Firewire ケーブル
- Dell インストールメディア

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 起動時に **オプション** を押し続けることで、外部起動ボリュームから起動します。

3 必要に応じて、ファームウェアパスワードを入力します。外部起動ボリュームを選択します。

4 .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。

> **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。

これらのファイルを USB ドライブなどの外部ドライブのルートに保存することをお勧めします。

> **メモ:**
> すべてのユーザーがリカバリキーを保管する USB またはその他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、復元操作の結果 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。

メモ:
ボリュームのルート近くにファイルを保管すると、入力する必要のあるパスが短くてすみます。

復元操作の結果 ダイアログにキーが表示されます。

Dell 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の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 復元操作の結果 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 / セルフテスト前およびコンピュータの起動時に **Command** および **R** キー（Command - R）を同時に押し続けます。
  または
- **オプション**キーを押して起動ピッカーを使用し、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、EMS について CD/DVD の書き込みはサポートされていません。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>EMSHFSPlusOptIn</key>

<true/>

メモ: デルでは、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イープ中は、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のコンピュータで認識するメディアは自動的にホワイトリストに登録され、バックアップが許可されて続行されます。

- 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: バックアップがまだない新しいドライブでは、ユーザーが自分のホワイトリストルールをコピーし、ルールを送信してホワイトリストの Time Machine でドライブを指定する必要があります。「ホワイトリストルールのコピー」を参照してください。

EMS とポリシーアップデート

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、マウント時にポリシーがメディアに対してアップデートされます。

暗号化例外

外部メディアでは、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ーが無効になっていると（たとえば、ファイルが EMS 制御外の新しいコンテンツで上書きされ、その後 EMS 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。

  a そのデバイス上で解放する必要の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。

  b ゴミ箱を空にします。領域を解放するたびに、EMS によって自動的に追加のファイルが暗号化されます。

  c 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

監査メッセージはデルサーバに送信されます。

Endpoint Security Suite Enterprise for Mac では、リモート管理コンソールを参照して **ポピュレーション、エンタープライズ またはエンドポイント** の順に選択します.次に **高度な脅威イベント** タブを選択します。詳細については、*AdminHelp* を参照してください。

Endpoint Security Suite Enterprise のログファイルの収集

DellLogs.zip には、Client Encryption and Advanced Threat Prevention 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。

the Encryption Client for Mac のアンインストール

Dell Data Protection のアンインストール アプリケーションを実行してクライアントソフトウェアをアンイストールする場合もあります。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 ディスクが現在暗号化されている場合は、リモート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 Data Protection 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-Data-Protection-<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。

the Encryption client 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。

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。

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。お使いのデルサーバにおける深刻なセキュリティ上の脆弱性、およびパフォーマンスの劣化につながる場合があります。

前提条件

- The Encryption client for Mac 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フェースからアクティブ化しないでください。

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。

メモ: アクティブ化した後は、Dell Data Protection 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。

Encryption クライアントの参照

オプションのファームウェアパスワード保護について

メモ: 最近の Mac コンピュータは、ファームウェアパスワード保護をサポートしていません。ファームウェアパスワード保護は、次のモデルでサポートされています。

- iMac10*
- iMac11*
- Macmini4*
- MacBook7*
- MacBookAir2*
- MacBookPro7*
- MacPro5*
- XServe3*

たとえば、iMac10.1、iMac11.1 および iMac11.2 はオプションのファームウェアパスワード保護をサポートしますが（* によって示されています）、iMac12.1 以降はサポートしません。

メモ: FirmwarePasswordMode キーオプションを オプション に設定すると、ファームウェアパスワード保護のクライアントの施行のみが無効になります。既存のファームウェアパスワード保護は削除されません。Mac OS X ファームウェアパスワードユーティリティを使用して、任意の既存ファームウェアパスワードを削除できます。

暗号化された Mac コンピュータで、Boot Camp を使用する予定の場合（手順は「Mac OS X Boot Camp を有効にする方法」を参照）は、クライアントでファームウェアパスワード保護を使用**しない**よう設定する**必要があります**。

Mac コンピュータは、ファームウェアパスワード保護を使用してコンピュータのアクセスセキュリティを強化します。Mac コンピュータでは、この保護がデフォルトで オフ に設定されています。クライアントのインストール中、新規のインストールまたは以前のクライアントバージョンからのアップグレードのいずれでも、既存の com.dell.ddp.plist ファイルを編集して、*FirmwarePasswordMode* キーを 必須 または オプション に設定することができます。必須 オプションはファームウェアパスワード保護を実施するデフォルト設定で、オプション 設定はファームウェアパスワードを実施しません。インストールまたはアップグレード後、クライアントは再起動中に変更されたインストーラ com.dell.ddp.plist ファイルを評価します。

メモ: ユーザーがコンピュータのセキュリティ方針を変更しないようにするため、クライアントソフトウェアのインストール後、クライアントは FirmwarePasswordMode キーに対する変更を許可しません。
このキーの値はインストールまたはアップグレード後、ディスク復号化プロセスを初期化してから、暗号化を再度有効にすることによって変更できます。

Mac OS X ファームウェアパスワード保護を **必須** にするには、「」「Encryption Client for Mac のインストール / アップグレード」を参照して通常のクライアントのインストール / アップグレード手順に従います。

Boot Camp の使用

Mac OS X Boot Camp のサポート

メモ: Boot Camp を使用するときは、Windows オペレーティングシステムを暗号化することができません。

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 および 8 Pro（64 ビット）
- Windows 8.1 および 8.1 Pro（64 ビット）

メモ: Windows 7 は Boot Camp 4 または 5.1 です。Windows 8 以降は Boot Camp 5.1 のみです。

Endpoint Security Suite Enterprise for Mac をインストールしたコンピュータ上の Boot Camp で Endpoint Security Suite Enterprise for Windows を使用するには、Dell Client Encryption または FileVault2 のいずれかで the Encryption client for Mac 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。ファームウェアパスワード保護を使用**しない**ようにクライアントインストール設定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。

メモ:

Windows パーティションが EMS 候補である場合には、これをホワイトリストに登録するようにしてください。登録しなければ、パーティションが暗号化されます。「ホワイトリストルールのコピー」を参照してください。

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 Endpoint Security Suite Enterprise for Windows のリカバリ

Boot Camp ボリュームで動作している Endpoint Security Suite 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、リモート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。固有 ID またはデバイス 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 リモート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 外部 Boot Camp ドライブからコンピュータを起動するには、コンピュータの電源投入中に **オプション** キーを押します。

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 Data Protection Encryption ダイアログで、次のオプションを選択します。

- システムが起動に失敗します....- 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へのアクセスを許可しません....- ユーザーがシステムへのログイン時に一部の暗号化されたファイルにアクセスできない場合は、この 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。

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。

ファームウェアパスワードの取得方法

クライアントコンピュータがファームウェアパスワードを実施するように設定されている場合でも、リカバリには不要なことがあります。リカバリの対象となるコンピュータが起動可能である場合、システム環境設定の 起動ディスク ペインで起動ターゲットを設定します。

リカバリを完了するためにファームウェアパスワードが必要とされるときは（コンピュータが起動可能ではなく、ファームウェアパスワード保護が実施されている場合）、次の手順に従います。

ファームウェアパスワードを取得するには、最初にディスクの暗号化キーを含むリカバリバンドルを取得する必要があります。

1 リモート管理コンソールに 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 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**、および **保存** をクリックします。

8 リカバリバンドルを開いて、リカバリの対象となるコンピュータのファームウェアパスワードを取得します。ファームウェアのパスワードは、**FirmwarePassword** キーの後のストリングタブ内にあります。

例：

<key>FirmwarePassword</key>

<string>Bo$vun8WDn</string>

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\ Data\ Protection.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\ Data\ Protection.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	ユーザーインタフェースを介さないで Mac クライアントをデルサーバに対して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。 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。	-a domainAccount domainPassword -a localAccount* domainAccount domainPassword **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。 **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。 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。 client -a <user to activate*> <domainUser> <domainPassword> 認証ユーザーリストなし ポリシーを使用してデルサーバ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。	0 = 成功 2 = アクティブ化の失敗、および失敗の理由 6 = ユーザーが見つかりませんでした
一時的なアクティブ化	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。	-at domainAccount domainPassword -at localAccount* domainAccount domainPassword	
ディスク	ディスクのステータスを要求します。	-d	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。 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。

コマンド	目的	構文	結果
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ついてデルサーバ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、デルサーバまたは 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\ Data\ Protection.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\ Data\ Protection.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\ Data\ Protection.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ついてデルサーバのポーリングを行い、画面に表示します。

Library/PreferencePanes/Dell\ Data\ Protection.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

4

Advanced Threat Prevention のタスク

Advanced Threat Prevention for Mac のインストール

このセクションでは、Advanced Threat Prevention のインストールについて説明します。

Advanced Threat Prevention をインストールするには 2 つの方法があります。

- インタラクティブなインストール - これは最も簡単なインストール方法です。ただし、この方法ではカスタマイズが一切できません。
- コマンドラインインストール - 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。

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。

- デルサーバ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。

  デルサーバ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。

  『*Enterprise Server* インストールおよびマイグレーションガイド 』

  『*Enterprise Server - Virtual Edition Quick Start Guide and Installation Guide*』(*Enterprise Server - Virtual Edition* クイックスタートガイドおよびインストールガイド)
- サーバのホスト名とポートを持ってい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に必要です。
- ターゲットコンピュータがデルサーバにネットワークに接続されていることを確認します。
- クライアントのサーバ証明書がない、または自己署名されている場合は、クライアント側のみで SSL 証明書の信頼を無効にする必要があります。

Advanced Threat Prevention のインタラクティブなインストール

このセクションでは、Mac のインストールプロセス用の Advanced Threat Prevention について説明します。

インタラクティブなインストールは、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。

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。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。

メモ: 作業を開始する前に、ユーザーの作業を保存し、他のアプリケーションを閉じます。

1 デルのインストールメディアから、**Endpoint-Security-Suite-Enterprise-<version>.dmg** ファイルをマウントします。
Endpoint Security Suite Enterprise for Mac パッケージが開きます。

2 **Endpoint Security Suite Enterprise** パッケージインストーラをダブルクリックします。「

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** をクリックします。

4 ようこそ 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 **Server Host** フィールドに、ターゲットユーザーを管理するデルサーバの完全修飾ホスト名（server.organization.com など）を入力します。

7 **Server Port** フィールドに、**8888** を入力し、**続行** をクリックします。
接続が確立されたら、接続インジケータが赤から緑に変化します。

メモ: このポートは、設定可能な Core サーバのサービスポートです。デフォルトのポート番号は 8888 です。

8 インストール 画面で、**インストール** をクリックします。

9 プロンプトが表示されたら、Mac OS X インストーラアプリケーションによって必要とされる管理者アカウントの資格情報を入力して、**OK** をクリックします。

10 インストールが完了したら、**閉じる** をクリックします。
Mac 用 Advanced Threat Prevention クライアントがインストールされます。

11 「Advanced Threat Prevention のインストールの確認」を参照してください。

インストールに失敗した場合は、お使いのデルサーバの有効な証明書を持っているか確認してください。「Advanced Threat Prevention の SSL 信頼証明書の無効化」を参照ください。

Advanced Threat Prevention クライアントのインタラクティブなアンインストール

Uninstall Endpoint Security Suite Enterprise アプリケーションを実行してクライアントソフトウェアを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。

1 Endpoint-Security-Suite-Enterprise-<version>.dmg ファイルをマウントします。

2 Utilities フォルダで、**Uninstall Endpoint Security Suite Enterprise** アプリケーションを起動します。

3 **アンインストール** をクリックします。

4 プロンプトが表示されたら、Mac OS X インストーラアプリケーションによって必要とされる管理者アカウントの資格情報を入力して、**OK** をクリックします。
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。

5 正常にアンインストールされたことを確認して、**OK** を押します。
Advanced Threat Prevention 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。

Advanced Threat Prevention のコマンドラインによるインストール

コマンドラインを使用して Advanced Threat Prevention クライアントをインストールするには、次の手順に従います。

1 デルのインストールメディアから、Endpoint-Security-Suite-Enterprise-<version>.dmg ファイルをマウントします。Endpoint Security Suite Enterprise for Mac パッケージが開きます。

2 Utilities フォルダから、**com.dell.esse.plist** ファイルをローカルドライブにコピーします。

3 .plist ファイルを開きます。

4 server.organization.com、およびポート番号 **8888** などのターゲットユーザーを管理するデルサーバの完全修飾ホスト名を使用してプレースホルダ値を編集します。

```
<?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>ServerHost</key>
```

```
  <string>deviceserver.company.com</string>
  <key>ServerPort</key>
  <array>
</dict>
</plist>
```

メモ: このポートは、設定可能な Core サーバのサービスポートです。デフォルトのポート番号は 8888 です。

5 ファイルを保存して閉じます。

6 各ターゲットコンピュータの場合は、**Endpoint Security Suite Enterprise for Mac** パッケージインストーラを一時フォルダにコピーし、変更した **com.dell.esse.plist** ファイルを **/Library/Preferences** にコピーします。

7 プロンプトが表示されたら、資格情報を入力します。

8 ターミナルウィンドウを起動します。

9 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 /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Endpoint\
Security\ Suite\ Enterprise.pkg -target /
```

メモ: -pkg パスは .dmg ファイルで検出される .pkg インストーラへのパスです。

10 **Enter** を押します。

11 「ESSE Advanced Threat Prevention の確認」を参照してください。

Advanced Threat Prevention for Mac のコマンドラインによるアンインストール

コマンドラインを使用して Advanced Threat Prevention クライアントをアンインストールするには、次の手順に従います。

1 ターミナルウィンドウを起動します。

2 次の **uninstaller** コマンドを使用して、パッケージのコマンドラインでのアンインストールを実行します。

```
sudo /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Utilities/Uninstall\ Endpoint\
Security\ Suite\ Enterprise.app/Contents/MacOS/Uninstall\ Endpoint\ Security\ Suite\
Enterprise --noui
```

メモ: コマンドの最後に --noui が含まれていることを確認します。

3 **Enter** を押します。

Advanced Threat Prevention 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。

Advanced Threat Prevention for Mac のトラブルシューティング

Advanced Threat Prevention の SSL 信頼証明書の無効化

クライアントのサーバ証明書がない、または自己署名されている場合は、クライアント側のみで SSL 証明書の信頼を無効にする必要があります。

1 クライアントで、ターミナルウィンドウを起動します。

2 DellCSFConfig.app にパスを入力します。

```
cd /Volumes/Endpoint\ Security\ Suite\ Enterprise\ for\ Mac/Utilities/DellCSFConfig.app/
Contents/MacOS/
```

3 DellCSFConfig.app を実行します。

```
sudo ./DellCSFConfig
```

デフォルトの設定では、次が表示されます。

```
Current Settings:

ServerHost = deviceserver.company.com
```

```
ServerPort = 8888

DisableSSLCertTrust = False

DumpXmlInventory = False

DumpPolicies = False
```

4 **-help** を入力してオプションを一覧表示します。

5 クライアントで SSL 証明書の信頼を無効にするには、`DisableSSLCertTrust` を **True** に変更します。

XML インベントリおよびポリシーの変更をログフォルダに追加します。

inventory.xml ファイルまたは policies.xml ファイルをログフォルダに追加します。

1 上記のとおり、DellCSFConfig.app を実行します。

2 DumpXmlInventory を **True** に変更します。

3 DumpPolicies を **True** に変更します。
ポリシーファイルは、ポリシーの変更が発生した場合にのみダンプされます。

4 inventory.xml ログファイルおよび policies.xml ログファイルを表示するには、**/Library/Application\ Support/Dell/Dell\ Data\ Protection/** を参照してください。

Advanced Threat Prevention のインストールの確認

オプションで、インストールを確認できます。

1 コマンドバーの Dell Advanced Threat Prevention アイコンに緑色のバッジ  があることを確認します。

2 アイコンに感嘆符が表示されている場合は、右クリックして、**詳細を表示** を選択します。ユーザーが登録されていないことが表示される場合があります。

アップデートのチェック - Advanced Threat Prevention エンジンのアップデートを確認します。デルサーバポリシーのアップデートではありません。

バージョン情報 - 次の情報が含まれます。

- バージョン
- ポリシー - [online] はサーバベースのポリシーを示し、[offline] は Airgap またはオフラインベースのポリシーを示します。
- シリアル番号 - これを使用してサポートに連絡します。この番号は、インストールの一意の識別子です。

3 /Applications に、Dell Advanced Threat Prevention フォルダが作成されます。

Endpoint Security Suite Enterprise のログファイルの収集

DellLogs.zip には、Client Encryption and Advanced Threat Prevention 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。

Advanced Threat Prevention の詳細の表示

Advanced Threat Prevention クライアントをエンドポイントコンピュータにインストールすると、デルサーバによってエージェントとして認識されます。

コマンドバーの Advanced Threat Prevention アイコン  を右クリックして、**詳細を表示** を選択します。Advanced Threat Prevention の詳細画面には次のタブが表示されます。

脅威 タブ

脅威 タブでは、デバイスで検出されたすべての脅威および実行されたアクションを表示します。脅威とは、安全ではないファイルまたはプログラムとして新規に検出され、指示による修復が必要なイベントのカテゴリです。

カテゴリ 列には、次が含まれます。

- **危険** マルウェアになる可能性のある不審なファイル
- **異常** - マルウェアになる場合のある不審なファイル
- **隔離済み** - 元の場所から移動したファイルで、隔離フォルダに保存され、デバイス上で実行できなくなります。
- **免除** - デバイスでの実行が許可されているファイル。
- **クリア** — 組織でクリアされているファイル。クリアされたファイルには、免除されたファイル、安全リストに追加されたファイル、デバイスの隔離フォルダから削除されたファイルが含まれます。

Advanced Threat Prevention 脅威の分類の詳細については、デルサーバリモート管理コンソールで *AdminHelp* を参照してください。

エクスプロイト タブ

エクスプロイト タブでは、脅威と見なされるエクスプロイトを一覧表示します。

デルサーバポリシーにより、エクスプロイトが検出された場合に実行するアクションが決定されます。

- **無視** - 特定されたメモリ違反に対してアクションは実行されません。
- **アラート** - メモリの違反が記録され、デルサーバに報告されます。
- **ブロック** - アプリケーションがメモリ違反のプロセスの呼び出しを試行した場合、そのプロセスの呼び出しをブロックします。呼び出しを実行したアプリケーションの実行の継続を許可します。
- **終了** - アプリケーションがメモリ違反のプロセスの呼び出しを試行した場合、そのプロセスの呼び出しをブロックします。コールを発信したアプリケーションが終了します。

次のタイプのエクスプロイトが検出されます。

- スタックピボット
- スタック保護
- スキャナーメモリ検索
- 悪質なペイロード

エクスプロイトポリシーの詳細については、デルサーバのリモート管理コンソールで *AdminHelp* を参照してください。

イベント タブ

メモ: イベントは必ずしも脅威であるとは限りません。イベントは、認識されたファイルもしくはプログラムが隔離された、安全リストに掲載された、または免除されたときに生成されます。

イベント タブでは、デバイス上で発生したすべての脅威イベントを表示し、Advanced Threat Prevention によって割り当てられたイベントの種類ごとに表示します。システムが再起動すると、データが削除されます。

イベントの種類の例には次のようなものがあります。

見つかった脅威

削除された脅威

隔離された脅威

免除された脅威

変更された脅威

Advanced Threat Prevention のためのテナントのプロビジョニング

組織で Advanced Threat Prevention が使用されている場合、Advanced Threat Prevention のポリシーの施行がアクティブになる前に、デルサーバでテナントをプロビジョニングする必要があります。

前提条件

- システム管理者の役割を持つ管理者が実行する必要があります。
- デルサーバ上でプロビジョニングするためにインターネット接続が必要です。
- リモート管理コンソールで Advanced Threat Prevention オンラインサービスの統合を表示するために、クライアント上でインターネット接続が必要です。
- プロビジョニングは、プロビジョニング中に証明書から生成されるトークンに基づいています。
- Advanced Threat Prevention のライセンスがデルサーバ内に存在している必要があります。

テナントのプロビジョニング

1 リモート管理コンソールにログインし、**サービス管理** へ移動します。

2 **Advanced Threat Protection サービスのセットアップ** をクリックします。障害がこの時点で発生した場合は、ATP ライセンスをインポートします。

3 ライセンスがインポートされると、ガイド付きのセットアップを開始します。**次へ** をクリックして開始します。

4 EULA を読んで同意し（チェックボックスはデフォルトでは **オフ** です）、**次へ** をクリックします。

5 テナントのプロビジョニングに DDP Server に証明書を提供します。**次へ** をクリックします。*Cylance* ブランドの既存テナントのプロビジョニングはサポートされていません。

6 証明書をダウンロードします。これは、DDP Server との災害シナリオが発生した場合のリカバリに必要です。この証明書は、v9.2「upgrader」を介して自動的にバックアップされません。別のコンピュータで、証明書を安全な場所にバックアップします。証明書のバックアップを確定するために、チェックボックスをオンにして、**次へ** をクリックします。

7 セットアップが完了しました。**OK** をクリックします。

Advanced Threat Prevention エージェント自動アップデートの設定

デルサーバリモート管理コンソールで、Advanced Threat Prevention エージェントの自動アップデートを受信するように登録することができます。エージェントの自動アップデートを受信するよう登録することで、クライアントが Advanced Threat Prevention サーバから自動的にアップデートをダウンロード、適用するようになります。アップデートは毎月リリースされます。

メモ: エージェントの自動アップデートはデルサーバ v9.4.1 以降でサポートされます。

エージェントの自動アップデートの受信

エージェントの自動アップデートを受信するよう登録するには、次の操作を行います。

1 リモート管理コンソールの左ペインで、**管理** > **サービス管理** とクリックします。

2 エージェントの自動アップデートの下の **高度な脅威** タブで **オン** ボタンをクリックして、**プリファレンスの保存** ボタンをクリックします。
情報が入力され、自動アップデートが表示されるまで数分間かかることがあります。

エージェントの自動アップデート受信の停止

エージェントの自動アップデート受信を停止するには、次の操作を行います。

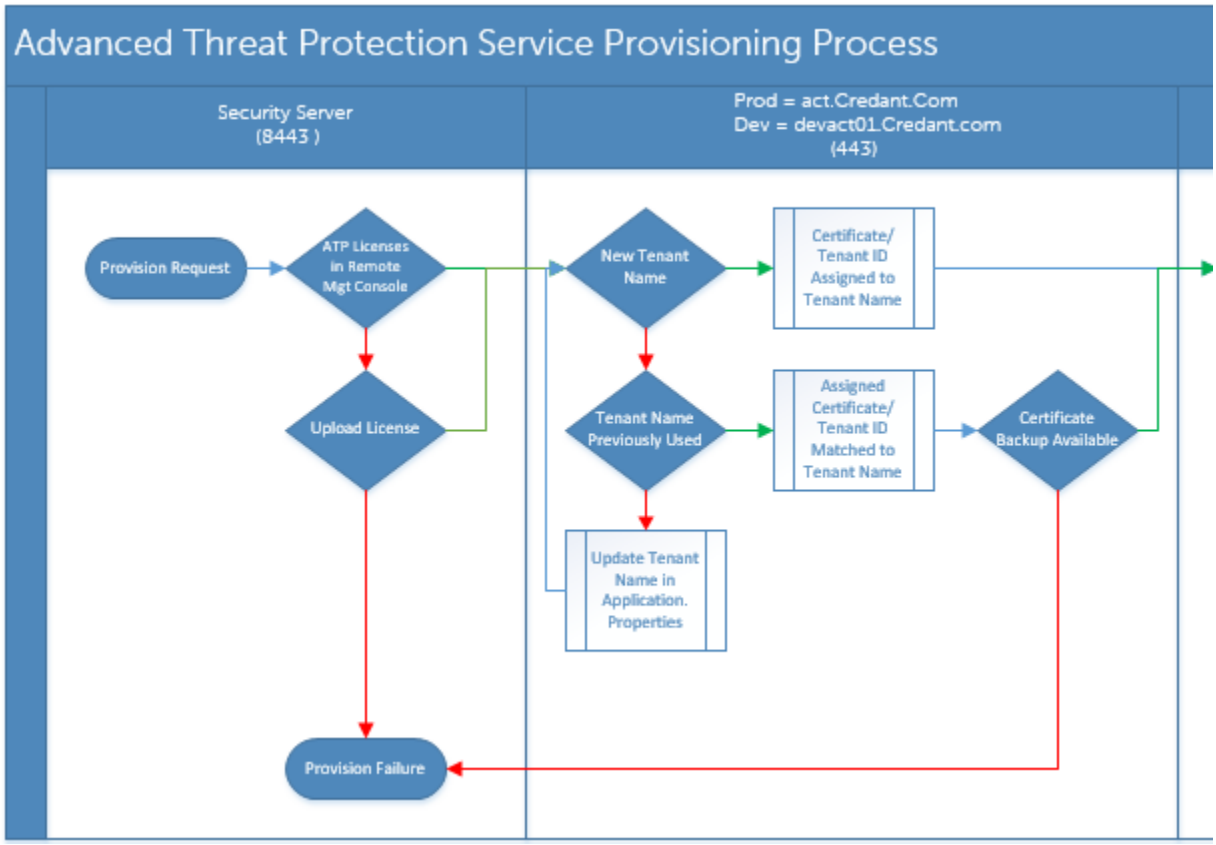
1 リモート管理コンソールの左ペインで、**管理** > **サービス管理** とクリックします。

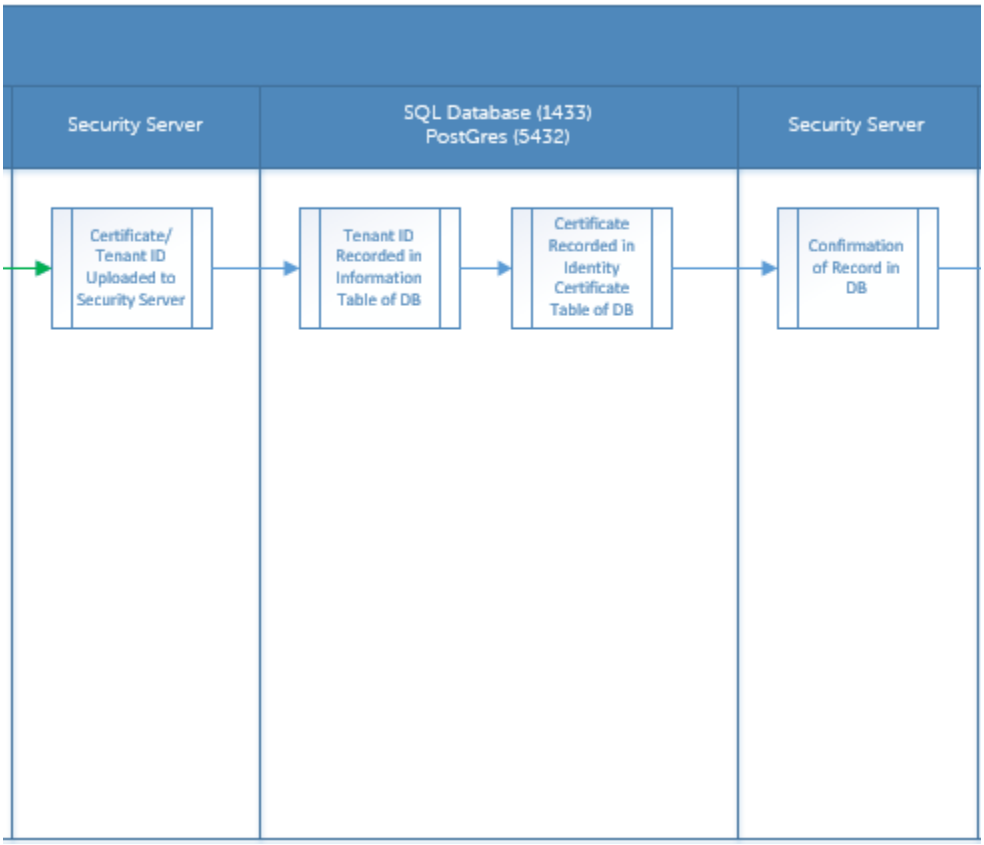
2 エージェントの自動アップデートの下の **高度な脅威** タブで **オフ** ボタンをクリックして、**プリファレンスの保存** ボタンをクリックします。

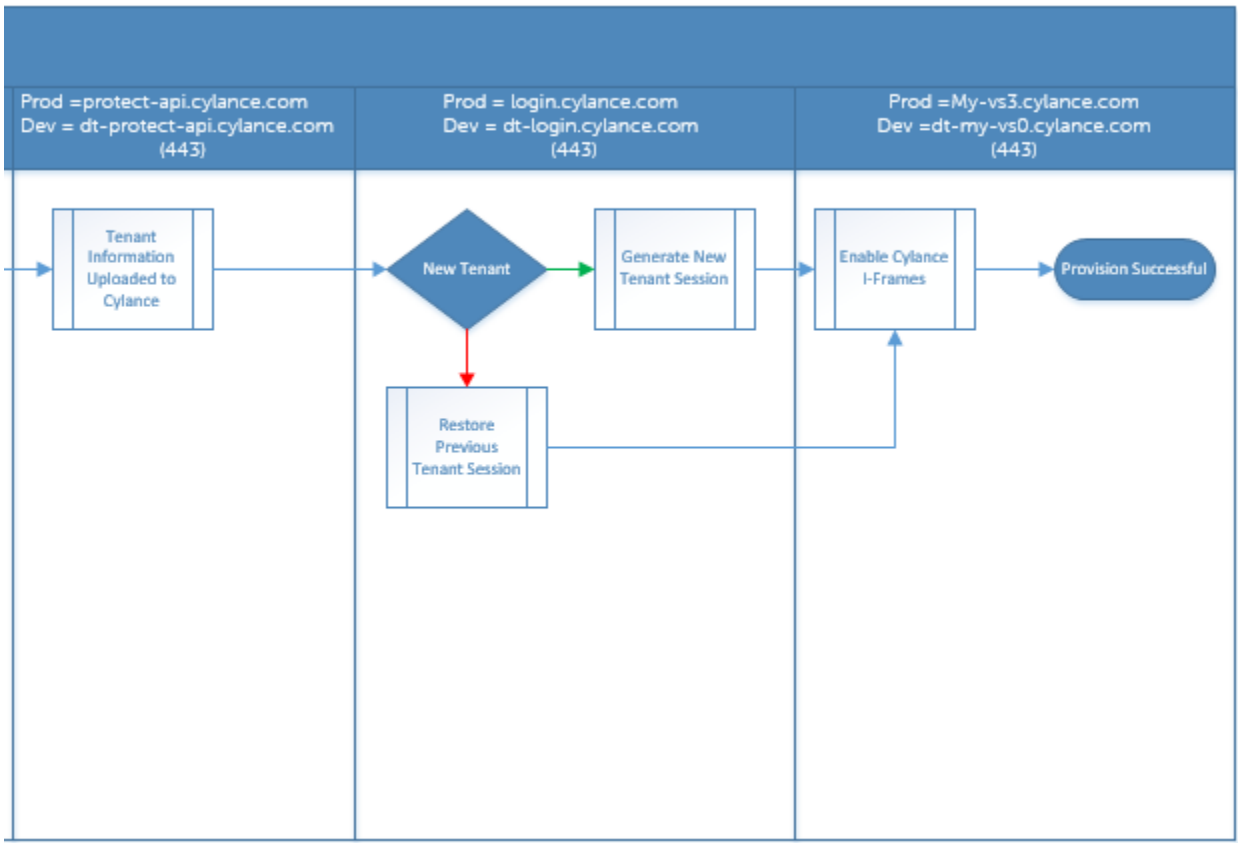
Advanced Threat Prevention クライアントのトラブルシューティング

Advanced Threat Prevention のプロビジョニングおよびエージェント通信

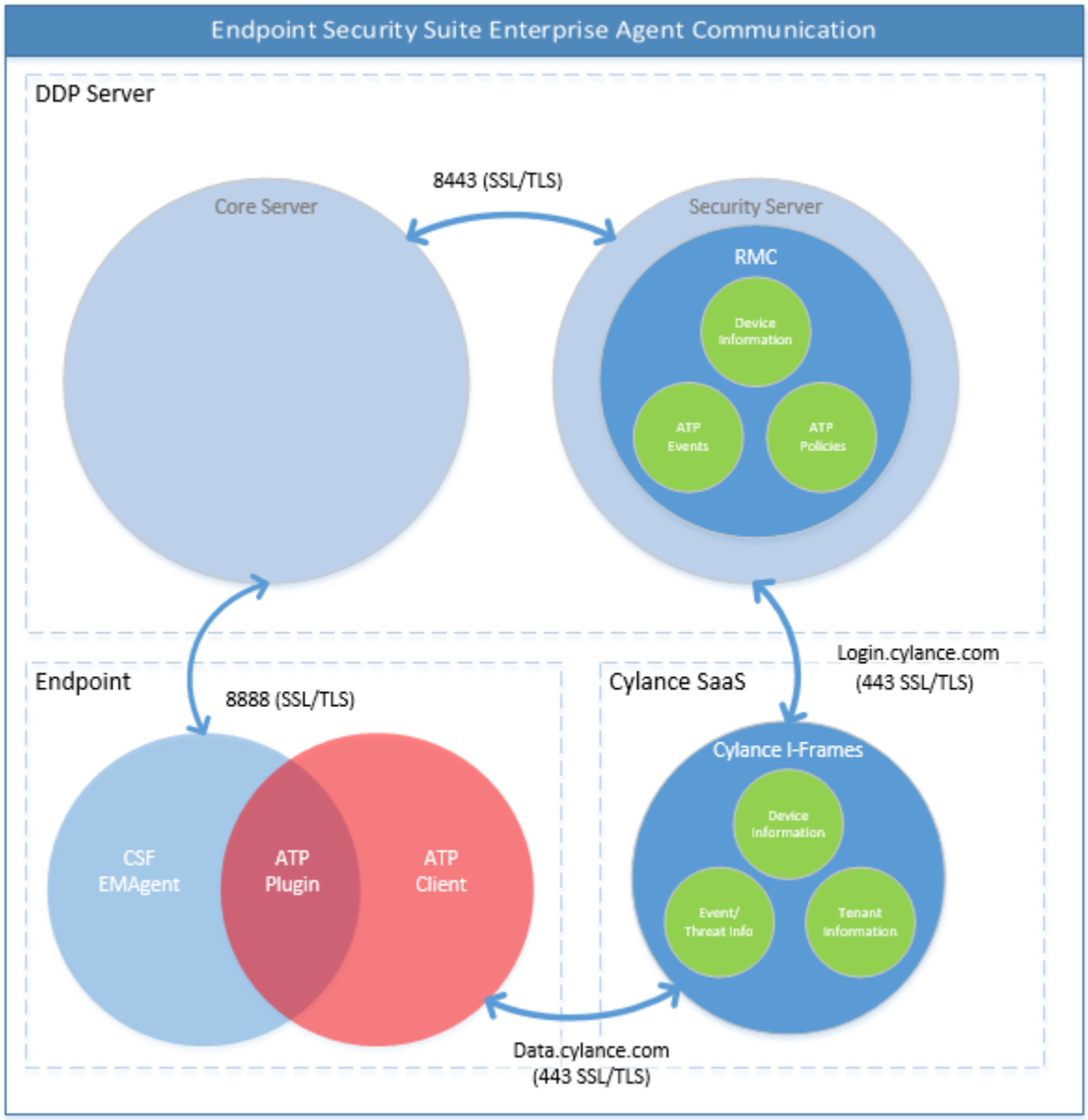
次の図は Advanced Threat Prevention サービスのプロビジョニングプロセスを表しています。







次の図は Advanced Threat Prevention のエージェント通信プロセスを表しています。


Endpoint Security Suite Enterprise Agent Communication
DDP Server
8443 (SSL/TLS)
Core Server
Security Server
RMC
Device Information
ATP Events
ATP Policies
Endpoint
8888 (SSL/TLS)
Cylance SaaS
Login.cylance.com
(443 SSL/TLS)
CSF EMAgent
ATP Plugin
ATP Client
Cylance I-Frames
Device Information
Event/ Threat Info
Tenant Information
Data.cylance.com
(443 SSL/TLS)

5

用語集

セキュリティサーバ - クライアント暗号化のアクティブ化に使用します。

ポリシープロキシ - ポリシーを Mac クライアント用ソフトウェアの Endpoint Security Suite Enterprise に配布するために使用します。

リモート管理コンソール - エンタープライズ全体の展開のために管理者コンソール。

Shield - 時折、マニュアルおよびクライアントユーザーインタフェースでこの用語が見られる場合があります。「Shield」は、クライアントソフトウェアを表すために使用される用語です。