Dell Endpoint Security Suite Enterprise for Mac

管理者ガイド v2.9

2021 年 3 月
Rev. A02

DELL EMC

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。**

目次

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 Server 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 Advanced Threat Prevention 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 Advanced Threat Prevention 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
- 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。

Endpoint Security Suite Enterprise for Mac には、2 つの.dmg ファイルがあります - 1 つは暗号化クライアント用で 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。

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、Endpoint Security Suite 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。

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 クライアント

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
• 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
• 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。 ○ 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）
• macOS High Sierra 10.13.6
• macOS Mojave 10.14.5 ~ 10.14.6
• 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

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

ハードウェア
• 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 • Mac OS X Yosemite 10.10.5 • macOS Sierra 10.12.6 **メモ:** Mac OS X Mavericks 10.9.5、Mac OS X Yosemite 10.10.5、および macOS Sierra 10.12 は、Advanced Threat Prevention でのみサポートされ、Encryption クライアントではサポートされません。
• macOS High Sierra 10.13.6 **メモ:** Encryption クライアントをサポートする特定の macOS High Sierra バージョンについては、「Encryption クライアントソフトウェア」を参照してください。
• macOS Mojave 10.14.5 ~ 10.14.6 **メモ:** ATP エージェントは macOS Mojave にインストールできますが、メモリ保護およびスクリプト制御機能は自動的に無効になり、現在はサポートされていません。
• macOS Catalina 10.15.3 ~ 10.15.4

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

互換性

次の表に、Windows、Mac、Linux との互換性の詳細を示します。

n/a：このプラットフォームにはテクノロジが適用されません。

空白：Endpoint Security Suite Enterprise のポリシーはサポートされません。

機能	ポリシー	Windows	macOS	Linux	
ファイルアクション					
	自動隔離（安全でない）	x	x	x	
	自動隔離（異常）	x	x	x	
	自動アップロード	x	x	x	
	ポリシー安全リスト	x	x	x	
メモリアクション					
	メモリ保護	x	x	x	
攻略					
	スタックピボット	x	x	x	
	スタック保護	x	x	x	
	コード上書き	x	n/a		
	RAM スクレイピング	x	n/a		
	悪質なペイロード	x			
プロセスインジェクション					
	メモリのリモート割り当て	x	x	n/a	
	メモリのリモートマッピング	x	x	n/a	
	メモリへのリモート書き込み	x	x	n/a	
	メモリへの PE のリモート書き込み	x	n/a	n/a	
	リモートでのコード上書き	x	n/a		
	メモリのリモートアンマップ	x	n/a		
	リモートでのスレッド作成	x	x		
	リモートでの APC スケジュール	x	n/a	n/a	
	DYLD インジェクション		x	x	
エスカレーション					
	LSASS 読み取り	x	n/a	n/a	
	ゼロ割り当て	x	x		
保護設定					
	実行制御	x	x	x	
	デバイスからのサービスシャットダウンを阻止する	x	x		

機能	ポリシー	Windows	macOS	Linux	
	安全でない実行中のプロセスとそのサブプロセスを強制終了する	x	x	x	
	バックグラウンド脅威検知	x	x	x	
	新しいファイルに注意する	x	x	x	
	スキャンするアーカイブファイルの最大サイズ	x	x	x	
	特定のフォルダを除外する	x	x	x	
	ファイルサンプルのコピー	x			
アプリケーション制御					
	変更ウィンドウ	x		x	
	フォルダの除外	x			
エージェントの設定					
	ログファイルの自動アップロードの有効化	x	x	x	
	デスクトップ通知の有効化	x			
スクリプト制御					
	アクティブスクリプト	x			
	Powershell	x			
	Office マクロ	x		n/a	
	Powershell コンソールの使用をブロック	x			
	当該フォルダ（およびサブフォルダ）内のスクリプトを承認	x			
	ロギングレベル	x			
	自己保護レベル	x			
	自動アップデート	x			
	検出の実行（エージェント UI から）	x			
	隔離対象を削除（エージェント UI およびコンソール UI）	x			
	接続切断モード	x		x	
	詳細脅威データ	x			
	安全リストの検証	x	x	n/a	
	マルウェアサンプルのコピー	x	x	x	
	プロキシ設定	x	x	x	

機能	ポリシー	Windows	macOS	Linux	
	手動ポリシーチェック (エージェント UI)	x	x		

3

Encryption クライアントのタスク

トピック：

Encryption Client 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 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。

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 client 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

Security Management Server Virtual クイック スタート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、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. Endpoint Security Suite 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
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 Credant Technologies (Dell, Inc*、旧称 *Credant Technologies) 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。	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 Credant Technologies (Dell, Inc*、旧称 *Credant Technologies) 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 Client 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 Endpoint Security Suite 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、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、Endpoint Security Suite 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 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/> [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>
```

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 Endpoint Security Suite Enterprise.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**

   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。
9. Encryption Client 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。

1. *[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。
2. 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。
3. 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。

4. 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 Client 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 client 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。

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。

   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	*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。
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。 管理コンソールで *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。
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、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 を使用して暗号化」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。
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。

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。

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、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に設定されています。
	メディアは Encryption External Media で暗号化され、Dell バッジで示されます。

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。

   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。

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。

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 にエスクロー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。

     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. 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。

   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、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 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 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 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**

  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、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。

- 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 暗号化がリカバリー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 クライアントで使用できます。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

- Recovery Utility を実行する暗号化されていない外部リカバリ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
- 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、管理コンソールで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. 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 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暗号化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. Recovery Utility を実行してリカバリ操作を行うために、外付けリカバリボリュームまたは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** をクリックして、[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。
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-Encryption-Enterprise-<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. 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。
10. (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。
11. **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、すべてのデータが透過的に暗号化および復号化されます。

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。個人リカバリー 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ーする (最も一般的な手順)
   - 非起動ボリュームをリカバリーする (まれに使用される手順)

起動ボリュームをリカバリーする (最も一般的な手順)

ほとんどのリカバリーでは、起動ボリュームをリカバリー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

- 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。

   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。

    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、*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。

    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すみます。

    [リカバリー操作の結果] 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 *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>EMSHFSPlusOptIn</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ー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。
  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。

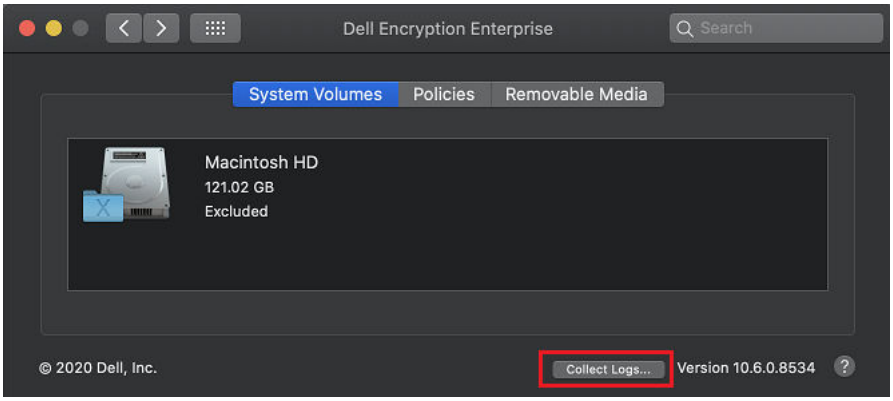
Endpoint Security Suite Enterprise for Mac の場合、次の監査メッセージを表示します。

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 > エンタープライズ または エンドポイント］の順にクリックします。
3. ［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 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 および 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。

Encryption Client 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 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 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 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 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。

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 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）

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。

Endpoint Security Suite Enterprise for Mac がインストールされたコンピューターの Boot Camp で Endpoint Security Suite Enterprise for Windows を使用するには、FileVault2 で 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。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 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。

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 の回復

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、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。

    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. 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\ 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	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。 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 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。	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	

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
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。
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

4

タスク

トピック：

Advanced Threat Prevention for Mac のインストール

このセクションでは、Advanced Threat Prevention のインストール方法を説明します。

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。

- 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 のインストールおよびマイグレーションガイド

  Security Management Server Virtual クイックスタートガイドおよびインストールガイド
- デルサーバのホスト名とポートが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に必要です。
- ターゲットコンピュータが Dell Server にネットワークで接続でき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。

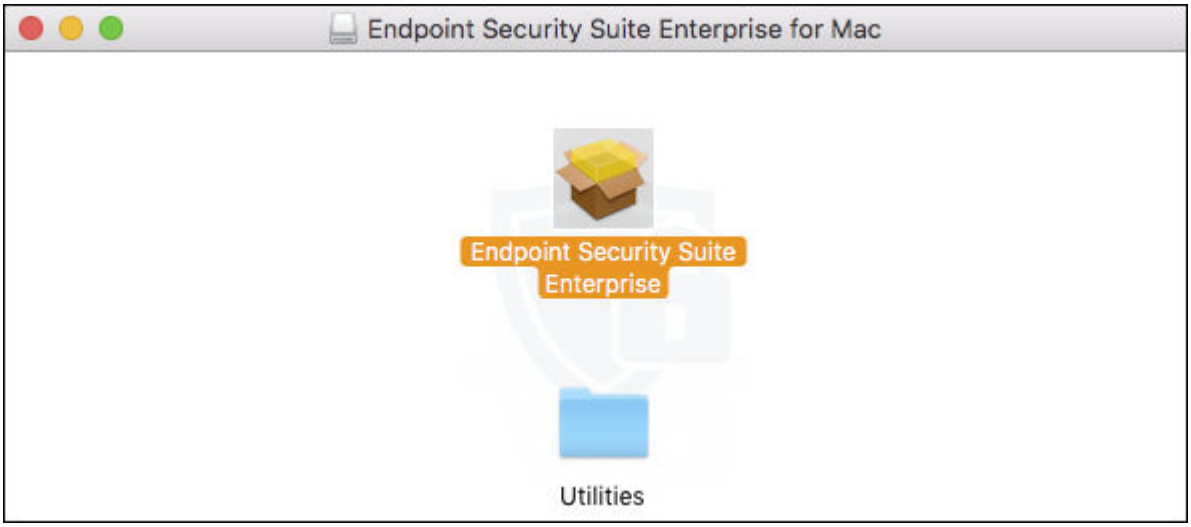
クライアントソフトウェアをインストールするには、次の手順に従います。これらの手順を実行するには、管理者アカウントが必要です。

メモ:

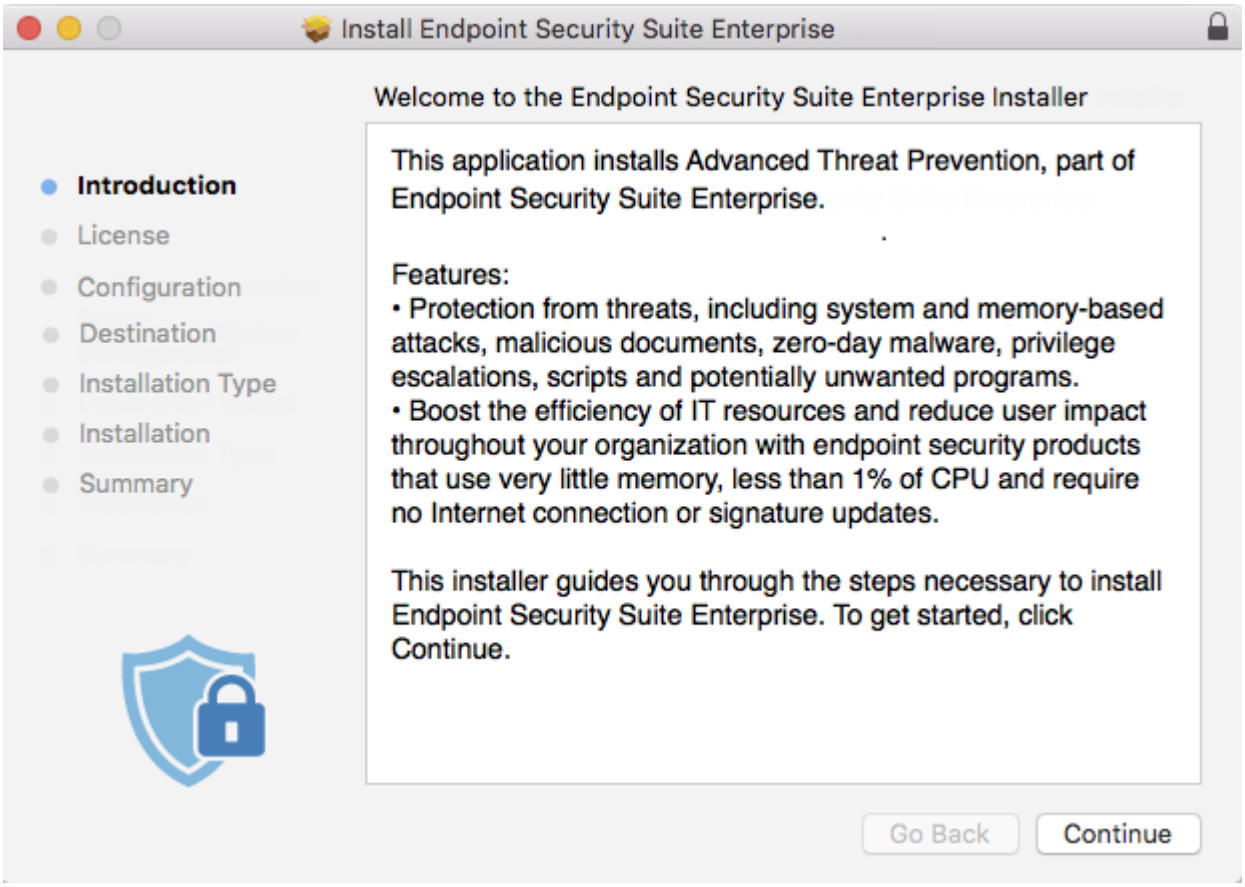
作業を開始する前に、ユーザーの作業を保存し、他のアプリケーションを閉じます。

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。

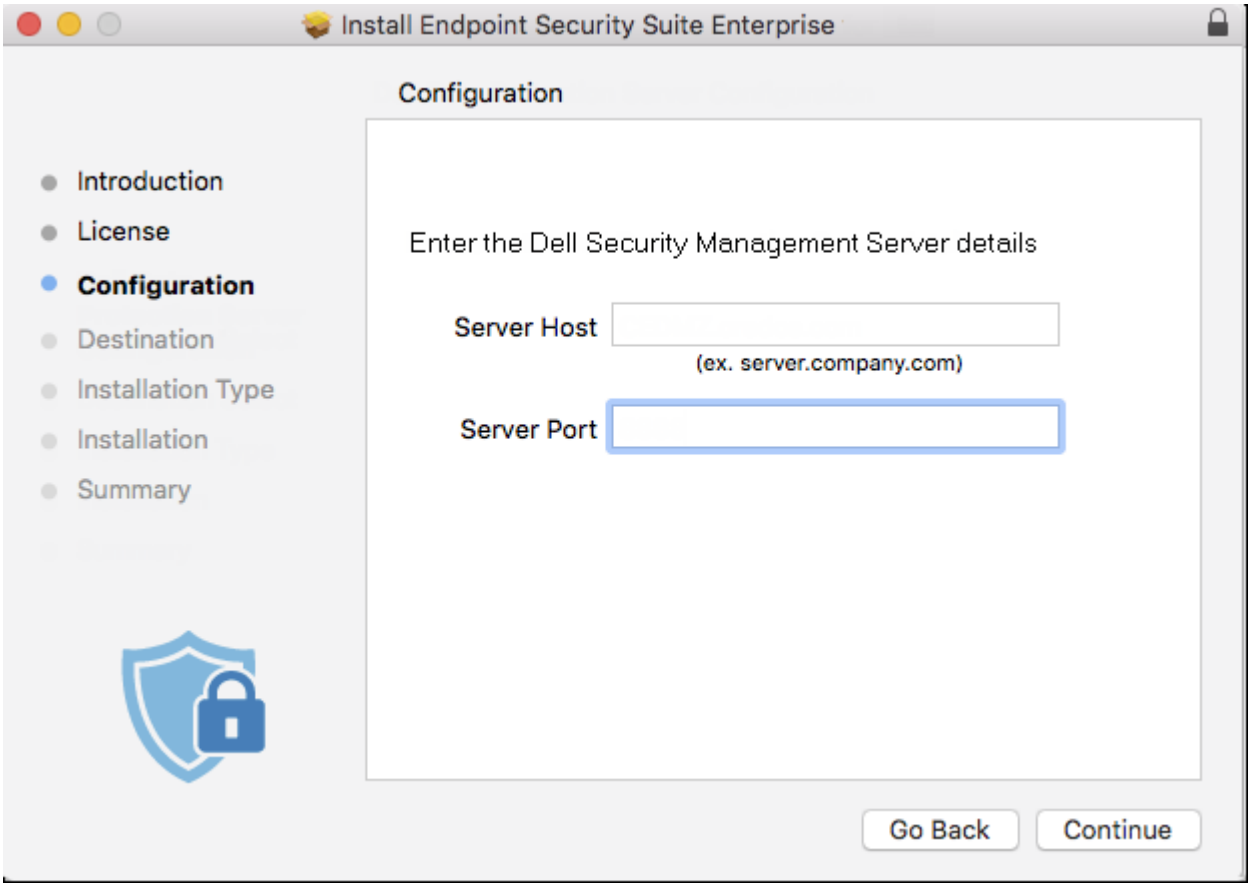
Endpoint Security Suite Enterprise for Mac パッケージが開きます。



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。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. *サーバホスト* フィールドに、ターゲットユーザーを管理する Dell Server 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が必要とする管理者アカウントの資格情報を入力して、[ソフトウェアをインストール] 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. パッケージを閉じます。
12. 「Advanced Threat Prevention のインストールの確認」を参照してください。

システムが Dell サーバに登録されていない場合は、ログを参照して Dell Server 上に有効な証明書があるかどうかを判断してください。「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

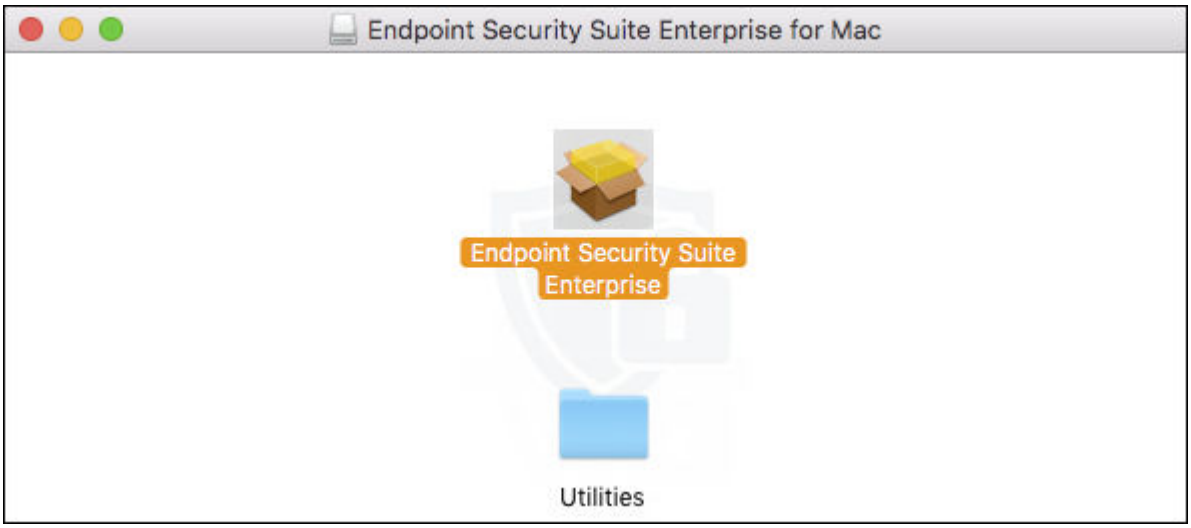
Endpoint Security Suite Enterprise のアンインストール アプリケーションを実行してクライアントソフトウェアをアンインストールする場合があります。クライアントソフトウェアをアンインストールするには、次の手順に従います。

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、**Endpoint Security Suite Enterprise のアンインストール** 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。

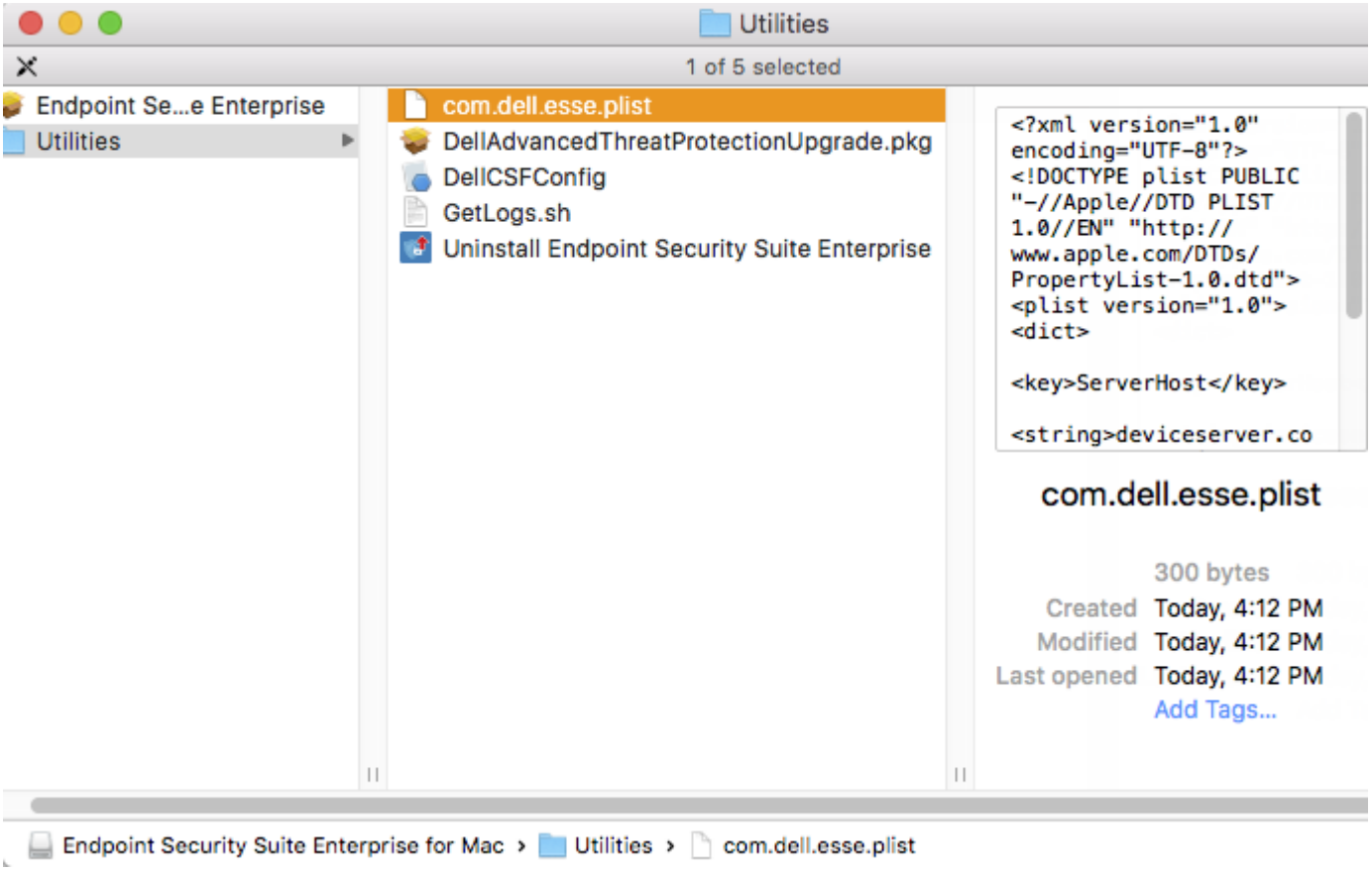
Advanced Threat Prevention のコマンドラインインストール

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 Dell Server 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>server.organization.com</string>
  <key>ServerPort</key>
  <string>8888</string>
  <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に対して **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 信頼証明書またはポリシーチェックの無効化

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。

お使いの環境で自己署名証明書を実行する場合は、PolicyCheck を無効にします。

お使いの環境内に自己署名証明書があり、Mac 上のキーチェーンに証明書をインポートしていない場合は、DisableCertTrust および DisablePolicyCheck の両方を False に設定してください。

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.app/Contents/MacOS/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
DisableCertTrust = False
DisablePolicyCheck = 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、`DisableCertTrust` を **True** に変更します。
6. クライアントでポリシー署名チェックを無効にするには、`DisablePolicyCheck` 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。

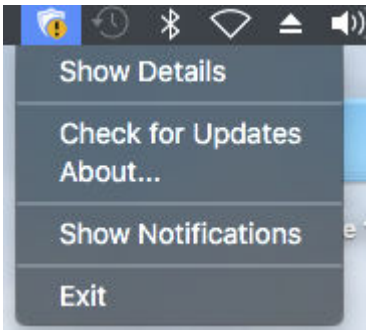
1. 上記のとおり、DellCSFConfig.app を実行します。
2. DumpXmlInventory を **True** に変更します。
3. DumpPolicies を **True** に変更します。

   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

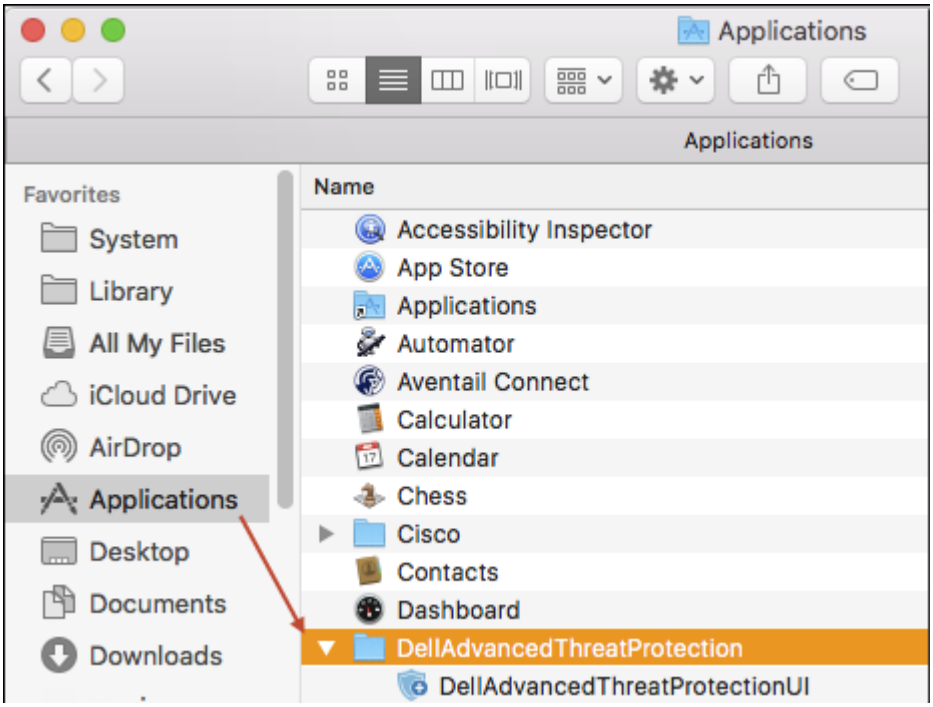
オプションで、インストールを確認できます。

1. コマンドバーの 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。



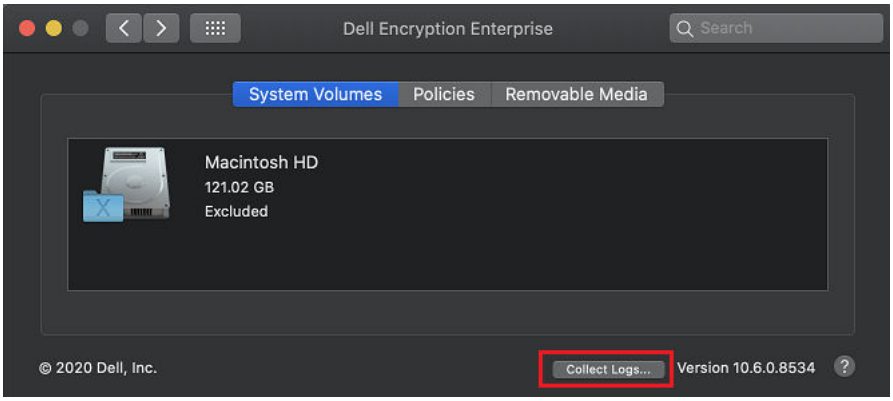
   アップデートのチェック - Advanced Threat Prevention エンジンのアップデートを確認します。Dell Server ポリシーのアップデートではありません。

   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、Advanced Threat Prevention フォルダが作成されます。



Endpoint Security Suite 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 および 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。

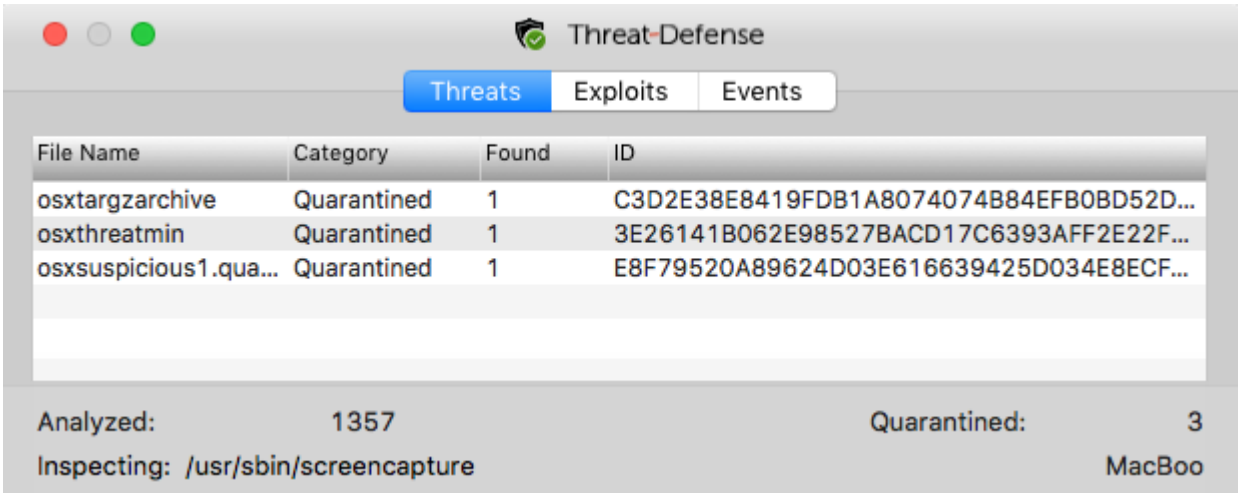
Advanced Threat Prevention の詳細表示

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、Dell Server 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。



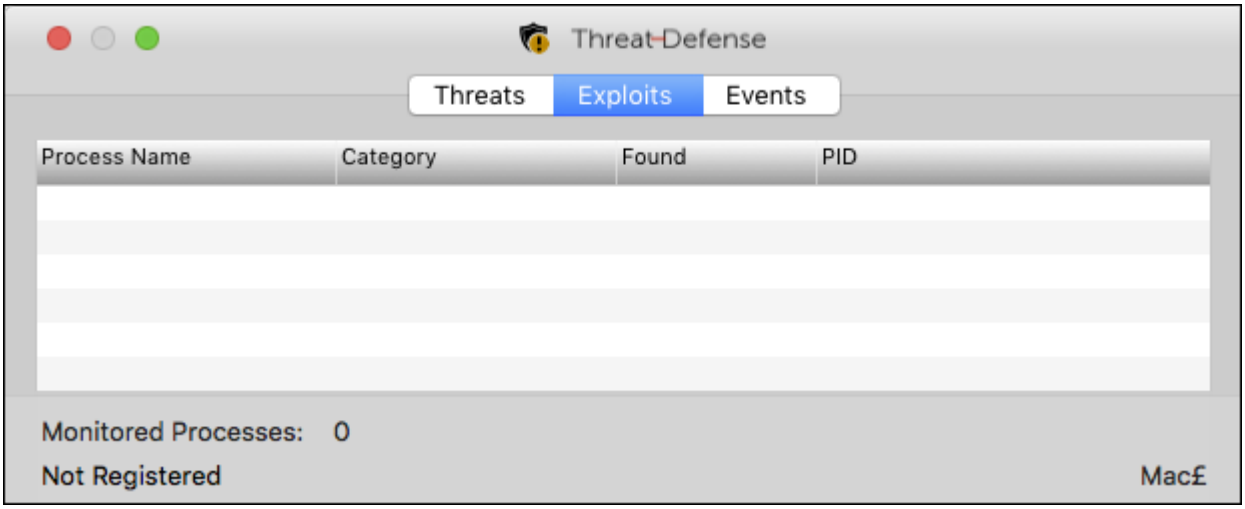
カテゴリ 列には、次が含まれます。

- **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 の脅威分類の詳細については、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。



Dell Server ポリシーで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まります。

- **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、Dell Server 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

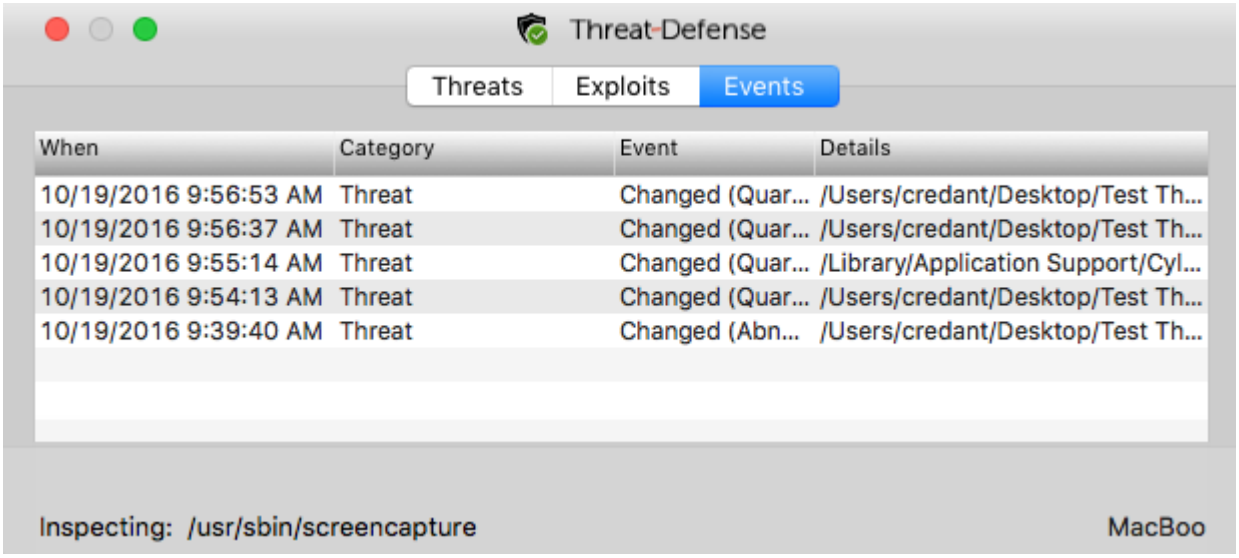
エクスプロイトポリシーの詳細については、管理コンソールで *AdminHelp* を参照してください。

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

テナントのプロビジョニング

Advanced Threat Prevention のポリシーの施行がアクティブになる前に、テナントが Dell Server にプロビジョニングされる必要があります。

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。
- Dell Server でプロビジョニングをするにはインターネット接続が必要です。
- 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 Dell Server 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. 管理コンソールに Dell 管理者としてログインします。
2. 管理コンソールの左ペインで、**管理** > **サービス管理** の順にクリックします。
3. **Advanced Threat Protection サービスのセットアップ** をクリックします。この時点で不具合が発生する場合は、Advanced Threat Prevention ライセンスをインポートします。
4. ライン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が始まります。**次へ** をクリックして開始します。
5. EULA を読み、合意した後、[次へ] をクリックします。
6. テナントのプロビジョニングのために Dell Server に ID 資格情報を入力します。**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。*
7. 証明書をダウンロードします。これは Dell Server での災害シナリオが発生した場合のリカバリに必要です。この証明書は自動的にバックアップされません。別のコンピュータの安全な場所に証明書をバックアップします。証明書をバックアップしたことを確認するチェックボックスを選択してから [次へ] をクリックします。
8. 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

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により、クライアントが Advanced Threat Prevention サービスからアップデートを自動ダウンロードして適用できるようになります。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 Dell Server 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. 管理コンソールの左ペインで、[管理] > [サービス管理] を順にクリックします。
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] をクリックして、[プリファレンスの保存] 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

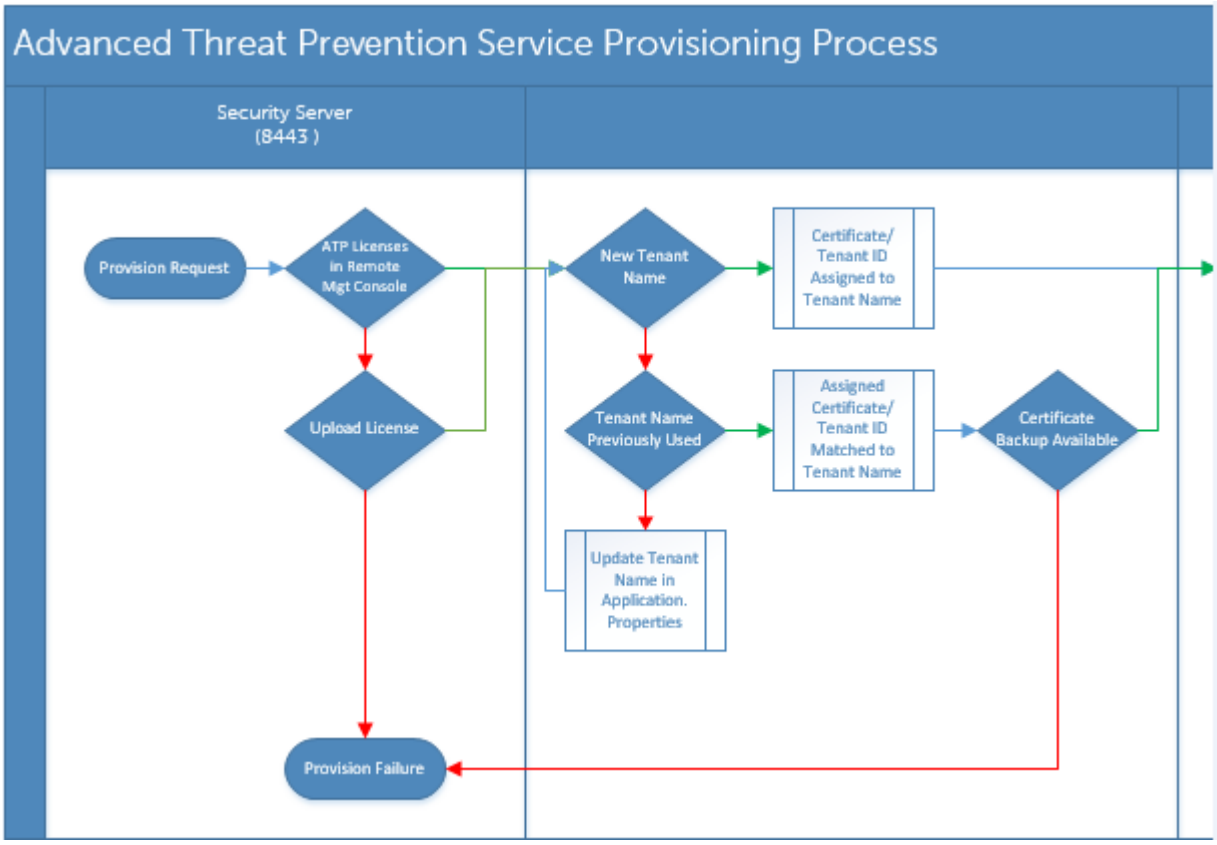
エージェントの自動アップデート受信を停止するには、次の操作を行います。

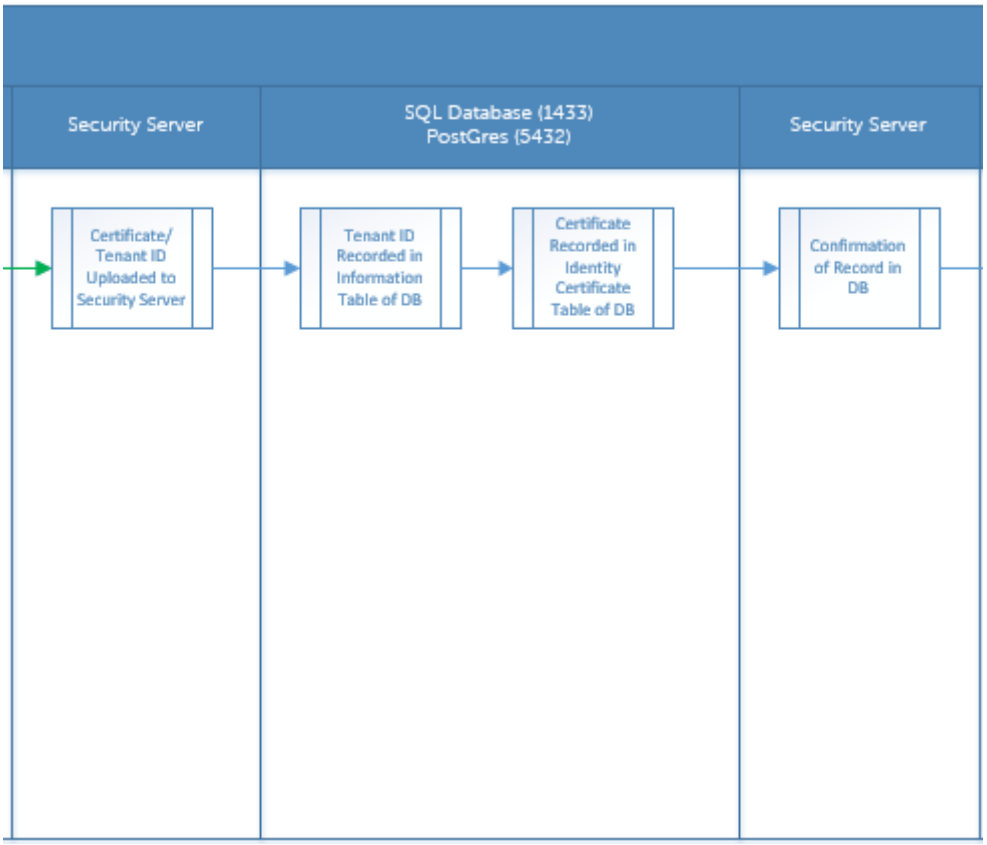
1. 管理コンソールの左ペインで、[管理] > [サービス管理] を順にクリックします。
2. *エージェントの自動アップデート* の下の *高度な脅威* タブで [オフ] をクリックして、[プリファレンスの保存] をクリックします。

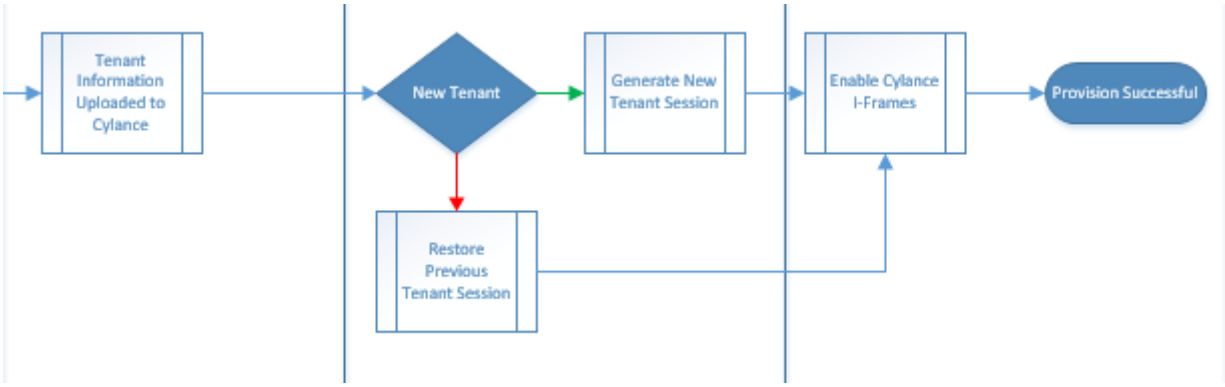
Advanced Threat Prevention のトラブルシューティング

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

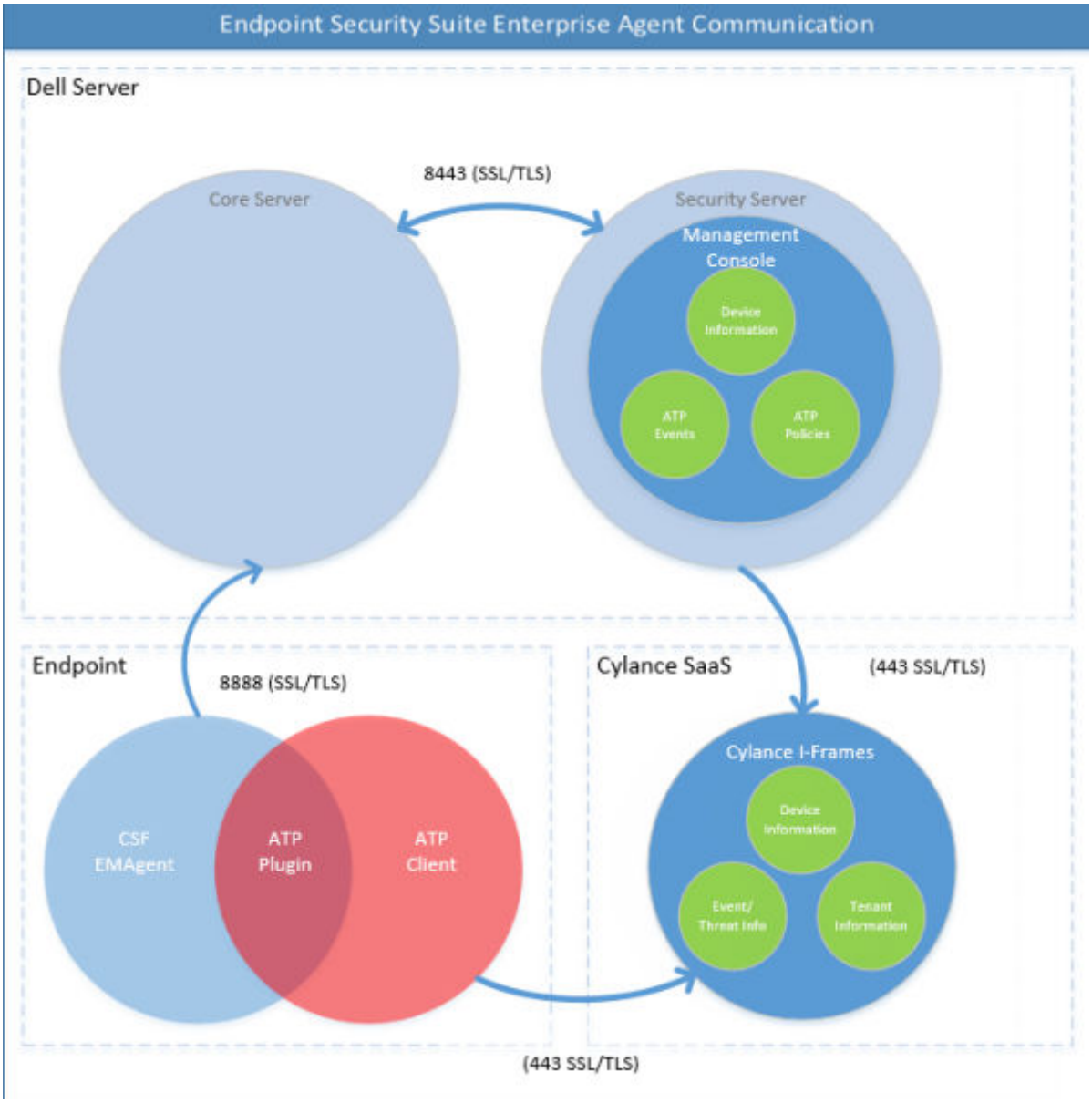
次の図は Advanced Threat Prevention サービスのプロビジョニングプロセスを表しています。


Advanced Threat Prevention Service Provisioning Process
Security Server
(8443)
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
New Tenant Name
Certificate/ Tenant ID Assigned to Tenant Name
Tenant Name Previously Used
Assigned Certificate/ Tenant ID Matched to Tenant Name
Certificate Backup Available
Update Tenant Name in Application. Properties
Provision Failure


Security Server
SQL Database (1433)
PostGres (5432)
Security Server
Certificate/ Tenant ID Uploaded to Security Server
Tenant ID Recorded in Information Table of DB
Certificate Recorded in Identity Certificate Table of DB
Confirmation of Record in DB



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。



5

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。