Endpoint Security Suite Enterprise

基本インストールガイド v2.1

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。

2018 - 11

Rev. A01

目次

1

はじめに

本書では、Endpoint Security Suite Enterprise を使用してアプリケーションをインストールおよび設定する方法について詳しく説明します。本書には、基本インストールの手順が記載されています。子インストーラのインストール、Security Management Server/Security Management Server Virtual の設定、または Endpoint Security Suite Enterprise マスターインストーラに関する詳細なサポート情報が必要な場合は、『詳細インストールガイド』を参照してください。

すべてのポリシー情報とその説明は AdminHelp で参照できます。

作業を開始する前に

1 クライアントを導入する前に、Dell Server をインストールしてください。次に示すように、正しいガイドを探し、記載されている手順に従った後、このガイドに戻ります。

- *Security Management Server Installation and Migration Guide*（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 Quick Start Guide and Installation Guide*（Security Management Server Virtual クイックスタートガイド / インストールガイド）
- 希望のポリシーを設定しているかを確認します。**?** のマークから AdminHelp を参照します。画面の右上にあります。AdminHelp はポリシーの設定および変更、Dell Server でのオプションを理解するのに役立つよう設計されたページヘルプです。

2 Advanced Threat Prevention のための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。

3 本書の「要件」の章をすべて読んでください。

4 ユーザーにクライアントを導入します。

このガイドの使用法

このガイドは次の順序で使用してください。

- クライアントの必要条件については、「要件」を参照してください。
- 次のいずれかを選択してください。
  - マスターインストーラを使用した対話型のインストール

    または
  - マスターインストーラを使用したコマンドラインによるインストール

Dell ProSupport へのお問い合わせ

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

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

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

米国外の電話番号については、Dell ProSupport の各国の電話番号を記載したページを参照してください。

2

要件

すべてのクライアント

- 導入中は、IT ベストプラクティスに従う必要があります。これには、初期テスト向けの管理されたテスト環境や、ユーザーへの時間差導入が含まれますが、それらに限定されるものではありません。
- インストール、アップグレード、アンインストールを実行するユーザーアカウントは、ローカルまたはドメイン管理者ユーザーである必要があります。これは、Microsoft SCCM または Quest KACE などの導入ツールによって一時的に割り当てることができます。昇格された権限を持つ非管理者ユーザーはサポートされません。
- インストールまたはアンインストールを開始する前に、重要なデータをすべてバックアップします。
- インストール中は、外付け（USB）ドライブの挿入や取り外しを含め、コンピュータに変更を加えないでください。
- 管理者は、必要なすべてのポートが使用可能であることを確認します。
- 必ず www.dell.com/support で、最新の文書およびテクニカルアドバイザリーを定期的に確認してください。
- **メモ: Dell Data Security の製品ラインでは、Windows Insider Preview リリースはサポートされていません。**

すべてのクライアント - 前提条件

- 以下の前提条件となるコンポーネントがコンピュータにインストールされていない場合は、マスターインストーラによってインストールされます。

前提条件
– Visual C++ 2012 更新プログラム 4 以降再頒布可能パッケージ（x86 および x64）
– Visual C++ 2015 更新プログラム 3 以降再頒布可能パッケージ（x86 および x64）

Windows 7 にインストールされている場合、Visual C++ 2015 には Windows Update KB2999226 が必要です。

Endpoint Security Suite Enterprise マスターインストーラおよび子インストーラのクライアントには、Microsoft .Net Framework 4.5.2 以降が必要です。インストーラは、Microsoft .Net Framework コンポーネントをインストールしません。

インストールされている Microsoft .Net のバージョンを検証するには、インストール対象のコンピュータで http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx に記載されている手順を実行します。Microsoft .Net Framework 4.5.2 をインストールするには、https://www.microsoft.com/ja-jp/download/details.aspx?id=42643 にアクセスします。

すべてのクライアント - ハードウェア

- 次の表に、最低限のサポート対象コンピュータハードウェアの詳細を示します。

ハードウェア
– Intel Pentium または AMD プロセッサ
– 500 MB の使用可能ディスク容量
– 2 GB RAM

メモ: エンドポイントでファイルを暗号化する場合は、追加の空きディスク容量が必要になります。このサイズは、ポリシーとドライブのサイズによって異なります。

すべてのクライアント - ローカライズ

- Encryption、、Advanced Threat Prevention、および BitLocker Manager クライアントは多言語ユーザーインタフェース(MUI)に対応しており、次の言語にローカライズされています。フルディスク暗号化は英語版のオペレーティングシステムでのみサポートされます。管理コンソールに表示されている Advanced Threat Prevention データは英語のみです。

  言語サポート

  - EN - 英語
  - ES - スペイン語
  - FR - フランス語
  - IT - イタリア語
  - DE - ドイツ語
  - JA - 日本語
  - KO - 韓国語
  - PT-BR - ポルトガル語 (ブラジル)
  - PT-PT - ポルトガル語 (ポルトガル (イベリア))

Encryption クライアント

- クライアントコンピュータは、アクティブ化するためにネットワーク接続が必要です。
- 最初の暗号化スイープ中にスリープモードをオフにして、誰も操作していないコンピュータがスリープ状態になるのを防ぎます。スリープ状態のコンピュータでは暗号化は行われません (復号化も行われません)。
- Encryption クライアントは、デュアルブート設定をサポートしていません。これは、もう一方のオペレーティングシステムのシステムファイルが暗号化され、その動作を妨げるおそれがあるためです。
- Encryption クライアントは、業界をリードするアンチウイルスプロバイダを使用して検証されます。これらのアンチウイルスプロバイダに関しては、アンチウイルススキャンおよび暗号化における互換性を確保するために、ハードコーディングされた除外が設定されています。Encryption クライアントは、Microsoft Enhanced Mitigation Experience Toolkit でもテスト済みです。

  リストにないアンチウイルスプロバイダが組織で使用されている場合は、http://www.dell.com/support/article/us/en/19/SLN288353/ を参照するか、Dell ProSupport に連絡してサポートを受けてください。
- インプレイスでのオペレーティングシステムの再インストールがサポートされていません。オペレーティングシステムを再インストールするには、ターゲットコンピュータをバックアップしてからそのコンピュータをワイプし、オペレーティングシステムをインストールした後、確立した回復手順に従って暗号化されたデータを回復してください。

Encryption クライアントの前提条件

Encryption クライアントのオペレーティングシステム

- 次の表は、対応オペレーティングシステムの詳しい説明です。

  Windows オペレーティングシステム (32 ビットと 64 ビット)

  - Windows 7 SP1：Enterprise、Professional、Ultimate
  - アプリケーション互換テンプレートでの Windows Embedded Standard 7
  - Windows 8： Enterprise、Pro
  - Windows 8.1：Enterprise、Pro
  - Windows Embedded 8.1 Industry Enterprise

Windows オペレーティングシステム（32 ビットと 64 ビット）

- Windows 10：Education、Enterprise、Pro バージョン 1607（Anniversary Update/Redstone 1）からバージョン 1803（April 2018 Update/Redstone 4）
- VMware Workstation 12.5 以降

メモ:
UEFI モードを使用すると、セキュアハイバネーションポリシーがサポートされません。

Deferred Activation が付属した Encryption クライアントのオペレーティングシステム

- Deferred Activation では、アクティブ化中に使用される Active Directory ユーザーアカウントは、エンドポイントへのログインに使用されるアカウントとは独立したものになります。ネットワークプロバイダが認証情報を取得する代わりに、プロンプトが表示されたときにユーザーが手動で Active Directory ベースのアカウントを指定します。資格情報が入力されると、認証情報は安全に Dell Server に送信され、構成された Active Directory ドメインに対して Dell サーバで認証情報が検証されます。詳細については、http://www.dell.com/support/article/us/en/19/sln306341 を参照してください。
- 次の表で、対応オペレーティングシステムについて詳しく説明します。

Windows オペレーティングシステム（32 ビットと 64 ビット）

- Windows 7 SP1：Enterprise、Professional、Ultimate
- アプリケーション互換テンプレートでの Windows Embedded Standard 7
- Windows 8： Enterprise、Pro
- Windows 8.1：Enterprise、Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10：Education、Enterprise、Pro バージョン 1607（Anniversary Update/Redstone 1）からバージョン 1803（April 2018 Update/Redstone 4）

Encryption External Media オペレーティングシステム

- 次の表に、Encryption External Media によって保護されているメディアにアクセスする場合にサポートされるオペレーティングシステムの詳細を示します。

メモ:
Encryption External Media をホストするには、外部メディア上の約 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。

Encryption External Media で保護されたメディアにアクセスする場合にサポートされる Windows オペレーティングシステム（32 ビットと 64 ビット）

- Windows 7 SP1：Enterprise、Professional、Ultimate
- アプリケーション互換テンプレートでの Windows Embedded Standard 7
- Windows 8： Enterprise、Pro
- Windows 8.1：Enterprise、Pro
- Windows Embedded 8.1 Industry Enterprise
- Windows 10：Education、Enterprise、Pro バージョン 1607（Anniversary Update/Redstone 1）からバージョン 1803（April 2018 Update/Redstone 4）

Encryption External Media で保護されたメディアにアクセスする場合にサポートされる Mac オペレーティングシステム（64 ビットカーネル）

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 ~ 10.13.6
- macOS Mojave 10.14

フルディスク暗号化

フルディスク暗号化は、コマンドラインインタフェース（CLI）で**のみ**インストールできます。フルディスク暗号化をインストールする場合、手順については『Endpoint Security Suite Enterprise 詳細インストールガイド』をダウンロードしてください。

- フルディスク暗号化では、v9.8.2 以降を実行する Dell サーバに対してアクティブ化が必要です。
- フルディスク暗号化は、仮想ホストコンピュータでは現在サポートされていません。
- マルチドライブ構成のフルディスク暗号化は、サポートされていません。
- インストールされた FDE 機能では、サードパーティ資格情報プロバイダは機能しません。PBA を有効にすると、サードパーティ資格情報プロバイダはすべて無効になります。
- クライアントコンピュータには、アクティブ化するためにネットワーク接続またはアクセスコードが必要です。
- スマートカードユーザーが最初に起動前認証でログインする場合には、有線ネットワーク接続が必要です。
- フルディスク暗号化が行われている場合、オペレーティングシステムの機能アップデートはサポートされません。
- PBA が Dell サーバと通信するためには有線接続が必要です。
- SED はターゲットコンピュータ上に存在することはできません。
- フルディスク暗号化は、BitLocker または BitLocker Manager ではサポートされていません。BitLocker または BitLocker Manager がインストールされているコンピュータには、フルディスク暗号化をインストールしないでください。
- PBA に利用されている NVMe ドライブ - デルの PBA 管理では NVMe ドライブ上の AHCI をサポートしていないため、BIOS の SATA 操作を RAID ON に設定する必要があります。
- PBA に利用されている NVMe ドライブ - BIOS のブートモードは UEFI である必要があります。またレガシーオプションの ROM は無効にする必要があります。
- PBA に利用されている非 NVMe ドライブ - Dell の PBA 管理では非 NVMe ドライブ上の RAID をサポートしていないため、BIOS の SATA 操作を AHCI に設定する必要があります。

  - （ロックされた非 NVMe ドライブで利用できないセクターでの）読み書き対象の RAID 関連データへのアクセスが起動時にサポートされておらず、ユーザーがログインした後までこのデータの読み取りを待機できないために、RAID ON がサポートされません。
  - AHCI コントローラドライバがあらかじめインストールされていない場合に RAID ON > AHCI から切り替えると、オペレーティングシステムがクラッシュします。RAID から AHCI（またはその逆）に切り替える方法については、http://www.dell.com/support/article/us/en/19/SLN306460 を参照してください。

    NVMe ドライブでは、Intel ラピッドストレージテクノロジードライバのバージョン 15.2.0.0 以降を推奨します。
- 最初の暗号化スイープ中にスリープモードをオフにして、誰も操作していないコンピュータがスリープ状態になるのを防ぎます。スリープ状態のコンピュータでは暗号化は行われません（復号化も行われません）。
- フルディスク暗号化クライアントは、デュアルブート設定をサポートしていません。これは、もう一方のオペレーティングシステムのシステムファイルが暗号化され、その動作を妨げるおそれがあるためです。
- インプレイスでのオペレーティングシステムの再インストールがサポートされていません。オペレーティングシステムを再インストールするには、ターゲットコンピュータをバックアップしてからそのコンピュータをワイプし、オペレーティングシステムをインストールした後、確立した回復手順に従って暗号化されたデータを回復してください。
- **メモ: 起動前認証ではパスワードが必要です。社内セキュリティポリシーに準拠した最小限のパスワード設定を行うことをお勧めします。**

メモ: フルディスク暗号化の設定では、暗号化アルゴリズムを AES 256 に、暗号化モードを CBC に設定する必要があります。

フルディスク暗号化クライアントの前提条件

- Microsoft .Net Framework 4.5.2（またはそれ以降）は、マスターインストーラおよび子インストーラクライアントに必要です。インストーラは、Microsoft .Net Framework コンポーネントをインストールしません。

  インストールされている Microsoft .Net のバージョンを検証するには、インストール対象のコンピュータで http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx に記載されている手順を実行します。Microsoft .Net Framework 4.5.2 をインストールするには、https://www.microsoft.com/ja-jp/download/details.aspx?id=42643 にアクセスします。

フルディスク暗号化クライアントのハードウェア

- 次の表は、サポートされているハードウェアの詳細です。

オプションの組み込みハードウェア
– TPM 1.2 または 2.0

フルディスク暗号化クライアントのオペレーティングシステム

- 次の表では、対応オペレーティングシステムが詳しく説明されています。

Windows オペレーティングシステム（64 ビット）
– Windows 7 SP1：Enterprise、Professional、Ultimate（レガシーブートモードが必要）
– Windows 10：Education、Enterprise、Pro バージョン 1607（Anniversary Update/Redstone 1）からバージョン 1803（April 2018 Update/Redstone 4）（UEFI ブートモードが必要）

Advanced Threat Prevention クライアント

- クライアントを管理している Dell Server を接続モード（デフォルト）で実行しているときに Advanced Threat Prevention のインストールを完了するには、コンピュータのネットワーク接続が必要です。ただし、管理用の Dell Server を切断モードで実行している場合は、Advanced Threat Prevention のインストールにネットワーク接続は**必要ありません**。
- Advanced Threat Prevention 用のテナントをプロビジョニングするには、Dell Server がインターネットに接続されている必要があります。
- 切断モードで実行している Dell Server によって管理されるクライアントコンピュータでは、オプションの Client Firewall および Web Protection の機能をインストール**しない**でください。
- 他のベンダーのウイルス対策、マルウェア対策およびスパイウェア対策のアプリケーションは、Advanced Threat Prevention クライアントと競合する可能性があります。可能な場合は、これらのアプリケーションをアンインストールしてください。拮抗するソフトウェアに、Windows Defender は含まれません。ファイアウォールアプリケーションは許可されます。

  他のウイルス対策、マルウェア対策およびスパイウェア対策のアプリケーションをアンインストールできない場合は、Dell Server で Advanced Threat Prevention と該当する他のアプリケーションに除外を追加する必要があります。Dell Server で Advanced Threat Prevention に除外を追加する手順については、http://www.dell.com/support/article/us/en/04/SLN300970 を参照してください。その他のウイルス対策アプリケーションに追加する除外リストについては、http://www.dell.com/support/article/us/en/04/sln301562 を参照してください。

Advanced Threat Prevention のオペレーティングシステム

- 次の表では、対応オペレーティングシステムが詳しく説明されています。

Windows オペレーティングシステム（32 ビットと 64 ビット）

- Windows 7 SP1：Enterprise、Professional、Ultimate
- Windows Embedded Standard 7
- Windows 8： Enterprise、Pro
- Windows 8.1：Enterprise、Pro
- Windows 10：Education、Enterprise、Pro バージョン 1607（Anniversary Update/Redstone 1）からバージョン 1803（April 2018 Update/Redstone 4）
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016

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

使用されている URL の詳細については、http://www.dell.com/support/article/us/en/19/SLN303898 を参照してください。

BIOS イメージの整合性検証

BIOS 保証の有効化 ポリシーが管理コンソールで選択されている場合は、Cylance のテナントが BIOS がデル工場出荷時のバージョンから変更されていないか（攻撃ベクターの 1 つ）を確認するために、エンドポイントコンピュータ上で BIOS ハッシュを検証します。脅威が検出された場合は、通知が Dell Server に渡され、IT 管理者は管理コンソールでアラートを受けます。プロセスの概要については、「BIOS イメージの整合性検証プロセス」を参照してください。

メモ: カスタマイズされた工場出荷時イメージは、BIOS が変更されているため、この機能では使用できません。

BIOS イメージの整合性検証でサポートされる Dell コンピュータモデル

- Latitude 3470
- Latitude 3570
- Latitude 7275
- Latitude 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- OptiPlex 5040
- OptiPlex 7040
- OptiPlex 7440
- Precision Mobile Workstation 3510
- Precision Mobile Workstation 5510
- VMware Workstation 3620
- VMware Workstation 7510

BIOS イメージの整合性検証でサポートされる Dell コンピュータモデル

- Latitude E7270
- Latitude E7470
- Latitude Rugged 5414
- Latitude Rugged 7214 Extreme
- Latitude Rugged 7414
- OptiPlex 3040
- OptiPlex 3240
- VMware Workstation 7710
- Precision Workstation T3420
- Venue 10 Pro 5056
- Venue Pro 5855
- Venue XPS 12 9250
- XPS 13 9350
- XPS 9550

Client Firewall および Web Protection クライアント

- Client Firewall と Web Protection を正しくインストールするには、コンピュータがネットワークに接続されている必要があります。
- インストールの失敗を防ぐため、Client Firewall と Web Protection のクライアントをインストールする前に、その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、およびファイアウォールアプリケーションをアンインストールしてください。拮抗するソフトウェアに、Windows Defender および Endpoint Security Suite Enterprise は含まれません。
- ウェブ保護機能がサポートされるのは Internet Explorer のみです。

Client Firewall および Web Protection クライアントのオペレーティングシステム

- 次の表では、対応オペレーティングシステムが詳しく説明されています。

Windows オペレーティングシステム（ 32 ビットと 64 ビット ）

- Windows 7 SP1：Enterprise、Professional、Ultimate
- Windows 8： Enterprise、Pro
- Windows 8.1：Enterprise、Pro
- Windows 10：Education、Enterprise、Pro バージョン 1607 (Anniversary Update/Redstone 1) からバージョン 1803 (April 2018 Update/Redstone 4)

Client Firewall および Web Protection クライアントのポート

- Client Firewall および Web Protection クライアントで最新の Client Firewall および Web Protection アップデートが確実に受信されるようにするには、クライアントが各種の宛先サーバと通信できるよう、ポート 443 および 80 を使用可能にする必要があります。ポート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	メモ
レピュテーションサービス	SSL	TCP	443	tunnel.web.trustedsource.org	アウトバウンド	
レピュテーションサービスフィードバック	SSL	TCP	443	gtifeedback.trustedsource.org	アウトバウンド	

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	メモ
URL レピュテーションデータベースアップデート	HTTP	TCP	80	list.smartfilter.com	アウトバウンド	
URL レピュテーションルックアップ	SSL	TCP	443	tunnel.web.trustedsource.org	アウトバウンド	

SED クライアント

- SED 管理を正しくインストールするには、コンピュータに有線ネットワーク接続が必要です。
- スマートカードユーザーが最初に起動前認証でログインする場合には、有線ネットワーク接続が必要です。
- インストールされた SED 管理では、サードパーティ資格情報プロバイダは機能しません。PBA を有効にすると、サードパーティ資格情報プロバイダはすべて無効になります。
- IPv6 はサポートされていません。
- SED Manager はマルチドライブ構成ではサポートされません。
- SED Manager は現在、仮想化ホストコンピュータではサポートされていません。
- ポリシーを適用し、ポリシーの実施を開始できる状態になったら、コンピュータをシャットダウンして再起動する準備を整えます。
- 自己暗号化ドライブが搭載されているコンピュータでは HCA カードを使用できません。HCA のプロビジョニングを妨げる非互換性が存在します。デルでは、HCA モジュールをサポートする自己暗号化ドライブを用いたコンピュータの販売を行っていません。この非対応構成は、アフターマーケット構成となります。
- 暗号化の対象となるコンピュータに自己暗号化ドライブが搭載されている場合、Active Directory オプションのユーザーは次回のログオン時にパスワードの変更が必要が無効になっていることを確認します。起動前認証は、この Active Directory オプションをサポートしていません。
- デルでは、PBA がアクティブ化された後で認証方法を変更しないことをお勧めしています。別の認証方法に切り替える必要がある場合は、次のいずれかの操作を行う必要があります。
  - PBA からすべてのユーザーを削除します。

    または
  - PBA を非アクティブ化し、認証方法を変更した後、PBA を再度アクティブ化します。

  重要:

  RAID と SED の性質により、SED 管理では RAID はサポートされません。SED の *RAID=On* には、RAID では、ディスクにアクセスして、SED がロック状態のために利用できない上位セクタの RAID 関連データを読み書きする必要があり、ユーザーがログオンするまで待機してこのデータを読み取ることができないという問題があります。この問題を解決するには、BIOS で SATA の動作を *RAID=On* から *AHCI* に変更します。オペレーティングシステムに AHCI コントローラドライバがプレインストールされていない場合、*RAID=On* から *AHCI* に切り替えるとオペレーティングシステムがクラッシュします。
- Dell の SED 管理用の自己暗号化ドライブの構成は、NVMe と非 NVMe（SATA）ドライブで次のように異なります。
  - SED として利用されている NVMe ドライブ - デルの SED 管理では NVMe ドライブ上の AHCI をサポートしていないため、BIOS の SATA 操作を RAID ON に設定する必要があります。
  - SED として利用されている NVMe ドライブ - BIOS のブートモードは UEFI である必要があります。またレガシーオプションの ROM は無効にする必要があります。
  - SED として利用されていない NVMe ドライブ - Dell の SED 管理では非 NVMe ドライブ上の RAID をサポートしていないため、BIOS の SATA 操作を AHCI に設定する必要があります。
    - （ロックされた非 NVMe ドライブで利用できないセクターでの）読み書き対象の RAID 関連データへのアクセスが起動時にサポートされておらず、ユーザーがログインした後までこのデータの読み取りを待機できないために、RAID ON がサポートされません。
    - AHCI コントローラドライバがあらかじめインストールされていない場合に RAID ON > AHCI から切り替えると、オペレーティングシステムがクラッシュします。RAID から AHCI（またはその逆）に切り替える方法については、http://www.dell.com/support/article/us/en/19/SLN306460 を参照してください。

サポートされている OPAL 準拠の SED には、http://www.dell.com/support にあるアップデートされた Intel Rapid Storage Technology ドライバが必要です。NVMe ドライブでは、Intel ラピッドストレージテクノロジードライバのバージョン 15.2.0.0 以降を推奨します。

メモ: Intel Rapid Storage Technology ドライバは、プラットフォームによって異なります。お使いのコンピュータのモデルに基づいたシステムのドライバは、上記のリンクから参照できます。

- SED 管理は、Server Encryption またはサーバオペレーティングシステム上の Advanced Threat Prevention ではサポートされません。
- **メモ: 起動前認証ではパスワードが必要です。社内セキュリティポリシーに準拠した最小限のパスワード設定を行うことをお勧めします。**

SED クライアントハードウェア

SED クライアントの国際キーボード

- 次の表に、UEFI および UEFI 非対応のコンピュータで起動前認証によりサポートされている国際キーボードを示します。

国際キーボードのサポート - UEFI

- DE-FR - (スイスフランス語)
- DE-CH - (スイスドイツ語)
- EN-US - 英語 (アメリカ英語)
- EN-GB - 英語 (イギリス英語)
- EN-CA - 英語 (カナダ英語)

国際キーボードのサポート - UEFI 非対応

- AR - アラビア語 (ラテン文字を使用)
- DE-FR - (スイスフランス語)
- DE-CH - (スイスドイツ語)
- EN-US - 英語 (アメリカ英語)
- EN-GB - 英語 (イギリス英語)
- EN-CA - 英語 (カナダ英語)

SED クライアントのローカライズ

SED クライアントは複数言語ユーザーインターフェイス (MUI) 対応で、次の言語にローカライズされています。UEFI モードおよび起動前認証は、ロシア語、繁体字中国語、または簡体字中国語を**除く**以下の言語でサポートされています。

言語サポート

- EN - 英語
- FR - フランス語
- KO - 韓国語
- ZH-CN - 中国語 (簡体字)

言語サポート

- IT - イタリア語
- DE - ドイツ語
- ES - スペイン語
- JA - 日本語
- ZH-TW - 中国語（繁体字）
- PT-BR - ポルトガル語（ブラジル）
- PT-PT - ポルトガル語（ポルトガル（イベリア））
- RU - ロシア語

SED クライアントのオペレーティングシステム

- 次の表は、対応オペレーティングシステムの詳しい説明です。

Windows オペレーティングシステム（32 ビットと 64 ビット）

- Windows 7 SP0-SP1：Enterprise、Professional、Ultimate（レガシーブートモードでのみサポート、UEFI では未サポート）

  メモ:
  NVMe 自己暗号化ドライブは Windows 7 ではサポートされません。

- Windows 8：Enterprise、Pro
- Windows 8.1：Enterprise、Pro
- Windows 10：Education、Enterprise、Pro バージョン 1607（Anniversary Update/Redstone 1）からバージョン 1803（April 2018 Update/Redstone 4）

BitLocker Manager クライアント

- BitLocker がまだお使いの環境に導入されていない場合は、「Microsoft BitLocker の要件」を確認してください。
- PBA パーティションがすでに設定されていることを確認します。PBA パーティションを設定する前に BitLocker Manager がインストールされている場合は、BitLocker を有効にできないため、BitLocker Manager は動作しません。
- BitLocker Manager を使用するには、Dell Server が必要です。
- データベース内で署名証明書が使用可能であることを確認してください。詳細については、http://www.dell.com/support/article/us/en/19/sln307028 を参照してください。
- キーボード、マウス、およびビデオコンポーネントは、コンピュータに直接接続する必要があります。周辺機器の管理に KVM スイッチは使用しないでください。KVM スイッチは、ハードウェアを正しく識別するコンピュータの機能を阻害するおそれがあるためです。
- TPM をオンにして有効にします。BitLocker Manager は TPM の所有権を取得しますが、再起動の必要はありません。ただし、TPM の所有権がすでに存在する場合は、BitLocker Manager で暗号化セットアップ処理が開始されます。再起動する必要はありません。ここでのポイントは、TPM が所有かつ有効化されている必要があるという点です。
- BitLocker Manager は、Server Encryption またはサーバオペレーティングシステム上の Advanced Threat Prevention ではサポートされません。

BitLocker Manager クライアントのハードウェア

- 次の表は、サポートされているハードウェアの詳細です。

オプションの組み込みハードウェア

- TPM 1.2 または 2.0

BitLocker Manager クライアントのオペレーティングシステム

- 次の表では、対応オペレーティングシステムが詳しく説明されています。

Windows オペレーティングシステム
– Windows 7 SP0-SP1: Enterprise、Ultimate（32 ビットと 64 ビット）
– Windows 8: Enterprise (64 ビット)
– Windows 8.1: Enterprise Edition、Pro Edition（64 ビット）
– Windows 10 : Enterprise、Pro バージョン 1607（Anniversary Update/Redstone 1）からバージョン 1803（April 2018 Update/Redstone 4）
– Windows Server 2008 R2: Standard Edition 、Enterprise Edition (64 ビット)
– Windows Server 2012 R2: Standard Edition、Enterprise Edition（64 ビット）
– Windows Server 2016

BitLocker Manager を Windows 7 上にインストールする場合は、Windows Update KB3133977 および KB3125574 をインストールする**必要はありません**。

3

マスターインストーラを使用したインストール

- コマンドラインのスイッチおよびパラメータは大文字と小文字を区別します。
- デフォルト以外のポートを使用してインストールするには、マスターインストーラの代わりに子インストーラを使用します。
- Endpoint Security Suite Enterprise のマスターインストーラのログファイルは、**C:\ProgramData\Dell\Dell Data Protection\Installer** にあります。
- アプリケーションに関するサポートが必要なときには、次のマニュアルとヘルプファイルを参照するようにユーザーに指示します。
  - Encryption クライアントの各機能の使用方法については、『DellEncrypt Help』(Dell Encrypt ヘルプ) を参照してください。このヘルプには、**<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help** からアクセスします。
  - Encryption External Media の機能については、*Encryption External Media* ヘルプを参照してください。このヘルプには、**<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS** からアクセスします。
  - Advanced Threat Prevention の機能の使用方法については、*Endpoint Security Suite Enterprise* のヘルプを参照してください。このヘルプには、**<Install dir>:\Program Files\Dell\Dell Data Protection\Client Security Framework\Help** からアクセスします。
- ユーザーは、インストールが完了した後、通知領域で Dell Encryption アイコンを右クリックし、**ポリシーアップデートのチェック** を選択して、ポリシーをアップデートする必要があります。
- マスターインストーラは、製品のスイート全体をインストールします。マスターインストーラを使用してインストールするには、2 つの方法があります。次のいずれかを選択します。
  - マスターインストーラを使用した対話型のインストール

  または
  - マスターインストーラを使用したコマンドラインによるインストール

マスターインストーラを使用した対話型のインストール

- Endpoint Security Suite Enterprise マスターインストーラは次の場所に置かれます。
  - **お使いのデル FTP アカウントから** - インストールバンドルを Endpoint-Security-Suite-Ent-1.x.x.xxx.zip の中から見つけます。
- 以下の手順に従い、Dell Endpoint Security Suite Enterprise を、Endpoint Security Suite Enterprise マスターインストーラを使用して対話形式でインストールまたはアップデートします。この方法では、コンピュータごとに製品スイートをインストールします。

1. デルのインストールメディア内で **DDSSuite.exe** を見つけます。それをローカルコンピュータにコピーします。
2. インストーラを起動するには **DDSSuite.exe** をダブルクリックします。これには数分かかる場合があります。
3. ようこそ ダイアログで **次へ** をクリックします。
4. ライセンス契約を読み、その条件に同意して **次へ** をクリックします。
5. オンプレミスデル管理サーバ名 に、Dell Server の完全修飾ホスト名を入力して、ターゲットユーザーを管理します (server.organization.com など)。

   Dell Server に、クライアントが通信するデルサーバの URL を入力します。

   の場合、形式は https://server.organization.com:**8443**/xapi/ (末尾のスラッシュを含む) です。

   次へ をクリックします。
6. **次へ** をクリックして、デフォルトの場所である **C:\Program Files\Dell\Dell Data Protection\.** にこの製品をインストールします。他の場所にインストールすると問題が発生する可能性があるため、**Dell recommends installing in the default location only。**
7. インストールするコンポーネントを選択します。

   Security Framework によって、基盤となるセキュリティフレームワークがインストールされます。

Encryption は、コンピュータがネットワークに接続されている、ネットワークに接続されていない、紛失された、または盗難されたかどうかにかかわらず、セキュリティポリシーを実施するコンポーネントである Encryption クライアントをインストールします。

Threat Protection は、Threat Protection クライアントをインストールします。これは、ウイルス、スパイウェア、および迷惑プログラムをスキャンするためのマルウェアおよびアンチウイルス保護、ネットワークおよびインターネット上におけるコンピュータとリソース間の通信を監視するクライアントファームウェア、ならびにオンライン参照中にウェブサイトの安全評価を表示、またはウェブサイトへのアクセスをブロックするためのウェブフィルタリングです。

BitLocker Manager は、BitLocker 暗号化ポリシーの一元的な管理を通じて所有コストを単純化および軽減することによって、BitLocker 導入のセキュリティを強化するように設計された BitLocker Manager クライアントをインストールします。

Advanced Threat Prevention は、Advanced Threat Prevention クライアントをインストールします。これは、アルゴリズム的科学および機械学習を使用して、既知および不明のサイバー攻撃を識別、分類し、エンドポイントの攻撃の実行や阻害を防止する、次世代のアンチウイルス対策です。

Web Protection およびファイアウォール は、オプション機能である Web Protection およびファイアウォールをインストールします。Client Firewall は、ルールのリストに従って、すべての受信トラフィックおよび発信トラフィックをチェックします。Web Protection は、ウェブサイトの評価に基づき、ウェブのブラウジングとダウンロードを監視して脅威を特定し、脅威が検知された場合はアクションを実行します。

メモ: Windows 10 October 2018 Update（ Redstone 5 ）以降でオプションの Advanced Threat Prevention 機能をインストールしようとすると、互換性の警告が表示されます。

メモ: Windows 10 October 2018 Update（ Redstone 5 ）以降でオプションの Web Protection およびファイアウォール機能をインストールしようとすると、互換性の警告が表示されます。

選択が完了したら、**次へ** をクリックします。

8 **インストール** をクリックしてインストールを開始します。インストールには数分かかります。

9 **はい、今すぐコンピュータを再起動します** を選択し、**終了**をクリックします。
インストールが完了しました。

マスターインストーラを使用したコマンドラインによるインストール

- コマンドラインでのインストールでは、最初にスイッチを指定する必要があります。その他のパラメータは、/v スイッチに渡される引数に指定します。

スイッチ

- Endpoint Security Suite Enterprise マスターインストーラで使用できるスイッチを、次の表に示します。

メモ: サードパーティ資格情報プロバイダを使用する必要がある場合は、Encryption Management Agent をインストールするか、FEATURE=BLM または FEATURE=BASIC パラメータを指定してアップグレードする必要があります。

メモ: Windows 10 October 2018 Update（ Redstone 5 ）以降では、Advanced Threat Prevention はサポートされません。

スイッチ	説明
-y -gm2	Endpoint Security Suite Enterprise マスターインストーラの事前抽出。y スイッチと -gm2 スイッチは一緒に使用する必要があります。 これらのスイッチを個別に使用しないでください。
/S	サイレントインストール
/z	DDSSuite.exe 内の .msi に変数を渡します。

パラメータ

- Endpoint Security Suite Enterprise マスターインストーラで使用できるパラメータについて、次の表で説明します。Endpoint Security Suite Enterprise マスターインストーラは、個々のコンポーネントを除外することはできませんが、どのコンポーネントをインストールするかを指定するコマンドを受け付けることができます。

パラメータ	説明
SUPPRESSREBOOT	インストールの完了後に自動的に行われる再起動を阻止します。SILENT モードで使用できます。
SERVER	Dell Server の URL を指定します。
InstallPath	インストールのパスを指定します。SILENT モードで使用できます。
FEATURES	SILENT モードでインストールできるコンポーネントを指定します。 ATP = Advanced Threat Prevention のみ DE-ATP = Advanced Threat Prevention と Encryption。これは、FEATURES パラメータが指定されていない場合のデフォルトのインストールオプションです。 DE = Drive Encryption クライアントのみ BLM = BitLocker Manager SED = SED 管理 (EMAgent / Manager、PBA / GPE ドライバ)(ワークステーションオペレーティングシステム上にインストールされる場合のみ使用可能) ATP-WEBFIREWALL = Advanced Threat Prevention (Client Firewall および Web Protection 機能付き) DE-ATP-WEBFIREWALL = Encryption および Advanced Threat Prevention (Client Firewall および Web Protection 機能付き) **メモ: Encryption Enterprise または v1.4 以前の Endpoint Security Suite Enterprise からのアップグレードの場合、Client Firewall および Web Protection をインストールするためには ATP-WEBFIREWALL または DE-ATP-WEBFIREWALL を指定する必要があります。クライアントをインストールする際に、切断モードで実行する Dell Server で管理されるようにする場合は、ATP-WEBFIREWALL または DE-ATP-WEBFIREWALL を指定しないでください。**
BLM_ONLY=1	SED Management のプラグインを除外するために FEATURES=BLM をコマンドラインに使用する時には、これを使用する必要があります。

コマンドラインの例

- コマンドラインパラメータでは大文字と小文字を区別します。
- (ワークステーションオペレーティングシステム上) この例では、Endpoint Security Suite Enterprise マスターインストーラを標準ポートで使用して、**C:\Program Files\Dell\Dell Data Protection** のデフォルトの場所にすべてのコンポーネントをサイレントインストールし、指定した Dell Server を使用するように設定します。

```
"DDSSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com\""
```

- (ワークステーションオペレーティングシステム上) この例では、Endpoint Security Suite Enterprise マスターインストーラを標準ポートで使用して **C:\Program Files\Dell\Dell Data Protection** のデフォルトの場所に Advanced Threat Prevention と Encryption ***のみ***をサイレントインストールし、指定した Dell Server を使用するように設定します。

```
"DDSSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE-ATP\""
```

- (ワークステーションオペレーティングシステム上) この例では、Endpoint Security Suite Enterprise マスターインストーラを標準ポートで使用して、**C:\Program Files\Dell\Dell Data Protection** のデフォルトの場所に Advanced Threat Prevention、Encryption および SED 管理を再起動なしでサイレントインストールし、指定した Dell Server を使用するように設定します。

```
"DDSSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP-SED,
SUPPRESSREBOOT=1\""
```

- （ワークステーションオペレーティングシステム上）この例では、Endpoint Security Suite Enterprise マスターインストーラを標準ポートで使用して **C:\Program Files\Dell\Dell Data Protection** のデフォルトの場所に Advanced Threat Prevention、Encryption、Web Protection、および Client Firewall をサイレントインストールし、指定した Dell Server を使用するように設定します。

  ```
  "DDSSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP-WEBFIREWALL\""
  ```

- （サーバオペレーティングシステム上）この例では、Endpoint Security Suite Enterprise マスターインストーラを標準ポートで使用して **C:\Program Files\Dell\Dell Data Protection** のデフォルトの場所に Advanced Threat Prevention と Encryption ***のみ***をサイレントインストールし、指定した Dell Server を使用するように設定します。

  ```
  "DDSSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE-ATP\""
  ```

- （サーバオペレーティングシステム上）この例では、Endpoint Security Suite Enterprise マスターインストーラを標準ポートで使用して **C:\Program Files\Dell\Dell Data Protection** のデフォルトの場所に Advanced Threat Prevention、Encryption、Web Protection、Client Firewall をサイレントインストールします。

  ```
  "DDSSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE-ATP-WEBFIREWALL\""
  ```

- （サーバオペレーティングシステム上）この例では、Endpoint Security Suite Enterprise マスターインストーラを標準ポートで使用して、**C:\Program Files\Dell\Dell Data Protection** のデフォルトの場所に Advanced Threat Prevention ***のみ***をサイレントインストールし、指定した Dell Server を使用するように設定します。

  ```
  "DDSSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=ATP\""
  ```

- （サーバオペレーティングシステム上）この例では、Endpoint Security Suite Enterprise マスターインストーラで標準ポートを使用して **C:\Program Files\Dell\Dell Data Protection** のデフォルトの場所に Encryption ***のみ***をサイレントインストールし、指定した Dell Server を使用するように設定します。

  ```
  "DDSSuite.exe" -y -gm2 /S /z"\"SERVER=server.organization.com, FEATURES=DE\""
  ```

4

マスターインストーラのアンインストール

- デルでは、データセキュリティスイートを削除するには、Data Security Uninstaller を使用することをお勧めします。
- 各コンポーネントを個別にアンインストールした後で、Endpoint Security Suite Enterprise マスターインストーラのアンインストールを行う必要があります。クライアントは、**アンインストールの失敗を防止するための特定の順序** でアンインストールする必要があります。
- 手順の説明をに 抽出します。マスターインストーラから子のインストーラの 子のインストーラを入手します。
- 必ず、インストール時と同じバージョンの Endpoint Security Suite Enterprise マスターインストーラ (およびそれに伴うクライアント) を使用してアンインストールを行ってください。
- 本章では、子インストーラのアンインストール方法の詳細な手順が記された他の章を参照します。この章で説明している手順の最後で **のみ**、マスターインストーラをアンインストールします。
- クライアントを以下の順序でアンインストールします。

  a Encryption クライアントのアンインストール。

  b Advanced Threat Prevention のアンインストール。

  c SED クライアントのアンインストール (これは、Advanced Threat Prevention がアンインストールされるまでアンインストールできない Dell Encryption Management Agent をアンインストールします)。

  d BitLocker Manager クライアントのアンインストール
- 「マスターインストーラのアンインストール」に進みます。

Endpoint Security Suite Enterprise マスターインストーラのアンインストール

個々のクライアントをすべてアンインストールしたら、マスターインストーラをアンインストールすることができます。

コマンドラインでのアンインストール

- 次の例では、Endpoint Security Suite Enterprise マスターインストーラのサイレントアンインストールを行います。

  ```
  "DDSSuite.exe" -y -gm2 /S /x
  ```

  終了したらコンピュータを再起動します。

5

子インストーラを使用したアンインストール

- デルでは、データセキュリティスイートを削除するには、Data Security Uninstaller を使用することをお勧めします。
- 各クライアントを個別にアンインストールするには、まず、マスターインストーラからの子インストーラの抽出で示すとおりに、Endpoint Security Suite Enterprise のマスターインストーラから子実行ファイルを抽出する必要があります。あるいは、管理者権限でのインストールを実行して .msi を抽出します。
- アンインストールには、インストール時と同じバージョンのクライアントを使用するようにしてください。
- コマンドラインのスイッチおよびパラメータは大文字と小文字を区別します。
- コマンドラインでは、空白などの特殊文字を 1 つ、または複数含む値は、エスケープされた引用符で囲むようにしてください。コマンドラインパラメータでは大文字と小文字を区別します。
- これらのインストーラを使用し、スクリプトインストールやバッチファイルを利用するか、組織で利用できる他のプッシュ技術を活用して、クライアントをアンインストールします。
- ログファイル - Windows はログインしたユーザー用に、固有の子インストーラアンインストールログファイルを **C:\Users\<UserName>\AppData\Local\Temp.** にある %temp% に作成します。

  インストーラの実行時に別のログファイルを追加することにした場合、子インストーラログファイルは付加しないことから、そのログファイルには独自の名前を付けるようにしてください。/l **C:\<any directory>\<any log file name>.log** を使用することによって、ログファイルの作成に標準の .msi コマンドを使用することができます。そのログファイルにユーザー名 / パスワードが記録されるため、デルではコマンドラインアンインストールで「/l*v」(詳細ロギング) を使用することをお勧めしません。
- すべての子インストーラは、特に記載がない限り、コマンドラインでのアンインストールで同じ基本的な .msi スイッチと表示オプションを使用します。スイッチは最初に指定する必要があります。/v スイッチは必須であり、引数が必要です。その他のパラメータは、/v スイッチに渡される引数に指定します。

  表示オプションは、目的の動作を実行させるために /v スイッチに渡される引数の末尾に指定することができます。同じコマンドラインで、/q と /qn の両方を使用しないでください。「 ! 」および「-」は「/qb」の後にのみ使用してください。

スイッチ	意味
/v	setup.exe 内の .msi に変数を渡します。コンテンツは、必ずプレーンテキストの引用符で囲む必要があります。
/s	サイレントモード
/x	アンインストールモード
/a	管理インストール (.msi 内のすべてのファイルがコピーされます)

メモ:
/v を使うと、Microsoft のデフォルトのオプションを使用できます。オプションのリストについては、https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx を参照してください。

オプション	意味
/q	進行状況ダイアログなし、処理完了後に自動で再起動
/qb	**キャンセル** ボタン付きの進捗状況ダイアログ、再起動のプロンプト表示
/qb-	**キャンセル** ボタン付きの進捗状況ダイアログ、処理完了後に自動で再起動

オプション	意味
/qb!	**キャンセル** ボタンなしの進捗状況ダイアログ、再起動のプロンプト表示
/qb!-	**キャンセル** ボタンなしの進捗状況ダイアログ、処理完了後に自動で再起動
/qn	ユーザーインタフェースなし

Encryption および Server Encryption クライアントのアンインストール

- 復号化にかかる時間を短縮するため、Windows ディスククリーンアップを実行して、一時ファイルやその他の不要なデータを削除します。
- 可能であれば、復号化は夜間に実行してください。
- スリープモードをオフにして、誰も操作していないコンピュータがスリープ状態になるのを防ぎます。スリープ状態のコンピュータでは復号化は行われません。
- ロックされたファイルが原因で複合化が失敗する可能性を最小限に抑えるために、すべてのプロセスおよびアプリケーションをシャットダウンします。
- アンインストールが完了して、復号化が進行中になったら、すべてのネットワーク接続を無効にします。そうしなければ、暗号化を再度有効にする新しいポリシーが取得される場合があります。
- ポリシーアップデートの発行など、データを復号化するための既存の手順に従います。
- Encryption クライアントのアンインストールプロセスの開始時に、Dell Encryption および Encryption External Media によってステータスが 保護なし に変更されるよう、Dell Server が更新されます。ただし、クライアントが Dell Server に接続できない場合は、理由にかかわらず、ステータスは更新されません。このような場合は、管理コンソールで、手動でエンドポイントを削除する必要があります。組織がコンプライアンス目的でこのワークフローを使用する場合は、管理コンソールまたは Compliance Reporter で想定どおりに 保護なし に設定されていることを確認することをお勧めします。

プロセス

- **Encryption Removal Agent のサーバからのキーのダウンロード** オプションを使用する場合は、アンインストール前に Key Server(および Security Management Server) を設定する必要があります。手順については、「Configure Key Server for Uninstallation of Encryption Client Activated Against Security Management Server」(Security Management Server に対してアクティブ化された Encryption クライアントのアンインストールのための Key Server の設定) を参照してください。Security Management Server Virtual は Key Server を使用しないので、アンインストールするクライアントが Security Management Server Virtual に対してアクティブ化される場合、事前のアクションは不要です。
- **Encryption Removal Agent - ファイルからキーをインポート** オプションを使用する場合、Encryption Removal Agent を起動する前に Dell Administrative Utility (CMGAd) を使用する必要があります。このユーティリティは、暗号化キーバンドルの取得に使用されます。手順については「Administrative Download Utility (CMGAd) の使用」を参照してください。このユーティリティは、Dell インストールメディアにあります。

コマンドラインでのアンインストール

- Endpoint Security Suite Enterprise マスターインストーラから抽出された Encryption クライアントインストーラは、**C:\extracted\Encryption \DDPE_XXbit_setup.exe** に置かれます。
- 次の表に、アンインストールで使用できるパラメータの詳細を示します。

パラメータ	選択
CMG_DECRYPT	Encryption Removal Agent のインストールタイプを選択するためのプロパティ： 3 - LSARecovery バンドルを使用 2 - 以前にダウンロードしたフォレンジックキーマテリアルを使用 1 - Dell Server からキーをダウンロード

パラメータ	選択
	0 - Encryption Removal Agent をインストールしない
CMGSILENTMODE	サイレントアンインストールのプロパティ 1 - サイレント 0 - 非サイレント
必須のプロパティ	
DA_SERVER	ネゴシエーションセッションをホストする Security Management Server の FQHN
DA_PORT	Security Management Server 上の要求用ポート (デフォルトは 8050)
SVCPN	Security Management Server で Key Server サービスがログオンされている UPN 形式のユーザー名。
DA_RUNAS	キーフェッチリクエストが行われるコンテキストでの SAM 対応形式のユーザー名。このユーザーは、Security Management Server の Key Server リストに存在している必要がある。
DA_RUNASPWD	runas ユーザーのパスワード。
FORENSIC_ADMIN	アンインストールまたはキーのフォレンジック要求に使用できる Dell Server 上のフォレンジック管理者アカウント。
FORENSIC_ADMIN_PWD	フォレンジック管理者アカウントのパスワード。
オプションのプロパティ	
SVCLOGONUN	パラメータとして Encryption Removal Agent サービスログオンするための UPN 形式のユーザー名。
SVCLOGONPWD	ユーザーとしてログオンするためのパスワード。

- 次の例では、サイレントに Encryption クライアントをアンインストールし、Security Management Server から暗号化キーをダウンロードします。

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1 DA_SERVER=server.organization.com
  DA_PORT=8050 SVCPN=administrator@organization.com DA_RUNAS=domain\username
  DA_RUNASPWD=password /qn"
  ```

  MSI コマンド :

  ```
  msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  CMG_DECRYPT="1" CMGSILENTMODE="1" DA_SERVER="server.organization.com" DA_PORT="8050"
  SVCPN="administrator@domain.com" DA_RUNAS="domain\username" DA_RUNASPWD="password" /qn
  ```

  終了したらコンピュータを再起動します。
- 次の例では、Encryption クライアントをアンインストールし、フォレンジック管理者アカウントを使用して暗号化キーをダウンロードします。

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=1 CMGSILENTMODE=1
  FORENSIC_ADMIN=forensicadmin@organization.com FORENSIC_ADMIN_PWD=tempchangeit /qn"
  ```

  MSI コマンド :

```
msiexec.exe /s /x "Dell Data Protection Encryption.msi" /qn CMG_DECRYPT=1 CMGSILENTMODE=1
FORENSIC_ADMIN=forensicadmin@organization.com FORENSIC_ADMIN_PWD=tempchangeit
REBOOT=REALLYSUPPRESS
```

終了したらコンピュータを再起動します。

重要:

デルでは、コマンドラインでフォレンジック管理者パスワードを使用する場合、次のアクションを推奨します

1. 管理コンソールで、サイレントアンインストール実行用のフォレンジック管理者アカウントを作成します。
2. そのアカウント用に、アカウントと期間に固有の一時的なパスワードを設定します。
3. サイレントアンインストールが完了したら、管理者のリストから一時的なアカウントを削除するか、そのパスワードを変更します。

メモ:

一部の古いクライアントでは、パラメータ値の前後にエスケープ文字（\"）が必要な場合があります。例：

```
DDPE_XXbit_setup.exe /x /v"CMG_DECRYPT=\"1\" CMGSILENTMODE=\"1\" DA_SERVER=
\"server.organization.com\" DA_PORT=\"8050\" SVCPN=\"administrator@organization.com\"
DA_RUNAS=\"domain\username\" DA_RUNASPWD=\"password\" /qn"
```

Advanced Threat Prevention のアンインストール

コマンドラインでのアンインストール

- 次の例では、Advanced Threat Prevention クライアントをアンインストールします。**このコマンドは管理者のコマンドプロンプトから実行する必要があります。**

  ```
  wmic path win32_product WHERE (CAPTION LIKE "%%CYLANCE%%") call uninstall
  ```

  コンピュータをシャットダウン、再起動してから Dell Encryption Management Agent のコンポーネントをアンインストールします。

- **重要: SED クライアントをインストールした場合、または起動前認証をアクティブ化した場合は、「SED クライアントのアンインストール」にあるアンインストールの指示に従います。**

  次の例では、SED クライアントではなく、Encryption Management Agent コンポーネントのみがアンインストールされます。

  ```
  EMAgent_XXbit_setup.exe /x /s /v" /qn"
  ```

SED クライアントのアンインストール

- PBA のアクティベーションを解除する場合は、Dell Server にネットワーク接続する必要があります。

プロセス

- PBA を非アクティブ化します。これにより、コンピュータからすべての PBA データが削除され、SED キーがロック解除されます。
- SED クライアントをアンインストールします。

PBA の非アクティブ化

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. 適切なエンドポイントの種類を選択します。
4. 表示 > 表示、非表示 または すべて を選択します。

5 コンピュータのホスト名がわかっている場合は、そのホスト名を ホスト名 フィールドに入力します。ワイルドカードも使用できます。このフィールドを空白のままにすると、すべてのコンピュータが表示されます。**検索** をクリックします。

ホスト名がわからない場合は、リストをスクロールして該当するコンピュータを探します。

検索フィルタに基づいて、1 台のコンピュータ、またはコンピュータのリストが表示されます。

6 該当するコンピュータのホスト名を選択します。

7 上部メニューの **セキュリティポリシー** をクリックします。

8 **ポリシーカテゴリ** ページから、**自己暗号化ドライブ** を選択します。

9 **自己暗号化ドライブ（ SED ）** およびポリシーを *On* から ***Off*** に変更します。

10 **保存** をクリックします。

11 左ペインで、**ポリシーのコミット** バナーをクリックします。

12 **ポリシーのコミット** をクリックします。

ポリシーが Dell Server からアクティベーション解除対象のコンピュータに反映されるまで待ちます。

PBA が非アクティブ化された後、SED および Advanced Authentication クライアントをアンインストールします。

SED クライアントのアンインストール

コマンドラインでのアンインストール

- マスターインストーラから抽出された SED クライアントインストーラは、**C:\extracted\Encryption Management Agent \EMAgent_XXbit_setup.exe** に置かれます。
  - 次の例は、SED クライアントをサイレントアンインストールします。

    ```
    EMAgent_XXbit_setup.exe /x /s /v" /qn"
    ```

    終了したらコンピュータをシャットダウンして再起動します。

BitLocker Manager クライアントのアンインストール

コマンドラインでのアンインストール

- Endpoint Security Suite Enterprise マスターインストーラから抽出された BitLocker クライアントインストーラは、**C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe** に置かれます。
- 次の例では、BitLocker Manager クライアントをサイレントアンインストールします。

  ```
  EMAgent_XXbit_setup.exe /x /s /v" /qn"
  ```

  終了したらコンピュータを再起動します。

6

Data Security Uninstaller

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

Dell では、マスターアンインストーラとして Data Security Uninstaller を提供しています。このユーティリティは、現在インストールされている製品を収集して、適切な順序で削除します。

Data Security Uninstaller は **C:\Program Files (x86)\Dell\Dell Data Protection** から入手できます。

詳細またはコマンドラインインタフェース（CLI）の使用については、KB 記事 SLN307791 を参照してください。

削除されたすべてのコンポーネントに関するログが、**C:\ProgramData\Dell\Dell Data Protection** に生成されます。

このユーティリティを実行するには、格納フォルダを開き、**DataSecurityUninstaller setup.exe** を右クリックして**管理者として実行します**。

次へ をクリックします。

必要に応じて任意のアプリケーションの削除をクリアし、**次へ** をクリックします。

メモ: 必要な依存関係が自動的に選択またはクリアされます。

Encryption Removal Agent をインストールせずにアプリケーションを削除するには、**Encryption Removal Agent** で **インストールしない** を選択して **次へ** を選択します。

Encryption Removal Agent - サーバからキーをダウンロード を選択します。

フォレンジック管理者の完全修飾された資格情報を入力し、**次へ** を選択します。

削除 を選択してアンインストールを開始します。

終了 をクリックして削除を完了し、コンピュータを再起動します。デフォルトでは、**完了をクリックした後マシンを再起動する** が選択されています。

アンインストールと削除が完了しました。

7

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。

8

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。

9

子インストーラの抽出

- マスターインストーラはマスターアンインストーラではありません。各クライアントを個別にアンインストールした後で、マスターインストーラのアンインストールを行う必要があります。このプロセスを使用します。アンインストール用にインストールできるように使用でき、マスタインストーラからクライアントを抽出します。

1 デルのインストールメディアから、**DDSSuite.exe** ファイルをローカルコンピュータにコピーします。

2 **DDSSuite.exe** ファイルと同じ場所でコマンドプロンプトを開き、次のように入力します。

```
DDSSuite.exe /z"\"EXTRACT_INSTALLERS=C:\extracted\""
```

抽出パスは 63 文字を超えられません。

抽出した子インストーラは **C:\extracted\.** にあります。

10

Key Server の設定

- 本項では、Security Management Server 使用時における Kerberos 認証 / 承認との使用のためにコンポーネントを設定する方法について説明します。Security Management Server Virtual は Key Server を使用していません。
- Kerberos 認証 / 承認を使用する場合は、Key Server コンポーネントを装備しているサーバを対象ドメインに含める必要があります。
- Security Management Server Virtual は Key Server を使用しないので、通常のアンインストールには影響しません。Security Management Server Virtual に対してアクティブ化されている Encryption クライアントがアンインストールされると、Key Server の Kerberos メソッドの代わりに、Security Server を通じた標準的なフォレンジックキーの取得が使用されます。詳細については、「コマンドラインアンインストール」を参照してください。

サービスパネル - ドメインアカウントのユーザーの追加

1 Security Management Server で、サービスパネル（スタート > ファイル名を指定して実行 > services.msc > OK）に移動します。

2 Key Server を右クリックし、**プロパティ** を選択します。

3 ログオン タブを選択し、**このアカウント：** オプションを選択します。

このアカウント：ドメインアカウントユーザーを追加します。このドメインユーザーには、少なくとも Key Server フォルダのローカル管理権限が必要です。つまり、Key Server の config ファイルに加え、log.txt ファイルにも書き込むことができる必要があります。

ドメインユーザーのパスワードを入力し確認します。

OK をクリックします。

4 Key Server サービスを再起動します（今後の操作のため、サービスパネルを開いたままにしておきます）。

5 <Key Server install dir> log.txt に移動して、サービスが正しく開始したことを確認します。

Key Server 設定ファイル - Security Management Server 通信のためのユーザーの追加

1 <Key Server install dir> に移動します。

2 テキストエディタで *Credant.KeyServer.exe.config* を開きます。

3 <add key="user" value="superadmin" /> に移動して、「superadmin」の値を適切なユーザーの名前に変更します。「superadmin」のままにしておくこともできます。

4 <add key="epw" value="<encrypted value of the password>" /> に移動して、「epw」を「password」に変更します。その後、"<encrypted value of the password>" を、手順 3 のユーザーのパスワードに変更します。このパスワードは、Security Management Server が再起動すると再度暗号化されます。

手順 3 の「superadmin」を使用していて、superadmin パスワードが「changeit」ではない場合は、ここで変更します。ファイルを保存して閉じます。

サービスパネル - Key Server サービスの再起動

1 サービスパネル（スタート > ファイル名を指定して実行 > services.msc > OK）に戻ります。

2 Key Server サービスを再起動します。

3 <Key Server インストールディレクトリ> log.txt に移動して、サービスが正しく開始したことを確認します。

4 サービスパネルを閉じます。

管理コンソール - フォレンジック管理者の追加

1 管理コンソールに Dell 管理者としてログインします。
2 **ポピュレーション** > **ドメイン** をクリックします。
3 適切なドメインを選択します。
4 **Key Server** タブをクリックします。
5 アカウント で、管理者アクティビティを実行するユーザーを追加します。形式は DOMAIN\Username です。**アカウントの追加** をクリックします。
6 左のメニューで **ユーザー** をクリックします。検索ボックスで、手順 5 で追加したユーザー名を検索します。**検索** をクリックします。
7 正しいユーザーが検索されたら、**管理者** アイコンをクリックします。
8 **フォレンジック管理者** を選択し、**アップデート** をクリックします。
これで、コンポーネントが Kerberos 認証 / 承認用に設定されました。

11

Administrative Download Utility (CMGAd) の使用

- このユーティリティでは、Security Management Server/Security Management Server Virtual に接続していないコンピュータ上で使用するためのキーマテリアルのバンドルをダウンロードできます。
- このユーティリティは、アプリケーションに渡されるコマンドラインパラメータに応じて、次のいずれかの方法を使用してキーバンドルをダウンロードします。
  - フォレンジックモード - コマンドラインで -f が渡された場合、またはコマンドラインパラメータが使用されていない場合に使用されます。
  - 管理者モード - コマンドラインで -a が渡された場合に使用されます。

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

フォレンジックモードでの Administrative Download Utility の使用

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

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

デバイスサーバーの URL：Security Server (Device Server) の完全修飾 URL。書式は、https://securityserver.domain.com:8443/xapi/ です。

Dell 管理者：jdoe など、フォレンジック管理者資格情報を持つ管理者の名前 (リモート管理コンソールで有効)

パスワード：フォレンジック管理者パスワード

MCID：マシン ID (machineID.domain.com など)

DCID：16 桁の Shield ID のうち最初の 8 桁

> **ヒント:**
> 通常、MCID または DCID のどちらかを指定すれば十分です。ただし、どちらもわかっている場合は、両方を入力すると役立ちます。各パラメータには、クライアントとクライアントコンピュータに関する異なる情報が含まれます。

次へ をクリックします。

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

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

次へ をクリックします。

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

4 完了したら、**終了** をクリックします。

管理者モードでの Administrative Download Utility の使用

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

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

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

サーバー：Key Server の完全修飾ホスト名 (keyserver.domain.com など)。

ポート番号：デフォルトのポートは 8050 です。

サーバーアカウント : Key Server を実行するときのドメインユーザー。この形式は domain\username です。ユーティリティを実行するドメインユーザーには、Key Server からダウンロードを実行する権限が与えられている必要があります。

MCID：マシン ID (machineID.domain.com など)

DCID：16 桁の Shield ID のうち最初の 8 桁

> **ヒント:**
> 通常、MCID または DCID のどちらかを指定すれば十分です。ただし、どちらもわかっている場合は、両方を入力すると役立ちます。各パラメータには、クライアントとクライアントコンピュータに関する異なる情報が含まれます。

次へ をクリックします。

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

パスフレーズを確認します。

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

次へ をクリックします。

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

4 完了したら、**終了** をクリックします。

12

トラブルシューティング

すべてのクライアントのトラブルシューティング

- Endpoint Security Suite Enterprisem **のマスターインストーラのログファイル**は、**C:\ProgramData\Dell\Dell Data Protection\Installer** に置かれます。
- Windows は、**C:\Users\<ユーザー名>\AppData\Local\Temp** に、ログインしたユーザーに関する独自の **子インストーラインストールログファイル**を作成します。
- Windows はログインしたユーザー用に、クライアントの前提条件(Visual C++ など)ログファイルを **C:\Users\<ユーザー名>\AppData\Local\Temp** にある %temp% に作成します。**例：C:\Users\<ユーザー名>\AppData\Local\Temp\dd_vcredist_amd64_20160109003943.log**
- インストール対象のコンピューターにインストールされている Microsoft .Net のバージョンを検証するには、http://msdn.microsoft.com の手順に従ってください。

  Microsoft .Net Framework 4.5.2 以降の完全バージョンをダウンロードするには、https://www.microsoft.com/ja-jp/download/details.aspx?id=30653 にアクセスします。
- インストール対象のコンピュータに Dell Access がインストールされている (または過去にされていた) 場合は、こちらのドキュメントを参照してください。DDP|A には、この製品スイートへの互換性はありません。

すべてのクライアント - 保護ステータス

デバイスの保護状態を導き出すための新しい方法は、Dell Security Management Server v9.8.2 で実装されています。以前は、管理コンソールのダッシュボードにあったエンドポイントの保護状態を示す領域は、デバイスごとの暗号化の状態のみを示していました。

次の条件のいずれかが満たされた場合に、保護状態が示されます。

- Advanced Threat Prevention がインストールされ、有効になっている。
- Web Protection または Client Firewall がインストールされ、Web Protection または Client Firewall のポリシーのいずれかが有効になっている。
- Dell Data Guardian がインストールされ、有効になっている。
- 自己暗号化ドライブ管理がインストールされて有効になっていて、Pre-Boot Authentication (PBA) が有効である。
- BitLocker Manager がインストールされて有効になっていて、暗号化が完了している。
- Dell Encryption (Mac の場合) がインストールされて有効になっていて、ポリシーベースの暗号化が実行されている。
- Dell Encryption (Windows の場合) がインストールされて有効になっていて、ポリシーベースの暗号化がエンドポイント用に設定済みで、デバイススイープが完了している。

Encryption および Server Encryption クライアントのトラブルシューティング

Windows 10 Creators Update へのアップグレード

Windows 10 October 2018 Update にアップグレードするには、次の文書の指示に従ってください。http://www.dell.com/support/article/us/en/19/SLN298382

サーバーオペレーティングシステム上でのアクティベーション

Encryption がサーバーオペレーティングシステム上にインストールされた場合、アクティベーションには、初期アクティベーションとデバイスアクティベーションの 2 つのアクティベーションフェーズが必要です。

初期アクティベーションのトラブルシューティング

初期アクティベーションは、次のときに失敗します。

- 提供された資格情報を使用して、有効な UPN を構築できない。
- エンタープライズ資格情報コンテナ内で資格情報が見つからない。
- アクティブ化に使用される資格情報がドメイン管理者の資格情報ではない。

エラーメッセージ：Unknown user name or bad password

ユーザー名とパスワードが一致しません。

可能な解決策：ユーザー名とパスワードを正確に入力して、ログインを再試行します。

エラーメッセージ：Activation failed because the user account does not have domain admin administrator rights.

アクティブ化に使用された資格情報にドメイン管理者権限がないか、管理者のユーザー名が UPN 形式ではありませんでした。

可能な対策：アクティベーションダイアログで、ドメイン管理者の資格情報を UPN 形式で入力します。

エラーメッセージ：A connection with the server could not be established.

または

```
The operation timed out.
```

Server Encryption が、DDP Server への https 経由でポート 8449 と通信することができませんでした。

可能な解決策

- ネットワークに直接接続し、アクティブ化を再試行します。
- VPN で接続されている場合は、ネットワークへの直接接続を試行して、アクティブ化を再試行します。
- Dell Server の URL をチェックして、管理者から提供された URL と一致していることを確認します。ユーザーがインストーラに入力した URL とその他のデータはレジストリに保存されています。[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] と [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet] にあるデータの正確性をチェックしてください。
- サーバーをネットワークから切り離します。サーバーを再起動して、ネットワークに再接続します。

エラーメッセージ：Activation failed because the Server is unable to support this request.

可能な解決策

- Server Encryption をレガシーサーバに対してアクティブ化することはできません。Dell Server のバージョンは、バージョン 9.1 以降である必要があります。必要に応じて、お使いの Dell Server をバージョン 9.1 以降にアップグレードしてください。
- Dell Server の URL をチェックして、管理者から提供された URL と一致していることを確認します。ユーザーがインストーラに入力した URL とその他のデータはレジストリに保存されています。
- [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield] と [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet] にあるデータの正確性をチェックしてください。

初期アクティベーションプロセス

次の図は、正常な初期アクティベーションを示します。

Server Encryption の初期アクティベーションプロセスでは、ライブユーザーがサーバーにアクセスする必要があります。ユーザーは、ドメインまたは非ドメイン、リモートデスクトップ接続またはインタラクティブなど、どのようなタイプのユーザーでもかまいませんが、ドメイン管理者資格情報にアクセスできなければなりません。

次の 2 つのうちのいずれかが起こると、アクティブ化 ダイアログボックスが表示されます。

- 新しい (非管理) ユーザーがコンピュータにログオンする。
- 新しいユーザーがシステムトレイ内の Encryption クライアントアイコンを右クリックし、Encryption のアクティブ化を選択したとき。

初期アクティベーションプロセスは次のとおりです。

1 ユーザーがログインします。
2 新しい (非管理) ユーザーを検出して、アクティブ化 ダイアログが表示されます。ユーザーが **キャンセル** をクリックします。
3 ユーザーが Server Encryption の バージョン情報 ボックスを開いて、Server Encryption がサーバーモードで実行中であることを確認します。
4 ユーザーが通知領域内の Encryption クライアントアイコンを右クリックし、**Dell Encryption のアクティブ化** を選択します。
5 ユーザーが アクティブ化 ダイアログにドメイン管理者資格情報を入力します。

> **メモ:**
> このドメイン管理者資格情報の要求は、Server Encryption が、それをサポートしていない他のサーバ環境にロールアウトされるのを防ぐための安全対策です。ドメイン管理者資格情報の要求を無効にするには「作業を開始する前に」を参照してください。

6 Dell Server がエンタープライズ資格情報コンテナ (Active Directory またはその同等物) 内の資格情報をチェックして、その資格情報がドメイン管理者資格情報であることを確認します。
7 資格情報を使用して UPN が構築されます。
8 その UPN を使用して、Dell Server が仮想サーバユーザー用の新しいユーザーアカウントを作成し、その資格情報を Dell Server の資格情報コンテナ内に保存します。

仮想サーバーユーザーアカウントは、Encryption クライアントの排他使用用です。これはサーバでの認証、共通暗号化キーの処理、ポリシーアップデートの受信のために使用されます。

> **メモ:**
> 仮想サーバーユーザーのみがコンピュータ上の暗号化キーにアクセスできるように、パスワードおよび DPAPI 認証はこのアカウントに対して無効化されます。このアカウントは、コンピュータ上、またはドメイン上の他のどのアカウントとも一致しません。

9 アクティベーションの成功後、ユーザーがコンピュータを再起動すると、第 2 フェーズ (認証とデバイスアクティベーション) が開始されます。

認証とデバイスアクティベーションのトラブルシューティング

デバイスアクティベーションは、次のときに失敗します。

- 初期アクティベーションが失敗した。
- サーバーとの接続を確立できなかった。
- 信頼する証明書を検証できなかった。

アクティベーション後コンピュータが再起動されると、Server Encryption は仮想サーバユーザーとして自動的にログインし、Dell Server にマシンキーを要求します。これは、ユーザーがまだログインできなくても行われます。

- バージョン情報 ダイアログを開いて、Server Encryption が認証済みで、サーバーモードになっていることを確認します。
- Encryption クライアント ID が赤色で表示されている場合、暗号化はまだアクティブ化されていません。
- 管理コンソールでは、Server Encryption がインストールされているサーバのバージョンは サーバ用 *Shield* としてリストされます。
- ネットワークの障害が原因でマシンキーの取得に失敗した場合、Server Encryption はオペレーティングシステムでネットワーク通知に登録します。
- マシンキーの取得に失敗した場合 :
  - 失敗しても、仮想サーバーユーザーのログオンは成功します。

– 設定した時間間隔でキーの取得を再試行するように、ネットワーク障害時の再試行間隔ポリシーをセットアップします。

ネットワーク障害時の再試行間隔ポリシーの詳細については、管理コンソールから利用できる AdminHelp を参照してください。

認証とデバイスアクティベーション

次の図は、正常な認証とデバイスアクティベーションを示します。

1 正常な初期アクティベーション後、再起動が行われると、Server Encryption を搭載したコンピュータは、仮想サーバーユーザーアカウントを使用して Encryption クライアントを自動的に認証し、サーバーモードで実行します。

2 コンピュータは、自身のデバイスアクティベーションステータスを Dell Server でチェックします。

- そのコンピュータがまだデバイスアクティブ化されていない場合、Dell Server は、そのコンピュータに MCID、DCID、および信頼証明書を割り当て、そのすべての情報を Dell Server の資格情報コンテナ内に保存します。
- そのコンピュータがすでにデバイスアクティブ化されている場合、Dell Server は信頼証明書を検証します。

3 Dell Server が信頼証明書をサーバに割り当てると、そのサーバはその暗号化キーにアクセスできます。

4 デバイスアクティベーションが成功します。

メモ:
サーバーモードで実行している場合、Encryption クライアントは、暗号化キーにアクセスするために、デバイスアクティベーションに使用されたのと同じ証明書にアクセスできなければなりません。

Encryption External Media と PCS の相互作用

メディアが読み取り専用ではなく、ポートがブロックされていないことを確実にする

EMS Access から unShielded Media へのポリシーは、Port Control System - Class: Storage > Subclass Storage: External Drive Control ポリシーと相互作用します。EMS Access から unShielded Media へのポリシーをフルアクセスに設定する場合は、メディアが読み取り専用に設定されず、ポートがブロックされないようにするために、Subclass Storage: External Drive Control ポリシーもフルアクセスに設定する必要があります。

CD/DVD に書き込まれたデータを暗号化する

- Windows Media Encryption = オンに設定します。
- EMS で CD/DVD 暗号化を除外 = 選択なしに設定します。
- サブクラスストレージの設定：光学ドライブコントロール = UDF Only に設定します。

WSScan の使用

- WSScan を使用すると、Encryption クライアントをアンインストールするとき、すべてのデータが復号化されていることを確認することができます。また、暗号化ステータスを表示し、暗号化されるべき非暗号化状態のファイルを特定することもできます。
- このユーティリティの実行には管理者権限が必要です。

WSScan

1 Dell インストールメディアから、スキャン対象の Windows コンピュータに WSScan.exe をコピーします。

2 上記の場所でコマンドラインを起動して、コマンドプロンプトに **wsscan.exe** と入力します。WSScan が起動します。

3 **詳細設定** をクリックします。

4 スキャンしたいドライブの種類を選択します：すべてのドライブ、固定ドライブ、リムーバブルドライブ、または *CDROM/DVDROM*。

5 暗号化レポートタイプを選択します：暗号化ファイル、非暗号化ファイル、すべてのファイル、または違反の非暗号化ファイル。

- 暗号化ファイル- Encryption クライアントをアンインストールするとき、すべてのデータが復号化されていることを確認するために使用します。復号化ポリシーアップデートの発行など、データを復号化するための既存の手順に従います。データを復号化した後は、アンインストール準備として再起動する前に、WSScan を実行してすべてのデータが復号化されていることを確認します。

- 非暗号化ファイル- 暗号化されていないファイルを特定するために使用します。それらのファイルを暗号化するべきかどうか(Y/N)も示されます。
- すべてのファイル- すべての暗号化および非暗号化ファイルのリストを表示するために使用します。それらのファイルを暗号化するべきかどうか(Y/N) も示されます。
- 違反の非暗号化ファイル- 暗号化すべき非暗号化ファイルを特定するために使用します。

6 **検索** をクリックします。

または

1 **詳細設定** をクリックし、ビューを **シンプル** に切り替えて、特定のフォルダをスキャンします。
2 スキャン設定 に移動して、検索パス フィールドにフォルダパスを入力します。このフィールドを使用した場合、メニューの選択は無視されます。
3 WSScan の出力をファイルに書き込まない場合は、**ファイルに出力** チェックボックスをオフにします。
4 必要に応じて、パスに含まれているデフォルトパスとファイル名を変更します。
5 既存のどの WSScan 出力ファイルも上書きしない場合は、**既存のファイルに追加** を選択します。
6 出力書式を選択します。

- スキャンした結果をレポートスタイルのリストで出力する場合は、レポート書式 を選択します。これがデフォルトの書式です。
- スプレッドシートアプリケーションにインポートできる書式で出力する場合は、値区切りファイル を選択します。デフォルトの区切り文字は「|」ですが、最大 9 文字の英数字、空白、またはキーボード上のパンクチュエーション文字に変更できます。
- 各値を二重引用符で囲むには、クォートされる値 オプションを選択します。
- 各暗号化ファイルに関する一連の固定長情報を含む区切りのない出力には、固定幅ファイル を選択します。

7 **検索** をクリックします。

検索の停止 をクリックして検索を停止します。**クリア** をクリックし、表示されているメッセージをクリアします。

WSScan 出力

暗号化ファイルに関する WSScan の情報には、次の情報が含まれています。

出力例：

[2015-07-28 07:52:33] SysData.7vdlxrsb._SDENCR_: "c:\temp\Dell - test.log" is still AES256 encrypted

出力	意味
日時のタイムスタンプ	ファイルがスキャンされた日時。
暗号化の種類	ファイルの暗号化に使用した暗号化の種類。 **SysData：** SDE キー。 **User：** ユーザー暗号化キー。 **Common：** 共通暗号化キー。 WSScan では、Encrypt for Sharing で暗号化されたファイルは報告されません。
KCID	キーコンピュータ ID。 上記の例では、「**7vdlxrsb**」 マッピングされているネットワークドライブをスキャンした場合、KCID はスキャンレポートに表示されません。
UCID	ユーザー ID。 上記の例では、「**_SDENCR_**」 UCID は、そのコンピュータのすべてのユーザーで共有されます。

出力	意味
ファイル	暗号化ファイルのパス。 上記の例では、「**c:\temp\Dell - test.log**」
アルゴリズム	ファイルの暗号化に使用した暗号化アルゴリズム。 上記の例では、「**is still AES256 encrypted**」 Rijndael 128 Rijndael 256 AES-128 AES-256 3DES

Encryption Removal Agent ステータスのチェック

Encryption Removal Agent は、サービスパネル (スタート > ファイル名を指定して実行 ... > services.msc > OK) の 説明 エリアに、次のようにステータスを表示します。ステータスをアップデートするために、サービスは定期的に更新してください (サービスをハイライト表示 > 右クリック > 更新)。

- **SED の非アクティブ化を待機中** – Encryption クライアントはまだインストールされているか、まだ設定されているか、またはその両方です。Encryption クライアントがアンインストールされるまで復号化は開始されません。
- **初期スイープ** – サービスは初期スイープを行っており、暗号化されたファイル数およびバイト数を計算しています。初期スイープは一度だけ実行されます。
- **復号化スイープ** – サービスはファイルを復号化しており、ロックされたファイルの復号化を要求している可能性もあります。
- **再起動時に復号化 (一部)** – 復号化スイープが完了し、一部の (すべてではない) ロックされたファイルが次回の再起動時に復号化されます。
- **再起動時に復号化** – 復号化スイープが完了し、すべてのロックされたファイルが次回の再起動に復号化されます。
- **すべてのファイルを復号化できませんでした** – 復号化スイープが完了しましたが、一部のファイルを復号化できませんでした。このステータスは、次のいずれかが発生したことを意味します。
  - ロックされたファイルが大きすぎた、またはロック解除の要求時にエラーが発生したため、ロックされたファイルの復号化をスケジュールできなかった。
  - ファイルの復号化中に入出力エラーが発生した。
  - ポリシーによりファイルを復号化できなかった。
  - ファイルが暗号化対象としてマーク付けされている。
  - 復号化スイープ中にエラーが発生した。
  - いずれの場合でも、LogVerbosity=2 (またはそれ以上) が設定されていれば、ログファイルが作成されます (ログが設定されている場合)。トラブルシューティングを行うには、ログの詳細度を 2 に設定して、Encryption Removal Agent Service を再起動し、復号化スイープを強制的に再実行します。
- **完了** – 復号化スイープが完了しました。サービス、実行ファイル、ドライバ、およびドライバ実行ファイルは、すべて次回の再起動で削除されるようにスケジュールされています。

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

Windows Powershell を使用した製品コードの検索

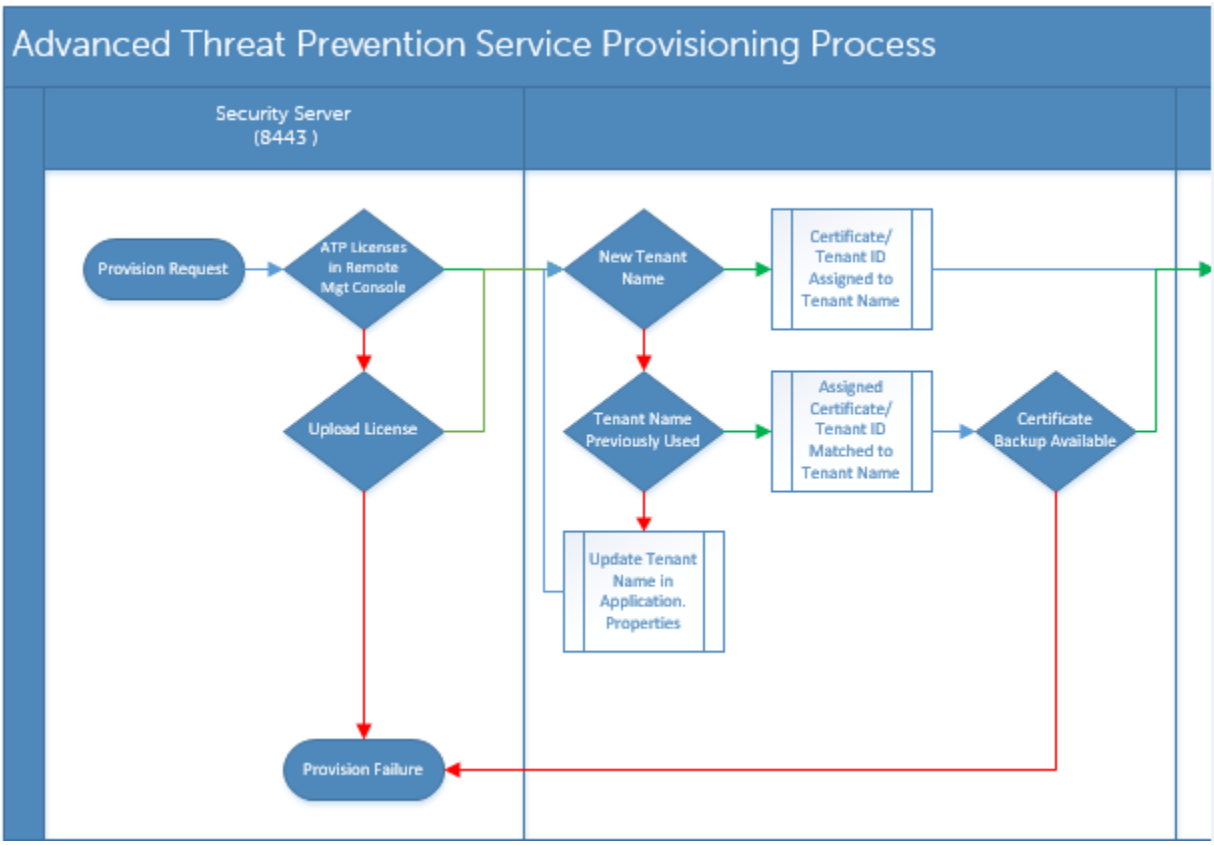
- この方法を使用すれば、将来製品コードに変更があった場合に、製品コードを容易に見つけることができます。

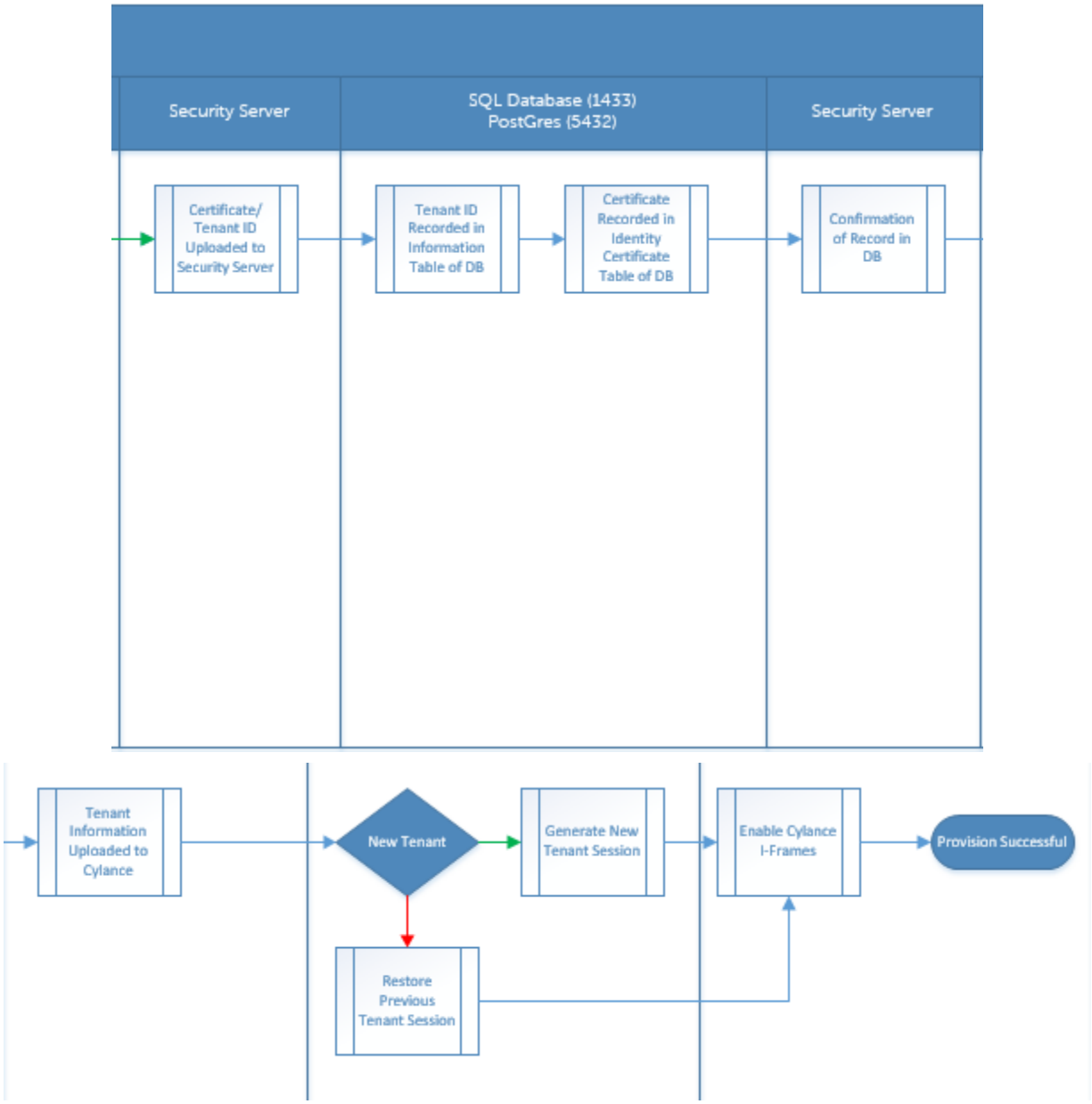
```
Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT
IdentifyingNumber, Name, LocalPackage
```

出力結果は、フルパスと .msi ファイル名（変換された 16 進法のファイル名）となります。

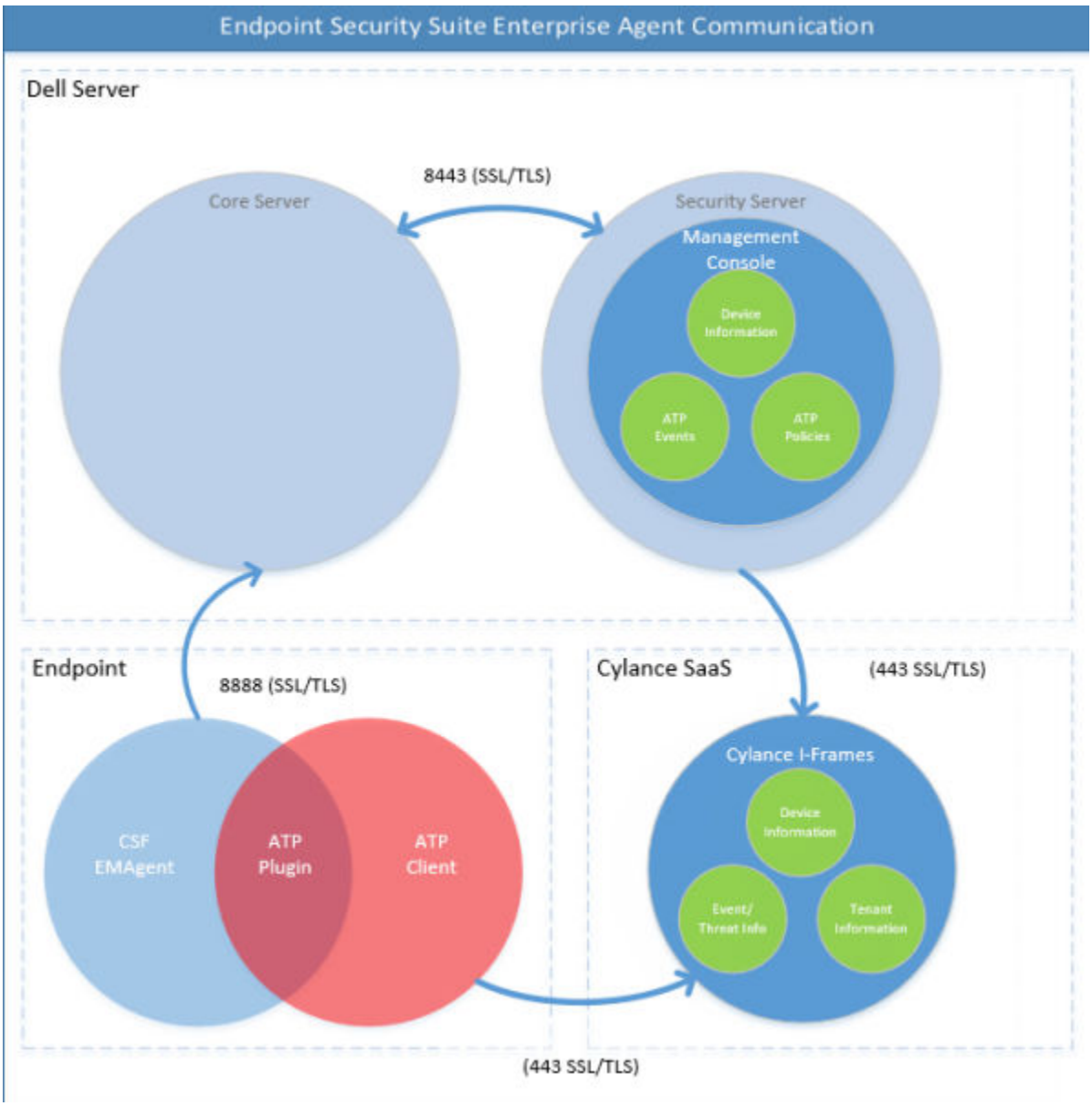
Advanced Threat Prevention のプロビジョニングおよびエージェント通信

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。



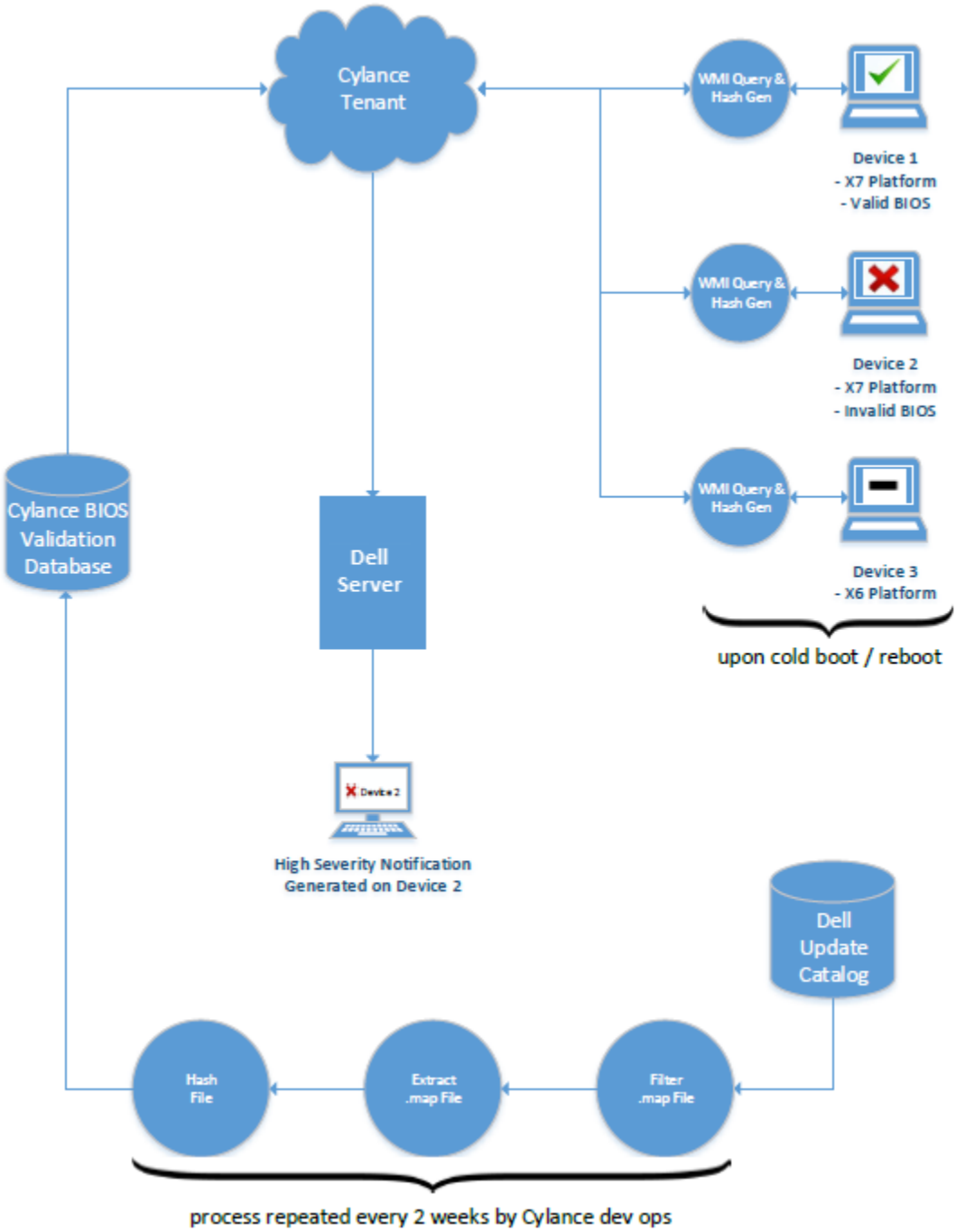


次の図は Advanced Threat Prevention のエージェント通信プロセスを表しています。



BIOS イメージの整合性検証プロセス

次の図は、BIOS イメージの整合性の検証プロセスを表しています。BIOS イメージの整合性検証によりサポートされる Dell コンピュータのモデル一覧については、「要件 - BIOS イメージの整合性検証」を参照してください。



Dell ControlVault ドライバ

Dell ControlVault ドライバおよびファームウェアのアップデート

工場で Dell コンピュータ にインストールされている Dell ControlVault ドライバおよびファームウェアは古いため、次の手順の順序にしたがってアップデートする必要があります。

クライアントのインストールの際に、Dell ControlVault のドライバをアップデートするためにインストーラを終了することを促すエラーメッセージが表示された場合、このメッセージは無視してクライアントのインストールを続行します。Dell ControlVault ドライバ（およびファームウェア）はクライアントのインストールが完了した後にアップデートすることができます。

最新のドライバのダウンロード

1 Support.dell.com に移動します。
2 お使いのコンピュータモデルを選択します。
3 **ドライバおよびダウンロード** を選択します。
4 ターゲットコンピューターの **オペレーティングシステム** を選択します。
5 **セキュリティ** カテゴリを展開します。
6 Dell ControlVault ドライバをダウンロードして保存します。
7 Dell ControlVault ファームウェアをダウンロードして保存します。
8 必要に応じて、ターゲットコンピュータにドライバとファームウェアをコピーします。

Dell ControlVault ドライバのインストール

ドライバのインストールファイルをダウンロードしたフォルダに移動します。

Dell ControlVault ドライバをダブルクリックして自己解凍形式の実行可能ファイルを実行します。

:

ドライバを先にインストールします。本文書の作成時における ドライバのファイル名は ControlVault_Setup_2MYJC_A37_ZPE.exe です。

続行 をクリックして開始します。

Ok をクリックして、ドライバファイルを **C:\Dell\Drivers\<新規フォルダ>** のデフォルトの場所に解凍します。

はい をクリックして新しいフォルダの作成を許可します。

正常に解凍しましたというメッセージが表示されたら **Ok** をクリックします。

抽出後、ファイルが含まれているフォルダが表示されます。表示されない場合は、ファイルを抽出したフォルダに移動します。この場合、フォルダは **JW22F** です。

CVHCI64.MSI をダブルクリックしてドライバインストーラを実行します。[この例の場合は **CVHCI64.MSI** です（32 ビットのコンピュータ用 CVHCI)]。
ようこそ画面で **次へ** をクリックします。

次へ をクリックしてドライバを **C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.** のデフォルトの場所にインストールします。

完了 オプションを選択して **次へ** をクリックします。

インストール をクリックしてドライバのインストールを開始します。

必要に応じて、インストーラのログファイルを表示するチェックボックスを選択します。**終了** をクリックしてウィザードを終了します。

ドライバのインストールの検証

オペレーティングシステムおよびハードウェアの構成によっては、デバイスマネージャに Dell ControlVault デバイス（ およびその他のデバイス ）が表示されます。

Dell ControlVault ファームウェアのインストール

1 ファームウェアのインストールファイルをダウンロードしたフォルダに移動します。
2 Dell ControlVault ファームウェアをダブルクリックして自己解凍形式の実行可能ファイルを実行します。
3 **続行** をクリックして開始します。
4 **Ok** をクリックして、ドライバファイルを **C:\Dell\Drivers\<新規フォルダ>** のデフォルトの場所に解凍します。
5 **はい** をクリックして新しいフォルダの作成を許可します。
6 正常に解凍しましたというメッセージが表示されたら **Ok** をクリックします。
7 抽出後、ファイルが含まれているフォルダが表示されます。表示されない場合は、ファイルを抽出したフォルダに移動します。**ファームウェア** フォルダを選択します。

8 **ushupgrade.exe** をダブルクリックしてファームウェアインストーラを実行します。

9 **スタート** をクリックしてファームウェアのアップグレードを開始します。

:

ファームウェアを旧バージョンからアップグレードする場合は、管理者パスワードの入力を求められることがあります。**Broadcom** をパスワードとして入力し、このダイアログが表示された場合は **Enter** をクリックします。

いくつかのステータスメッセージが表示されます。

10 **再起動** をクリックしてファームウェアのアップグレードを完了します。

Dell ControlVault ドライバおよびファームウェアのアップデートが完了しました。

13

用語集

Advanced Threat Prevention - Advanced Threat Prevention 製品は、アルゴリズム的科学および機械学習を使用して、既知および不明のサイバー攻撃や、エンドポイントの攻撃を識別、分類、および防止する、次世代のアンチウイルス対策です。オプションのクライアントファイアウォール機能は、コンピュータと、ネットワークおよびインターネット上のリソースとの通信をモニタし、潜在的に悪意のある通信を中断します。オプションのウェブプロテクション機能は、オンラインのブラウジングおよび検索中に、ウェブサイトの安全評価とレポートに基づいて、安全でないウェブサイトおよびそれらのウェブサイトからのダウンロードをブロックします。

BitLocker Manager – Windows BitLocker は、データファイルとオペレーティングシステムファイルの両方を暗号化することによって Windows コンピュータの保護を助けるように設計されています。BitLocker 展開のセキュリティを高め、所有コストを単純化および軽減するために、デルでは、多くのセキュリティ問題に対処する単一の一元管理コンソールを用意しており、BitLocker 以外の他のプラットフォーム (物理、仮想、クラウドベースにかかわらない) にわたって暗号を管理するための統合アプローチを提供しています。BitLocker Manager は、オペレーティングシステム、固定ドライブ、および BitLocker To Go 用の BitLocker 暗号化をサポートしています。BitLocker Manager を使用すれば、BitLocker を既存の暗号化ニーズにシームレスに統合でき、セキュリティとコンプライアンスを合理化しながらわずかな作業で BitLocker を管理できます。BitLocker Manager は、キーの復元、ポリシーの管理および適用、自動 TPM 管理、FIPS コンプライアンス、コンプライアンスレポートに関する統合管理を提供します。

非アクティブ化 – 非アクティブ化は、管理コンソールで SED 管理がオフになるときに実行されます。コンピュータが非アクティブ化されると、PBA データベースが削除され、キャッシュされたユーザーの記録がなくなります。

Encryption External Media Dell Encryption クライアント内のこのサービスは、リムーバブルメディアおよび外付けストレージデバイスにポリシーを適用します。

Encryption External Media アクセスコード - Dell Server 内のこのサービスでは、ユーザーがパスワードを忘れてログインできなくなった場合に、Encryption External Media で保護されたデバイスを復旧可能にします。この処理が完了したら、ユーザーはメディアに設定されたパスワードをリセットできます。

Encryption クライアント – Encryption クライアントは、エンドポイントがネットワークに接続されている、ネットワークから切断されている、または盗難されているかどうかに関わらず、セキュリティポリシーを適用するオンデバイスコンポーネントです。Encryption クライアントは、エンドポイントに信頼できるコンピュータ環境を作成しながら、デバイスのオペレーティングシステム上のレイヤとして動作し、一貫して適用される認証、暗号、および承認を提供して機密情報を最大限に保護します。

エンドポイント - Dell Server によって管理されているコンピュータ。

暗号化スイープ - 暗号化スイープは、含まれるファイルが適切な暗号化状態になるように、管理下のエンドポイントで暗号化するフォルダをスキャンするプロセスです。通常のファイル作成および名前変更操作では、暗号化スイープはトリガされません。次のように、暗号化スイープが行われる可能性のある場合と、その結果生じるスイープ時間に影響を与える可能性のあるものを理解することが重要です。暗号化スイープは、暗号化を有効にしたポリシーの最初の受信時に行われます。これは、ポリシーで暗号化を有効にしている場合にアクティブ化直後に行われることがあります。- ログオン時にワークステーションをスキャン ポリシーを有効にしている場合、暗号化用に指定されたフォルダはユーザーログオンごとにスイープされます。- その後、特定のポリシー変更があると、スイープが再度トリガされる場合があります。暗号化フォルダ、暗号化アルゴリズム、暗号化キーの使用 (共通対ユーザー) の定義に関連したポリシー変更はスイープをトリガします。さらに、暗号化の有効化と無効化を切り替えると、暗号化スイープがトリガされます。

SED Management – SED Management は、自己暗号化ドライブを安全に管理するためのプラットフォームを提供します。SED は独自の暗号化を備えていますが、その暗号化および使用できるポリシーを管理するためのプラットフォームがありません。SED Management は、データを効果的に保護および管理できる、一元的で拡張可能な管理コンポーネントです。SED Management は、企業の管理の迅速化および簡略化を可能にします。

Server ユーザー - 暗号化キーの操作とポリシーアップデートのために、Dell Server Encryption によって作成される仮想ユーザーアカウントです。このユーザーアカウントは、コンピュータ上、またはドメイン内の他のどのユーザーアカウントとも一致しません。また、このアカウントには、実際に使用できるユーザー名とパスワードはありません。管理コンソールでは、このアカウントに一意の UCID 値が割り当てられます。