Dell Data Protection | Endpoint Security Suite Enterprise

基本インストールガイド v1.4

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。

Endpoint Security Suite Enterprise Basic Installation Guide（Endpoint Security Suite Enterprise 基本インストールガイド）

2017 - 04

Rev. A01

目次

1 はじめに 5
作業を開始する前に 5
このガイドの使用法 5
Dell ProSupport へのお問い合わせ 5

2 要件 6
すべてのクライアント 6
すべてのクライアント - 前提条件 6
すべてのクライアント - ハードウェア 6
すべてのクライアント - 言語サポート 7
Encryption クライアント 7
Encryption クライアントの前提条件 8
Encryption クライアントのオペレーティングシステム 8
外付けメディアシールド (EMS) のオペレーティングシステム 8
Advanced Threat Prevention クライアント 9
Advanced Threat Prevention のオペレーティングシステム 9
Advanced Threat Prevention のポート 9
BIOS イメージの整合性検証 10
SED クライアント 10
SED クライアントの前提条件 11
SED クライアントハードウェア 11
SED クライアントのオペレーティングシステム 11
Advanced Authentication クライアント 12
Advanced Authentication クライアントハードウェア 12
Advanced Authentication クライアントのオペレーティングシステム 12
BitLocker Manager クライアント 13
BitLocker Manager クライアントの前提条件 13
BitLocker Manager クライアントのオペレーティングシステム 14

3 ESSE マスターインストーラを使用したインストール 15
ESSE 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 15
ESSE 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 16

4 ESSE マスターインストーラを使用したアンインストール 19
ESSE マスターインストーラのアンインストール 19
コマンドラインでのアンインストール 19

5 子インストーラを使用したアンインストール 20
Encryption および Server Encryption クライアントのアンインストール 21
プロセス 21
コマンドラインでのアンインストール 21

Advanced Threat Prevention のアンインストール 23
コマンドラインでのアンインストール 23
SED クライアントおよび Advanced Authentication クライアントのアンインストール 23
プロセス 23
PBA の非アクティブ化 23
SED クライアントおよび Advanced Authentication クライアントのアンインストール 24
BitLocker Manager クライアントのアンインストール 24
コマンドラインでのアンインストール 24

6 Advanced Threat Prevention のためのテナントのプロビジョニング 25
テナントのプロビジョニング 25

7 Advanced Threat Prevention エージェント自動アップデートの設定 26

8 ESSE マスターインストーラからの子インストーラの抽出 27

9 EE Server に対してアクティブ化した Encryption クライアントをアンインストールするための Key Server の設定 28
サービスパネル - ドメインアカウントのユーザーの追加 28
キーサーバーの設定ファイル - EE Server の通信のためのユーザーの追加 28
サービスパネル - キーサーバーサービスの再起動 29
リモート管理コンソール - フォレンジック管理者の追加 29

10 Administrative Download Utility （ CMGAd ）の使用 30
フォレンジックモードでの Administrative Download Utility の使用 30
管理者モードでの Administrative Download Utility の使用 31

11 トラブルシューティング 32
すべてのクライアントのトラブルシューティング 32
Encryption および Server Encryption クライアントのトラブルシューティング 32
Windows 10 Anniversary アップデートへのアップグレード 32
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 32
EMS と PCS の相互作用 35
WSScan の使用 35
Encryption Removal Agent ステータスのチェック 37
Advanced Threat Prevention クライアントのトラブルシューティング 37
Windows Powershell を使用した製品コードの検索 37
Advanced Threat Prevention のプロビジョニングおよびエージェント通信 37
BIOS イメージの整合性検証プロセス 40
Dell ControlVault ドライバ 41
Dell ControlVault ドライバおよびファームウェアのアップデート 41

12 用語集 44

1

はじめに

本書では、ESS マスターインストーラを使用したアプリケーションのインストールおよび設定方法を詳しく説明します。本書には、基本インストールの手順が記載されています。ESS マスターインストーラを使用した基本手順の範囲を超える子インストーラのインストール、EE Server/VE Server の設定または情報が必要である場合は、『*Advanced Installation Guide*』(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 にあります。

作業を開始する前に

1 クライアントを導入する前に、EE Server/VE Server をインストールします。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。

- 『*DDP Enterprise Server* インストールおよびマイグレーションガイド 』
- 『*DDP Enterprise Server - Virtual Edition* クイックスタートガイドおよびインストールガイド』

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。画面の右端にあります。AdminHelp はポリシーの設定および変更、EE Server/VE 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 DDP 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 エンド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。
  - ESSE 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 内部接続ポートを編集... のいずれかをクリックします。
  - ESSE 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

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

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

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

米国外の電話番号については、Dell ProSupport の国際電話番号をチェックしてください。

2

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 SMS または Dell 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。
- ESSE マスターインストーラクライアントが Dell Digital Delivery（DDD）を使用して資格を得る場合は、アウトバウンドポート 443 が EE Server/VE Server と通信できるようにしてください。資格機能はポート 443 が（何らかの理由で）ブロックされている場合には機能しません。子インストーラを使用してインストールする場合、DDD は使用されません。
- 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。

すべてのクライアント - 前提条件

- ESSE マスターインストーラクライアントと子インストーラクライアントには、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。

  デルの工場から出荷されるすべてのコンピュータには、Microsoft .Net Framework 4.5.2 以降の完全バージョンが事前インストールされています。ただし、Dell ハードウェア上にインストールしていない、または旧型の Dell ハードウェア上で Security Tools をアップグレードしている場合は、インストール / アップグレードの失敗を防ぐため、**Security Tools をインストールする前に**、インストールされている Microsoft .Net のバージョンを確認し、バージョンをアップデートするようにしてください。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/en-us/download/details.aspx?id=42643 に進みます。
- ControlVault、指紋リーダー、およびスマートカード（下記参照）のドライバとファームウェアは、ESSE マスターインストーラや子インストーラの実行可能ファイルには含まれていません。ドライバとファームウェアは最新の状態にしておく必要があります。これらは、http://www.dell.com/support から、お使いのコンピュータモデルを選択してダウンロードできます。認証ハードウェアに基づいて、適切なドライバとファームウェアをダウンロードします。

  - ControlVault
  - NEXT Biometrics Fingerprint ドライバ
  - Validity Fingerprint Reader 495 ドライバ
  - O2Micro スマートカードドライバ

  デル以外のハードウェアにインストールしている場合は、そのベンダーのウェブサイトからアップデート済みのドライバとファームウェアをダウンロードしてください。ControlVault ドライバのインストール手順は、「Dell ControlVault ドライバおよびファームウェアのアップデート」に記載されています。

すべてのクライアント - ハードウェア

- 次の表に、サポートされているコンピュータハードウェアについて詳しく示します。

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。

すべてのクライアント - 言語サポート

- Encryption、、Advanced Threat Prevention、および BitLocker Manager クライアント、複数言語ユーザーインタフェース (MUI) に対応しており、次の言語をサポートします。リモート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))

- SED および Advanced Authentication のクライアントは、複数言語ユーザーインターフェイス (MUI) に対応しており、次の言語をサポートしています。ロシア語、繁体字中国語、または簡体字中国語では、UEFI モードおよび起動前認証はサポートされていません。

言語サポート

- EN - 英語
- FR - フランス語
- IT - イタリア語
- DE - ドイツ語
- ES - スペイン語
- JA - 日本語
- KO - 韓国語
- ZH-CN - 中国語 (簡体字)
- 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

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、McAfee、Symantec クライアント、Kaspersky、および MalwareBytes を使用してテスト済みです。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/SLN298707 を参照するか、Contact Dell ProSupport にお問い合わせください。
- インプレイスでのオペレーティングシステムのアップグレードは、Encryption クライアントがインストールされている場合ではサポートされていません。Encryption クライアントをアンインストールおよび復号化し、新しいオペレーティングシステムにアップグレードした後、Encryption クライアントを再度インストールしてください。

さらに、オペレーティングシステムの再インストールも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

- Microsoft Visual C++ 2012 更新プログラム 4 がコンピュータにまだインストールされていない場合は、ESSE マスターインストーラがこれをインストールします。

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）

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 SP0-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（ハードウェア暗号化はサポートされていません）
- Windows 8： Enterprise、Pro
- Windows 8.1 Update 0-1： Enterprise Edition、Pro Edition
- Windows Embedded 8.1 Industry Enterprise（ハードウェア暗号化はサポートされていません）
- Windows 10： Education、Enterprise、Pro
- VMWare Workstation 5.5 以降

> **メモ:**
> UEFI モードは、Windows 7、Windows Embedded Standard 7、または Windows Embedded 8.1 Industry Enterprise ではサポートされていません。

外付けメディアシールド（EMS）のオペレーティングシステム

- 次の表に、EMS 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:**
> EMS をホストするには、外部メディア上の約 55MB 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。

> **メモ:**
> Windows XP は、EMS Explorer を使用する場合にのみサポートされています。

EMS 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 SP0-SP1： Enterprise、Professional、Ultimate、Home Premium
- Windows 8： Enterprise、Pro、Consumer
- Windows 8.1 Update 0-1： Enterprise Edition、Pro Edition
- Windows 10： Education、Enterprise、Pro

EMS 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 ）

- Mac OS X Yosemite 10.10.5
- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.0

Advanced Threat Prevention クライアント

- Advanced Threat Prevention クライアントは、コンピュータで Dell Client Security Framework (EMAgent) クライアントが検出されない状態でインストールすることはできません。インストールしようとしても失敗します。
- クライアントを管理している Dell Enterprise Server/VE 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、管理用のデルサーバを 切断モード で実行している場合は、Advanced Threat Prevention をインストールするための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、デルサーバがインターネットに接続されている必要があります。

  メモ: デルサーバを切断モードで実行しているときは、インターネット接続は必要ありません。
- 切断モードで実行している Dell Enterprise Server/VE 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、デルサーバの Advanced Threat Protection 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。デルサーバの Advanced Threat Protection 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。他のウイルス対策アプリケーションに追加する除外のリストについては、「http://www.dell.com/support/article/us/en/19/SLN301134」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 SP0-SP1：Enterprise、Professional、Ultimate
- Windows 8： Enterprise、Pro
- Windows 8.1 Update 0-1： Enterprise Edition、Pro Edition
- Windows 10： Education、Enterprise、Pro
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- 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

BIOS イメージの整合性検証

BIOS 保証の有効化 ポリシーがリモート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、エンドユーザーシステム上で 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 DDP をサーバに渡され、IT 管理者はリモート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
- Latitude E7270
- Latitude E7470
- Latitude Rugged 5414
- Latitude Rugged 7214 Extreme
- Latitude Rugged 7414
- OptiPlex 3040
- OptiPlex 3240
- OptiPlex 5040
- OptiPlex 7040
- OptiPlex 7440
- Precision Mobile Workstation 3510
- Precision Mobile Workstation 5510
- VMware Workstation 3620
- VMware Workstation 7510
- VMware Workstation 7710
- Precision Workstation T3420
- Venue 10 Pro 5056
- Venue Pro 5855
- Venue XPS 12 9250
- XPS 13 9350
- XPS 9550

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。
- IPv6 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は、*RAID=On* から *AHCI* に切り替えるときにオペレーティングシステムがブルースクリーンになります。

- SED 管理は、Server Encryption またはサーバ OS 上の Advanced Threat Prevention ではサポートされません。

SED クライアントの前提条件

- Microsoft Visual C++2010 SP1 **および** Microsoft Visual C++ 2012 更新プログラム 4 がコンピュータにまだインストールされていない場合、ESSE マスターインストーラがこれらのプログラムをインストールします。

前提条件

- Visual C++ 2010 SP1 以降再頒布可能パッケージ（x86 および x64）
- 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）

SED クライアントハードウェア

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-CH - ドイツ語（スイス）
- DE-FR - フランス語（スイス）

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-CH - ドイツ語（スイス）
- DE-FR - フランス語（スイス）

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（レガシー起動モードではサポートされていますが、UEFI ではサポートされていません）

  メモ:
  Legacy ブートモードは Windows 7 でサポートされています。Windows 7 では UEFI はサポートされていません。

- Windows 8：Enterprise、Pro

Windows オペレーティングシステム（32 ビットと 64 ビット）

- Windows 8.1：Enterprise Edition、Pro Edition
- Windows 10： Education、Enterprise、Pro

Advanced Authentication クライアント

- Advanced Authentication を使用する場合、ユーザーは、Security Tools で管理および登録されている高機能認証資格情報を使用して、コンピュータへのアクセスをセキュア化します。Security Tools は、Windows パスワード、指紋、スマートカードなど、Windows サインイン用の認証資格情報のプライマリマネージャになります。Microsoft オペレーティングシステムを使用して登録されている画像パスワード、PIN、および指紋資格情報は、Windows サインインでは認識されません。

  ユーザー資格情報の管理に引き続き Microsoft オペレーティングシステムを使用するには、Security Tools Authentication をインストールしないでください。インストールした場合はアンインストールしてください。
- ワンタイムパスワード（OTP）機能には、TPM が存在し、有効化され、所有されている必要があります。OTP は TPM 2.0 でサポートされていません。TPM の所有権をクリアし、設定するには、https://technet.microsoft.com を参照してください。

Advanced Authentication クライアントハードウェア

- 次の表に、サポートされる認証ハードウェアについて詳しく示します。

指紋およびスマートカードリーダー

- セキュアモードの Validity VFS495
- ControlVault Swipe Reader
- UPEK TCS1 FIPS 201 Secure Reader 1.6.3.379
- Authentec Eikon および Eikon To Go USB Reader

非接触型カード

- 指定された Dell ノートブックに内蔵された非接触型カードリーダーを使用する非接触型カード

スマートカード

- ActivIdentity クライアントを使用した PKCS #11 スマートカード

  メモ:
  ActivIdentity クライアントは事前にロードされていないため、別途インストールする必要があります。
- CSP カード
- 共通アクセスカード（CAC）
- クラス B/SIPR ネットカード

Advanced Authentication クライアントのオペレーティングシステム

Windows 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 SP0-SP1: Enterprise、Professional、Ultimate

Windows オペレーティングシステム（32 ビットと 64 ビット）

- Windows 8: Enterprise、Pro
- Windows 8.1 Update 0-1: Enterprise Edition、Pro Edition
- Windows 10: Education、Enterprise、Pro

ⓘ | **メモ: Windows 7 では UEFI モードはサポートされていません。**

モバイルデバイスオペレーティングシステム

- 次のモバイルオペレーティングシステムは、Security Tools ワンタイムパスワード機能対応です。

Android オペレーティングシステム

- 4.0 ~ 4.0.4 Ice Cream Sandwich
- 4.1 ~ 4.3.1 Jelly Bean
- 4.4 ~ 4.4.4 KitKat
- 5.0 ~ 5.1.1 Lollipop

iOS オペレーティングシステム

- iOS 7.x
- iOS 8.x

Windows Phone オペレーティングシステム

- Windows Phone 8.1
- Windows 10 Mobile

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。
- 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、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」され有効化される必要があるという点です。
- BitLocker Manager は、Server Encryption またはサーバ OS 上の Advanced Threat Prevention ではサポートされません。

BitLocker Manager クライアントの前提条件

- Microsoft Visual C++2010 SP1 **および** Microsoft Visual C++ 2012 更新プログラム 4 がコンピュータにまだインストールされていない場合、ESSE マスターインストーラがこれらのプログラムをインストールします。

前提条件

- Visual C++ 2010 SP1 以降再頒布可能パッケージ（x86 および x64）
- 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）

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: Education、Enterprise 、Pro
- Windows Server 2008 R2: Standard Edition 、Enterprise Edition (64 ビット)
- Windows Server 2012
- Windows Server 2012 R2: Standard Edition、Enterprise Edition（64 ビット）
- Windows Server 2016

ESSE 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、ESSE 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。
- ESS マスターインストーラログファイルは、**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、『Dell Encrypt 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。
  - External Media Shield の各機能の使用方法については、『EMS Help』(EMS 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 Authentication および Advanced Threat Prevention の機能の使用方法については、*Endpoint Security Suite Enterprise* ヘルプを参照してください。ヘルプには、**<Install dir>:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Help** からアクセスしてください。
- ユーザーは、インストールが完了した後、システムトレイで Dell Data Protection 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。
- ESSE 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。ESSE 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。
  - ESSE 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 内部接続ポートを編集... のいずれかをクリックします。
  - ESSE 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

ESSE 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

- ESSE マスターインストーラは次の場所にあります。
  - **お使いの Dell FTP アカウントから** - インストールバンドルを DDP-Endpoint-Security-Suite-1.x.x.xxx.zip の中から見つけます。
- これらの手順に従い、ESSE マスターインストーラを使用して Dell Endpoint Security Suite Enterprise を対話形式でインストールします。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 Dell インストールメディアから 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 **DDPSuite.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 **Enterprise Server 名** フィールドに、ターゲットユーザーを管理する EE Server/VE Server の完全修飾ホスト名 (server.organization.com など) を入力します。

Device Server URL フィールドに、クライアントが通信する Device Server (Security Server) の URL を入力します。

場合、フォーマットは 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 は、基本的なセキュリティフレームワーク、ならびに PBA および指紋やパスワードなどの資格情報といった複数の認証方法を管理する高度な認証クライアントである Security Tools をインストールします。

Advanced Authentication は、高度な認証に必要なファイルとサービスをインストールします。

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 Protection 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、分類して、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。

ウェブプロテクションおよびファイアウォールは、オプション機能であるウェブプロテクションおよびファイアウォールをインストールします。クライアントファイアウォールは、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。ウェブプロテクションは、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: Threat Protection および Advanced Threat Prevention は同じコンピュータに共存できません。インストーラによって、両方のコンポーネントの選択が自動的に禁止されます。Threat Protection をインストールする場合、手順については『Endpoint Security Suite 詳細インストールガイド』をダウンロードしてください。

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。

ESSE 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

- 次の表は、ESSE マスターインストーラで使用できるスイッチについて説明しています。

スイッチ	説明
-y -gm2	ESSE マスターインストーラの事前抽出です。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	DDPSuite.exe 内の .msi に変数を渡します。

パラメータ

- 次の表は、ESSE 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説明しています。ESSE 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	EE Server/VE 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 = サーバ OS 上には Advanced Threat Prevention **のみ**、ワークステーション OS 上には Advanced Threat Prevention **および** Encryption。 DE-ATP = サーバ OS 上に Advanced Threat Prevention および Encryption。サーバー OS 上のインストールに対して**のみ**使用します。これは、FEATURES パラメータが指定されていない場合のサーバー OS 上のデフォルトのインストールです。 DE = Drive Encryption（ Encryption クライアント ）**のみ**。サーバー OS 上のインストールに対して**のみ**使用します。 BLM = BitLocker Manager SED = 自己暗号化ドライブ管理（ EMAgent/Manager、PBA/GPE ドライバ ）(ワークステーション OS 上にインストールされる場合のみ使用可能) ATP-WEBFIREWALL = ワークステーション OS 上のクライアントファイアウォールおよびウェブプロテクション DE-ATP-WEBFIREWALL = サーバ OS 上にクライアントファイアウォールおよびウェブプロテクション **メモ: Enterprise Edition 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、クライアントファイアウォールおよびウェブプロテクションをインストールするために 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 Enterprise Server/VE で管理されるようにする場合は、ATP-WEBFIREWALL および 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 OS 上)この例では、標準ポートで ESSE マスターインストーラを使用して 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、それが指定した EE Server/VE Server を使用するように設定します。

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

- (ワークステーション OS 上)この例では、標準ポートで ESSE マスターインストーラ**のみ**を使用して C:\Program Files\Dell\Dell Data Protection\ のデフォルトの場所に Advanced Threat Prevention と Encryption をサイレントインストールし、それが指定した EE Server/VE Server を使用するように設定します。

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

- (ワークステーション OS 上) この例では、標準ポートで ESSE マスターインストーラを標準ポートで使用して、再起動なしで、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 管理をサイレントインストールし、それが指定した EE Server/VE Server を使用するように設定します。

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

- (ワークステーション OS 上)この例では、標準ポートで ESSE マスターインストーラを使用して C:\Program Files\Dell\Dell Data Protection\ のデフォルトの場所に Advanced Threat Prevention、Encryption、ウェブプロテクション、およびクライアントファイアウォールをサイレントインストールし、それが指定した EE Server/VE Server を使用するように設定します。

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

- （サーバ OS 上）この例では、標準ポートで ESSE マスターインストーラを**のみ**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 および Encryption をサイレントインストールし、それが指定した EE Server/VE Server を使用するように設定します。

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

- （サーバ OS 上）この例では、標準ポートで ESSE マスターインストーラを使用してデフォルトの場所（C:\Program Files\Dell\Dell Data Protection \）に Advanced Threat Prevention、Encryption、ウェブプロテクション、およびクライアントファイアウォールをサイレントインストールします。

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

- （サーバ OS 上）この例では、標準ポートで ESSE マスターインストーラを使用してデフォルトの場所（C:\Program Files\Dell\Dell Data Protection \）に Advanced Threat Prevention **のみ**をサイレントインストールし、それが指定した EE Server/VE Server を使用するように設定します。

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

- （サーバー OS 上）この例では、標準ポートで ESSE マスターインストーラを使用して 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、それが指定した EE Server/VE Server を使用するように設定します。

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

ESSE マスターインストーラを使用したアンインストール

- 各コンポーネントを個別にアンインストールした後で、ESSE 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。
- 子インストーラを取得するには、「ESSE マスターインストーラからの子インストーラの抽出」に記載されている手順に従います。
- インストールと同じバージョンの ESSE マスターインストーラ (つまりクライアント) をアンインストールにも使用するようにしてください。
- 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。本章では、最後の手順である ESSE マスターインストーラのアンインストール**のみ**を説明します。
- 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 および Advanced Authentication 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 Client Security Framework 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
- 「ESSE マスターインストーラのアンインストール」に進みます。

ESSE 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、ESSE 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、ESSE マスターインストーラをサイレントにアンインストールします。

  ```
  "DDPSuite.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

- 各クライアントを個別にアンインストールするには、「ESSE マスターインストーラからの子インストーラの抽出」にあるように、まず始めに ESSE マスターインストーラから子実行可能ファイルを抽出する必要があります。あるいは、管理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
/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

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、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。
- Windows Shield は、Shield アンインストール処理の開始時に EE Server/VE Server をアップデートして、ステータスを 保護されていません に変更します。ただし、クライアントが EE Server/VE Server に接続できない場合は、理由にかかわらず、ステータスはアップデートされません。このような場合は、リモート管理コンソールで、エンドポイントを手動で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、リモート管理コンソールまたは Compliance Reporter で、保護されていません が予測どおりに設定されていることを確認することが推奨されます。

プロセス

- **Encryption Removal Agent のサーバー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 EE Server）を設定する必要があります。手順については、「EE 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。VE Server 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 VE Server 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

- ESSE マスターインストーラから抽出した後、Encryption クライアントインストーラは C:\extracted\Encryption\DDPE_XXbit_setup.exe で見つけることができます。
- 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 サーバ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 EE Server の FQHN。
DA_PORT	EE Server 上の要求用ポート (デフォルトは 8050)。
SVCPN	EE 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、EE Server の Key Server リストに存在している必要があります。
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 サーバ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、EE 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 Administrator 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 リモート管理コンソールで、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 Client Security Framework のコンポーネントをアンインストールします。

- **重要: SED と Advanced Authentication クライアントの両方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 および Advanced Authentication 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 Dell Client Security Framework のコンポーネントのみをアンインストールしますが、SED および Advanced Authentication クライアントはアンストールされません。

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

SED クライアントおよび Advanced Authentication クライアントのアンインストール

- PBA 非アクティブ化には、EE Server/VE Server へのネットワーク接続が必要です。

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。
- Advanced Authentication 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 リモート管理コンソールに Dell 管理者としてログインします。
2 左ペインで、**保護と管理** > **エンドポイント** をクリックします。
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 **詳細** アイコンを選択します。

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** ドロップダウンメニューから、**自己暗号化ドライブ** を選択します。

9 **SED 管理** エリアを展開し、**SED 管理の有効化** ポリシーおよび **PBA のアクティブ化** ポリシーを `True` から `False` に変更します。

10 **保存** をクリックします。

11 左ペインで、**アクション** > **ポリシーのコミット** をクリックします。

12 **変更の適用** をクリックします。

ポリシーが EE Server/VE Server から非アクティブ化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 クライアントおよび Advanced Authentication 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

- ESSE マスターインストーラから抽出した後は、**C:\extracted\Security Tools\EMAgent_XXbit_setup.exe** で SED クライアントインストーラを見つけることができます。
- ESSE マスターインストーラから抽出した後は、**C:\extracted\Security Tools\Authentication\<x64/x86>\setup.exe** で SED クライアントインストーラを見つけることができます。
- 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。

次の操作：

- 次の例は、Advanced Authentication クライアントをサイレントアンインストールします。

```
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

- ESSE マスターインストーラから抽出した後は、**C:\extracted\Security Tools\EMAgent_XXbit_setup.exe** で BitLocker クライアントインストーラを見つけることができます。
- 次の例は、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。

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

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

前提条件

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

テナントのプロビジョニング

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

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

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

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

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

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

7 セットアップが完了しました。**OK** をクリックします。

7

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

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

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

エージェントの自動アップデートの受信

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

1 リモート管理コンソールの左ペインで、**管理** > **サービス管理** とクリックします。
2 エージェントの自動アップデートの下の **高度な脅威** タブで **オン** ボタンをクリックして、**プリファレンスの保存** ボタンをクリックします。
情報が入力され、自動アップデートが表示されるまで数分間かかることがあります。

エージェントの自動アップデート受信の停止

エージェントの自動アップデート受信を停止するには、次の操作を行います。

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

8

ESSE マスターインストーラからの子インストーラの抽出

- ESSE 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、ESSE 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。アンインストールに使用できるように、このプロセスを使用して ESSE マスターインストーラからクライアントを抽出します。

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

2 **DDPSuite.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。

```
DDPSuite.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。

9

EE Server に対してアクティブ化した Encryption クライアントをアンインストールするための Key Server の設定

- 本項では、EE 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。VE Server では Key Server は使用しません。
- 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ーを対象ドメインに含める必要があります。
- VE Server 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。VE Server 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、「コマンドラインのアンインストール」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 EE 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）に進みます。

2 Key Server を右クリックして、**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： フィールドに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（さらなる操作のため、サービスパネルを開いたままにしておきます）。

5 <Key Server 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ていることを確認します。

キーサーバーの設定ファイル - EE Server の通信のためのユーザーの追加

1 <Key Server インストールディレクトリ> 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」のままとすることもできます。

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、EE 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 - キーサーバーサービスの再起動

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ていることを確認します。
4 サービスパネルを閉じます。

リモート管理コンソール - フォレンジック管理者の追加

1 必要な場合は、リモート管理コンソールにログオンします。
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 フィールドで、管理者アクティビティを実行しているユーザーを追加します。この形式は 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。

Administrative Download Utility （CMGAd）の使用

- このユーティリティでは、EE Server/VE Server に接続していないコンピュータ上で使用するために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

VE Server は Key Server を使用しないので、管理者モードを使用して VE Server からキーバンドルを取得することはできません。VE Server 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。

11

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

- **ESSE マスターインストーラログファイル**は C:\ProgramData\Dell\Dell Data Protection\Installer にあります。
- Windows は、C:\Users\<UserName>\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\<UserName>\AppData\Local\Temp. にある %temp% に作成します。For example, C:\Users\<UserName>\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 の完全バージョンをダウンロードするには、https://www.microsoft.com/en-us/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、『*Dell Data Protection | Security Tools Compatibility*』(Dell Security Tools 互換性) 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。

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 Anniversary アップデートへのアップグレード

Windows 10 Anniversary アップデートバージョンへアップグレードするには、次の記事の指示に従います。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 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、または管理者のユーザー名が UPN 形式ではありませんでした。

可能な解決策：アクティブ化 ダイアログでドメイン管理者用の資格情報を入力し、それらが UPN 形式になっていることを確認します。

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

または 内部接続ポートを編集... のいずれかをクリックします。

```
The operation timed out.
```

Server Encryption は、DDP Security 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。
- DDP Server URL をチェックして、それが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 をレガシーサーバーに対してアクティブ化することはできません。DDP 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 DDP 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。
- DDP Server URL をチェックして、それが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。このユーザーは、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よいですが、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、**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ー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 DDP 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、DDP Server が仮想サーバー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 DDP 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。サーバーで認証するため、共通暗号化キーを処理するため、およびポリシーアップデートを受信する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が成功すると、ユーザーがコンピュータを再起動します。それにより、アクティベーションの第 2 部（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たとき、Server Encryption は仮想サーバーユーザーとして自動的にログインし、DDP Enterprise 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。
- Shield 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。
- リモート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ーのバージョンは サーバー用 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、リモート管理コンソールから利用できる AdminHelp を参照してください。

認証とデバイスアクティベーションのプロセス

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 DDP 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、DDP 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 DDP 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、DDP Server は信頼証明書を検証します。

3 DDP Server が信頼証明書をサーバーに割り当てた後、そのサーバー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。

EMS 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 - Storage Class: 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ないこと、およびポートがブロックされないことを確実にするために、Storage Class: 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

- 外部メディアの EMS 暗号化 = True に設定します。
- EMS で CD/DVD 暗号化を除外 = False 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 次のドロップダウンメニューから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 ドロップダウンメニューから該当する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、ドロップダウンボックス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 暗号化キー。 **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。
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、次のように、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 エリアにそのステータスを表示します。サービスのステータスをアップデートするために、サービスを定期的に更新します（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

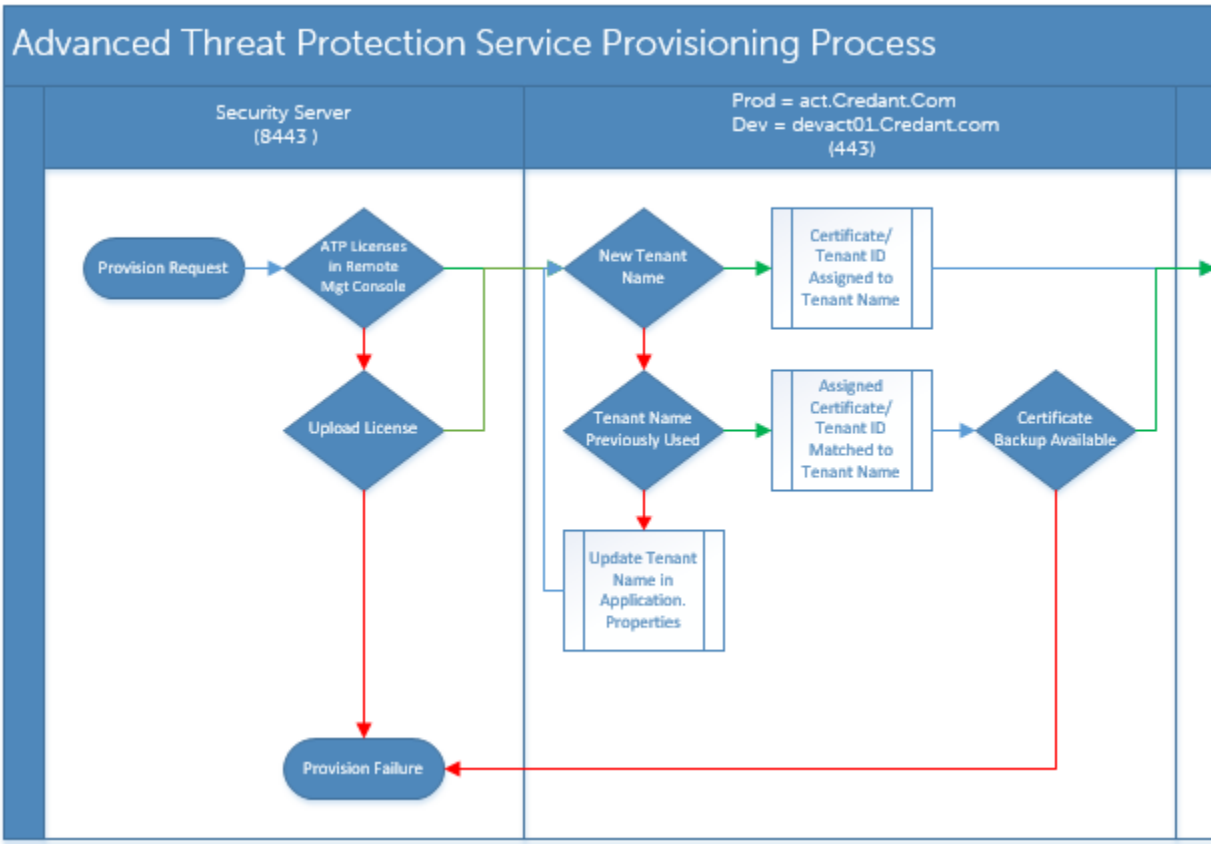
- この方法を使用すれば、将来製品コードに変更があった場合に、製品コードを容易に見つけることができます。

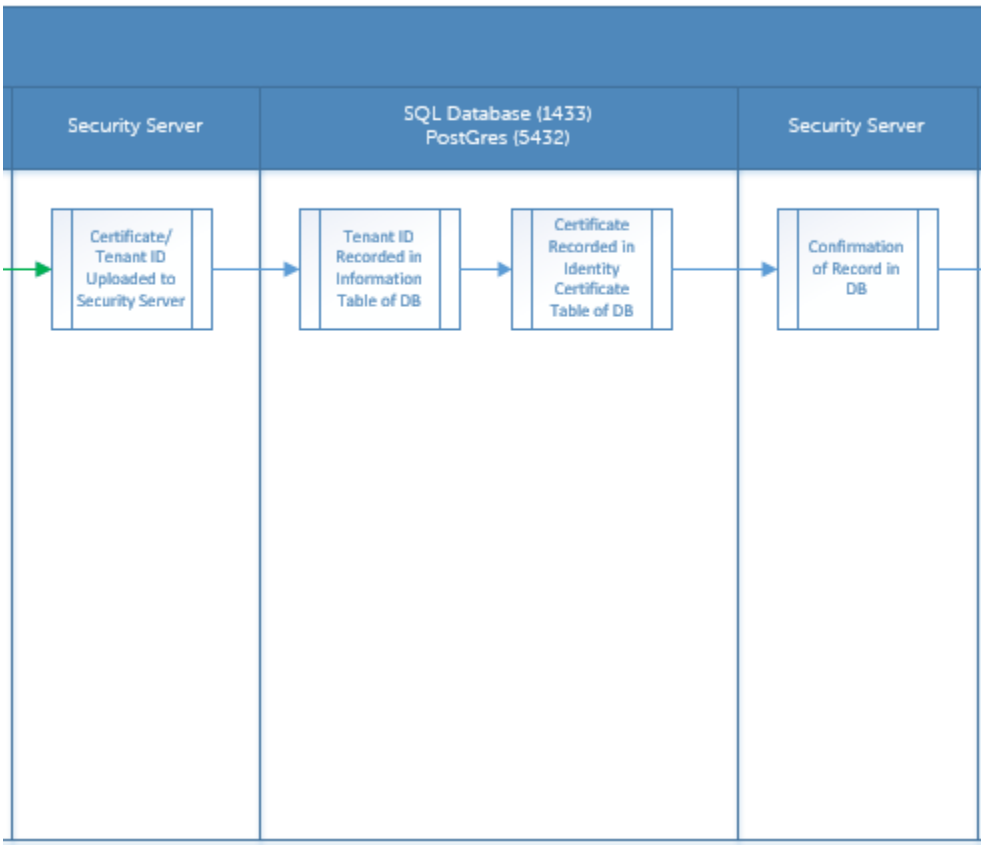
  ```
  Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT
  IdentifyingNumber, Name, LocalPackage
  ```

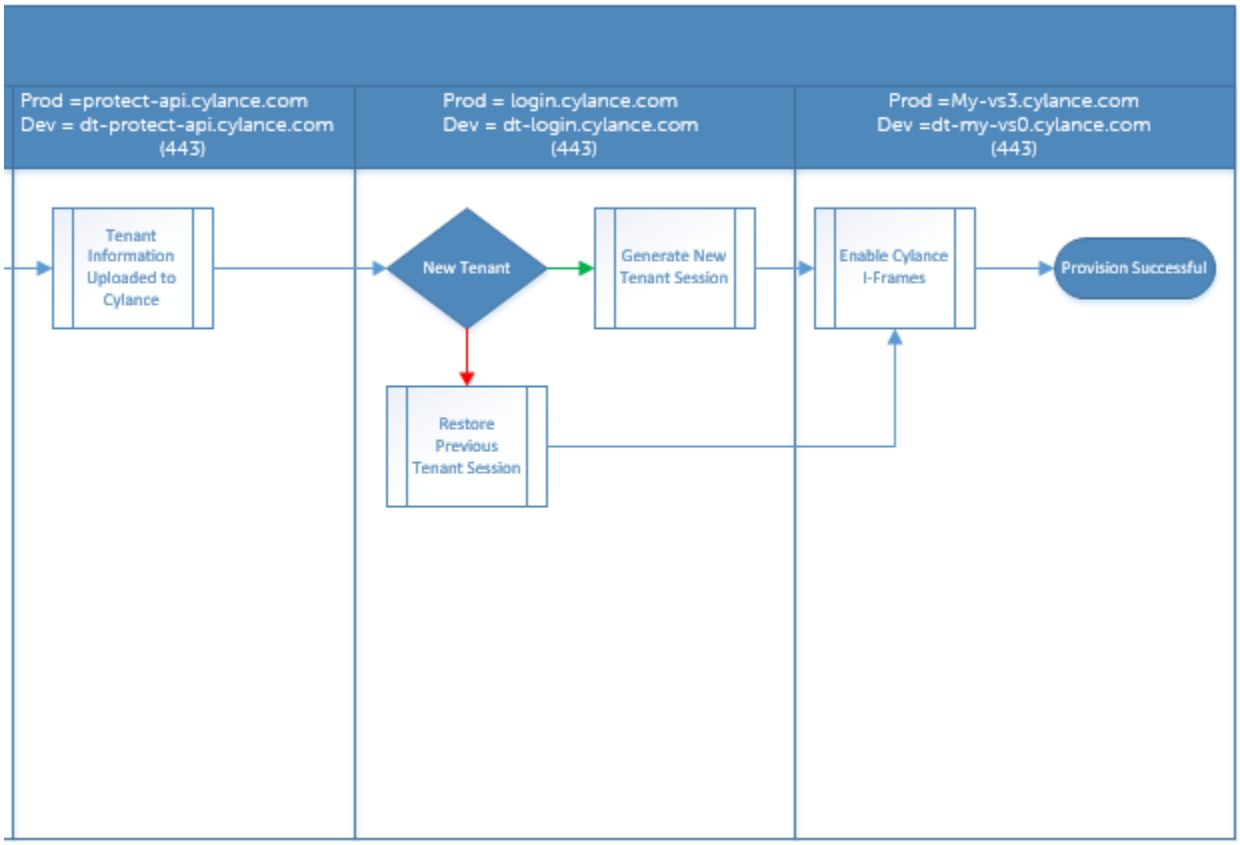
  出力結果は、フルパスと .msi ファイル名（変換された 16 進法のファイル名）となります。

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

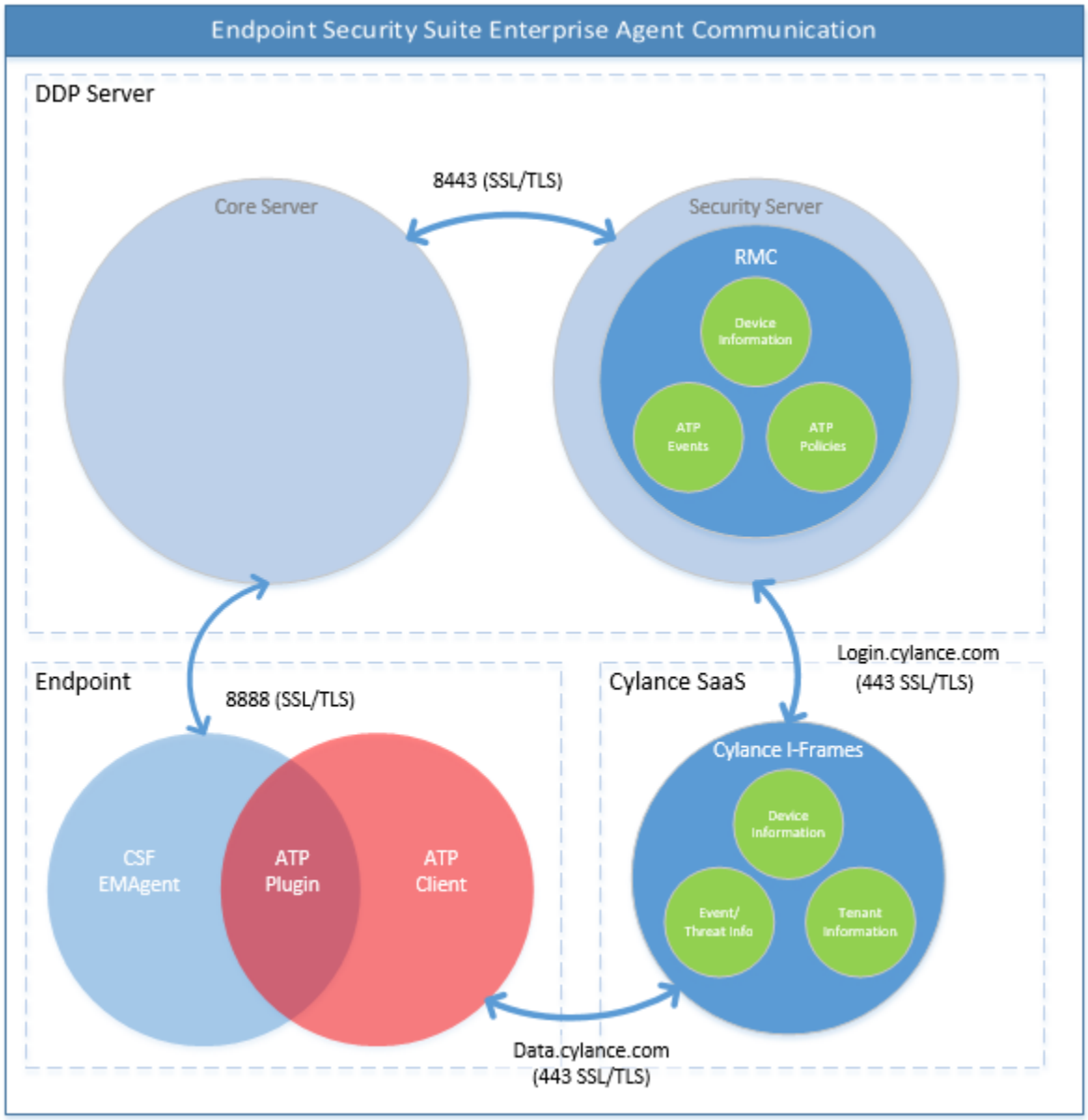
次の図は Advanced Threat Prevention サービスのプロビジョニングプロセスを表しています。


Advanced Threat Protection Service Provisioning Process
Security Server
(8443)
Prod = act.Credant.Com
Dev = devact01.Credant.com
(443)
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

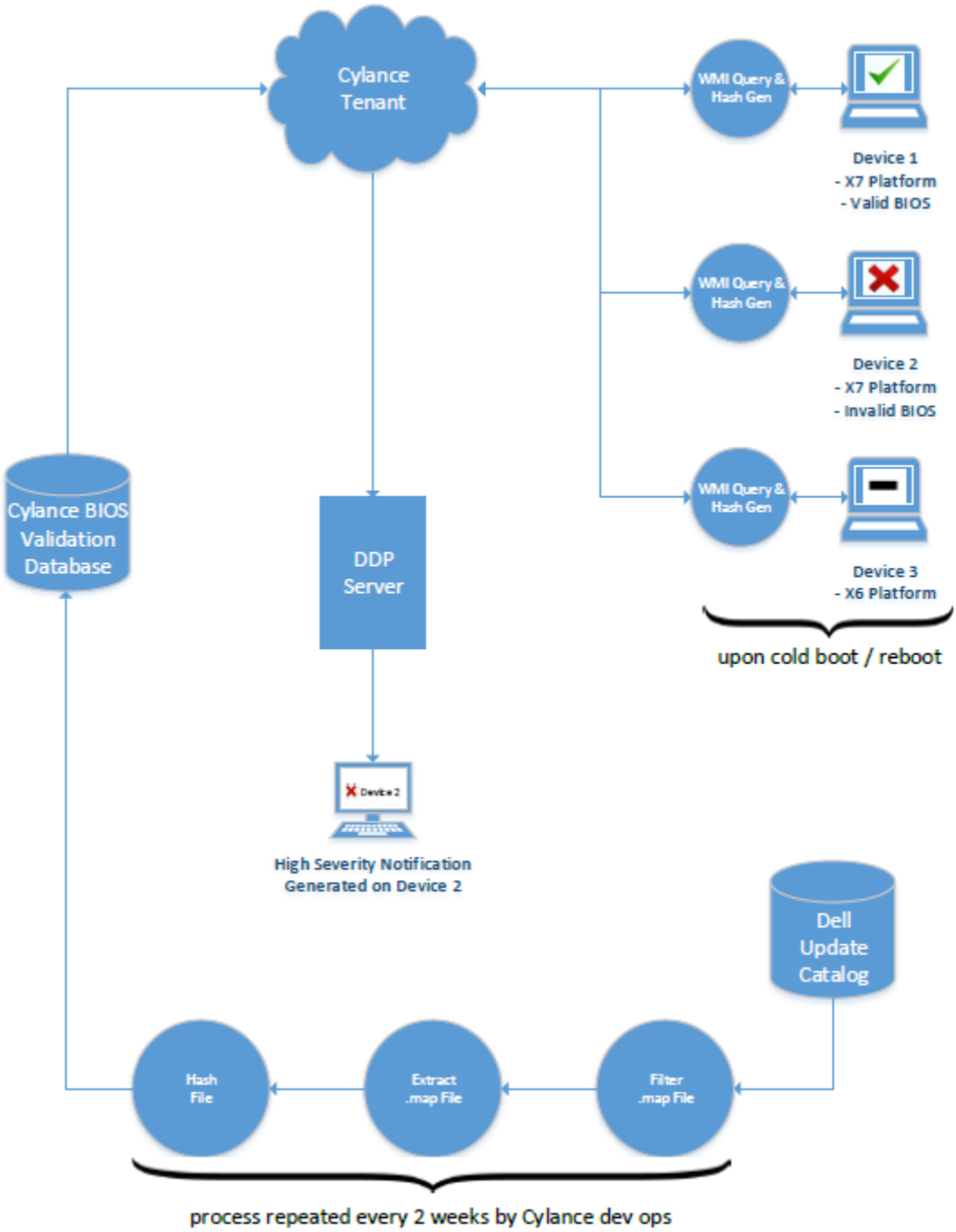


次の図は Advanced Threat Prevention のエージェント通信プロセスを表しています。



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\<New Folder> 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\<New Folder> 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。

:

ファームウェアの旧バージョンからアップグレードする場合は、管理者パスワードを入力するよう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。

用語集

Advanced Authentication – Advanced Authentication 製品は、指紋、スマートカード、非接触型スマートカードリーダーが完全に統合されたオプションを備えています。Advanced Authentication は、これらの複数のハードウェア認証方法の管理を支援し、自己暗号化ドライブ、SSO でのログインをサポートし、ユーザーの資格情報およびパスワードを管理します。さらに、Advanced Authentication は、PC だけでなく、ウェブサイト、SaaS、またはアプリケーションへのアクセスにも使用できます。ユーザーが一度その資格情報を登録すると、Advanced Authentication によって、デバイスにログオンしたりパスワードの変更を行うときにこれらの資格情報が使用できるようになります。

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、リモート管理コンソールで 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。

EMS - External Media Shield - 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。

EMS Access Code - Dell Enterprise Server/VE 内のこのサービスを使用すると、External Media Shield で保護されているデバイスで、ユーザーがパスワードを忘れてしまい、ログインできなくなった場合に、そのデバイスをリカバリできます。この処理が完了したら、ユーザーはリムーバブルメディアまたは外付けストレージデバイス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 Enterprise Server/VE によって管理されるコンピュータまたはモバイルハードウェアデバイス。

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。

ワンタイムパスワード (OTP) - ワンタイムパスワードは、一度しか使用できないパスワードで、有効時間が限定されています。OTP には、TPM が存在し、有効化され、所有されている必要があります。OTP を有効にするには、Security Console および Security Tools Mobile アプリを使用して、モバイル

デバイスをコンピュータとペアリングします。Security Tools Mobile アプリは、Windows ログオン画面でのコンピュータへのログオンに使用されるパスワードをモバイルデバイス上に生成します。コンピュータへのログオンに OTP を使用しなかった場合は、ポリシーに基づき、パスワードの期限が切れたときに、またはパスワードを忘れたときに、OTP 機能を使用してコンピュータへのアクセスを回復することができます。OTP 機能は、認証またはリカバリのいずれかに使用できますが、両方には使用できません。生成されたパスワードが一度しか使用できず、短時間で失効するため、OTP セキュリティは他の認証手法よりも優れています。

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。Dell Enterprise Server/VE リモート管理コンソールでは、このアカウントに固有の UCID 値が割り当てられます。