Dell Encryption Enterprise

Advanced Installation Guide v11.9

January 2023
Rev. A01

DELL Technologies

メモ、注意、警告

メモ: 「メモ」は、製品をより上手に使用するための重要な情報であることを示します。

注意: **「注意」は、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: **「警告」は、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。**

Contents

1

はじめに

本書では、、Encryption、SED 管理、フル ディスク暗号化、Web Protection と Client Firewall、BitLocker Manager のインストールおよび設定の方法について詳しく説明します。

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* インストールおよびマイグレーション ガイド
   - *Security Management Server Virtual* クイック スタートおよびインストール ガイド
   - 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. 本書の「要件」の章をすべて読んでください。
3. 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、コンピュータハードウェアおよびソフトウェア情報、制限事項、および機能で必要になる特殊なレジストリの変更については、「条件」を参照してください。
- 必要に応じて、「SED UEFI および BitLocker のための事前インストール設定」を参照してください。
- Dell Digital Delivery を使用して資格を取る場合は、「資格を有効にするためのドメインコントローラ上での GPO の設定」を参照してください。
- マスターインストーラを使用してクライアントをインストールする場合は、次の項目を参照してください。
  - 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
- 子インストーラを使用してクライアントをインストールする場合、子インストーラの実行可能ファイルをマスターインストーラから抽出する必要があります。「マスターインストーラからの子インストーラの抽出」を参照して、ここに戻ります。
  - コマンドラインで子インストーラをインストールします。
    - Encryption のインストール - コンピュータがネットワークに接続されている、いないにかかわらず、あるいは紛失または盗難に遭ったかどうかにかかわらず、セキュリティポリシーを適用するコンポーネントである Encryption をインストールするには、これらの手順に従います。
    - フルディスク暗号化クライアントのインストール - コンピュータがネットワークに接続されている、いないにかかわらず、あるいは紛失または盗難に遭ったかどうかにかかわらず、セキュリティポリシーを適用するコンポーネントであるフルディスク暗号化をインストールするには、これらの手順に従います。
    - SED Manager のインストール - SED の暗号化ソフトウェアをインストールするには、これらの手順に従います。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 Manager では、すべてのポリシー、ストレージ、SED 管理を使用すると、すべてのポリシー、ストレージ、暗号化キーの取得は、単一のコンソールから使用でき、紛失や不正なアクセスの場合にコンピューターが保護されないというリスクを軽減します。
    - BitLocker Manager のインストール - 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ように設計されている、BitLocker Manager をインストールする場合にこれらの手順に従います。

      メモ:

      ほとんどの子インストーラは対話形式でインストールできますが、このガイドでは説明していません。

- 最も一般的なシナリオのスクリプトについては、「一般的に使用されるシナリオ」を参照してください。

Dell ProSupport for Software へのお問い合わせ

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

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

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 for Software 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

次の要件はすべてのクライアントに適用されます。他のセクションで挙げられる要件は、特定のクライアントに適用されます。

- 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 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。
- 最新のマニュアルや技術アドバイザリーについて、dell.com/support を定期的に確認してください。
- 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。

前提条件

- マスター インストーラーおよび子インストーラー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これらの手順に従います。Microsoft .NET Framework 4.5.2 をインストールするには、これらの手順を参照してください。
- FIPS モードで Encryption をインストールする場合は、Microsoft .NET Framework 4.6 が必要です。

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 ○ 110 MB の使用可能ディスク容量 ○ 512 MB 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。サイズは、有効なポリシーとドライブ容量によって異なります。

ローカライズ

- Dell Encryption、SED Manager、PBA Advanced Authentication、、、BitLocker Manager は、多言語対応のユーザー インターフェイスであり、次の言語にローカライズされています。

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

暗号化

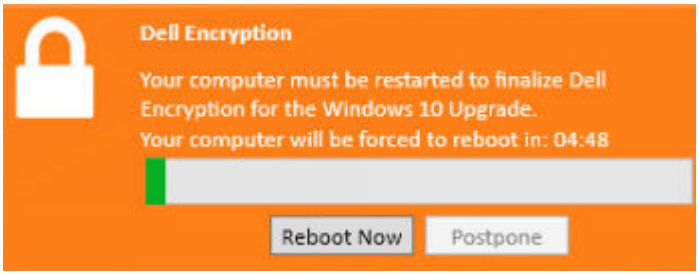
- クライアント コンピューターは、アクティブ化するためにネットワーク接続が必要です。
- Dell Encryption で Microsoft Live アカウントを有効にするには、この KB 記事 124722 を参照してください。
- 最初の暗号化にかかる時間を短縮するために、Windows ディスク クリーンアップ ウィザードを実行して、一時ファイルおよびその他の不必要なデータを削除します。
- Windows Hello for Business に対応するには、Encryption Enterprise v11.0 以降が Windows 10 で実行されている必要があります。
- Windows Hello for Business に対応するには、v11.0 以降を実行する Dell サーバーに対するアクティブ化が必要です。
- 最初の暗号化スイープ中は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ー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ーでは暗号化は行われません（復号化も行われません）。
- Encryption 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。
- Dell Encryption は、v8.16.0 より前のバージョンから v10.7.0 にアップグレードすることはできません。v8.16.0 より前のバージョンを実行しているエンドポイントは、まず v8.16.0 にアップグレードしてから、v10.7.0 にアップグレードする必要があります。
- マスター インストーラーでは、v8.0 より前のコンポーネントからのアップグレードはサポートされていません。マスター インストーラーから子インストーラーを抽出し、コンポーネントを個々にアップグレードします。抽出手順については、マスター インストーラーからの子インストーラーの抽出を参照してください。
- Encryption は監査モードをサポートするようになりました。監査モードは管理者がサードパーティの SCCM または類似のソリューションを使用するのではなく、企業用イメージの一部として、Encryption を展開することを可能にします。企業用イメージに Encryption をインストールする手順については、KB 記事 129990 を参照してください。
- Encryption クライアントは、一般に使用されているいくつかのシグネチャーベースのウイルス対策ソリューションや AI 駆動型のウイルス対策ソリューション（McAfee Virus Scan Enterprise、McAfee Endpoint Security、Symantec Endpoint Protection、CylancePROTECT、CrowdStrike Falcon、Carbon Black Defense など）に対してテスト済みであり、互換性があります。アンチウイルス スキャンと暗号化の非互換性を回避するため、多くのウイルス対策プロバイダーを除外するハードコード機能をデフォルトで内蔵しています。

  組織がリストに記載のないウイルス対策プロバイダーを使用している場合、または何らかの互換性の問題に遭遇している場合は、KB 記事 126046 を参照するか、Dell ProSupport に問い合わせてお使いのソフトウェア ソリューションと Dell Data Security ソリューションの相互運用性の設定を確認してください。

- Dell Encryption は、インテルの暗号化命令セットであるインテグレーテッド・パフォーマンス・プリミティブ（IPP）を使用しています。詳細については、KB 記事 126015 を参照してください。
- TPM は汎用キーのシーリングに使用されます。したがって、Encryption を実行している場合は、ターゲット コンピューターに新しいオペレーティング システムをインストールする前に、BIOS で TPM をクリアする必要があります。
- インプレー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 コンピューターをバックアップしてからそのコンピューターをワイプし、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。
- これらのコンポーネントがターゲット コンピューターにインストールされていない場合は、マスター インストーラーがインストールを行います。**子インストーラーを使用する場合**、クライアントをインストールする前に、これらのコンポーネントをインストールする必要があります。

動作条件
○ Visual C++ 2012 更新プログラム 4 以降再頒布可能パッケージ（x86 または x64） ○ Visual C++ 2017 以降の再頒布可能パッケージ（x86 または x64） ○ 2020 年 1 月をもって、SHA1 署名証明書の有効性は失われ、更新することはできません。Windows Server 2008 R2 を実行しているデバイスには、アプリケーションおよびインストール パッケージの SHA256 署名証明書を検証するために、Microsoft KB で提供されている更新プログラム（https://support.microsoft.com/help/4474419 および https://support.microsoft.com/help/4490628）をインストールする必要があります。 SHA1 証明書で署名されたアプリケーションおよびインストール パッケージは機能しますが、SHA1 証明書の更新プログラムがインストールされていないアプリケーションをインストールまたは実行すると、エンドポイントにエラーが表示されます。

- UEFI モードでは、保護された *Windows* 休止状態ファイルと保護されていない休止状態の防止ポリシーはサポートされていません。
- 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 サーバーで認証情報が検証されます。詳細については、KB 記事 124736 を参照してください。
- Windows 10 の機能アップグレードの後、Dell Encryption を完了させるには再起動が**必要**です。Windows 10 の機能アップグレードの後、通知領域に次のメッセージが表示されます。



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

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 10：Education、Enterprise、Pro v1909～v22H2 (November 2019 Update/19H2～November 2022 Update/22H2) **メモ：**OEM および ODM では、32 ビット アーキテクチャの Windows 10 v2004（May 2020 Update/20H1 以降）は出荷していません。詳細については、https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview を参照してください。 ■ Windows 10 2019 LTSC ■ Windows 10 2021 LTSC ○ Windows 11：Enterprise、Pro v21H2～22H2 ○ **Deferred Activation** には、上記のすべてのサポートが含まれます。

Encryption External Media

オペレーティング システム

- 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。
- 次の表では、 Encryption External Media によって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オペレーティング システムを詳細に示します。

暗号化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 10：Education、Enterprise、Pro v1909～v22H2 (November 2019 Update/19H2～November 2022 Update/22H2) **メモ：**OEM および ODM では、32 ビット アーキテクチャの Windows 10 v2004（May 2020 Update/20H1 以降）は出荷していません。詳細については、https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview を参照してください。 ■ Windows 10 2019 LTSC ■ Windows 10 2021 LTSC ○ Windows 11：Enterprise、Pro v21H2～22H2

暗号化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）
○ **Deferred Activation** には、上記のすべてのサポートが含まれます。

暗号化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 High Sierra 10.13.5 - 10.13.6 ○ macOS Mojave 10.14.0～10.14.4 ○ macOS Catalina 10.15.5～10.15.6

フルディスク暗号化

- フルディスク暗号化では、v9.8.2 以降を実行する Dell サーバー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 コンピューターでは現在サポートされていません。
- フル ディスク暗号化には、個別のハードウェア TPM が必要です。現時点では、PTT およびファームウェアベースの TPM 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 パーティー認証情報プロバイダーは機能しません。PBA を有効にすると、サード パーティー認証情報プロバイダーはすべて無効になります。
- クライアント コンピューターには、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 サーバー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 コンピューター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ーには、フルディスク暗号化をインストールしないでください。
- Dell は、NVMe ドライブには、最新のインテル® ラピッド・ストレージ・テクノロジー・ドライバーを推奨しています。
- PBA に利用されている NVMe ドライブ:
  - 2018 以降に製造された Dell 製デバイスの場合は、RAID ON または AHCI のいずれかを NVMe ドライブで使用できる場合があります。
  - BIOS 起動モードは、統合拡張可能ファームウェア インターフェイス（UEFI）に設定する必要があります。レガシー オペレーション 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：
  - BIOS SATA 操作は、AHCI または RAID ON のいずれかに設定できます。
  - AHCI コントローラー ドライバーがあらかじめインストールされていない場合に 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。RAID から AHCI（またはその逆）に切り替える方法については、KB 記事 124714 を参照してください。
- フルディスク暗号化管理は、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。
- インプレー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 コンピューターをバックアップしてからそのコンピューターをワイプし、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。
- Windows 10 v1607（Anniversary Update/Redstone 1）から Windows 10 v1903（May 2019 Update/19H1）への直接機能アップデートは FDE ではサポートされていません。Windows 10 v1903 にアップデートする場合は、オペレーティング システムを新しい機能アップデートにアップデートすることをお勧めします。Windows 10 v1607 から v1903 に直接アップデートしようとすると、エラー メッセージが表示され、アップデートできなくなります。
- フル ディスク暗号化を有効にする前に、すべてのディスクを初期化してフォーマットする必要があります。
- フルディスク暗号化でマルチディスク暗号化を設定するには、次の条件を満たしている必要があります。
  - ターゲット システム内のすべてのディスクは、次の構成である必要があります。
    - 非 SED ドライブ
    - 同じ起動モードで構成されている
    - GUID パーティション テーブル(GPT)として初期化されている
    - ディスクはプライマリー パーティションにする必要がある
    - ディスクにはドライブ レターが割り当てられている必要がある
  - 初期設定後に新しいディスクを暗号化するには、再起動が必要です。
  - 最大 16 台のディスクを暗号化することができます。
  - UEFI ブート モードでは、オペレーティング システムはどのターゲット ディスクにもインストールできます。

- レガシー ブート モードでは、オペレーティング システムは最初のディスク（ディスク#0）にインストールされる必要があります。オペレーティング システムが最初のディスクにインストールされていない場合、マルチディスク暗号化は無効になります。

  管理コンソールでマルチディスク暗号化を有効にします。マルチディスク暗号化およびマルチスイープの Windows レジストリー値については、「レジストリー設定」を参照してください。

- フル ディスク暗号化では、Windows パスワードの変更とデータ暗号化キーを同期するために、Dell のカスタム認証情報プロバイダーを使用する必要があります。フル ディスク暗号化により保護されたコンピューターで実行されているカスタム認証情報プロバイダーを使用するサード パーティー アプリケーションを使用する必要がある場合は、Data Security Console を通じて Windows パスワードの変更を開始する必要があります。Data Security Console でのパスワード変更については、『Data Security Console ユーザー ガイド』『』の「パスワード」の章を参照してください。

- これらのコンポーネントがターゲット コンピューターにインストールされていない場合は、マスター インストーラーがインストールを行います。**子インストーラーを使用する場合**、クライアントをインストールする前に、これらのコンポーネントをインストールする必要があります。

動作条件
○ Visual C++ 2017 以降の再頒布可能パッケージ（x86 または x64）
○ 2020 年 1 月をもって、SHA1 署名証明書の有効性は失われ、更新することはできません。Windows Server 2008 R2 を実行しているデバイスには、アプリケーションおよびインストール パッケージの SHA256 署名証明書を検証するために、Microsoft KB で提供されている更新プログラム（https://support.microsoft.com/help/4474419 および https://support.microsoft.com/help/4490628）をインストールする必要があります。 SHA1 証明書で署名されたアプリケーションおよびインストール パッケージは機能しますが、SHA1 証明書の更新プログラムがインストールされていないアプリケーションをインストールまたは実行すると、エンドポイントにエラーが表示されます。

- **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:** PBA を使用する場合、コンピューターに複数のユーザーがいる場合は、すべてのユーザーの同期ポリシーを有効にする必要があります。また、すべてのユーザーがパスワードを持っている必要があります。長さがゼロのパスワード ユーザーは、アクティブ化後にコンピューターからロックアウトされます。

- **メモ:** Full Disk Encryption で保護されているコンピューターは、Windows 10 v1703（Creators Update/Redstone 2）以降にアップデートしてから Windows 10 v1903（May 2019 Update/19H1）以降にアップデートする必要があります。このアップグレード パスを試行すると、エラー メッセージが表示されます。

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。

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認証オプション

- スマート カードを使用したり、UEFI コンピューターで認証を行ったりするためには、特殊なハードウェアが必要となります。起動前認証でスマート カードを使用するには、設定が必要です。以下の表では、ハードウェアと構成の要件が満たされているときに使用できる認証オプションをオペレーティング システム別に示しています。

UEFI				
	PBA - サポートされる Dell コンピューター上			
	パスワード	**指紋**	**接触型スマート カード**	**SIPR カード**
Windows 10	X[1]		X[1]	

UEFI				
	PBA - サポートされる Dell コンピューター上			
	パスワード	指紋	接触型スマート カード	SIPR カード
Windows 11	X[1]		X[1]	
1. サポート対象の UEFI コンピューターで利用できます。				

UEFI ブート モードがサポートされているで Dell コンピューター モデル

- フル ディスク暗号化でサポートされているプラットフォームの最新リストについては、KB 記事 126855 を参照してください。
- フル ディスク暗号化でサポートされているドッキング ステーションとアダプターのリストについては、KB 記事 124241 を参照してください。

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 10：Education、Enterprise、Pro v1909～v22H2 (November 2019 Update/19H2～November 2022 Update/22H2) **メモ：**OEM および ODM では、32 ビット アーキテクチャの Windows 10 v2004（May 2020 Update/20H1 以降）は出荷していません。詳細については、https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview を参照してください。 ■ Windows 10 2019 LTSC ■ Windows 10 2021 LTSC ○ Windows 11：Enterprise、Pro v21H2～22H2

サーバー オペレーティング システムの Encryption

サーバー オペレーティング システムの Encryption は、サーバー モードで動作しているコンピューター、特にファイル サーバー上での使用を対象にしています。

- サーバー オペレーティング システム上の Encryption は、Encryption Enterprise および Endpoint Security Suite Enterprise とのみ互換性があります。
- サーバー オペレーティング システム上の Encryption には、次の機能があります。
  - ソフトウェアの暗号化
  - リムーバブル メディア暗号化
  - ポート制御

    メモ:

    サーバーはポート制御をサポートしている必要があります。

    ポート制御システムのポリシーは、たとえば、USB デバイスによるサーバーの USB ポートへのアクセスおよび使用を制御することにより、保護対象サーバ上のリムーバブル メディアに影響します。USB ポート ポリシーは外部 USB ポートに適用されます。内部 USB ポート機能は、USB ポート ポリシーの影響を受けません。USB ポート ポリシーが無効化されると、クライアント USB キーボードおよびマウスは機能しなくなり、このポリシーが適用される前にリモート デスクトップ接続がセットアップされない限り、ユーザーはコンピューターを使用することができなくなります。
- これらのコンポーネントがターゲット コンピューターにインストールされていない場合は、マスター インストーラーがインストールを行います。**子インストーラーを使用する場合**、クライアントをインストールする前に、これらのコンポーネントをインストールする必要があります。

動作条件
○ Visual C++ 2012 更新プログラム 4 以降再頒布可能パッケージ（x86 または x64） ○ Visual C++ 2017 以降の再頒布可能パッケージ（x86 または x64） ○ 2020 年 1 月をもって、SHA1 署名証明書の有効性は失われ、更新することはできません。Windows Server 2008 R2 を実行しているデバイスには、アプリケーションおよびインストール パッケージの SHA256 署名証明書を検証するために、Microsoft KB で提供されている更新プログラム（https://support.microsoft.com/help/4474419 および https://support.microsoft.com/help/4490628）をインストールする必要があります。 SHA1 証明書で署名されたアプリケーションおよびインストール パッケージは機能しますが、SHA1 証明書の更新プログラムがインストールされていないアプリケーションをインストールまたは実行すると、エンドポイントにエラーが表示されます。

サーバー オペレーティング システムの Encryption は、次の機能で使用されます。

- ローカル ドライブを持つファイル サーバー
- サーバー オペレーティング システム、またはシンプル ファイル サーバーとして非サーバー オペレーティング システムを実行している仮想マシン (VM)ゲスト
- サポートされている構成:
  - RAID 5 または 10 ドライブ搭載のサーバー。RAID 0（ストライピング）と RAID 1（ミラーリング）は互いに独立してサポートされています。
  - Multi TB RAID ドライブ搭載のサーバー
  - コンピューターをシャットダウンせずに交換可能なドライブ搭載のサーバー
  - Server Encryption は、業界をリードするウイルス対策プロバイダーを使用して検証されます。アンチウイルス スキャンと暗号化の間における非互換性を防ぐため、これらのウイルス対策プロバイダーに対するハードコーディングされた除外が設定されています。組織がリストに記載のないウイルス対策プロバイダーを利用している場合は、KB 記事 126046 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。

サーバー オペレーティング システムの Encryption は、次の機能では使用されません。

- Security Management Server/Security Management Server Virtual または Security Management Server/Security Management Server Virtual のデータベースを実行しているサーバー。
- Encryption Personal。
- SED Manager、PBA Advanced Authentication、または BitLocker Manager。
- 分散ファイル システム（DFS）の一部であるサーバー。
- サーバー オペレーティング システムの Encryption 間の移行。External Media Edition からサーバー オペレーティング システムの Encryption にアップグレードするには、サーバー オペレーティング システム上の Encryption をインストールする前に、以前の製品を完全にアンインストールする必要があります。
- VM ホスト（通常、VM ホストには複数の VM ゲストが含まれています。）
- ドメイン コントローラ
- Exchange サーバー
- データベース（SQL、Sybase、SharePoint、Oracle、MySQL、Exchange など）をホストしているサーバー
- 次のいずれかのテクノロジを使用しているサーバー
  - Resilient File System
  - Fluid File System
  - Microsoft 記憶域
  - SAN/NAS ネットワーク ストレージ ソリューション
  - iSCSI 接続デバイス
  - 重複排除ソフトウェア
  - ハードウェア重複排除
  - 分割された RAID（単一の RAID に複数のボリュームが存在）
  - SED（RAID および非 RAID）
  - Microsoft Storage Server 2012
- サーバー オペレーティング システム上の Encryption 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。
- インプレー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 コンピューターをバックアップしてからそのコンピューターをワイプし、オペレーティング システムをインストールした後、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。暗号化されたデータのリカバリーの詳細については、『リカバリー ガイド』を参照してください。

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。

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 v1909～v22H2 (November 2019 Update/19H2～November 2022 Update/22H2) **メモ：**OEM および ODM では、32 ビット アーキテクチャの Windows 10 v2004（May 2020 Update/20H1 以降）は出荷していません。詳細については、https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview を参照してください。 ○ Windows 10 2019 LTSC ○ Windows 10 2021 LTSC • Windows 11：Enterprise、Pro v21H2～22H2 • **Deferred Activation** には、上記のすべてのサポートが含まれます。

サポートされているサーバー オペレーティング システム
• Windows Server 2008 R2 SP1: Standard Edition、Datacenter Edition、Enterprise Edition、Webserver Edition • Windows Server 2012: Standard Edition、Essentials Edition、Datacenter Edition（Server Core はサポートされません） • Windows Server 2012 R2: Standard Edition、Essentials Edition、Datacenter Edition（Server Core はサポートされません） • Windows Server 2016: Standard Edition、Essentials Edition、Datacenter Edition（Server Core はサポートされません） • Windows Server 2019: Standard Edition、Datacenter Edition • Windows Server 2022: Standard Edition、Datacenter Edition

UEFI モードがサポートされるオペレーティング システム
• Windows 10：Education、Enterprise、Pro v1909～v22H2 (November 2019 Update/19H2～November 2022 Update/22H2) **メモ：**OEM および ODM では、32 ビット アーキテクチャの Windows 10 v2004（May 2020 Update/20H1 以降）は出荷していません。詳細については、https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview を参照してください。 ○ Windows 10 2019 LTSC ○ Windows 10 2021 LTSC • Windows 11：Enterprise、Pro v21H2～22H2

メモ:

サポートされる UEFI コンピューターでは、メイン メニューから［**再起動**］を選択した後にコンピューターが再起動し、2 つのログオン画面のいずれかが表示されます。表示されるログオン画面は、コンピューター プラットフォーム アーキテクチャにおける違いによって決定します。

Encryption External Media

オペレーティング システム

- 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。
- Dell で保護されたメディアにアクセスする際にサポートされるオペレーティング システムの詳細は、次のとおりです。

暗号化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 10：Education、Enterprise、Pro v1909～v22H2 (November 2019 Update/19H2～November 2022 Update/22H2)

暗号化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）

メモ：OEM および ODM では、32 ビット アーキテクチャの Windows 10 v2004（May 2020 Update/20H1 以降）は出荷していません。詳細については、https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview を参照してください。

- Windows 10 2019 LTSC
- Windows 10 2021 LTSC

- Windows 11：Enterprise、Pro v21H2～22H2
- **Deferred Activation** には、上記のすべてのサポートが含まれます。

サポートされているサーバー オペレーティング システム

- Windows Server 2012 R2

暗号化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 High Sierra 10.13.5 - 10.13.6
- macOS Mojave 10.14.0～10.14.4
- macOS Catalina 10.15.1～10.15.4

SED Manager

- SED Manager を正しくインストールするには、コンピューター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。
- インストールされている SED Manager では、サード パーティー認証情報プロバイダーは機能しません。PBA を有効にすると、サード パーティー認証情報プロバイダー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、仮想化ホスト コンピューターでは現在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、コンピューターをシャットダウンして再起動する準備を整えます。
- 自動暗号化ドライブが搭載されているコンピューターでは 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。Dell では、HCA モジュールをサポートする自動暗号化ドライブを用いたコンピューター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ーに自動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。
- Dell では、PBA がアクティブ化された後には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。
- SED Manager 用の自動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。
  - PBA に利用されている NVMe ドライブ:
    - 2018 以降に製造された Dell 製デバイスの場合は、RAID ON または AHCI のいずれかを NVMe ドライブで使用できる場合があります。
    - BIOS 起動モードは、統合拡張可能ファームウェア インターフェイス（UEFI）に設定する必要があります。レガシー オペレーション 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：
    - BIOS SATA 操作は、AHCI または RAID ON のいずれかに設定できます。
    - AHCI コントローラー ドライバー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、KB 記事 124714 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、www.dell.com/support にあるアップデートされたインテル® ラピッド・ストレージ・テクノロジー・ドライバーが必要です。Dell は、最新のインテル® ラピッド・ストレージ・テクノロジー・ドライバーを推奨しています。

メモ: インテル® ラピッド・ストレージ・テクノロジー・ドライバーは、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ーのモデルに基づいたシステムのドライバーは、上記のリンクから参照できます。

- SED Manager では、Windows パスワードの変更とデータ暗号化キーを同期させるために、Dell のカスタム認証情報プロバイダーを使用する必要があります。SED Manager により保護されたコンピューターで実行されているカスタム認証情報プロバイダーを使用するサード パーティー アプリケーションを使用する必要がある場合は、Data Security Console を通じて Windows パスワードの変更を開始する必要があります。Data Security Console でのパスワード変更については、『Data Security Console ユーザー ガイド』『』の「パスワード」の章を参照してください。
- これらのコンポーネントがターゲット コンピューターにインストールされていない場合は、マスター インストーラーがインストールを行います。**子インストーラーを使用する場合**、クライアントをインストールする前に、これらのコンポーネントをインストールする必要があります。

動作条件
○ Visual C++ 2017 以降の再頒布可能パッケージ（x86 または x64）
○ 2020 年 1 月をもって、SHA1 署名証明書の有効性は失われ、更新することはできません。Windows Server 2008 R2 を実行しているデバイスには、アプリケーションおよびインストール パッケージの SHA256 署名証明書を検証するために、Microsoft KB で提供されている更新プログラム（https://support.microsoft.com/help/4474419 および https://support.microsoft.com/help/4490628）をインストールする必要があります。 SHA1 証明書で署名されたアプリケーションおよびインストール パッケージは機能しますが、SHA1 証明書の更新プログラムがインストールされていないアプリケーションをインストールまたは実行すると、エンドポイントにエラーが表示されます。

- SED Manager は、サーバー オペレーティング システム上の Encryption ではサポートされません。
- SED Manager でマルチディスク暗号化を設定するには、次の条件を満たしている必要があります。
  - ターゲット システム内のすべてのディスクは、次の構成である必要があります。
    - SED ドライブ
    - ディスクにはドライブ レターが割り当てられている必要がある
  - UEFI ブート モードでは、オペレーティング システムはどのターゲット ディスクにもインストールできます。
  - レガシー ブート モードでは、オペレーティング システムは最初のディスク（ディスク#0）にインストールされる必要があります。オペレーティング システムが最初のディスクにインストールされていない場合、マルチディスク暗号化は無効になります。

    管理コンソールでマルチディスク暗号化を有効にします。マルチディスク暗号化およびマルチスイープの Windows レジストリー値については、「レジストリー設定」を参照してください。
- **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:** PBA を使用する場合、コンピューターに複数のユーザーがいる場合は、すべてのユーザーの同期ポリシーを有効にする必要があります。また、すべてのユーザーがパスワードを持っている必要があります。長さがゼロのパスワード ユーザーは、アクティブ化後にコンピューターからロックアウトされます。
- **メモ:** SED Manager で保護されているコンピューターは、Windows 10 v1703（Creators Update/Redstone 2）以降にアップデートしてから Windows 10 v1903（May 2019 Update/19H1）以降にアップデートする必要があります。このアップグレード パスを試行すると、エラー メッセージが表示されます。
-

ハードウェア

OPAL 対応の SED

- SED Manager でサポートされている Opal 準拠 SED の最新リストについては、この KB 記事 126855 を参照してください。
- SED Manager でサポートされているプラットフォームの最新リストについては、KB 記事 126855 を参照してください。
- SED Manager でサポートされているドッキング ステーションとアダプターのリストについては、KB 記事 124241 を参照してください。

SED Manager による起動前認証オプション

- スマート カードを使用したり、UEFI コンピューターで認証を行ったりするには、特殊なハードウェアが必要です。起動前認証でスマート カードを使用するには、設定が必要です。以下の表では、ハードウェアと構成の要件が満たされているときに使用できる認証オプションをオペレーティング システム別に示しています。

非 UEFI				
	PBA			
	パスワード	指紋	接触型スマート カード	SIPR カード
Windows 10	X[1]		X[1 2]	
Windows 11	X[1]		X[1 2]	
1. 認証ドライバーを dell.com/support からダウンロードすれば使用可能 2. サポート対象 OPAL SED で使用可能				

UEFI				
	PBA - サポートされる Dell コンピューター上			
	パスワード	指紋	接触型スマート カード	SIPR カード
Windows 10	X[1]		X[1]	
Windows 11	X[1]		X[1]	
1. サポート対象 UEFI コンピューター上のサポート対象 OPAL SED で使用可能				

国際キーボード

次の表に、UEFI 対応および UEFI 非対応のコンピューター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）	EN-GB - 英語（イギリス英語）
DE-CH - （スイスドイツ語）	EN-CA - 英語（カナダ英語）
EN-US - 英語（アメリカ英語）	

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

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 10：Education、Enterprise、Pro v1909～v22H2 (November 2019 Update/19H2～November 2022 Update/22H2) **メモ：**OEM および ODM では、32 ビット アーキテクチャの Windows 10 v2004（May 2020 Update/20H1 以降）は出荷していません。詳細については、https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview を参照してください。

Windows オペレーティング システム（32 ビットと 64 ビット）
▪ Windows 10 2019 LTSC ▪ Windows 10 2021 LTSC ○ Windows 11：Enterprise、Pro v21H2～22H2

ローカライズ

SED Manager は複数の言語のユーザー インターフェイスに準拠しており、次の言語にローカライズされています。UEFI モードと PBA Advanced Authentication は、次の言語でサポートされています。

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

BitLocker Manager

- 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 PBA パーティションを設定する事前インストール設定」を参照してください。
- 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、KB 記事 124931 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、コンピューター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ー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。
- FIPS モードが GPO セキュリティ設定「システム暗号化：暗号化、ハッシュ、署名に FIPS 対応のアルゴリズムを使用」で有効になった場合、BitLocker Manager は、認定した AES FIPS が検証したアルゴリズムを使用するので、製品を介してそのデバイスを管理します。現在 Microsoft では、アプリケーション互換性、回復、およびメディア暗号化における多数の問題のために FIPS 検証済みアルゴリズムを使用しないことをお客様に勧めていることから、BitLocker Manager でもこのモードを BitLocker 暗号化クライアントのデフォルトとして設定することを必須とはしていません: http://blogs.technet.com。
- BitLocker Manager は、サーバー オペレーティング システムの Encryption ではサポートされません。
- BitLocker Manager を使用するエンドポイントとのリモート デスクトップ接続を使用する場合、次のコマンドを使用して、既存のユーザーセッションで UI の対話の問題を回避するために、コンソール モードでリモート デスクトップ セッションを実行することをお勧めします。

  ```
  mstsc /admin /v:<target_ip_address>
  ```

- これらのコンポーネントがターゲット コンピューターにインストールされていない場合は、マスター インストーラーがインストールを行います。**子インストーラーを使用する場合**、クライアントをインストールする前に、これらのコンポーネントをインストールする必要があります。

動作条件
○ Visual C++ 2017 以降の再頒布可能パッケージ（x86 または x64） ○ 2020 年 1 月をもって、SHA1 署名証明書の有効性は失われ、更新することはできません。Windows Server 2008 R2 を実行しているデバイスには、アプリケーションおよびインストール パッケージの SHA256 署名証明書を検証するために、Microsoft KB で提供されている更新プログラム（https://support.microsoft.com/help/4474419 および https://support.microsoft.com/help/4490628）をインストールする必要があります。

動作条件
SHA1 証明書で署名されたアプリケーションおよびインストール パッケージは機能しますが、SHA1 証明書の更新プログラムがインストールされていないアプリケーションをインストールまたは実行すると、エンドポイントにエラーが表示されます。

- **メモ:** Bitlocker Manager で保護されているコンピューターは、Windows 10 v1703（Creators Update/Redstone 2）以降にアップデートしてから、Windows 10 v1903（May 2019 Update/19H1）以降にアップデートする必要があります。このアップグレード パスを試行すると、エラー メッセージが表示されます。
- **メモ:** オペレーティング システムの新しいバージョンへのインプレース アップグレード（Windows 10 から Windows 11 など）はサポートされません。

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

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 10：Education、Enterprise、Pro v1909～v22H2 (November 2019 Update/19H2～November 2022 Update/22H2) **メモ：**OEM および ODM では、32 ビット アーキテクチャの Windows 10 v2004（May 2020 Update/20H1 以降）は出荷していません。詳細については、https://docs.microsoft.com/windows-hardware/design/minimum/minimum-hardware-requirements-overview を参照してください。 ■ Windows 10 2019 LTSC ■ Windows 10 2021 LTSC ○ Windows 11：Enterprise、Pro v21H2～22H2

Windows Server オペレーティング システム
○ 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: Standard Edition、Datacenter Edition（64 ビット） ○ Windows Server 2019: Standard Edition、Datacenter Edition（64 ビット） ○ Windows Server 2022: Standard Edition、Datacenter Edition

3

レジストリ設定

- この項では、レジストリ設定の理由に関係なく、ローカル **クライアント** コンピュータでの Dell ProSupport 承認レジストリ設定すべてについて詳しく説明します。レジストリ設定が 2 つの製品で重複している場合は、それぞれのカテゴリでリストされます。
- これらのレジストリ変更は管理者のみが行うべきであり、すべての状況に適しているわけではなく、機能しない場合もあります。

暗号化

- Dell Server で自己署名証明書が使用されている場合。Windows では、クライアント コンピューターの証明書信頼検証を無効にしておく必要があります（信頼検証は Dell Server ではデフォルトで無効）。クライアントコンピューターで信頼検証を有効にする場合は、次の要件を満たしている必要があります。
  - ルート証明機関（EnTrust や Verisign など）によって署名された証明書が Dell Server にインポートされている。
  - 証明書の完全な信頼チェーンがクライアントコンピュータの Microsoft キーストアに格納されている。
  - Encryption で信頼検証を有効にするには、ターゲットコンピュータ上で次のレジストリエントリの値を 0 に変更します。

    [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

    "IgnoreCertErrors"=DWORD:00000000

    0 = 証明書エラーが発生した場合に失敗する

    1= エラーを無視する
- Encryption Removal Agent ログファイルを作成するには、復号化のターゲットとなるコンピュータ上で次のレジストリエントリを作成します。「（オプション） Encryption Removal Agent のログファイルの作成」を参照してください。

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=DWORD:2

  0：ログを記録しない

  1：サービスを実行できなくなるエラーをログに記録する

  2：完全なデータ復号化を妨げるエラーをログに記録する（推奨レベル）

  3：すべての復号化ボリュームとファイルに関する情報をログに記録する

  5：デバッグ情報をログに記録する
- Encryption Removal Agent が復号化プロセスの最終状態を終了した後、コンピューターの再起動をユーザーに求めるプロンプトの表示を無効にするには、次のレジストリー値を変更するか、管理コンソールでアップデート時に再起動を強制ポリシーを変更します。

  [HKLM\Software\Dell\Dell Data Protection]

  "ShowDecryptAgentRebootPrompt"=DWORD

  1 = 有効（プロンプトを表示）

  0 = 無効（プロンプトを非表示）
- インストール中にデフォルトで、通知領域アイコンが表示されます。次のレジストリ設定を使用して、最初のインストール後に、コンピュータ上のすべての管理対象のユーザーに対して、通知領域アイコンを非表示にします。レジストリ設定を作成または変更します。

  [HKLM\Software\CREDANT\CMGShield]

  "HIDESYSTRAYICON"=DWORD:1
- デフォルトで、c:\windows\temp ディレクトリ内のすべての一時ファイルは、インストール中に自動的に削除されます。一時ファイルの削除は、最初の暗号化を高速化し、最初の暗号化スイープ前に行われます。

  ただし、組織において \temp ディレクトリ内のファイル構成の維持を要求するサードパーティのアプリケーションを使用している場合は、この削除を防止する必要があります。

  一時ファイルの削除を無効にするには、次のようにレジストリ設定を作成または変更します。

  [HKLM\SOFTWARE\CREDANT\CMGShield]

"DeleteTempFiles"=REG_DWORD:0

一時ファイルを削除しないと、最初の暗号化時間が増大します。

- Encryption は、毎回 5 分間各ポリシーアップデート遅延時間の長さプロンプトを表示します。このプロンプトに反応しないと、次の遅延が始まります。最後の遅延プロンプトには、カウントダウンとプログレスバーが表示され、ユーザーが反応するか最終遅延が時間切れになり必要なログオフ / 再起動が発生するまで表示されています。

  ユーザープロンプトの動作を変更し、暗号化を開始または遅延するようにして、ユーザーがプロンプトに反応しない場合の暗号化処理を防止することができます。これには、次の値を設定します。

  [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

  "SnoozeBeforeSweep"=DWORD:1

  ゼロ以外の値にすると、デフォルトの動作がスヌーズに変更されます。ユーザーの操作がない場合、暗号化処理は設定可能な許容遅延回数まで遅延されます。最後の遅延が時間切れになると、暗号化処理が開始されます。

  最大可能遅延時間は次のように計算します（最大遅延時間は、ユーザーが 5 分間表示される遅延プロンプトに 1 度も反応しない場合を指します）。

  （ポリシー更新遅延の許容回数 x 各ポリシー更新遅延の長さ） + （5 分 x [ポリシー更新遅延の許容回数 - 1]）。

- 強制的なポリシー アップデートのために、レジストリー設定を使用して Encryption に Dell Server へのポーリングを行わせます。レジストリ設定を作成または変更します。

  [HKLM\SOFTWARE\Credant\CMGShield\Notify]

  "PingProxy"=DWORD value:1

  操作が終わると、レジストリ設定は自動的に非表示になります。

- レジストリー設定を使用して、Encryption から Dell サーバーに最適化済み、フル（アクティブ化ユーザーと非アクティブ化ユーザー）、またはフル（アクティブ化ユーザーのみ）インベントリーを送信できるようにします。
  - 最適化されたインベントリーを Dell Server に送信するには、次を実行します。

    レジストリ設定を作成または変更します。

    [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

    "OnlySendInvChanges"=REG_DWORD:1

    エントリーが存在しない場合、最適化されたインベントリーが Dell Server に送信されます。
  - Dell Server にフル インベントリーを送信するには、次を実行します。

    レジストリ設定を作成または変更します。

    [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

    "OnlySendInvChanges"=REG_DWORD:0

    エントリーが存在しない場合、最適化されたインベントリーが Dell Server に送信されます。
  - フル インベントリーをすべてのアクティブ化されたユーザーに送信する場合：

    [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

    "RefreshInventory"=REG_DWORD:1

    このエントリは、処理されるとすぐにレジストリから削除されます。値はヴォールトに保存されるので、インベントリのアップロードが行われる前にコンピュータが再起動する場合でも、Encryption は、次回にインベントリのアップロードが成功したときにもまだこの要求を受け入れます。

    このエントリは、OnlySendInvChanges レジストリ値に置き換わります。

- スロット アクティブ化は、大規模導入中の Dell Server のロードを軽減するために、クライアントのアクティブ化を一定の期間に分散できるようにする機能です。アクティブ化時間を均等に配分できるように、アクティブ化は、アルゴリズムで生成された時間スロットに基づいて遅らせられます。

  VPN を通じたアクティブ化が必要なユーザーの場合は、VPN クライアントがネットワーク接続を確立する時間を確保できるだけ最初のアクティブ化を遅らせるような、クライアントのスロットアクティブ化設定が必要になることがあります。

  これらのレジストリエントリの更新が有効になるには、コンピュータを再起動する必要があります。

  - **スロットアクティブ化**

    この機能を有効または無効にするには、次の親キーの下に **SlottedActivation** という名前の DWORD を作成します。

[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\]

- **アクティブ化スロット**

  この機能を有効または無効にするには、次の親キーの下に **ActivationSlot** という名前のサブキーを作成します。

  [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\]

  アクティブ化スロット - Dell Server で Encryption がアクティブ化を試行する期間を定義する文字列です。これらの値は秒単位で定義され、構文は <lowervalue>,<uppervalue> で定義されます。たとえば、120,300 となります。これは、ユーザーのログイン後 2 ～ 5 分の間のランダムな時間に Encryption がアクティブ化を試みるということです。

  - **カレンダーの繰り返し**

    この機能を有効または無効にするには、次の親キーの下に **CalRepeat** という名前のサブキーを作成します。

    [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot]

    CalRepeat - アクティブ化スロット間隔が繰り返される時間を秒単位で定義する DWORD。この設定を使用して、アクティブ化スロット間隔が繰り返される秒単位の期間をオーバーライドします。7 時間の期間でのアクティベーションスロットには 25200 秒を使用できます。デフォルト設定は 86400 秒であり、これは毎日繰り返されることを示します。ここから提示される 10 進値は 600 で、10 分を表します。

  - **スロット間隔**

    この機能を有効または無効にするには、次の親キーの下に **SlotInterval** という名前のサブキーを作成します。

    [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot]

    スロット間隔 - スロットアクティブ化の間隔を定義する文字列値。推奨される設定は 45,120 です。これは、アクティブ化のタイミングが 45 ～ 120 秒の間でランダムに割り当てられていることを表します。

  - **失敗しきい値**

    この機能を有効または無効にするには、次の親キーの下に **MissThreshold** という名前のサブキーを作成します。

    [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot]

    MissThreshold - ログオフが必要になるまでのアクティブ化の試行回数を定義する正の整数を含む DWORD 値。MissThreshold に到達すると、非アクティブ化されたユーザーが次にログインするまでアクティブ化の試行は停止されます。MissThreshold のカウントは、ログオフ時にかならずリセットされます。

    レジストリキーが、スロットアクティブ化のユーザーデータを収集します。

    [HKCU/Software/CREDANT/ActivationSlot]（ユーザーごとのデータ）

    アクティブ化を試行するための据え置き時間。これは、スロットアクティブ化が有効になった後はじめてユーザーがネットワークにログオンするときに設定されます。アクティブ化スロットは、アクティブ化試行ごとに再計算されます。

    [HKCU/Software/CREDANT/SlotAttemptCount]（ユーザーごとのデータ）

    時間スロットに達し、アクティブ化が試行されたが失敗したときの失敗または失われた試行の数。この数が ACTIVATION_SLOT_MISSTHRESHOLD に設定された値に達すると、コンピュータは、ネットワークへの接続時に即時アクティブ化を 1 度試行します。

- クライアントコンピュータ上で管理対象外のユーザーを検出するには、クライアントコンピュータ上でレジストリ値を設定します。

  [HKLM\SOFTWARE\Credant\CMGShield\ManagedUsers\]

  "UnmanagedUserDetected"=DWORD value:1

  この computer=1 では管理対象外のユーザーを検出します

  この computer=0 では管理対象外のユーザーを検出しません

- Encryption External Media で暗号化された外付けメディアへのアクセスを、メディアの暗号化に使用した暗号化キーを生成した Dell Server へのアクセス権のあるコンピューターに制限することができます。

  この機能を有効にするにはレジストリを設定します。

  [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

  "EnterpriseUsage"=DWORD:0

  Off (default)=0

  File Access Restricted to Enterprise=1

  外付けメディアのファイルを暗号化した後にこの値を変更すると、レジストリ設定が更新されたコンピュータにメディアを接続したときに、更新されたレジストリキー値でファイルが再度暗号化されます。

- ユーザーが非アクティブ化されるという稀なケースにおいてサイレント自動再アクティブ化を有効にするには、クライアントコンピュータにレジストリ値を設定する必要があります。

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CMGShield]

  "AutoReactivation"=DWORD:00000001

  0 = 無効（デフォルト）

  1 = 有効

- System Data Encryption（SDE）は、SDE 暗号化ルールのポリシー値に基づいて実施されます。SDE 暗号化の有効化 ポリシーが選択されている場合、追加のディレクトリがデフォルトで保護されます。詳細については、AdminHelp で「SDE 暗号化ルール」を検索してください。アクティブな SDE ポリシーを含むポリシーアップデートを暗号化する場合、現在のユーザープロファイルディレクトリは、SDE キー（デバイスキー）ではなく、デフォルトで SDUser キー（ユーザーキー）で暗号化されます。SDUser キーは、SDE で暗号化されないユーザーディレクトリにコピーされる（移動ではない）ファイルまたはフォルダを暗号化するためにも使用されます。

  SDUser キーを無効化して、これらのユーザーディレクトリの暗号化に SDE キーを使用するには、コンピュータにレジストリを作成します。

  [HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]

  "EnableSDUserKeyUsage"=DWORD:00000000

  このレジストリキーが存在しない、または 0 以外に設定されている場合、これらのユーザーディレクトリの暗号化には SDUser キーが使用されます。

  SDUser の詳細については、KB 記事 131035 を参照してください。

- 共通キーにより暗号化されたデータあるいはフォルダ内の多数のファイルの暗号化、復号化、または解凍についてコンピュータ上の Microsoft アップデートに関連する問題が発生する場合には、レジストリエントリ EnableNGMetadata を設定します。

  次の場所に EnableNGMetadata レジストリエントリを設定します。

  [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CmgShieldFFE]

  "EnableNGMetadata" = DWORD:1

  0 = 無効（デフォルト）

  1 = 有効

- Dell ProSupport に連絡して指示を求めることで、非ドメインアクティブ化機能を有効にできます。
- Encryption Management Agent は、デフォルトでポリシー出力をしないようになりました。将来使用されるポリシーを出力するには、次のレジストリー キーを作成します。

  HKLM\Software\Dell\Dell Data Protection\

  "DumpPolicies" = DWORD

  Value=1

  メモ：ログは C:\ProgramData\Dell\Dell Data Protection\Policy に書き込まれます。

- 右クリック メニューで *Encrypt for Sharing* オプションを無効または有効にするには、次のレジストリー キーを使用します。

  HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection\Encryption

  "DisplaySharing"=DWORD

  0 =右クリックのコンテキスト メニューで Encrypt for Sharing オプションを無効化

  1 =右クリックのコンテキスト メニューで Encrypt for Sharing オプションを有効化

SED Manager

- SED Manager との通信に Dell Server を使用できない場合の再試行間隔を設定するには、次のレジストリー値を追加します。

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "CommErrorSleepSecs"=DWORD:300

  この値は、通信に Dell Server を使用できない場合に、SED Manager が Dell サーバーとの接続を試みるために待機する秒数です。デフォルトは 300 秒（5 分）です。

- 自己署名証明書が SED Manager 向けの Dell Server で使用されている場合、クライアント コンピューターで SSL/TLS 信頼検証を無効のままにしておく必要があります（SED Manager では SSL/TLS 信頼検証はデフォルトで無効です）。クライアントコンピュータで SSL/TLS 信頼検証を有効にする場合は、次の要件を満たしている必要があります。
  - ルート証明機関（EnTrust や Verisign など）によって署名された証明書が Dell Server にインポートされている。
  - 証明書の完全な信頼チェーンがクライアントコンピュータの Microsoft キーストアに格納されている。
  - SED Manager で SSL/TLS 信頼検証を有効にするには、クライアント コンピューター上で次のレジストリー エントリーの値を 0 に変更します。

    [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

    "DisableSSLCertTrust"=DWORD:0

    0 = 有効

    1 = 無効
- PBA がアクティブ化されているかどうかを判断するには、次の値が設定されていることを確認します。

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent\Parameters]

  "PBAIsActivated"=DWORD (32-bit):1

  1 の値は PBA がアクティブ化されていることを示します。0 の値は PBA がアクティブ化されていないことを示します。
- スマートカードが存在し、アクティブになっていることを確認するには、次の値が設定されていることを確認します。

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

  SmartcardEnabled が見つからない、または値がゼロの場合、資格情報プロバイダーは認証のためのパスワードだけを表示します。

  SmartcardEnabled の値がゼロ以外の場合、資格情報プロバイダーはパスワードとスマートカード認証のオプションを表示します。
- 次のレジストリ値は、Winlogon がスマートカードからのログオンイベントの通知を生成する必要があるかどうかを示します。

  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

  "SmartCardLogonNotify"=DWORD:1

  0 = 無効

  1 = 有効
- SED Manager で、サード パーティーの資格情報プロバイダーによる無効化ができないようにするには、次のレジストリー キーを作成します：

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "AllowOtherCredProviders" = DWORD:1

  0 = 無効（デフォルト）

  1 = 有効

  メモ：この値を用いると、サード パーティーの資格情報プロバイダーが無効化されることで、Dell 資格情報プロバイダーによる資格情報の最初の同期が正しく行えなくなる可能性があります。このレジストリー キーを使用するデバイスが Dell サーバーと正しく通信できることを確認してください。
- 通信に Dell Server を使用できないときに SED Manager が Dell サーバーとの接続を試みる間隔を設定するには、ターゲット コンピューターで次の値を設定します。

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "CommErrorSleepSecs"=DWORD Value:300

  この値は、通信に Dell Server を使用できない場合に、SED Manager が Dell サーバーとの接続を試みるために待機する秒数です。デフォルトは 300 秒（5 分）です。
- 必要に応じて、Security Server ホストを元のインストール先から変更することができます。ホスト情報は、ポリシーのポーリングが行われるたびに読み取られます。クライアントコンピュータ上で次のレジストリ値を変更してください。

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerHost"=REG_SZ:<newname>.<organization>.com
- 必要に応じて、Security Server のポートが元のインストール先から変更されることがあります。この値は、ポリシーのポーリングが行われるたびに読み取られます。クライアントコンピュータ上で次のレジストリ値を変更してください。

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

ServerPort=REG_SZ:8888

- 必要に応じて、Security Server の URL が元のインストール場所から変更されることがあります。この値は、ポリシーのポーリングが行われるたびにクライアントコンピュータに読み取られます。クライアントコンピュータ上で次のレジストリ値を変更してください。

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerUrl"=REG_SZ:https://<newname>.<organization>.com:8888/agent

- （起動前認証を使用する場合のみ）スマートカードおよびバイオメトリックデバイスに関連付けられているサービスを PBA Advanced Authentication に「自動」起動タイプに**変更させたくない**場合は、サービス起動機能を無効にします。また、この機能を無効化すると、実行されていない必須サービスに関連する警告も抑制されます。

  無効化すると、PBA Advanced Authentication は次のサービスの起動を試行しなくなります。

  - SCardSvr - コンピュータが読み取るスマートカードへのアクセスを管理します。このサービスが停止されると、コンピュータはスマートカードを読み取ることができなくなります。このサービスが無効化されると、このサービスに確実に依存するサービスの開始が失敗するようになります。
  - SCPolicySvc - スマートカード取り外し時にユーザーのデスクトップをロックするようシステムを設定することができます。
  - WbioSrvc - Windows 生体認証サービスは、クライアントアプリケーションに対し、生体認証ハードウェアやサンプルに直接アクセスすることなく、生体認証データの取得、比較、 操作、および保存する機能を提供します。このサービスは特権 SVCHOST プロセスでホストされます。

    レジストリキーが存在しない、または値が 0 に設定されている場合、この機能はデフォルトで有効化されます。

    [HKLM\SOFTWARE\DELL\Dell Data Protection]

    SmartCardServiceCheck=REG_DWORD:0

    0 = 有効

    1 = 無効

- SED PBA Authentication でスマートカードを使用するには、SED を搭載しているクライアントコンピュータで次のレジストリ値を設定します。

  [HKLM\SOFTWARE\DigitalPersona\Policies\Default\SmartCards]

  "MSSmartcardSupport"=DWORD:1

  管理コンソールで認証方法ポリシーをスマートカードに設定し、変更をコミットします。

- Encryption Management Agent からのトースター通知が表示されないようにするには、クライアントコンピュータで次のレジストリ値を設定する必要があります。

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "PbaToastersAllowClose" =DWORD:1

  0 = 有効（デフォルト）

  1 = 無効

フルディスク暗号化

- この項では、レジストリ設定の理由に関係なく、ローカルコンピュータでの Dell ProSupport 承認レジストリ設定すべてについて詳しく説明します。レジストリ設定が 2 つの製品で重複している場合は、それぞれのカテゴリでリストされます。
- これらのレジストリ変更は管理者のみが行うべきであり、すべての状況に適しているわけではなく、機能しない場合もあります。
- フル ディスク暗号化との通信に Dell Server を使用できない場合の再試行間隔を設定するには、次のレジストリー値を追加します。

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "CommErrorSleepSecs"=DWORD:300

  この値は、フル ディスク暗号化との通信に Dell Server を使用できない場合に、フル ディスク暗号化が Dell サーバーとの接続を試みるために待機する秒数です。デフォルトは 300 秒（5 分）です。

- 自己署名証明書がフル ディスク暗号化向けの Dell Server で使用されている場合、クライアント コンピューターで SSL/TLS 信頼検証を無効のままにしておく必要があります（フル ディスク暗号化では SSL/TLS 信頼検証はデフォルトで無効です）。クライアントコンピュータで SSL/TLS 信頼検証を有効にする場合は、次の要件を満たしている必要があります。
  - ルート証明機関（EnTrust や Verisign など）によって署名された証明書が Dell Server にインポートされている。
  - 証明書の完全な信頼チェーンがクライアントコンピュータの Microsoft キーストアに格納されている。

- Dell Encryption 管理で SSL / TLS 信頼検証を有効にするには、クライアントコンピュータ上で次のレジストリエントリの値を 0 に変更します。

  [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

  "DisableSSLCertTrust"=DWORD:0

  0 = 有効

  1 = 無効

- PBA がアクティブ化されているかどうかを判断するには、次の値が設定されていることを確認します。

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent\Parameters]

  "PBAIsActivated"=DWORD (32-bit):1

  1 の値は PBA がアクティブ化されていることを示します。0 の値は PBA がアクティブ化されていないことを示します。

  メモ: このキーを手動で削除すると、ユーザーが PBA と同期して手動でのリカバリが必要になるという、意図しない結果をもたらすことがあります。

- スマートカードが存在し、アクティブになっていることを確認するには、次の値が設定されていることを確認します。

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "SmartcardEnabled"=DWORD:1

  SmartcardEnabled が見つからない、または値がゼロの場合、資格情報プロバイダーは認証のためのパスワードだけを表示します。

  SmartcardEnabled の値がゼロ以外の場合、資格情報プロバイダーはパスワードとスマートカード認証のオプションを表示します。

- 次のレジストリ値は、Winlogon がスマートカードからのログオンイベントの通知を生成する必要があるかどうかを示します。

  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

  "SmartCardLogonNotify"=DWORD:1

  0 = 無効

  1 = 有効

- 必要に応じて、Security Server ホストを元のインストール先から変更することができます。ホスト情報は、ポリシーのポールが行われるたびにクライアントコンピュータに読み取られます。クライアントコンピュータ上で次のレジストリ値を変更してください。

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  "ServerHost"=REG_SZ:<newname>.<organization>.com

- 必要に応じて、Security Server のポートが元のインストール先から変更されることがあります。この値は、ポリシーのポーリングが行われるたびにクライアントコンピュータに読み取られます。クライアントコンピュータ上で次のレジストリ値を変更してください。

  [HKLM\SYSTEM\CurrentControlSet\services\DellMgmtAgent]

  ServerPort=REG_SZ:8888

- （起動前認証を使用する場合のみ）スマートカードおよびバイオメトリックデバイスに関連付けられているサービスを PBA Advanced Authentication に「自動」起動タイプに**変更させたくない**場合は、サービス起動機能を無効にします。また、この機能を無効化すると、実行されていない必須サービスに関連する警告も抑制されます。

  無効化すると、PBA Advanced Authentication は次のサービスの起動を試行しなくなります。

  - SCardSvr - コンピュータが読み取るスマートカードへのアクセスを管理します。このサービスが停止されると、コンピュータはスマートカードを読み取ることができなくなります。このサービスが無効化されると、このサービスに確実に依存するサービスの開始が失敗するようになります。
  - SCPolicySvc - スマートカード取り外し時にユーザーのデスクトップをロックするようシステムを設定することができます。
  - WbioSrvc - Windows 生体認証サービスは、クライアントアプリケーションに対し、生体認証ハードウェアやサンプルに直接アクセスすることなく、生体認証データの取得、比較、 操作、および保存する機能を提供します。このサービスは特権 SVCHOST プロセスでホストされます。

    レジストリキーが存在しない、または値が 0 に設定されている場合、この機能はデフォルトで有効化されます。

    [HKLM\SOFTWARE\DELL\Dell Data Protection]

    SmartCardServiceCheck=REG_DWORD:0

    0 = 有効

1 = 無効

- フル ディスク暗号化で、サード パーティーの資格情報プロバイダーによる無効化ができないようにするには、次のレジストリー キーを作成します：

  HKLM\SOFTWARE\Dell\Dell Data Protection\

  "AllowOtherCredProviders" = DWORD:1

  0 = 無効（デフォルト）

  1 = 有効

  メモ：この値を用いると、サード パーティーの資格情報プロバイダーが無効化されることで、Dell 資格情報プロバイダーによる資格情報の最初の同期が正しく行えなくなる可能性があります。このレジストリー キーを使用するデバイスが Dell サーバーと正しく通信できることを確認してください。

- Encryption Management Agent からのトースター通知が表示されないようにするには、クライアントコンピュータで次のレジストリ値を設定する必要があります。

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  "PbaToastersAllowClose" =DWORD:1

  0 = 有効（デフォルト）

  1 = 無効

- Policy Based Encryption を使用してフルディスク暗号化のインストールを許可するには、次のレジストリ値をクライアントコンピュータに設定する必要があります。

  [HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection]

  " EnableFDE" = DWORD: 1

  0 = 無効（デフォルト）

  1 = 有効

BitLocker Manager

- 自己署名証明書が BitLocker Manager 向けの Dell Server で使用されている場合は、クライアントコンピュータで SSL / TLS 信頼検証を無効のままにしておく必要があります（BitLocker Manager では SSL / TLS 信頼検証はデフォルトで 無効 です）。クライアントコンピュータで SSL/TLS 信頼検証を有効にする場合は、次の要件を満たしている必要があります。
  - ルート証明機関（EnTrust や Verisign など）によって署名された証明書が Dell Server にインポートされている。
  - 証明書の完全な信頼チェーンがクライアントコンピュータの Microsoft キーストアに格納されている。
  - BitLocker Manager で SSL/TLS 信頼検証を有効にするには、クライアントコンピュータ上で次のレジストリエントリの値を 0 に変更します。

    [HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

    "DisableSSLCertTrust"=DWORD:0

    0 = 有効

    1 = 無効

  - Bitlocker Manager でリムーバブル ディスクが固定ディスクとして検知されないようにするには、次のレジストリー キーを追加します：

    HKLM\Software\Dell\Dell Data Protection\

    "UseEncryptableVolumeType" = DWORD:1

    0 = 無効（デフォルト）

    1 = 有効

4

マスターインストーラを使用してインストールする

- 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。
- のマスター インストーラーのログ ファイルは、次のディレクトリーにあります。 `C:\ProgramData\Dell\Dell Data Protection\Installer.`

  メモ: Encryption Management Agent の前に Policy-Based Encryption がインストールされている場合、コンピューターでクラッシュが発生する可能性があります。この問題は、PBA 環境を管理する暗号化スリープ ドライバーのロードに失敗したことが原因で発生します。回避策としては、マスター インストーラーを使用するか、Encryption Management Agent の後に Policy-Based Encryption がインストールされていることを確認します。

- 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 の機能の使用方法については、*Dell Encrypt* の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\Encryption\Help` からアクセスできます。
  - Encryption External Media の機能については、*Encryption External Media* の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\Encryption\EMS` からアクセスできます。
  - の機能の使用方法については、*Encryption Enterprise* の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\Client Security Framework\Help` からアクセスできます。
- 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

- マスターインストーラは次の場所に置かれます。
  - **dell.com/support から** - 必要に応じて、**dell.com/support** からソフトウェアを入手します。
  - **お使いの Dell FTP アカウントから** - インストール バンドルを Dell-Encryption-8.x.x.xxx.zip の中から見つけます。
- 以下の手順に従い、Dell Encryption Enterprise を、 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. Dell インストール メディア内で、**DDSSetup.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 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 *Dell* サーバー名に Dell サーバー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。

   組織が標準以外のポートを使用している場合、コア サーバー ポートおよびセキュリティ サーバー ポートにポート値を入力します。

   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\. Dell recommends installing in the default location only` に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ります。
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、基盤となるセキュリティフレームワーク、Encryption Management Agent、および PBA Authentication をインストールします。

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。

Encryption は、コンピュータがネットワークに接続されている、いないにかかわらず、あるいは紛失または盗難に遭っ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をインストールします。

Encryption External Media は、Encryption External Media を強制するコンポーネントをインストールします。

フル ディスク暗号化は、フル ディスク暗号化を強制するコンポーネントをインストールします。

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

- 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 パーティー認証情報プロバイダー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 パラメーターを指定してアップグレードする必要があります。

スイッチ	説明
/s	サイレントインストール
/z	DDSSetup.exe 内の .msi に変数を渡します。

パラメータ

- 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。

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。 DE = Drive Encryption クライアントのみ EME = Encryption External Media のみ BLM = BitLocker Manager SED = SED Manager（Encryption Management Agent/Manager、PBA/GPE ドライバー）
BLM_ONLY=1	SED Manager プラグインを除外するために FEATURES=BLM をコマンド ラインで使用する場合は、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。

- この例では、マスター インストーラー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。

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com\""
  ```

- この例では、マスター インストーラー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 SED Manager および Encryption External Media 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。

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=EME-SED,
  SUPPRESSREBOOT=1\""
  ```

- この例では、マスター インストーラー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 SED Manager 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。

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=SED, SUPPRESSREBOOT=1\""
  ```

- この例では、マスター インストーラー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 SED Manager 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。

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=SED\""
  ```

- この例では、マスター インストーラー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 Encryption および BitLocker Manager（SED Manager プラグインなし）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。

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=DE-BLM, BLM_ONLY=1\""
  ```

- この例では、マスター インストーラー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 BitLocker Manager（SED Manager プラグインあり）および Encryption External Media 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。

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=BLM-EME,
  SUPPRESSREBOOT=1\""
  ```

- この例では、マスター インストーラー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 BitLocker Manager（SED Manager プラグインなし）および Encryption External Media 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。

  ```
  "DDSSetup.exe" /s /z"\"SERVER=server.organization.com, FEATURES=BLM-EME, BLM_ONLY=1,
  SUPPRESSREBOOT=1\""
  ```

5

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、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に特定の順序**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 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。
  1. Encryption をアンインストールします。
  2. SED Manager をアンインストールします。
  3. フル ディスク暗号化のアンインストール
  4. Uninstall BitLocker をアンインストールします。
- 「マスターインストーラのアンインストール」に進みます。

マスター インストーラー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、マスター インストーラーのサイレント アンインストールを行います。

  ```
  "DDSSetup.exe" /s /x
  ```

  終了したらコンピュータを再起動します。

6

子インストーラを使用したインストール

- 各クライアントを個別にインストールまたはアップグレードするには、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」の説明に従って、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。
- このセクションに記載されているコマンドの例は、コマンドを `C:\extracted` から実行することが前提になっています。
- 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。
- 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、クライアントをインストールします。
- コマンドラインの例では、再起動は省略されています。ただし、最終的には再起動する必要があります。

  メモ：ポリシーベースの暗号化は、コンピューターが再起動されるまで開始できません。

- ログファイル - Windows は、`C:\Users\<UserName>\AppData\Local\Temp.` にある %temp% に、ログインしたユーザー用の固有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。

  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ので、必ずそのログファイルには独自に名前を付けてください。`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。

- すべての子インストーラは、特に断りがない限り、コマンドラインでの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。最初にスイッチを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 スイッチに渡された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内で /q と /qn を同時に使用しないでください。を使用してだけです！および - /qb を指定した後です。

スイッチ	意味
/v	setup.exe 内の .msi に変数を渡します。入力内容は、常に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

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、この記事を参照してください。

以下に説明されている、	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
/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
/norestart	再起動の抑制

- 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 の機能の使用方法については、*Dell Encrypt* 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\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。
- PBA 認証 の機能の使用方法については、*Encryption Enterprise* 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。

ドライバのインストール

- ControlVault 対応のドライバおよびファームウェア、指紋リーダー、およびスマートカードは、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含まれません。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。

Encryption のインストール

- EnTrust または Verisign などのルート証明機関によって署名された証明書を使用している場合は、「Encryption 要件」を確認してください。証明書検証を有効にするには、クライアントコンピュータでレジストリ設定を変更する必要があります。
- 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。
- Encryption インストーラは次の場所にあります。
  - **dell.com/support** - 必要に応じて、dell.com/support からソフトウェアを入手して、マスターインストーラから子インストーラを抽出します。抽出後、`C:\extracted\Encryption` でファイルを見つけます。
  - **お使いのデル FTP アカウントから** - Encryption-Enterprise-10.x.x.xxx.zip でインストールバンドルを見つけてから、マスターインストーラから子インストーラを抽出します。抽出後、`C:\extracted\Encryption` でファイルを見つけます。
  - **メモ:** ディスクストレージが不足しているためにインストールできない場合は、Dell Encryption ログを指定しないでください。

コマンドラインでのインストール

- 次の表に、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
SERVERHOSTNAME=<ServerName>（再アクティブ化用の Dell Server の FQDN）
POLICYPROXYHOSTNAME=<RGKName>（デフォルトポリシープロキシの FQDN）
MANAGEDDOMAIN=<MyDomain>（デバイスに対して使用するドメイン）
DEVICESERVERURL=<DeviceServerName/SecurityServerName>（アクティブ化に使用する URL、通常はサーバ名、ポート、xapi を含む）
GKPORT=<NewGKPort>（ゲートキーパーポート）
MACHINEID=<MachineName>（コンピュータ名）

パラメータ
RECOVERYID=<RecoveryID>（リカバリ ID）
REBOOT=ReallySuppress（Null は自動再起動に対応し、ReallySuppress は再起動を無効化）
HIDEOVERLAYICONS=1（0 はオーバーレイアイコンを有効化、1 はオーバーレイアイコンを無効化）
HIDESYSTRAYICON=1（0 は通知領域のアイコンを有効化、1 は通知領域のアイコンを無効化）。
ENABLE_FDE_LM=1（フルディスク暗号化がアクティブになっているコンピュータに対する Dell Encryption のインストールを許可）
EME=1（Encryption External Media モードをインストール）

コマンドラインで使用することができる基本的な .msi スイッチと表示オプションのリストについては、「子インストーラを使用したインストール」を参照してください。

- 次の表に、アクティブ化に関連するその他のオプションパラメータの詳細を示します。

パラメータ
SLOTTEDACTIVATON=1（0 は遅延またはスケジュールされたアクティブ化を無効化、1 は遅延またはスケジュールされたアクティブ化を有効化）
SLOTINTERVAL=45,120（x,x の表記によりアクティブ化をスケジュール。ここで、最初の値はスケジュールの下限、2 番目の値はスケジュールの上限であり、単位は秒）
CALREPEAT=600（SLOTINTERVAL で設定された上限以上である必要があります。SLOTINTERVAL に基づいてアクティブ化の試行を行うまでに Encryption が待機する秒数です。）

コマンドラインの例

メモ: Security Management Server が v7.7 より前の場合は、 `DEVICESERVERURL=https://server.organization.com:8081/xapi`（末尾のスラッシュなし）を置き換えます。

- 次の例では、Encryption、Encrypt for Sharing、ダイアログなし、プログレスバーなし、自動再起動、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection\Encryption` にインストールというデフォルトのパラメーターを使用して、Dell Encryption をインストールします。

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
```

MSI コマンド：

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
```

- 次の例では、Dell Encryption 通知領域アイコンの非表示、オーバーレイアイコンの非表示、ダイアログなし、プログレスバーなし、再起動なし、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection\Encryption.` にインストールという設定で Encryption および Encrypt for Sharing をインストールします。

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESERVERURL=https://server.organization.com:8443/xapi/ HIDESYSTRAYICON=1
HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
```

MSI コマンド：

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
HIDESYSTRAYICON="1" HIDEOVERLAYICONS="1"
```

Encryption External Media のみをインストールするためのコマンドライン例

- サイレントインストール、プログレスバーなし、自動再起動、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection\Encryption.` にインストールという設定で行われます。

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESERVERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
```

MSI コマンド：

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
```

- サイレントインストール、再起動なし、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection\Encryption` にインストールという設定で行われます。

```
DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com DEVICESERVERURL=https://
server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /norestart /qn"
```

MSI コマンド：

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress" EME="1"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
DEVICESERVERURL="https://server.organization.com:8443/xapi/" MANAGEDDOMAIN="ORGANIZATION"
```

- **メモ:**

  クライアントのバージョン情報ボックスにはソフトウェアのバージョン番号情報が表示されますが、Encryption（フルインストール）か、Encryption External Media のみがインストールされているかどうかは表示されません。この情報を探すには、`C:\ProgramData\Dell\Dell Data Protection\Encryption\CMGShield.log` に移動し、次のエントリを探します。

  [<date/timestamp> DeviceInfo: < >] ***Shield Information - SM=External Media Only***, SB=DELL, UNF=FQUN, last sweep={0, 0}

Encryption External Media を Encryption（フルインストール）へ変換するためのコマンドライン例

メモ: アップグレードでは、Encryption External Media の Encryption（フル インストール）への変換はサポートされていません。

- Encryption External Media から Encryption（フルインストール）へ変換する際には、復号は必要ありません。

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESERVERURL=https://server.organization.com:8443/xapi/ REINSTALL=ALL EME=0
REINSTALLMODE=vamus /qn"
```

MSI コマンド：

```
msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/xapi/"
REINSTALL="ALL" EME="0" REINSTALLMODE="vamus"
```

- **フルディスク暗号化を使用して Dell Encryption をインストールするためのコマンドラインの例**

  暗号化

- 次の例では、Encryption、Encrypt for Sharing、ダイアログなし、プログレスバーなし、自動再起動、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection\Encryption` にインストールというデフォルトのパラメーターを使用して、Dell Encryption をインストールします。

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
```

次の操作：

\Encryption Management Agent

次の例では、サイレントインストール、再起動なし、コントロールパネルのプログラムリストにエントリなし、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection\Encryption` にインストールという設定で、リモート管理されるフルディスク暗号化をインストールし、Dell Encryption 保護コンピュータでのインストールを許可します。

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1 FEATURE=FDE
SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
norestart /qn"
```

- **Encryption External Media とフルディスク暗号化をインストールするためのコマンドラインの例。**

  暗号化

  次の例では、サイレントインストール、プログレスバーなし、自動再起動、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection\Encryption` にインストールするという設定で、Encryption External Media をインストールします。

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
  ```

  次の操作：

  \Encryption Management Agent

  次の例では、サイレントインストール、再起動なし、コントロールパネルのプログラムリストにエントリなし、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection` にインストールという設定で、リモート管理されるフルディスク暗号化をインストールし、Dell Encryption 保護コンピュータでのインストールを許可します。

  ```
  EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1 FEATURE=FDE
  SERVERHOST=server.organization.com SERVERPORT=8888
  SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 ARPSYSTEMCOMPONENT=1 /
  norestart /qn"
  ```

- **既存のフルディスク暗号化のインストールの上から Encryption External Media をインストールするコマンドラインの例。**

  次の例では、サイレントインストール、プログレスバーなし、自動再起動、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection` にインストールするという設定で、既存のフルディスク暗号化のインストールの上から Encryption External Media をインストールします。

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ ENABLE_FDE_LM=1 /norestart /
  qn"
  ```

- **既存のフルディスク暗号化のインストールの上から Remotely Managed Encryption クライアントをインストールするコマンドラインの例。**

  次の例では、Encryption クライアント、Encrypt for Sharing、ダイアログなし、プログレス バーなし、自動再起動、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection\Encryption` にインストールというデフォルトのパラメーターおよび `C:\Dell` のインストール ログを使用して、既存のフル ディスク暗号化のインストールの上から Dell Encryption をインストールします。**メモ：**ログを生成するには、インストールの前に `C:\Dell` ディレクトリーが存在している必要があります。

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ ENABLE_FDE_LM=1 /norestart /
  qn /l*v C:\Dell\DellEncryptionInstall.log"
  ```

メモ：一部の古いバージョンでは、パラメーター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 /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
```

フルディスク暗号化のインストール

- EnTrust または Verisign などのルート証明機関によって署名された証明書を使用している場合は、「フルディスク暗号化の要件」を見直します。SSL/TLS 信頼検証を有効にするには、クライアントコンピュータでレジストリ設定を変更する必要があります。
- ユーザーは、Windows 資格情報を使用して PBA にログインします。

コマンドラインでのインストール

- 次の表は、インストールで使用できるパラメータの詳細です。

パラメータ
CM_EDITION=1 (remote management)
INSTALLDIR=(change the installation destination)
SERVERHOST=(securityserver.organization.com)
SERVERPORT=8888
SECURITYSERVERHOST=(securityserver.organization.com)
SECURITYSERVERPORT=8443
FEATURE=FDE
ENABLE_FDE_LM=1（Dell Encryption がアクティブなコンピュータにフルディスク暗号化のインストールを許可）

コマンドラインで使用することができる基本的な .msi スイッチと表示オプションのリストについては、「子インストーラを使用したインストール」を参照してください。

コマンドラインの例

Encryption Management Agent

- 次の例では、サイレントインストール、再起動なし、デフォルト場所の `C:\Program Files\Dell\Dell Data Protection\Encryption` にインストールするという設定で、リモート管理されたフルディスク暗号化をインストールします。

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 FEATURE=FDE SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /
norestart /qn"
```

- **Encryption Management Agent**
- 次の例では、サイレントインストール、再起動なし、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection\Encryption` にインストールするという設定で、リモート管理されたフルディスク暗号化をインストールし、Dell Encryption 保護コンピュータでのインストールを許可します。

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1 FEATURE=FDE
SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /norestart /qn"
```

- **フルディスク暗号化と Encryption External Media をインストールするためのコマンドライン例**

  暗号化

  次の例では、サイレントインストール、プログレスバーなし、自動再起動、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection\Encryption` にインストールするという設定で、Encryption External Media をインストールします。

```
DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
DEVICESERVERURL=https://server.organization.com:8443/xapi/ EME=1 /qn"
```

  次の操作：

  Encryption Management Agent

  次の例では、サイレントインストール、再起動なし、コントロールパネルのプログラムリストにエントリなし、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection\Encryption` にインストールという設定で、リモート管理されるフルディスク暗号化をインストールし、Dell Encryption 保護コンピュータでのインストールを許可します。

```
EMAgent_64bit_setup.exe /s /v"CM_EDITION=1 ENABLE_FDE_LM=1 FEATURE=FDE
SERVERHOST=server.organization.com SERVERPORT=8888
SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /norestart /qn"
```

サーバオペレーティングシステム上の Encryption のインストール

サーバオペレーティングシステム上の Encryption をインストールするには、2 つの方法があります。以下のいずれかの方法を選択します。

- サーバオペレーティングシステム上の Encryption を対話形式でインストール

  サーバオペレーティングシステム上の Encryption は、サーバオペレーティングシステムを実行しているコンピュータ上でのみ対話形式でインストールできます。非サーバーオペレーティングシステムを実行しているコンピュータ上でのインストールは、コマンドラインで、SERVERMODE=1 のパラメータを指定して、実行する必要があります。

- コマンドラインを使用したサーバオペレーティングシステム上の Encryption のインストール

仮想ユーザーアカウント

- インストールの一環として、サーバオペレーティングシステム上の Encryption を排他的に使用するための**仮想サーバユーザーアカウント**が作成されます。仮想サーバユーザーのみが暗号化キーにアクセスできるよう、パスワードおよび DPAPI 認証は無効になっています。

作業を開始する前に

- インストールを実行するユーザーアカウントは、管理者レベルの権限を持つドメインユーザーである必要があります。
- この要件をオーバーライドする、あるいはドメイン以外のサーバまたはマルチドメインサーバでサーバオペレーティングシステム上の Encryption を実行したりするには、application.properties ファイルで *ssos.domainadmin.verify* プロパティを *false* に設定します。このファイルは、お使いの Dell Server に基づいて、次のファイルパスに保存されています。

  Security Management Server - *<installation dir>*/Security Server/conf/application.properties

  Security Management Server Virtual - /opt/dell/server/security-server/conf/application.properties

- サーバーはポート制御をサポートしている必要があります。

  ポート制御システムのポリシーは、たとえば、USB デバイスによるサーバの USB ポートへのアクセスおよび使用を制御することにより、保護対象サーバ上のリムーバブルメディアに影響します。USB ポートポリシーは外部 USB ポートに適用されます。内部 USB ポート機能は、USB ポートポリシーの影響を受けません。USB ポートポリシーが無効化されると、USB キーボードおよびマウスは機能しなくなり、このポリシーが適用される前にリモートデスクトップ接続がセットアップされない限り、ユーザーはコンピュータを使用することができなくなります。

- 正常にアクティブ化するには、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。
- Trusted Platform Module（TPM）が使用可能な場合、デルハードウェア上の汎用キーを封印するために TPM が使用されます。TPM が使用できない場合、Microsoft のデータ保護 API（DPAPI）を使用して汎用キーを保護します。

  Server Encryption を実行している、TPM を搭載した Dell コンピュータに、新しいオペレーティングシステムをインストールするときは、BIOS で TPM をクリアしてください。手順については、この記事を参照してください。

- インストールのログファイルはユーザー %temp% ディレクトリ内にあり、このディレクトリは `C:\Users\<user name>\AppData\Local\Temp` にあります。正しいログファイルを見つけるには、ファイル名が MSI で始まり、.log 拡張子で終わるファイルを探してください。このファイルには、インストーラの実行時刻と一致する日時スタンプが含まれています。
- 分散ファイルシステム（DFS）の一部であるサーバでは、暗号化はサポートされません。

子インストーラの抽出

- サーバオペレーティングシステム上の Encryption をインストールするには、最初に子インストーラ **DDPE_xxbit_setup.exe** をマスターインストーラから抽出する必要があります。マスターインストーラからの子インストーラの抽出 を参照してください。

対話形式でインストール

- サーバオペレーティングシステム上の Encryption を対話形式でインストールするには、次の手順に従います。このインストーラには、ソフトウェア暗号化に必要なコンポーネントが含まれています。

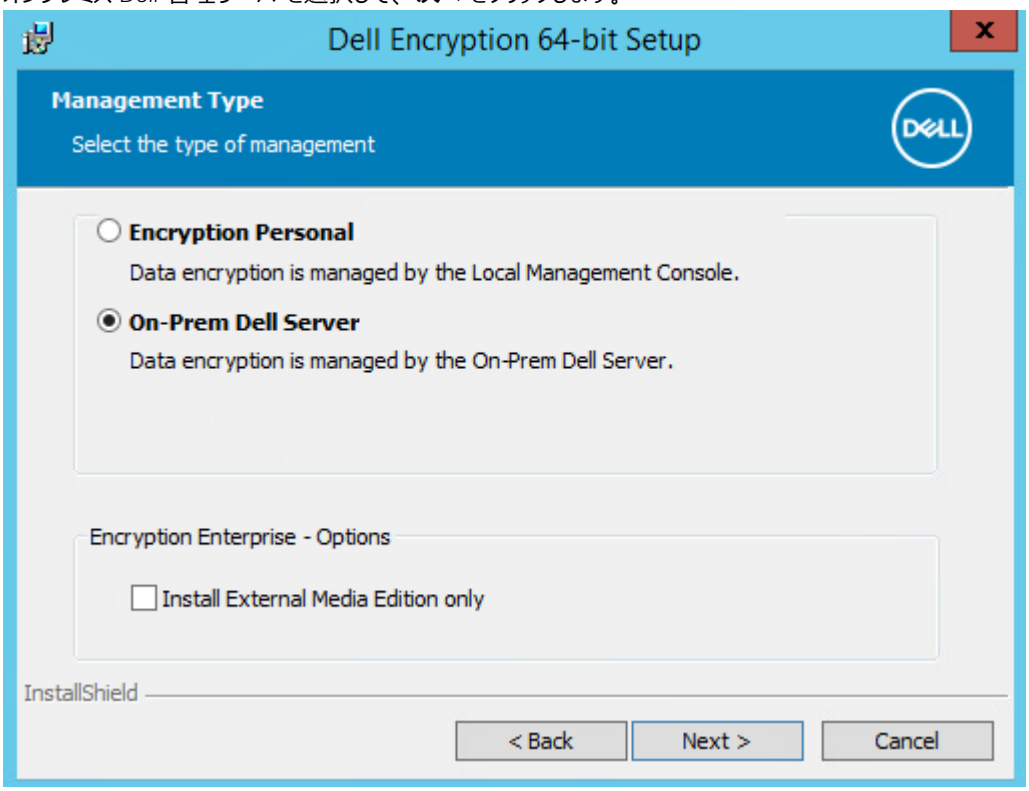
1. `C:\extracted\Encryption` フォルダ内で **DDPE_XXbit_setup.exe** を見つけます。それをローカルコンピュータにコピーします。
2. サーバオペレーティングシステム上の Encryption をインストールしている場合は、**DDPE_XXbit_setup.exe** をダブルクリックしてインストーラを起動します。

   メモ:

   Windows Server 2012 R2 などのサーバオペレーティングシステムを実行しているコンピュータ上にサーバオペレーティングシステム上の Encryption がインストールされている場合、サーバモードが自動的にインストールされます。

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 画面で契約を読み、諸条件に同意して、**次へ** をクリックします。

5. オンプレミス *Dell* 管理サーバ を選択して、**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にインストールします。
7. **次へ** をクリックして、管理タイプ ダイアログをスキップします。
8. *Security Management Server* の名前に、デルサーバの完全修飾ホスト名を入力 / 検証して、ターゲットユーザーを管理します（*server.organization.com* など）。
   管理対象ドメインにドメイン名（organization など）を入力します。**次へ** をクリックします。
9. ポリシープロキシのホスト名とポートで、情報を入力 / 検証して **次へ** をクリックします。
10. デバイスサーバの URL で、情報を入力 / 検証して **次へ** をクリックします。
11. **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る場合があります。
12. 設定が完了したら、**終了** をクリックします。
    インストールが完了しました。
13. コンピュータを再起動します。作業を保存してアプリケーションを閉じるのに時間が必要な場合のみ、再起動をスヌーズすることをお勧めします。暗号化は、コンピュータが再起動されるまで開始できません。

コマンドラインを使用したインストール

インストーラーは `C:\extracted\Encryption` にあります。

- **DDPE_xxbit_setup.exe** を使用して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、インストールまたはアップグレードを行います。

スイッチ

次の表に、インストールで使用できるスイッチの詳細を示します。

スイッチ	意味
/v	DDPE_XXbit_setup.exe 内の .msi に変数を渡します。
/a	管理インストール

スイッチ	意味
/s	サイレントモード

パラメータ

次の表に、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。

コンポーネント	ログファイル	コマンドラインパラメータ
すべて	/l*v [fullpath][filename].log *	SERVERHOSTNAME=<Security Management Server Name>
		SERVERMODE=1
		POLICYPROXYHOSTNAME=<RGK Name>
		MANAGEDDOMAIN=<My Domain>
		DEVICESERVERURL=<Activation Server Name>
		GKPORT=<New GK Port>
		MACHINEID=<Machine Name>
		RECOVERYID=<Recovery ID>
		REBOOT=ReallySuppress
		HIDEOVERLAYICONS=1
		HIDESYSTRAYICON=1
		EME=1

メモ:
再起動を控えてもかまいませんが、最終的には再起動する必要があります。暗号化は、コンピュータが再起動されるまで開始できません。

オプション

次の表では、表示オプションが詳しく説明されています。これらのオプションは、/v スイッチに渡された引数の末尾に指定することができます。

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
/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

メモ:
同じコマンドライン内で **/q** と **/qn** を同時に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。

- コマンドラインパラメータ SERVERMODE=1 は、新規インストール時にのみ有効です。アンインストールでは、このパラメータは無視されます。

- 空白など、特殊文字を 1 つ以上含む値は、エスケープした引用符で囲みます。
- DEVICESERVERURL パラメーターでは、大文字と小文字が区別されます。

コマンドラインインストールの例

- 次の例では、Encryption、サイレントインストール、Encrypt for Sharing、ダイアログなし、プログレスバーなし、自動再起動、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection` にインストールというデフォルトのパラメーターでサーバオペレーティングシステムの Encryption をインストールします。

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
  ```

  MSI コマンド：

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn REBOOT="ReallySuppress"
  SERVERMODE="1" SERVERHOSTNAME="server.organization.com"
  POLICYPROXYHOSTNAME="rgk.organization.com" MANAGEDDOMAIN="ORGANIZATION"
  DEVICESERVERURL="https://server.organization.com:8443/xapi/"
  ```

- 次の例では、ログファイルと Encryption、サイレントインストール、Encrypt for Sharing、ダイアログなし、プログレスバーなし、再起動なし、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection\Encryption` というデフォルトのパラメーターでサーバオペレーティングシステムの Encryption をインストールし、このコマンドラインが同じサーバ上で複数回実行される場合は末尾の数字が 1 ずつ増えるカスタムログファイル名（DDP_ssos-090.log）を指定します。実行可能ファイルが格納されているデフォルトの場所以外にログの場所を指定するには、コマンドに完全なパスを指定します。たとえば、/l*v C:\Logs\DDP_ssos-090.log では、C:\Logs にインストールログが作成されます。

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERMODE=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /l*v DDP_ssos-090.log /
  norestart/qn"
  ```

  MSI コマンド：

  ```
  msiexec.exe /i "Dell Data Protection Encryption.msi" /qn SERVERMODE="1"
  SERVERHOSTNAME="server.organization.com" POLICYPROXYHOSTNAME="rgk.organization.com"
  MANAGEDDOMAIN="ORGANIZATION" DEVICESERVERURL="https://server.organization.com:8443/
  xapi/" /l*v DDP_ssos-090.log /norestart/qn"
  ```

インストール後にコンピュータを再起動します。作業を保存してアプリケーションを閉じるのに時間が必要な場合のみ、再起動をスヌーズすることをお勧めします。暗号化は、コンピュータが再起動されるまで開始できません。

アクティブ化

- サーバのコンピュータ名が、管理コンソールで表示させたいエンドポイント名になっていることを確認します。
- 初期アクティベーション目的のため、ドメイン管理者資格情報を有するインタラクティブユーザーが、少なくとも一度はサーバにログオンする必要があります。ログオンしたユーザーは、そのサーバにおいて、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あってもよいですが、アクティベーションにはドメイン管理者資格情報が必要です。
- インストール後の再起動に続いて、アクティブ化 ダイアログが表示されます。管理者は、ユーザープリンシパル名（UPN）形式のユーザー名でドメイン管理者資格情報を入力する必要があります。サーバオペレーティングシステムの Encryption は自動的にアクティブ化されません。
- 初期アクティベーション中、仮想サーバーユーザーアカウントが作成されます。初期アクティベーション後、コンピュータは再起動され、デバイスアクティベーションを開始できるようになります。
- 認証およびデバイスアクティベーションフェーズ中、コンピュータに固有のマシン ID が割り当てられ、暗号化キーが作成されてバンドルされ、暗号化キーバンドルと仮想サーバユーザーの間に関係が確立されます。暗号化キーバンドルは、暗号化キーおよびポリシーを新しい仮想サーバーユーザーと関連付けることで、暗号化されたデータ、特定のコンピュータ、および仮想サーバーユーザーの間に永続的な関係を確立します。デバイスアクティベーション後、仮想サーバユーザーは管理コンソールに SERVER-USER@<*fully qualified server name*> の形式で表示されます。アクティベーションの詳細については、「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」を参照してください。

メモ:

アクティベーション後にサーバの名前を変更しても、管理コンソールではそのサーバの表示名は変更されません。ただし、サーバ名が変更された後、サーバオペレーティングシステムの Encryption が再度アクティブ化されると、新しいサーバ名が管理コンソールに表示されます。

アクティブ化ダイアログは、再起動が終わるたびに表示され、サーバオペレーティングシステム上の Encryption をアクティブ化するようにユーザーを促します。アクティブ化を完了するには、次の手順を実行します。

1. サーバーに直接またはリモートデスクトップ接続を介してログオンします。

2. ドメイン管理者の UPN 形式のユーザー名とパスワードを入力し、**アクティブ化** をクリックします。これは、アクティブ化されていないシステムが再起動されるたびに表示される アクティブ化 ダイアログと同じものです。

   Dell Server は、マシン ID 用の暗号化キーの発行、**仮想サーバユーザーアカウント**の作成、ユーザーアカウント用の暗号化キーの作成、暗号化キーのバンドル化を行い、暗号化バンドルと仮想サーバユーザーアカウントの間の関係を確立します。

3. **閉じる** をクリックします。

   アクティベーション後、暗号化が開始されます。

4. 暗号化スイープが完了した後、前に使用中だったファイルを処理するために、コンピュータを再起動します。これは、セキュリティ上重要な手順です。

   メモ:

   Windows 資格情報のセキュア化ポリシーが有効な場合、サーバオペレーティングシステムの Encryption は Windows 資格情報を含む `\Windows\system32\config` ファイルを暗号化します。`\Windows\system32\config` 内のファイルは、*SDE* 暗号化有効ポリシーが無効の場合でも暗号化されます。デフォルトでは、*Windows* 資格情報のセキュア化ポリシーは選択済みです。

   メモ:

   コンピュータの再起動後、共有暗号化キーの認証には保護対象サーバのマシンキーが常に必要となります。Dell Server は、ヴォールト内の暗号化キーとポリシーにアクセスするためにロック解除キーを返します（キーとポリシーは、ユーザーではなくサーバ用です）。サーバのマシンキーなしでは、共有暗号化キーのロックを解除することはできず、コンピュータはポリシーアップデートを受信することができません。

アクティベーションの確認

ローカルコンソールから、**バージョン情報**ダイアログを開いて、サーバオペレーティングシステムの Encryption がインストール済みかつ認証済みであり、サーバモードで動作していることを確認します。暗号化クライアント ID が**赤色**で表示されている場合、暗号化はアクティブ化されていません。

仮想サーバユーザー

- 管理コンソールでは、保護対象サーバはそのマシン名の下で確認できます。さらに、各保護対象サーバーは、独自の仮想サーバーユーザーアカウントを持っています。各アカウントには、固有の静的ユーザー名と固有のマシン名があります。
- 仮想サーバユーザーアカウントは、サーバオペレーティングシステム上の Encryption によってのみ使用され、それ以外の面では保護対象サーバの動作に対して透過的です。仮想サーバユーザーは、暗号化キーバンドルとポリシープロキシに関連付けられます。
- アクティベーション後、仮想サーバーユーザーアカウントは、アクティブ化済みで、サーバーに関連付けられているユーザーアカウントです。
- 仮想サーバーユーザーアカウントがアクティブ化された後、すべてのサーバーログオン / ログオフ通知は無視されます。代わりに、コンピュータは起動中に仮想サーバユーザーで自動的に認証し、デルサーバからマシンキーをダウンロードします。

SED Manager と PBA Advanced Authentication のインストール

- EnTrust または Verisign などのルート証明機関によって署名された証明書を組織で使用している場合は、「SED 要件」を見直します。SSL/TLS 信頼検証を有効にするには、クライアントコンピュータでレジストリ設定を変更する必要があります。
- ユーザーは、Windows 資格情報を使用して PBA にログインします。
- SED Manager および PBA Advanced Authentication インストーラーは次の場所にあります。
  - **dell.com/support** - 必要に応じて、dell.com/support からソフトウェアを入手して、マスターインストーラから子インストーラを抽出します。抽出後、`C:\extracted\Encryption Management Agent` でファイルを見つけます。
  - **お使いの Dell FTP アカウントから** - Encryption-Enterprise-10.x.x.xxx.zip でインストールバンドルを見つけてから、マスターインストーラから子インストーラを抽出します。抽出後、`C:\extracted\Encryption Management Agent` でファイルを見つけます。

コマンドラインでのインストール

- 次の表に、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
CM_EDITION=1 <remote management>

パラメータ
INSTALLDIR=<change the installation destination>
SERVERHOST=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>
SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list>

コマンドラインで使用することができる基本的な .msi スイッチと表示オプションのリストについては、「子インストーラを使用したインストール」を参照してください。

以下は、Encryption Management Agent をインストールまたはアップグレードするコマンドの例です。

コマンドラインの例

\Encryption Management Agent

- 次の例では、サイレント インストール、再起動なし、コントロール パネルのプログラム リストにエントリーなし、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection\Encryption` にインストールという設定で、リモート管理される SED Manager、Encryption Management Agent、ローカル セキュリティ コンソールをインストールします。

```
EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
ARPSYSTEMCOMPONENT=1 /norestart /qn"
```

BitLocker Manager のインストール

- **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。

- EnTrust または Verisign などのルート証明機関によって署名された証明書を組織で使用している場合は、「BitLocker Manager クライアントの要件」 を見直します。SSL/TLS 信頼検証を有効にするには、クライアントコンピュータでレジストリ設定を変更する必要があります。
- BitLocker Manager クライアントインストーラは、次の場所に置かれます。
  - **dell.com\support** - 必要に応じて、dell.com\support からソフトウェアを入手して、マスターインストーラから子インストーラを抽出します。抽出後、`C:\extracted\Encryption Management Agent` でファイルを見つけます。
  - **お使いの Dell FTP アカウントから** - Encryption-Enterprise-10.x.x.xxx.zip でインストールバンドルを見つけてから、マスターインストーラから子インストーラを抽出します。抽出後、`C:\extracted\Encryption Management Agent` でファイルを見つけます。

コマンドラインでのインストール

- 次の表に、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
CM_EDITION=1 <remote management>
INSTALLDIR=<change the installation destination>
SERVERHOST=<securityserver.organization.com>
SERVERPORT=8888
SECURITYSERVERHOST=<securityserver.organization.com>

パラメータ
SECURITYSERVERPORT=8443
FEATURE=BLM <install BitLocker Manager only>
FEATURE=BLM,SED <install BitLocker Manager with SED>
ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list>

コマンドラインで使用可能な基本的な .msi スイッチおよび表示オプションについては、「子インストーラを使用したインストール」を参照してください。

コマンドラインの例

- 次の例では、サイレントインストール、再起動なし、コントロールパネルプログラム リストにエントリしない、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection` にインストールするという設定で、BitLocker Manager のみをインストールします。

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM /norestart /qn"
  ```

- 次の例では、サイレントインストール、再起動なし、コントロールパネルプログラム リストにエントリしない、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection` にインストールという設定で、BitLocker Manager を SED と一緒にインストールします。

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM,SED /norestart /qn"
  ```

- **BitLocker Manager と Dell Encryption をインストールするためのコマンドラインの例**

  次の例では、サイレントインストール、再起動なし、コントロールパネルプログラム リストにエントリしない、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection` にインストールするという設定で、BitLocker Manager のみをインストールします。

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM /norestart /qn"
  ```

  次の操作：

  次の例では、Encryption クライアントと Encrypt for Sharing、ダイアログなし、プログレスバーなし、自動再起動、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection` にインストールというデフォルトのパラメータでクライアントをインストールします。

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /qn"
  ```

7

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、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述されているように、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
/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 およびサーバオペレーティングシステム上の Encryption 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。
- クライアントのアンインストールプロセスの開始時に、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管理対象レポートで想定どおりに［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

- **アンインストール処理を開始する前に**、（オプション）Encryption Removal Agent のログ ファイルの作成を参照してください。このログファイルは、アンインストールや復号化操作のトラブルシューティングを行う際に便利です。アンインストール処理中にファイルの復号化を行うつもりがない場合は、Encryption Removal Agent ログファイルを作成する必要はありません。
- **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、Security Management 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。
- WSScan を実行して、アンインストールが完了した後でコンピュータを再起動する前に、すべてのデータが復号化されていることを確認します。手順については、WSScan の使用を参照してください。
- 「Encryption Removal Agent ステータスのチェック」を定期的に行ってください。Encryption Removal Agent サービスが引き続きサービスパネルに存在している場合、データ復号化はまだ進行中です。

コマンドラインでのアンインストール

- Encryption インストーラーは、マスター インストーラーから抽出された後、`C:\extracted\Encryption\DDPE_XXbit_setup.exe` にあります。
- 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 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

パラメータ	選択
	1 - サイレント - /q または/qn を含む msiexec 変数を使用して実行する場合に必須 0 - 非サイレント - /q を含む msiexec 変数がコマンドライン構文に存在しない場合にのみ利用可
必須のプロパティ	
DA_KM_PATH	keybundle への完全修飾パス。
DA_KM_PW	keybundle に設定されたパスワード。
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 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 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。

- 次の例では、フォレンジック管理者パスワードを使用し、C:\Users\administrator\Desktop\Admin\にある事前ダウンロード済みキーを使用して Encryption をサイレント アンインストールし、C:\SheildUninstall にログを書き込みます。

  ```
  DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=2 CMGSILENT=1
  DA_KM_PATH=C:\Users\administrator\Desktop\Admin\<HOSTNAME>.bin DA_KM_PW=qwert12345 /l*v
  c:\ShieldUninstall.log /qn /norestart"
  ```

  MSI コマンド

  ```
  msiexec.exe /s /x "Dell Data Protection Encryption.msi" CMG_DECRYPT=2 CMGSILENT=1
  DA_KM_PATH=C:\Users\administrator\Desktop\Admin\<HOSTNAME>.bin DA_KM_PW=qwert12345 /l*v
  c:\ShieldUninstall.log /qn /norestart
  ```

メモ:

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。

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"
```

Encryption External Media のアンインストール

Encryption インストーラーは、マスター インストーラーから解凍した後、`C:\extracted\Encryption\DDPE_XXbit_setup.exe` で見つけることができます。

コマンドラインでのアンインストール

次のようなコマンドラインを実行します。

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

終了したらコンピュータを再起動します。

フル ディスク暗号化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。コンピューターからすべての PBA データが削除され、フル ディスク暗号化キーがロック解除されます。
- フル ディスク暗号化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. [**Windows 暗号化**] グループから [**フル ディスク暗号化**] を選択します。
9. [**フル ディスク暗号化**] 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 を無効にした後、フル ディスク暗号化および PBA Advanced Authentication をアンインストールします。

フル ディスク暗号化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 インストーラーから抽出されたフル ディスク暗号化は、`C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe` に置かれます。
  - 次の例は、フル ディスク暗号化をサイレント 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。

SED Manager 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 Manager 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 を無効にした後、SED Manager と PBA Advanced Authentication 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 インストーラーから抽出された SED Manager インストーラーは、`C:\extracted\Encryption Management Agent\EMAgent_XXbit_setup.exe` に置かれます。
  - 次の例は、SED Manager 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 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 BitLocker Manager 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、BitLocker Manager 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。

8

Data Security アンインストーラ

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。

この Data Security アンインストーラーは、次のフォルダーにあります： `C:\Program Files (x86)\Dell\Dell Data Protection`

詳細またはコマンド ライン インターフェイス（CLI）の使用方法については、KB 記事 125052 を参照してください。

`C:\ProgramData\Dell\Dell Data Protection\`に、削除されたすべてのコンポーネントのログが生成されます。

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

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。

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 を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。

9

一般的なシナリオ

- 各クライアントを個別に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、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。
- 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。
- 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、クライアントをインストールします。
- コマンドラインの例では、再起動は省略されています。ただし、最終的には再起動する必要があります。暗号化は、コンピュータが再起動されるまで開始できません。
- ログファイル - Windows は、`C:\Users\<UserName>\AppData\Local\Temp.` にある %temp% に、ログインしたユーザー用の固有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。

  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。`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。

- 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	*.exe 内の .msi に変数を渡す
/s	サイレントモード
/i	インストールモード

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
/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

- 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 の各機能の使用方法については、*Dell Encrypt* 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\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。
  - の機能の使用方法については、*Encryption Enterprise* のヘルプ を参照してください。ヘルプには、<インストール先ディレクトリ>`:\Program Files\Dell\Dell Data Protection\Authentication \Help` からアクセスしてください。

Encryption クライアント、、

- 次の例では、サイレントインストール、再起動なし、コントロールパネルプログラムリストにエントリなし、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection\Encryption` にインストールという設定で、SED 管理および Encryption Management Agent をインストールします。

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  ARPSYSTEMCOMPONENT=1 /norestart /qn"
  ```

  次の操作：

- 次の例では、Encryption と Encrypt for Sharing、ダイアログなし、プログレスバーなし、再起動なし、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection\Encryption` にインストールというデフォルトのパラメーターで Encryption をインストールします。

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /norestart /qn"
  ```

  Security Management Server が v7.7 より前の場合は、 `DEVICESERVERURL=https://server.organization.com:`**`8081/xapi`**（末尾のスラッシュなし）を置き換えます。

SED Manager（Advanced Authentication を含む）および Encryption クライアント

- 次の例では、指定した場所に、TPM 用の信頼済みソフトウェアスタック（TSS）、および Microsoft ホットフィックスのドライバをインストールし、コントロールパネルプログラムリストにはエントリを作成せず、再起動は実行しません。

  これらのドライバは Encryption クライアントをインストールする際にインストールする必要があります。

  ```
  setup.exe /S /z"\"InstallPath=<c:\location>, ARPSYSTEMCOMPONENT=1, SUPPRESSREBOOT=1\""
  ```

  次の操作：

- 次の例では、サイレント インストール、再起動なし、コントロール パネル プログラム リストにエントリーなし、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection` にインストールという設定で、リモート管理される SED Manager をインストールします。

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  ARPSYSTEMCOMPONENT=1 /norestart /qn"
  ```

  次の操作：

- 次の例では、サイレントインストール、再起動なし、デフォルト場所の `C:\Program Files\Dell\Dell Data Protection\Authentication` にインストールするという設定で Advanced Authentication をインストールします。

  ```
  setup.exe /s /v"/norestart /qn ARPSYSTEMCOMPONENT=1"
  ```

  次の操作：

- 次の例では、Encryption クライアントと Encrypt for Sharing、ダイアログなし、プログレスバーなし、再起動なし、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection` にインストールというデフォルトのパラメータでクライアントをインストールします。

  ```
  DDPE_XXbit_setup.exe /s /v"SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com MANAGEDDOMAIN=ORGANIZATION
  DEVICESERVERURL=https://server.organization.com:8443/xapi/ /norestart /qn"
  ```

  Security Management Server が v7.7 より前の場合は、 `DEVICESERVERURL=https://server.organization.com:`**`8081/xapi`**（末尾のスラッシュなし）を置き換えます。

SED Manager および Encryption External Media

- 次の例では、サイレント インストール、再起動なし、コントロール パネルのプログラム リストにエントリーなし、デフォルトの場所 `C:\Program Files\Dell\Dell Data Protection\Encryption` にインストールという設定で、SED Manager、Encryption Management Agent、ローカル セキュリティ コンソールをインストールします。

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  ARPSYSTEMCOMPONENT=1 /norestart /qn"
  ```

  次の操作：

- 次の例では、サイレントインストール、再起動なし、デフォルト場所の `C:\Program Files\Dell\Dell Data Protection` にインストールするという設定で Encryption External Media のみをインストールします。

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com DEVICESERVERURL=https://
  server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /norestart /qn"
  ```

  Security Management Server が v7.7 より前の場合は、 `DEVICESERVERURL=https://server.organization.com:` **`8081/xapi`**（末尾のスラッシュなし）を置き換えます。

BitLocker Manager と Encryption External Media

- BitLocker Manager と Encryption External Media は、暗号化シーケンスに基づいて相互作用します。BitLocker Manager 暗号化ドライブを Encryption External Media を使用しているコンピュータに挿入する場合、Encryption External Media がドライブを読み取って暗号化をする前に BitLocker Manager のパスワードを**入力する必要があります。**
- Encryption External Media がドライブ上でアクティブになっている場合、BitLocker Manager の暗号化を同じドライブに適用できます。
- 次の例では、再起動なしのサイレントインストール、コントロールパネルのプログラムリストにエントリなし、デフォルトの場所（`C:\Program Files\Dell\Dell Data Protection`）にインストールという設定で、BitLocker Manager をインストールします。

  ```
  EMAgent_XXbit_setup.exe /s /v"CM_EDITION=1 SERVERHOST=server.organization.com
  SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443
  FEATURE=BLM /norestart /qn"
  ```

  次の操作：

- 次の例では、サイレントインストール、再起動なし、デフォルト場所の `C:\Program Files\Dell\Dell Data Protection` にインストールするという設定で Encryption External Media のみをインストールします。

  ```
  DDPE_XXbit_setup.exe /s /v"EME=1 SERVERHOSTNAME=server.organization.com
  POLICYPROXYHOSTNAME=rgk.organization.com DEVICESERVERURL=https://
  server.organization.com:8443/xapi/ MANAGEDDOMAIN=ORGANIZATION /norestart /qn"
  ```

Security Management Server が v7.7 より前の場合は、 `DEVICESERVERURL=https://server.organization.com:` **`8081/xapi`**（末尾のスラッシュなし）を置き換えます。

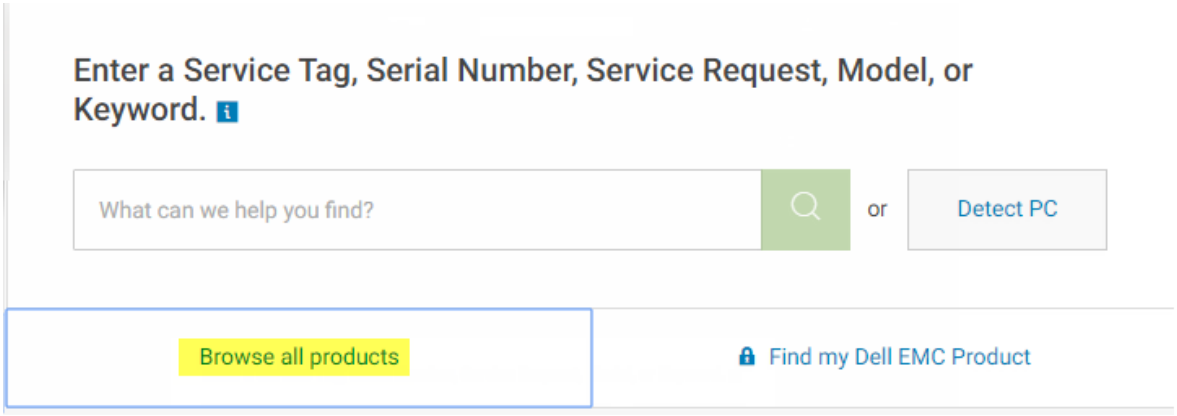
10

ソフトウェアのダウンロード

このセクションでは、dell.com/support からソフトウェアを取得する方法の詳細について説明します。ソフトウェアをすでに取得している場合は、本項を省略できます。

dell.com/support にアクセスして手順を開始します。

1. Dell サポート Web ページで、［**すべての製品の参照**］を選択します。



2. 製品のリストから **セキュリティ** を選択します。
3. **Dell Data Security** を選択します。

   一度選択を行った内容は、Web サイトに記憶されます。
4. デル製品を選択します。

   例：

   Dell Encryption Enterprise

   Dell Endpoint Security Suite Enterprise
5. **ドライバおよびダウンロード** を選択します。
6. 目的のクライアントのオペレーティングシステムの種類を選択します。
7. 一致する **Dell Encryption** を選択します。これは一例ですので、実際には内容が一部異なる場合があります。たとえば、選択対象は 4 ファイルとは限りません。
8. ［**ダウンロード**］を選択します。

11

SED UEFI および BitLocker Manager のための事前インストール設定

TPM の初期化

- ローカル管理者グループまたは同等のグループのメンバーである必要があります。
- コンピュータには互換性のある BIOS および TPM が搭載されている必要があります。
- http://technet.microsoft.com/en-us/library/cc753140.aspx に記載された指示に従ってください。

UEFI コンピュータ用の事前インストール設定

UEFI 起動前認証中におけるネットワーク接続の有効化

UEFI ファームウェア搭載のコンピュータで起動前認証を正常に行うには、PBA にネットワーク接続が必要です。デフォルトでは、UEFI ファームウェア搭載のコンピュータには、オペレーティングシステムがロードされるまでネットワーク接続がなく、これは PBA モードの後で実行されます。

次の手順は、UEFI 対応のコンピュータ用の PBA 中にネットワーク接続を有効にします。設定手順は UEFI コンピュータモデルによって異なるので、次の手順は一例に過ぎません。

1. UEFI ファームウェア設定を開始します。
2. 起動中に、「ワンタイム起動メニューの準備中」のようなメッセージが画面の右上に表示されるまで、F2 キーを押し続けます。
3. プロンプトが表示されたら、BIOS 管理者パスワードを入力します。

   メモ:

   通常、新しいコンピュータの場合は BIOS パスワードが設定されていないため、入力が求められることはありません。
4. **システム設定** を選択します。
5. **統合 NIC** を選択します。
6. **UEFI ネットワークスタックを有効にする** チェックボックスをオンにします。
7. **有効** または **PXE で有効** を選択します。
8. **適用** を選択します。

   メモ:

   UEFI ファームウェア非搭載のコンピュータには、設定は不要です。

レガシーオプション ROM の無効化

BIOS で **レガシーオプション ROM を有効にする** 設定が無効化されていることを確認します。

1. コンピュータを再起動します。
2. 再起動中に、繰り返し **F12** を押して UEFI コンピュータの起動設定を表示します。
3. 下向き矢印を押して **BIOS 設定** オプションをハイライト表示し、**Enter** を押します。
4. **設定** > **一般** > **詳細起動オプション** の順に選択します。
5. **レガシーオプション ROM を有効にする** チェックボックスのチェックを外して、**適用** をクリックします。

BitLocker PBA パーティションを設定する事前インストール設定

- BitLocker Manager をインストールする **前に**、PBA パーティションを作成しておく必要があります。
- TPM をオンにしてアクティブ化**してから**、BitLocker Manager をインストールします。BitLocker Manager が TPM の所有権を取得します（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 が暗号化セットアッププロセスを開始します。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。
- 場合によっては、ディスクのパーティションを手動で作成する必要があります。詳細については、BitLocker ドライブ準備ツールについての Microsoft による説明を参照してください。
- BdeHdCfg.exe コマンドを使用して PBA パーティションを作成します。default パラメータを指定すると、コマンドラインツールは BitLocker セットアップウィザードと同じ手順に従います。

```
BdeHdCfg -target default
```

メモ:

BdeHdCfg コマンドで使用可能な追加オプションについては、「Microsoft の BdeHdCfg.exe パラメーターリファレンス」を参照してください。

12

レジストリーによる Dell Server の指定

- クライアントの利用資格を Dell Digital Delivery を使用して取得した場合、次の手順に従ってグループ ポリシー オブジェクトによりレジストリーを設定し、インストール後に使用する Dell サーバーを事前設定します。
- ワークステーションは、グループ ポリシー オブジェクトを適用する OU のメンバーである必要があります。さもなければ、エンドポイントでレジストリー設定を手動で行う必要があります。
- Dell Server から cloud.dell.com への通信に送信ポート 443 が使用可能であることを確認します。ポート 443 が（何らかの理由で）ブロックされている場合、利用資格を取得することはできず、その資格は利用可能なプールから消尽されます。

  メモ: Dell Digital Delivery を使用してインストールするときにこのレジストリー値を設定しなかった場合、またはマスター インストーラーでサーバーを指定しなかった場合には、アクティベーション URL はデフォルトの 199.199.199.199 に設定されます。

レジストリー キーの手動での設定

エンドポイントがドメインに参加していない場合、またはグループ ポリシー オブジェクトを設定できない環境である場合は、インストール中に特定の Dell Server に対してアクティブ化が行われるようにレジストリー キーを事前設定します。

1. タスクバーの検索ボックスに「**regedit**」と入力し、右クリックして［**管理者として実行**］を選択します。
2. 次のレジストリーに移動してレジストリー キーを作成します。

   HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Data Protection

   REG_SZ：Server

   値：<Dell Server の FQDN または IP アドレス>

3. Dell Digital Delivery またはマスター インストーラーを使用して Encryption をインストールします。

グループ ポリシー オブジェクトの作成

1. クライアントを管理するドメインコントローラで、**スタート** > **管理ツール** > **グループポリシーの管理** の順にクリックします。
2. ポリシーが適用される OU を右クリックし、［**このドメインでの GPO の作成**］と［**このコンテナにリンクする**］を選択します。
3. 新しい GPO の名前を入力し、ソーススターター GPO には （なし） を選択して、**OK** をクリックします。
4. 作成された GPO を右クリックして **編集** を選択します。
5. グループポリシー管理エディタがロードされます。**コンピュータ設定** > **プリファレンス** > **Windows 設定** > **レジストリ** の順にアクセスします。
6. レジストリを右クリックし、**新規** > **レジストリ項目** の順に選択します。次のように設定します。

   アクション：作成

   ハイブ：HKEY_LOCAL_MACHINE

   キーパス：SOFTWARE\Dell\Dell Data Protection

   値の名前：Server

   値の種類：REG_SZ

   値のデータ：<Dell Server の FQDN または IP アドレス>

7. **OK** をクリックします。
8. ログアウトしてもう一度ワークステーションにログイン、または **`gpupdate /force`** を実行してグループ ポリシーを適用します。

13

子インストーラの抽出

- 各クライアントを個別にインストールするには、子の実行可能ファイルをインストーラから抽出します。
- 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. Dell インストール メディアから、**DDSSetup.exe** ファイルをローカル コンピューターにコピーします。
2. **DDSSetup.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。

   ```
   DDSSetup.exe /s /z"\"EXTRACT_INSTALLERS=C:\Extracted""
   ```

   抽出パスは 63 文字を超えられません。

   インストールを開始する前に、すべての前提条件が満たされており、インストールする予定の各子インストーラに対して必要なすべてのソフトウェアがインストールされていることを確認します。参照を 要件の 詳細については。

   抽出した子インストーラは `C:\extracted\.`

14

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。

  Key Server は、ソケット上で接続されるクライアントをリスンするサービスです。クライアントが接続されたら、Kerberos API を使用して、セキュア接続のネゴシエーション、認証、暗号化が行われます。セキュア接続がネゴシエーションできない場合、クライアントが切断されます。

  Key Server は、クライアントを実行しているユーザーがキーにアクセスできるかどうかを Security Server（以前の Device Server）に確認します。このアクセスは、管理コンソールの個々のドメインを介して付与されます。

- 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。

   「superadmin」形式には、Security Management Server に対する認証を行うことが可能な任意の方法を使用できます。SAM アカウント名、UPN、または DOMAIN\Username を使用できます。Active Directory に対する承認のためのユーザーアカウントには検証が必要であることから、Security Management Server に対して認証できる方法ならどれでも使用できます。

   例えば、マルチドメイン環境では、「jdoe」などの SAM アカウント名のみを入力すると失敗する場合があります。これは、Security Management Server が「jdoe」を見つけられず、「jdoe」を認証できないためです。マルチドメイン環境では、UPN が推奨されますが、DOMAIN\Username の形式も使用できます。単一ドメイン環境では、SAM アカウント名が容認できます。
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。

サンプル設定ファイル

<?xml version="1.0" encoding="utf-8" ?>

<configuration>

<appSettings>

<add key=”port” value=”8050" /> [Key Server がリッスンする TCP ポート。デフォルトは 8050 です。]

<add key=”maxConnections” value=”2000” /> [Key Server で許可されるアクティブなソケット接続数]

<add key="url" value="https://keyserver.domain.com:8443/xapi/" /> [Security Server（以前の Device Server）URL（v7.7 より前の Security Management Server では、形式は 8081/xapi）]

<add key="verifyCertificate" value="false" /> [true では証明書が検証されます / 検証しない場合、または自己署名暗号化を使用する場合は false に設定してください]

<add key=”user” value=”superadmin” /> [Security Server との通信に使用されるユーザー名。このユーザーには、管理コンソールで選択した管理者ロールが必要です。「superadmin」形式には、Security Management Server に対する認証を行うことが可能な任意の方法を使用できます。SAM アカウント名、UPN、または DOMAIN\Username を使用できます。Active Directory に対する承認のためのユーザーアカウントには検証が必要であることから、Security Management Server に対して認証できる方法ならどれでも使用できます。例えば、マルチドメイン環境では、「jdoe」などの SAM アカウント名のみを入力すると失敗する場合があります。これは、Security Management Server が「jdoe」を見つけられず、「jdoe」を認証できないためです。マルチドメイン環境では、UPN が推奨されますが、DOMAIN\Username の形式も使用できます。単一ドメイン環境では、SAM アカウント名を容認できます。]

<add key="cacheExpiration” value="30" /> [誰がキーの要求を許可されているかをサービスがチェックする必要がある頻度（秒単位）。このサービスは、キャッシュを維持して、キャッシュがどれほど古いかを追跡します。キャッシュがこの値より古くなると、新しいリストが取得されます。ユーザーが接続するときに、Key Server は権限のあるユーザーを Security Server からダウンロードする必要があります。ユーザーのキャッシュがない場合、または最後の「x」秒でリストがダウンロードされなかった場合は、再度ダウンロードされます。ポーリングはありませんが、この値によって、リストがどの程度古くなったときに、必要に応じてリストが更新されるかが設定されます。]

<add key="epw" value="encrypted value of the password" /> [Security Management Server との通信に使用されるパスワード。superadmin パスワードが変更された場合、ここで変更する必要があります。]

</appSettings>

</configuration>

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。

15

Administrative Download Utility（CMGAd）の使用

- このユーティリティを使用して、デルサーバに接続していないコンピュータで使用する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ーに応じて、次のいずれかの方法でキーマテリアルの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。お使いのデルサーバが v7.7 より前の場合は、書式は https://deviceserver.domain.com:8081/xapi（ポート番号が違う、末尾のスラッシュなし）です。

   デル管理者：JDOE など、フォレンジック管理者の資格情報を持つ管理者の名前（管理コンソールで有効にする）

   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

   メモ:

   通常は 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、このユーティリティが使用する情報が別々に含まれています。

   次へ をクリックします。
3. パスフレーズ：には、ダウンロードファイルを保護するための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使用するか、... 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。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

メモ:

通常は 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、このユーティリティが使用する情報が別々に含まれています。

次へ をクリックします。

3. パスフレーズ：には、ダウンロードファイルを保護するための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使用するか、... 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。

16

サーバオペレーティングシステムの Encryption の設定

サーバオペレーティングシステム上の Encryption の有効化

メモ:

サーバオペレーティングシステムの Encryption により、ユーザー暗号化が共通暗号化に変換されます。

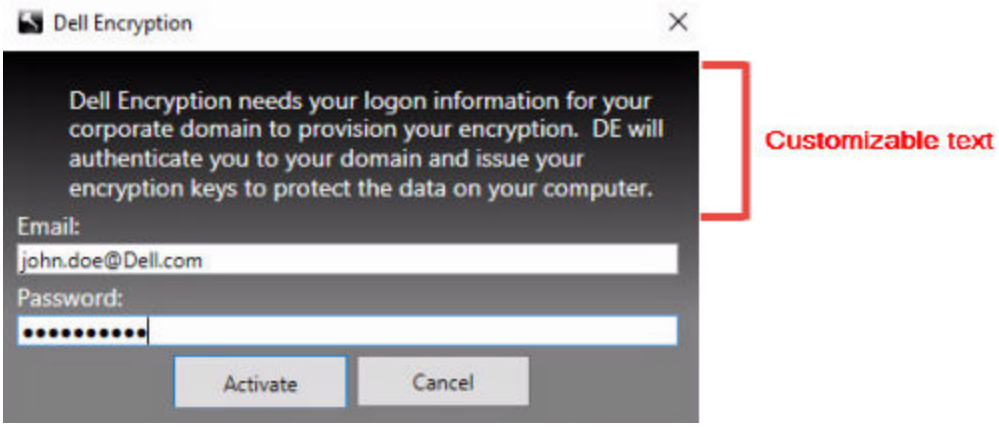
1. 管理コンソールに Dell 管理者としてログインします。
2. **エンドポイントグループ**（または **エンドポイント**）を選択し、有効にするエンドポイントまたはエンドポイントグループを検索して **セキュリティポリシー** を選択した後、**Server Encryption** ポリシーカテゴリを選択します。
3. 次のポリシーを設定します。
   - Server Encryption - **選択して**サーバオペレーティングシステム上の Encryption と関連するポリシーを有効にします。
   - SDE Encryption 有効 - **選択して** SDE 暗号化をオンにします。
   - 暗号化有効 - **選択して**共有暗号化をオンにします。
   - Windows 資格情報のセキュア化 - デフォルトでこのポリシーが**選択**されています。

     Windows 資格情報のセキュア化ポリシーが**選択されている**（デフォルト）場合は、\Windows\system32\config ファイルフォルダ内にある Windows 資格情報も含めたすべてのファイルが暗号化されます。Windows 資格情報が暗号化されないようにするには、*Windows* 資格情報のセキュア化ポリシーを［**選択しない**］に設定します。Windows 資格情報の暗号化は、*SDE* 暗号化有効 ポリシーの設定とは無関係に行われます。
4. ポリシーを保存してコミットします。

アクティベーションログオンダイアログのカスタマイズ

アクティブ化ログオン ダイアログは、次の場合に表示されます。

- 管理対象外のユーザーがログオンするとき。
- ユーザーが通知領域にある Encryption アイコンのメニューから Dell Encryption のアクティブ化 を選択するとき。



Encryption External Media ポリシーの設定

暗号化開始コンピュータ とは、リムーバブルデバイスを最初に暗号化するコンピュータです。暗号化開始コンピュータが**保護対象サーバ**（サーバオペレーティングシステム上の Encryption がインストール、アクティブ化されているサーバ）で、その保護対象サーバがリムーバブルデバイスの存在を初めて検知するとき、リムーバルデバイスを暗号化するためのプロンプトがユーザーに表示されます。

- Encryption External Media ポリシーは、リムーバブルメディアのサーバへのアクセス、認証、暗号化などを制御します。
- ポート制御ポリシーは、例えば、USB デバイスによるサーバの USB ポートへのアクセスおよび使用を制御することにより、保護対象サーバ上のリムーバブルメディアに影響します。

リムーバブルメディア暗号化用のポリシーは、管理コンソールの *Server Encryption* テクノロジグループにあります。

サーバオペレーティングシステム上の Encryption および外部メディア

保護対象サーバーの *EMS* 暗号化外部メディアポリシー**選択されている場合**、外部メディアは暗号化されます。Encryption はマシンキーでそのデバイスを保護対象サーバに関連付け、リムーバブルデバイスの所有者 / ユーザーのユーザーローミングキーでデバイスをユーザーに関連付けます。その後でリムーバルデバイスに追加されるすべてのファイルは、デバイスの接続先のコンピュータに関わらず、これら同じキーで暗号化されます。

メモ:

サーバオペレーティングシステム上の Encryption はユーザー暗号化を共有暗号化に変換しますが、リムーバブルデバイス上では行われません。リムーバブルデバイス上では、コンピュータに関連付けられているユーザーローミングキーで暗号化が実行されます。

ユーザーがリムーバブルデバイスの暗号化に同意しない場合、デバイスへのユーザーアクセスは、保護対象サーバ上で使用されるときは ブロック、保護対象サーバ上で使用されるときは 読み取り専用 または 完全アクセス に設定することができます。保護対象サーバーのポリシーは、保護されていないリムーバブルデバイス上でのアクセスレベルを決定します。

リムーバブルデバイスが保護対象の暗号化開始サーバに再挿入されると、ポリシーアップデートが行われます。

認証と外部メディア

保護対象サーバーのポリシーは、認証機能を決定します。

リムーバブルデバイスの暗号化が完了すると、保護対象サーバー上でそのリムーバブルデバイスにアクセスできるのは、そのデバイスの所有者 / ユーザーのみになります。それ以外のユーザーは、そのリムーバブルメディアの暗号化されたファイルにアクセスできなくなります。

ローカル自動認証では、そのメディアの所有者がログインしているときに保護対象リムーバブルストレージが保護対象サーバーに挿入されると、そのメディアを自動認証することが可能になります。自動認証が無効になっている際には、所有者 / ユーザーが保護対象リムーバブルデバイスへのアクセスを認証する必要があります。

リムーバブルデバイスの暗号化開始コンピュータが保護対象サーバの場合、所有者 / ユーザーは、暗号化を開始したコンピュータ以外のコンピュータ上でリムーバブルデバイスを使用している際に、その他のコンピュータ上で定義されている Encryption External Media ポリシーに関わらず、常にそのリムーバブルデバイスにログインする必要があります。

Server Encryption のポート制御および Encryption External Media ポリシーの詳細については管理者ヘルプを参照してください。

サーバオペレーティングシステム上の Encryption の中断

暗号化されたサーバーをサスペンドすることで、再起動後のそのサーバーの暗号化されたデータへのアクセスを防ぎます。仮想サーバーのユーザーをサスペンドすることはできません。代わりに、暗号化されたサーバのマシンキーがサスペンドされます。

メモ:

サーバーのエンドポイントをサスペンドしても、サーバーはすぐにはサスペンドされません。このサスペンドは、キーが次に要求されたとき（通常はサーバーが次に再起動されたとき）に行われます。

メモ:

使用する際は注意が必要です。暗号化されたサーバをサスペンドすると、ポリシー設定、または保護対象サーバがネットワークから切断されているかどうかにより、不安定になることがあります。

動作条件

- エンドポイントをサスペンドするには、管理コンソールで割り当てられたヘルプデスク管理者の権限が必要です。
- 管理者が管理コンソールにログインしている必要があります。

  管理コンソールの左ペインで、**ポピュレーション** > **エンドポイント**をクリックします。

  ホスト名を検索または選択してから、**詳細とアクション** タブをクリックします。

  サーバデバイス制御 の下で、**サスペンド**、**はい** の順にクリックします。

  メモ:

  復帰 をクリックすると、サーバオペレーティングシステムの Encryption は再起動後にサーバ上の暗号化データにアクセスできるようになります。

17

Deferred Activation の設定

Deferred Activation が付属した Encryption クライアントは、2 つの点で Encryption クライアントのアクティベーションと異なります。

デバイスベースの暗号化ポリシー

Encryption クライアントのポリシーはユーザーベースですが、Deferred Activation 付属の Encryption クライアントの暗号化ポリシーはデバイスベースです。ユーザー暗号化は共有暗号化に変換されます。この違いによって、ユーザーは組織のドメイン内で個人的なデバイスを使用することができます。組織は暗号化ポリシーを一元管理することでセキュリティを維持します。

アクティベーション

Encryption クライアントでは、アクティベーションは自動で行われます。Deferred Activation が と一緒にインストールされる場合、自動アクティベーションが無効になります。代わりに、ユーザーは暗号化をアクティブ化するかどうか、いつアクティブ化するかを選択できます。

メモ:

ユーザーは組織を完全に離れる場合、離れる前の自分の電子メールアドレスがアクティブな間に Encryption 削除エージェントを実行して、自分の個人用コンピュータから Encryption クライアントをアンインストールする必要があります。

Deferred Activation のカスタマイズ

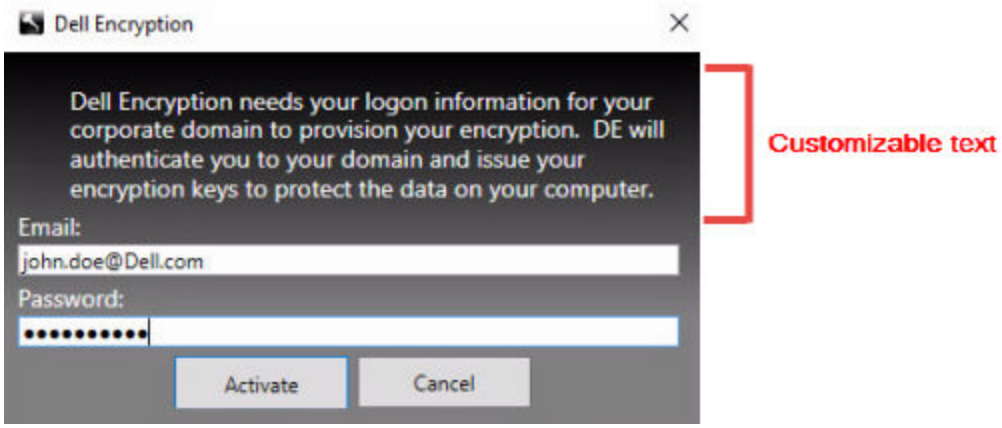
以下のクライアント側タスクで Deferred Activation をカスタマイズできます。

- アクティブ化の際のログオンダイアログボックスに免責事項を追加する
- 自動再アクティブ化を無効にする（オプション）

  アクティブ化の際のログオンダイアログボックスに免責事項を追加する

  アクティブ化の際のログオンダイアログは次の場合に表示されます。

- 管理対象外のユーザーがログオンするとき。
- ユーザーが通知領域にある Encryption アイコンのメニューから Dell Encryption のアクティブ化 を選択するとき。



インストールのためのコンピュータの準備

データがデル以外の暗号化製品で暗号化されている場合は、Encryption クライアントをインストールする前に、既存の暗号化ソフトウェアを使用してデータを復号化し、次に既存の暗号化ソフトウェアをアンインストールします。コンピュータが自動的に再起動しない場合は、コンピュータを再起動します。

Windows パスワードの作成

デルでは、暗号化データへのアクセスを保護するため、Windows パスワードの作成を強く推奨しています（まだパスワードが存在しない場合）。コンピュータにパスワードを作成すると、他のユーザーがパスワードなしでユーザーアカウントにログインすることを防止できます。

旧バージョンの Encryption クライアントのアンインストール

旧バージョンの Encryption クライアントをアンインストールする前に、必要に応じて、暗号化スイープを停止または一時停止します。

コンピュータがバージョン 8.6 より前のバージョンの Dell Encryption を実行している場合は、コマンドラインから Encryption クライアントをアンインストールします。手順については、「*Encryption* および *Server Encryption* クライアントのアンインストール」を参照してください。

メモ:

アンインストール後にすぐに Encryption クライアントの最新バージョンをインストールする予定の場合は、Encryption 削除エージェントを実行してファイルを復号化する必要はありません。

Deferred Activation と一緒にインストールされた旧バージョンの Encryption クライアントをアップグレードするには、Data Security Uninstaller または子インストーラを使用します。このアンインストール方法は、OPTIN が無効の場合でも可能です。

メモ:

以前アクティブ化されたユーザーがいない場合は、Encryption クライアントは、以前のインストールの残りである OPTIN 設定を SDE ボールトからクリアします。ユーザーが以前にアクティブ化した OPTIN フラグが SDE ボールトで設定されていない場合は、Encryption クライアントは、Deferred Activation をブロックします。

Deferred Activation による暗号化のインストール

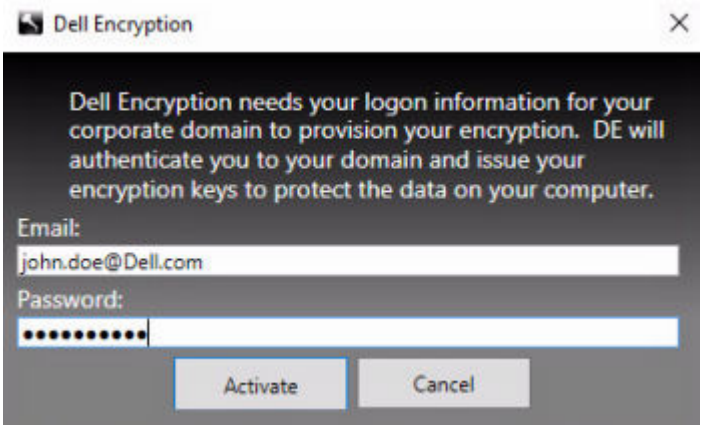
Deferred Activation 付属 Encryption クライアントをインストールするには、OPTIN=1 パラメーターを使用して Encryption クライアントをインストールします。OPTIN=1 パラメーターを使用したクライアントのインストールの詳細については、「Encryption のインストール」を参照してください。

Deferred Activation による暗号化の起動

- アクティブ化は、ローカルユーザーアカウントと特定のコンピュータを持つドメインユーザーに関連付けられます。
- 固有のローカルアカウントを使用し、固有のドメインの電子メールアドレスを持っている場合は、複数のユーザーが同じコンピュータをアクティブ化できます。
- ユーザーはドメインアカウントごとに、1 人につき一度だけ、Encryption クライアントをアクティブ化できます。

  Encryption クライアントをアクティブ化する前に、次の操作を実行します。
- 最もよく使用するローカルアカウントにログインします。このアカウントに関連付けられているデータが暗号化されます。
- 組織のネットワークに接続します。

1. ワークステーションまたはサーバにログオンします。
2. ドメインの電子メールアドレスとパスワードを入力し、**アクティブ化** をクリックします。



メモ:

ドメイン以外または個人の電子メールアドレスはアクティブ化に使用できません。

3. **閉じる** をクリックします。

   Dell サーバは、暗号化キーバンドルとユーザーの資格情報およびコンピュータの固有 ID（マシン ID）を組み合わせて、キーバンドル、特定のコンピュータ、およびユーザーの間に突破不可能な関係を作成します。

4. コンピュータを再起動して暗号化スイープを開始します。

メモ:

通知領域のアイコンからアクセスできる、ローカルの管理コンソールは、 有効なポリシーではなく、サーバが送信したポリシーを表示します。

Deferred Activation のトラブルシューティング

アクティブ化のトラブルシューティング

問題：特定のファイルおよびフォルダにアクセスできない

特定のファイルおよびフォルダにアクセスできなくなるのは、ユーザーがアクティブ化したのとは異なるアカウントでログインしたときに発生する現象です。

アクティブ化の際のログオンダイアログは、ユーザーが以前にアクティブ化していても、自動的に表示されます。

可能な解決策

ログアウトして、アクティブ化されたアカウントの資格情報を使用して再度ログインし、ファイルに再度アクセスしてみてください。

Encryption クライアントがユーザーを認証できない場合、アクティブ化の際にログオンダイアログが表示され、ユーザー認証の資格情報とアクセスの暗号化キーをユーザーに要求することがまれにあります。自動再アクティブ化機能を使用するには、*AutoReactivation* および *AutoPromptForActivation* レジストリキーの両方を有効にする必要があります。この機能はデフォルトで有効になっていますが、手動で無効にすることができます。詳細については、「自動再アクティブ化を無効化する」を参照してください。

エラーメッセージ：サーバ認証に失敗しました

サーバは、電子メールアドレスとパスワードを認証できませんでした。

可能な解決策

- 組織に関連付けられたメールアドレスを使用します。個人の電子メールアドレスは、アクティブ化に使用できません。
- 入力ミスがないように、電子メールアドレスとパスワードを再入力します。
- 管理者に電子メールアカウントがアクティブ化され、ロックされていないことの確認を依頼します。
- 管理者にユーザーのドメインパスワードのリセットを依頼します。

  エラーメッセージ：ネットワーク接続エラー

  Encryption クライアントが Dell サーバと通信できなくなった。

  可能な解決策

- 組織の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。
- ネットワークに接続するには VPN アクセスが必要です。VPN 接続を確認して、再試行します。
- Dell Server の URL を確認して、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] and [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet] でデータが正確であることを確認します

- 切断して再接続します：

  コンピュータをネットワークから切断します。

  ネットワークに再接続します。

  コンピュータを再起動します。

  ネットワークへの接続を再試行します。

  エラーメッセージ：レガシーサーバはサポートされません。

  レガシーサーバの場合には Encryption をアクティブ化できません。Dell Server はバージョン 9.1 以降である必要があります。

  可能な解決策

- Dell Server の URL を確認して、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] and [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet] でデータが正確であることを確認します

  エラーメッセージ：ドメインユーザーはすでにアクティブ化されています

  2 番目のユーザーがローカルのコンピュータにログオンして、すでにアクティブ化されているドメインアカウントのアクティブ化を試行しました。

  ユーザーはドメインアカウントごとに、1 人につき一度だけ、Encryption クライアントをアクティブ化できます。

  可能な解決策

  2 番目のアクティブ化ユーザーとしてログインしている間に、復号化して Encryption クライアントをアンインストールします。

  エラーメッセージ：一般的なサーバエラー

  サーバでエラーが発生しました。

  可能な解決策

  管理者は、サーバログを確認してサービスが実行されていることを確認する必要があります。

  ユーザーは後でアクティブ化を試行する必要があります。

ツール

CMGAd

Encryption 削除エージェントを起動する前に CMGAd ユーティリティを使用して、暗号化キーのバンドルを取得します。CMGAd ユーティリティとその使用手順は、Dell インストールメディア（Dell-Offline-Admin-XXbit）にあります。

ログファイル

`C:\ProgramData\Dell\Dell Data Protection\Encryption` で、**CmgSysTray** という名のログファイルを検索します。

「Manual activation result」というフレーズで検索します。

エラーコードと、それに続いて「status = 」が同じ行に表示され、発生した問題を示します。

18

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

- **マススタースイート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\<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。Dell Access 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 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。

Dell Server v9.8.2 においては、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。
- 自己暗号化ドライブ マネージャーがインストールされて有効になっていて、PBA が有効である。
- フル ディスク暗号化がインストールされて有効になっていて、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、*FileVault for Mac* を使用した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。

Dell Encryption のトラブルシューティング（クライアントおよびサーバ）

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：不明なユーザー名または不正なパスワードです

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：ユーザーアカウントにドメイン管理者権限がないため、アクティブ化に失敗しました。

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：サーバーとの接続を確立できませんでした。

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：サーバーがこのリクエストをサポートできないため、アクティブ化に失敗しました。

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。

サーバオペレーティングシステムの 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。

2 つのワークフローのいずれかが発生すると、アクティブ化 ダイアログが表示されます。

- 新しい（非管理）ユーザーがコンピュータにログオンする。
- 新しいユーザーが通知領域内の *Encryption* アイコンを右クリックし、*Dell 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）ユーザーの検出時に、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* 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:

   ドメイン管理者の資格情報の要件は、サーバオペレーティングシステムの Encryption がサポートされていないサーバ環境に展開されるのを防ぐ安全対策です。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ーが再起動されると、サーバオペレーティングシステムの 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、サーバオペレーティングシステムの Encryption が認証済みで、サーバモードになっていることを確認します。
- Encryption client 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、管理コンソールで使用可能な 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。

（オプション）Encryption Removal Agent ログファイルの作成

- アンインストール処理を開始する前に、オプションで Encryption Removal Agent のログファイルの作成を行います。このログファイルは、アンインストールや復号化操作のトラブルシューティングを行う際に便利です。アンインストール処理中にファイルの復号化を行うつもりがない場合は、このログファイルを作成する必要はありません。
- Encryption Removal Agent ログファイルは Encryption Removal Agent サービスが実行されるまで作成されず、このサービスはコンピュータが再起動されるまで実行されません。クライアントが正常にアンインストールされ、コンピュータが完全に復号化されると、ログファイルは完全に削除されます。
- ログファイルのパスは `C:\ProgramData\Dell\Dell Data Protection\Encryption.` です。
- 復号化の対象となるコンピュータに次のレジストリキーを作成します。

  [HKLM\Software\Credant\DecryptionAgent]

  "LogVerbosity"=DWORD:2

  0：ログを記録しない

  1：サービスを実行できなくなるエラーをログに記録する

2：完全なデータ復号化を妨げるエラーをログに記録する（推奨レベル）

3：すべての復号化ボリュームとファイルに関する情報をログに記録する

5：デバッグ情報をログに記録する

TSS バージョンの確認

- TSS は、TPM と連動するコンポーネントです。TSS バージョンを確認するには、`C:\Program Files\Dell\Dell Data Protection\Drivers\TSS\bin > tcsd_win32.exe` と移動します。ファイルを右クリックして、**プロパティ** を選択します。**詳細** タブでファイルのバージョンを確認します。

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 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。

  メモ: ターゲットファイルがシステムアカウントによって所有されている場合、WSScan は PsExec ツールを使用してシステムモードで実行する必要があります。

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 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 コマンドラインの使用

```
WSScan [-ta] [-tf] [-tr] [-tc] [drive] [-s] [-o<filepath>] [-a] [-f<format specifier>] [-r]
[-u[a][-|v]] [-d<delimeter>] [-q] [-e] [-x<exclusion directory>] [-y<sleep time>]
```

スイッチ	意味
ドライブ	スキャンするドライブ。 指定しない場合、デフォルトは、 すべてのローカルの固定ハードドライブになります。 マップされたネットワークドライブにすることができます。
-ta	すべてのドライブをスキャンします。
-tf	固定ドライブをスキャンします（デフォルト）。
-tr	リムーバブルドライブをスキャンします。
-tc	CDROM/DVDROM をスキャンします。
-s	サイレント操作
-o	出力ファイルパス
-a	出力ファイルに付加します。 デフォルトの動作は出力ファイルを切り捨てます。
-f	レポート書式指定子（レポート、固定、区切り）
-r	管理者権限なしに WSScan を実行します。**このモードでは、 一部のファイルが表示されないことがあります。**
-u	出力ファイルに非暗号化ファイルを含めます。 このスイッチは順序に敏感です。「u」を最初に、「a」を 2 番目に（または省略）、「-」または「v」を最後にする必要があります。
-u-	出力ファイルに非暗号化ファイルだけを含めます。
-ua	非暗号化ファイルも報告しますが、 すべてのユーザーポリシーを使用して「should」フィールドを表示します。
-ua-	非暗号化ファイルだけを報告しますが、 すべてのユーザーポリシーを使用して「should」フィールドを表示します。
-uv	ポリシーだけに違反した非暗号化ファイルをレポートします（Is=No / Should=Y）。
-uav	すべてのユーザーポリシーを使用して、 ポリシーだけに違反した非暗号化ファイルをレポートします（Is=No / Should=Y）。
-d	区切り付き出力の値区切り文字として使用する文字を指定します。
-q	区切り付き出力で、 引用符で囲む必要のある値を指定します。
-e	区切り付きファイルに、 拡張暗号化フィールドを含めます。

スイッチ	意味
-x	スキャンからディレクトリを除外します。複数の除外が許可されます。
-y	ディレクトリ間のスリープ時間（ミリ秒単位）。このスイッチを指定すると、スキャンが遅くなりますが、CPU の応答が向上する可能性があります。

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。
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

WSProbe の使用

Probing Utility は、Encryption External Media ポリシーを除き、すべてのバージョンの Encryption で使用するためのものです。次の目的で Probing Utility を使用します。

- 暗号化されたコンピュータをスキャンする、またはスキャンのスケジュールを設定するため。Probing Utility は、ワークステーションのスキャン優先度ポリシーに従います。
- 現在のユーザーアプリケーションデータ暗号化リストを一時的に無効または有効にするため。
- 権限リストでプロセス名を追加または削除するため。

- Dell ProSupport からの指示に従ってトラブルシューティングするため。

データ暗号化へのアプローチ

Windows デバイス上でデータを暗号化するようにポリシーを指定した場合、 次のアプローチのいずれかを使用できます。

- 最初のアプローチは、クライアントのデフォルトの動作を受け入れるというものです。 共通暗号化フォルダまたはユーザー暗号化フォルダ内のフォルダを指定するか、「マイドキュメント」の暗号化、Outlook Personal フォルダの暗号化、 一時ファイルの暗号化、 一時インターネットファイルの暗号化、または Windows ページファイルの暗号化を選択対象に設定した場合、 対象のファイルは、 作成されるとき、 または （管理対象外ユーザーが作成した後で） 管理対象ユーザーがログオンしたときに暗号化されます。 クライアントは、 フォルダの名前が変更されるか、 クライアントがこれらのポリシーに対する変更を受信したときに、 これらのポリシーで、 またはこれらのポリシーに関連して指定されたフォルダもスキャンして、 可能性のある暗号化 / 復号化がないかどうかを調べます。
- また、ログオン時にワークステーションをスキャン を 選択済み に設定することもできます。 ログオン時にワークステーションをスキャン が 選択済み の場合、 クライアントは、 ユーザーがログオンすると、 現在暗号化されているフォルダと以前に暗号化されていたフォルダ内のファイルの暗号化方法をユーザーポリシーと比較して、 必要な変更を行います。
- 暗号化条件を満たしているファイルで暗号化ポリシーが有効になる前に作成されたファイルを暗号化するが、 頻繁なスキャンによってパフォーマンスが影響されないようにするには、 このユーティリティを使用して、 コンピュータをスキャンするか、 そのスキャンのスケジュールを設定することができます。

前提条件

- 使用する Windows デバイスを暗号化する必要があります。
- 連携するユーザーがログオンする必要があります。

Probing Utility の使用

WSProbe.exe はインストールメディアにあります。

構文

```
wsprobe [path]
wsprobe [-h]
wsprobe [-f path]
wsprobe [-u n] [-x process_names] [-i process_names]
```

パラメータ

パラメータ	目的
path	オプションで、 可能性のある暗号化 / 復号化についてスキャンするデバイス上の特定のパスを指定します。 パスを指定しない場合、 このユーティリティは、 暗号化ポリシーに関連したすべてのフォルダをスキャンします。
-h	コマンドラインヘルプを表示します。
-f	TrouDell ProSupport からの指示に従ってトラブルシューティングします。
-u	ユーザーアプリケーションデータ暗号化リストを一時的に無効または有効にします。 このリストは、 現在のユーザーに対して暗号化有効が選択されている場合に有効です。 無効にするには 0 を、 再度有効にするには 1 を指定します。 ユーザーにとって有効な現在のポリシーは、 次回のログオン時に復元されます。
-x	権限リストにプロセス名を追加します。 このリスト上のコンピュータおよびインストーラプロセス名と、 このパラメータまたは HKLM\Software\CREDANT\CMGShield\EUWPrivilegedList を使用して追加するプロセス名は、 アプレケーションデータ暗号化リストで指定されている場合に無視されます。 コンマでプロセス名を区切ります。 リストに 1 つまたは複数の空白が含まれている場合は、 二重引用符でリストを囲みます。
-i	以前に権限リストに追加されたプロセス名を削除します （ハードコード化されたプロセス名は削除できません）。 コンマでプロセス名を区切ります。 リストに 1 つまたは複数の空白が含まれている場合は、 二重引用符でリストを囲みます。

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）の説明領域に、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、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 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 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。手順については、「(オプション) Encryption Removal Agent のログファイルの作成」を参照してください。
- **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。

SED のトラブルシューティング

初期アクセスコードの使用

- このポリシーは、ネットワークアクセスが使用できない場合に、コンピュータにログオンするために使用されます。つまり、Dell Server と AD のどちらにもアクセスできません。初期アクセスコード ポリシーは、絶対に必要な場合にしか使用しないでください。デルはこのログイン方法を推奨しません。初期アクセスコードポリシーを使用しても、ユーザー名、ドメイン、およびパスワードを使用する通常のログイン方法とは同じセキュリティレベルにはなりません。

  ログインの安全性が低くなる他に、初期アクセスコードでユーザーのアクティブ化すると、Dell Server にこのユーザーがコンピュータでアクティベーションを実行したレコードが残りません。その結果、パスワードおよびセルフヘルプの質問に正しく入力できない場合、Dell Server で応答コードを生成できなくなります。

- 初期アクセスコードを使用できるのは、アクティブ化直後 *1* 回限り です。エンドユーザーがログインした後は、初期アクセスコードが再度利用可能になることはありません。初期アクセスコードの入力後に初めて行われたドメインログインがキャッシュされ、初期アクセスコード入力フィールドは再表示されません。
- 初期アクセス コードは、次の状況下**限定**で表示されます。
  - ユーザーが PBA 内でアクティブ化されたことがない。
  - クライアントがネットワークまたは Dell Server に接続できない。

初期アクセスコードの使用

1. 管理コンソールで **初期アクセスコード** ポリシーの値を設定します。
2. ポリシーを保存してコミットします。
3. ローカルコンピュータを起動します。
4. アクセスコード画面が表示されたら、**初期アクセスコード**を入力します。
5. **青色矢印** をクリックします。
6. 法的通知画面が表示されたら、**OK** をクリックします。
7. このコンピュータのユーザー資格情報で Windows にログインします。この資格情報は、ドメインの一部である必要があります。

8. ログインしたら、Data Security Console を開き、PBA ユーザーが正常に作成されていることを確認します。

   一番上のメニューの **ログ** をクリックし、処理が正常に完了していることを示すメッセージ「*<DOMAIN\Username> の PBA* ユーザーが作成されました」を探します。

9. コンピュータをシャットダウンして再起動します。
10. ログイン画面で、以前に Windows にログインする際に使用したユーザー名、ドメイン、およびパスワードを入力します。

    PBA ユーザーの作成時のユーザー名形式と一致している必要があります。したがって、DOMAIN\Username という形式を使用した場合は、DOMAIN\Username という形式でユーザー名を入力する必要があります。

11. 法的通知画面が表示されたら、**ログイン** をクリックします。

    これで Windows が起動され、通常どおりにコンピュータを使用できます。

トラブルシューティングのための PBA ログファイルの作成

- 以下のように、PBA 問題のトラブルシューティングに PBA ログファイルが必要となる場合があります。
  - ネットワーク接続があるにも関わらず、ネットワーク接続アイコンが表示されない。ログファイルには、問題を解決するための DHCP 情報が記載されています。
  - Dell Server 接続アイコンが表示されない。ログファイルには、接続の問題を診断するのに役立つ情報が記載されています。
  - 正しい資格情報を入力しても認証に失敗する。この問題の診断には、Dell Server のサーバログと併用されるログファイルが役立ちます。

PBA（レガシー PBA）起動時のログのキャプチャ

1. USB ドライブに USB ドライブのルートレベルでフォルダを作成し、**\CredantSED** と命名します。
2. actions.txt という名前のファイルを作成し、**\CredantSED** フォルダ内に格納します。
3. actions.txt に、次の行を追加します。

   ```
   get logs
   ```

4. ファイルを保存して閉じます。

   コンピュータの電源がオフのときには *USB* ドライブを挿入しないでください。シャットダウン状態の間に USB ドライブがすでに挿入されている場合は、USB ドライブを取り外します。

5. コンピューターの電源を入れて、問題を再現させます。この手順でログが収集されるように、USB ドライブをコンピュータに挿入します。
6. USB ドライブを挿入後、5～10 秒待機してからそのドライブを取り外します。

   credpbaenv.tgz ファイルが、必要なログファイルが含まれる **\CredantSED** フォルダに作成されます。

PBA（UEFI PBA）起動時のログのキャプチャ

1. USB ドライブのルートレベルに **PBAErr.log** という名前のファイルを作成します。
2. コンピュータの電源を**入れる前に**、USB ドライブを挿入します。
3. ログが必要な問題を再度発生させた **後で** USB ドライブを取り外します。

PBAErr.log ファイルがアップデートされ、リアルタイムで書き込まれます。

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. dell.com/support にアクセスします。
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**カテゴリーを選択します。
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

1. 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。
2. 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。

   メモ:

   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。

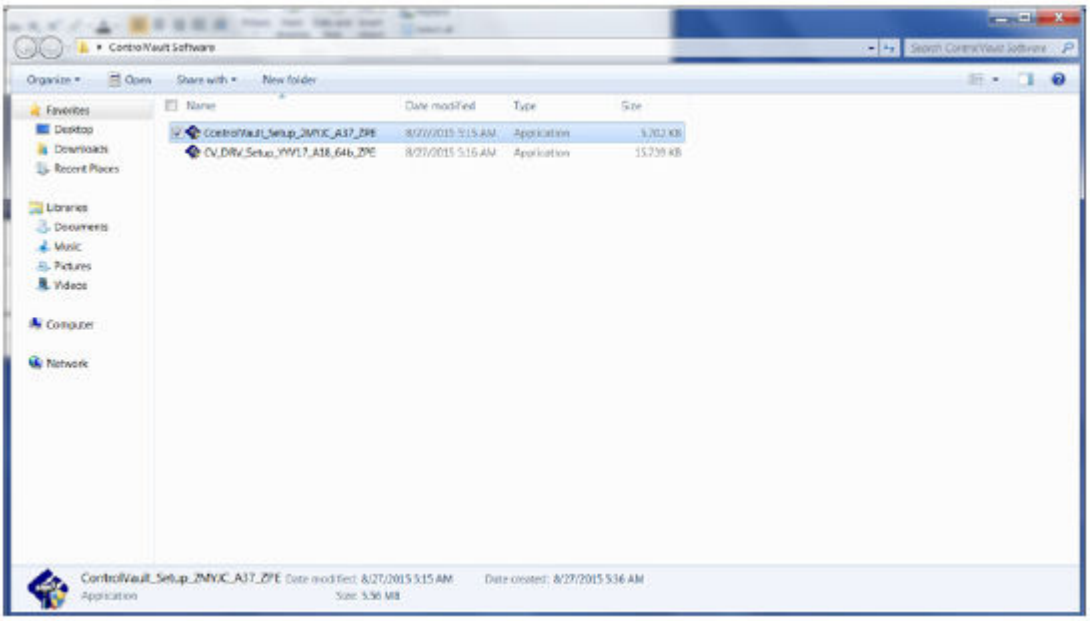
3. **続行** をクリックして開始します。
4. **Ok** をクリックして、ドライバー ファイルをデフォルトの場所である `C:\Dell\Drivers\<New Folder>`に解凍します。
5. **はい** をクリックして新しいフォルダの作成を許可します。
6. 正常に解凍しましたというメッセージが表示されたら **Ok** をクリックします。
7. 抽出後、ファイルが含まれているフォルダが表示されます。表示されない場合は、ファイルを抽出したフォルダに移動します。この場合、フォルダは **JW22F** です。
8. **CVHCI64.MSI** をダブルクリックしてドライ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）]。
9. ようこその画面で次へをクリックします。
10. **次へ**をクリックして、ドライバーを次のデフォルトの場所にインストールします。 `C:\Program Files\Broadcom Corporation\Broadcom USH Host Components\.`
11. **完了**オプションを選択して、**次へ**をクリックします。
12. **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。
13. 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

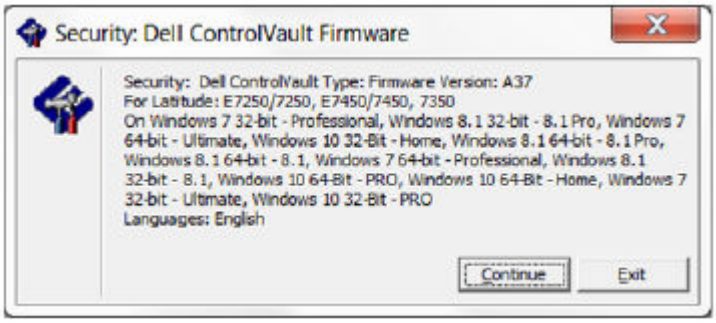
- オペレーティングシステムおよびハードウェアの構成によっては、デバイスマネージャに Dell ControlVault デバイス（およびその他のデバイス）が表示されます。

Dell ControlVault ファームウェアのインストール

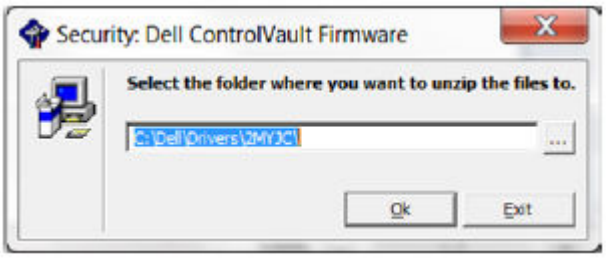
1. ファームウェアのインストールファイルをダウンロードしたフォルダに移動します。



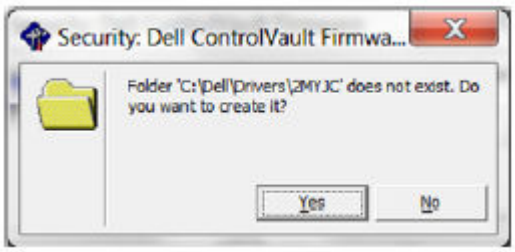
2. Dell ControlVault ファームウェアをダブルクリックして自己解凍形式の実行可能ファイルを実行します。
3. **続行** をクリックして開始します。



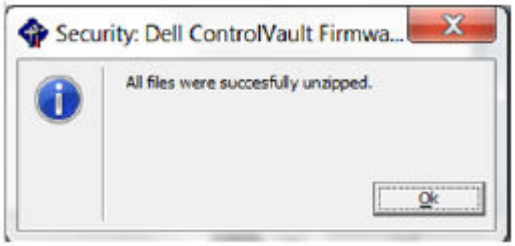
4. **Ok** をクリックして、ドライバー ファイルをデフォルトの場所である `C:\Dell\Drivers\<New Folder>`に解凍します。



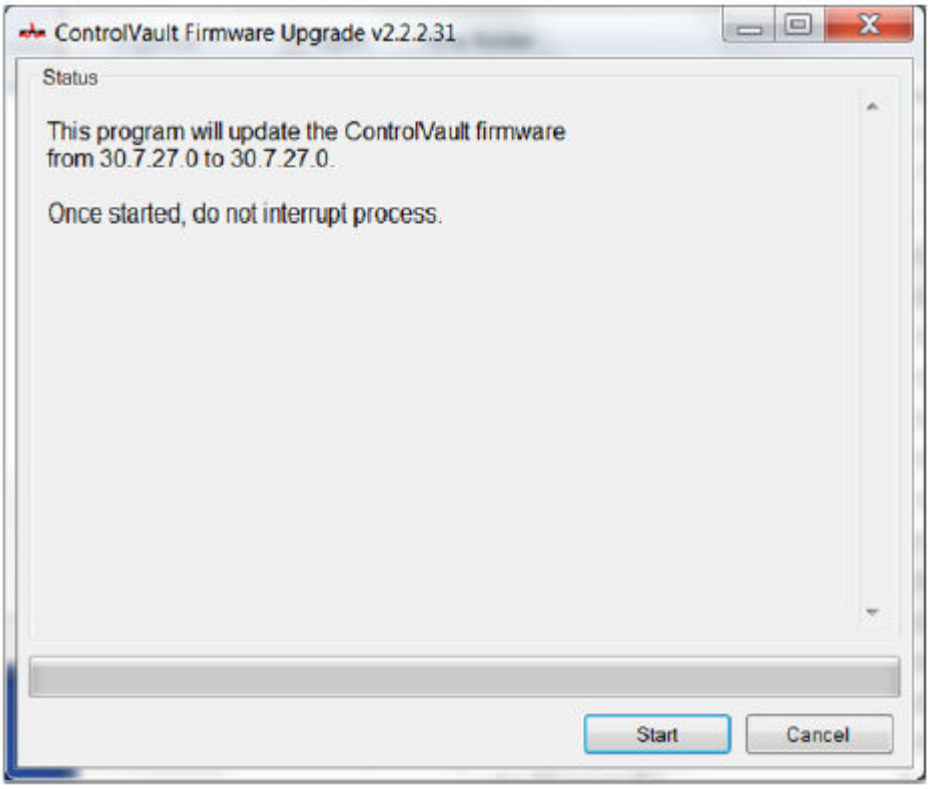
5. **はい** をクリックして新しいフォルダの作成を許可します。



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。



メモ:

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。

UEFI コンピュータ

ネットワーク接続のトラブルシューティング

- UEFI ファームウェア搭載のコンピュータで起動前認証を正常に行うには、PBA モードにネットワーク接続が必要です。デフォルトでは、UEFI ファームウェア搭載のコンピュータには、オペレーティングシステムがロードされるまでネットワーク接続がなく、これは PBA モードの後で実行されます。「UEFI コンピュータ用の事前インストール設定」で概要が説明されているコンピュータ手順が完了し、適切に設定されると、コンピュータがネットワークに接続するとき、起動前認証画面にネットワーク接続アイコンが表示されます。

- 依然として起動前認証中にネットワーク接続アイコンが表示されない場合は、ネットワークケーブルを調べてコンピュータに接続していることを確認してください。接続していなかったり、失われていた場合、コンピュータを再起動して PBA モードを再開します。

TPM および BitLocker

TPM および BitLocker のエラーコード

定数 / 値	説明
TPM_E_ERROR_MASK 0x80280000	これは、TPM ハードウェアエラーを win エラーに変換するためのエラーマスクです。
TPM_E_AUTHFAIL 0x80280001	認証に失敗しました。
TPM_E_BADINDEX 0x80280002	PCR、DIR、または他のレジスタのインデックスが正しくありません。
TPM_E_BAD_PARAMETER 0x80280003	1 つまたは複数のパラメータが間違っています。
TPM_E_AUDITFAILURE 0x80280004	操作は正しく完了したが、その操作の監査が失敗しました。
TPM_E_CLEAR_DISABLED 0x80280005	クリア無効フラグが設定され、すべてのクリア操作で物理的なアクセスが必要になりました。
TPM_E_DEACTIVATED 0x80280006	TPM をアクティブ化します。
TPM_E_DISABLED 0x80280007	TPM を有効にします。
TPM_E_DISABLED_CMD 0x80280008	ターゲットコマンドが無効になっています。
TPM_E_FAIL 0x80280009	操作が失敗しました。
TPM_E_BAD_ORDINAL 0x8028000A	序数が不明または一貫していませんでした。
TPM_E_INSTALL_DISABLED 0x8028000B	所有者をインストールする機能が無効です。
TPM_E_INVALID_KEYHANDLE 0x8028000C	キーハンドルを解釈できません。

定数 / 値	説明
TPM_E_KEYNOTFOUND 0x8028000D	キーハンドルが無効なキーを示しています。
TPM_E_INAPPROPRIATE_ENC 0x8028000E	受け入れられない暗号化スキーマです。
TPM_E_MIGRATEFAIL 0x8028000F	移行承認に失敗しました。
TPM_E_INVALID_PCR_INFO 0x80280010	PCR 情報を解釈できませんでした。
TPM_E_NOSPACE 0x80280011	キーをロードする余裕がありません。
TPM_E_NOSRK 0x80280012	ストレージルートキー（SRK）セットがありません。
TPM_E_NOTSEALED_BLOB 0x80280013	暗号化された BLOB が無効であるか、この TPM では作成されませんでした。
TPM_E_OWNER_SET 0x80280014	TPM にはすでに所有者がいます。
TPM_E_RESOURCES 0x80280015	TPM には、リクエストされたアクションを実行するための内部リソースが不足しています。
TPM_E_SHORTRANDOM 0x80280016	ランダム文字列が短すぎました。
TPM_E_SIZE 0x80280017	TPM には、操作を実行するための容量がありません。
TPM_E_WRONGPCRVAL 0x80280018	名前付き PCR 値が現在の PCR 値に一致していません。
TPM_E_BAD_PARAM_SIZE 0x80280019	コマンドに対する paramSize 引数の値が正しくありません。
TPM_E_SHA_THREAD 0x8028001A	既存の SHA-1 スレッドがありません。
TPM_E_SHA_ERROR 0x8028001B	既存の SHA-1 スレッドでエラーがすでに発生しているので、計算を続行できません。
TPM_E_FAILEDSELFTEST 0x8028001C	TPM ハードウェアデバイスが、その内部セルフテスト中に障害を報告しました。問題を解決するには、コンピュータを再起動してみてください。問題が解決しない場合、TPM ハードウェアまたはマザーボードの交換が必要になることがあります。
TPM_E_AUTH2FAIL 0x8028001D	2 キー機能での 2 番目のキーの認証が失敗しました。

定数 / 値	説明
TPM_E_BADTAG 0x8028001E	コマンドに送信されたタグ値が正しくありません。
TPM_E_IOERROR 0x8028001F	TPM への情報の転送中に IO エラーが発生しました。
TPM_E_ENCRYPT_ERROR 0x80280020	暗号化プロセスに問題が発生しました。
TPM_E_DECRYPT_ERROR 0x80280021	復号化プロセスが完了しませんでした。
TPM_E_INVALID_AUTHHANDLE 0x80280022	無効なハンドルが使用されました。
TPM_E_NO_ENDORSEMENT 0x80280023	TPM には、保証キー（EK）がインストールされていません。
TPM_E_INVALID_KEYUSAGE 0x80280024	キーの使用は許可されていません。
TPM_E_WRONG_ENTITYTYPE 0x80280025	送信されたエンティティタイプは許可されていません。
TPM_E_INVALID_POSTINIT 0x80280026	コマンドは、TPM の初期およびその後の TPM スタートアップに関連して間違った順序で受信されました。
TPM_E_INAPPROPRIATE_SIG 0x80280027	署名データには、追加の DER 情報を含められません。
TPM_E_BAD_KEY_PROPERTY 0x80280028	TPM_KEY_PARM におけるキープロパティは、この TPM によってサポートされません。
TPM_E_BAD_MIGRATION 0x80280029	このキーの移行プロパティは正しくありません。
TPM_E_BAD_SCHEME 0x8028002A	このキーの署名および暗号化スキーマが正しくないか、この状況では許可されていません。
TPM_E_BAD_DATASIZE 0x8028002B	データ（または BLOB）パラメータのサイズが間違っているか、参照キーと一致していません。
TPM_E_BAD_MODE 0x8028002C	TPM_GetCapability の capArea および subCapArea、TPM_PhysicalPresence の phsicalPresence パラメータ、TPM_CreateMigrationBlob の migrationType などのモードパラメータが間違っています。
TPM_E_BAD_PRESENCE 0x8028002D	physicalPresence または physicalPresenceLock ビットのいずれかの値が間違っています。
TPM_E_BAD_VERSION 0x8028002E	TPM は、このバージョンの機能を実行できません。

定数 / 値	説明
TPM_E_NO_WRAP_TRANSPORT 0x8028002F	TPM が、ラップされたトランスポートセッションを許可していません。
TPM_E_AUDITFAIL_UNSUCCESSFUL 0x80280030	TPM 監査構築が失敗し、基盤となるコマンドが失敗コードも返しました。
TPM_E_AUDITFAIL_SUCCESSFUL 0x80280031	TPM 監査構築が失敗し、基盤となるコマンドが成功を返しました。
TPM_E_NOTRESETABLE 0x80280032	リセット可能な属性を持たない PCR レジスタをリセットしようとしています。
TPM_E_NOTLOCAL 0x80280033	コマンドトランスポートの一部ではないローカリティおよびローカリティ修飾子を必要とする PCR レジスタをリセットしようとしています。
TPM_E_BAD_TYPE 0x80280034	識別情報 BLOB が正しく入力されないようにします。
TPM_E_INVALID_RESOURCE 0x80280035	コンテキストの保存時に、識別されたリソースタイプが実際のリソースに一致していません。
TPM_E_NOTFIPS 0x80280036	TPM が、FIPS モードの場合にのみ利用できるコマンドを実行しようとしています。
TPM_E_INVALID_FAMILY 0x80280037	コマンドが、無効なファミリー ID を使用しようとしています。
TPM_E_NO_NV_PERMISSION 0x80280038	NV ストレージを操作するための許可が利用できません。
TPM_E_REQUIRES_SIGN 0x80280039	操作には署名済みコマンドが必要です。
TPM_E_KEY_NOTSUPPORTED 0x8028003A	NV キーをロードする操作が間違っています。
TPM_E_AUTH_CONFLICT 0x8028003B	NV_LoadKey BLOB には所有者と BLOB 認証の両方が必要です。
TPM_E_AREA_LOCKED 0x8028003C	NV 領域はロックされ、書き込みできません。
TPM_E_BAD_LOCALITY 0x8028003D	ローカリティは、試みた操作にとって正しくありません。
TPM_E_READ_ONLY 0x8028003E	NV 領域は読み取り専用で、書き込みできません。
TPM_E_PER_NOWRITE 0x8028003F	NV 領域への書き込みが保護されていません。

定数 / 値	説明
TPM_E_FAMILYCOUNT 0x80280040	ファミリーカウント値が一致していません。
TPM_E_WRITE_LOCKED 0x80280041	NV 領域はすでに書き込まれています。
TPM_E_BAD_ATTRIBUTES 0x80280042	NV 領域属性が競合しています。
TPM_E_INVALID_STRUCTURE 0x80280043	構造タグおよびバージョンが無効であるか、 一貫していません。
TPM_E_KEY_OWNER_CONTROL 0x80280044	キーが、TPM 所有者の制御下にあり、TPM 所有者によってのみ排除できます。
TPM_E_BAD_COUNTER 0x80280045	カウンタハンドルが正しくありません。
TPM_E_NOT_FULLWRITE 0x80280046	書き込みは、 領域の完全な書き込みではありません。
TPM_E_CONTEXT_GAP 0x80280047	保存したコンテキストカウントのギャップが大きすぎます。
TPM_E_MAXNVWRITES 0x80280048	所有者なしの NV 書き込みの最大数を超過しました。
TPM_E_NOOPERATOR 0x80280049	演算子 AuthData 値が設定されていません。
TPM_E_RESOURCEMISSING 0x8028004A	コンテキストで示されたリソースがロードされていません。
TPM_E_DELEGATE_LOCK 0x8028004B	委任管理者がロックされています。
TPM_E_DELEGATE_FAMILY 0x8028004C	委任されたファミリー以外のファミリーを管理しようとしています。
TPM_E_DELEGATE_ADMIN 0x8028004D	委任テーブル管理が有効ではありません。
TPM_E_TRANSPORT_NOTEXCLUSIVE 0x8028004E	排他的なトランスポートセッションの外部で実行されたコマンドがありました。
TPM_E_OWNER_CONTROL 0x8028004F	所有者排除制御キーをコンテキスト保存しようとしています。
TPM_E_DAA_RESOURCES 0x80280050	DAA コマンドにはその実行に利用できるリソースがありません。

定数 / 値	説明
TPM_E_DAA_INPUT_DATA0 0x80280051	DAA パラメータ inputData0 の整合性チェックが失敗しました。
TPM_E_DAA_INPUT_DATA1 0x80280052	DAA パラメータ inputData1 の整合性チェックが失敗しました。
TPM_E_DAA_ISSUER_SETTINGS 0x80280053	DAA_issuerSettings の整合性チェックが失敗しました。
TPM_E_DAA_TPM_SETTINGS 0x80280054	DAA_tpmSpecific の整合性チェックが失敗しました。
TPM_E_DAA_STAGE 0x80280055	送信された DAA コマンドで示された原子的なプロセスが、 予想されたプロセスではありません。
TPM_E_DAA_ISSUER_VALIDITY 0x80280056	発行者の妥当性チェックが不整合を検出しました。
TPM_E_DAA_WRONG_W 0x80280057	w の整合性チェックが失敗しました。
TPM_E_BAD_HANDLE 0x80280058	ハンドルが正しくありません。
TPM_E_BAD_DELEGATE 0x80280059	委任が正しくありません。
TPM_E_BADCONTEXT 0x8028005A	コンテキスト BLOB が無効です。
TPM_E_TOOMANYCONTEXTS 0x8028005B	TPM によって保持されているコンテキスが多すぎます。
TPM_E_MA_TICKET_SIGNATURE 0x8028005C	移行承認機関署名検証が失敗しました。
TPM_E_MA_DESTINATION 0x8028005D	移行先が認証されていません。
TPM_E_MA_SOURCE 0x8028005E	移行元が正しくありません。
TPM_E_MA_AUTHORITY 0x8028005F	移行承認機関が正しくありません。
TPM_E_PERMANENTEK 0x80280061	EK を呼び出そうとしており、 EK は呼び出し可能ではありません。
TPM_E_BAD_SIGNATURE 0x80280062	CMK チケットの署名が間違っています。

定数 / 値	説明
TPM_E_NOCONTEXTSPACE 0x80280063	コンテキストリストにコンテキストを追加するための余裕がありません。
TPM_E_COMMAND_BLOCKED 0x80280400	コマンドはブロックされました。
TPM_E_INVALID_HANDLE 0x80280401	指定されたハンドルが見つかりませんでした。
TPM_E_DUPLICATE_VHANDLE 0x80280402	TPM が重複したハンドルを返したので、コマンドを再送信する必要があります。
TPM_E_EMBEDDED_COMMAND_BLOCKED 0x80280403	トランスポート内のコマンドがブロックされました。
TPM_E_EMBEDDED_COMMAND_UNSUPPORTED 0x80280404	トランスポート内のコマンドがサポートされていません。
TPM_E_RETRY 0x80280800	TPM は非常にビジーでコマンドにすぐには反応できませんが、後からコマンドを再送信できます。
TPM_E_NEEDS_SELFTEST 0x80280801	SelfTestFull が実行されていません。
TPM_E_DOING_SELFTEST 0x80280802	TPM は現在、完全な自己テストを実行しています。
TPM_E_DEFEND_LOCK_RUNNING 0x80280803	TPM は、辞書攻撃に対して防御しており、タイムアウト時間内です。
TBS_E_INTERNAL_ERROR 0x80284001	内部ソフトウェアエラーが検出されました。
TBS_E_BAD_PARAMETER 0x80284002	1 つまたは複数の入力パラメータが間違っています。
TBS_E_INVALID_OUTPUT_POINTER 0x80284003	指定された出力ポインタが間違っています。
TBS_E_INVALID_CONTEXT 0x80284004	指定されたコンテキストハンドルは、有効なコンテキストを参照していません。
TBS_E_INSUFFICIENT_BUFFER 0x80284005	指定の出力バッファが小さすぎます。
TBS_E_IOERROR 0x80284006	TPM との通信中にエラーが発生しました。
TBS_E_INVALID_CONTEXT_PARAM 0x80284007	1 つまたは複数のコンテキストパラメータが無効です。

定数 / 値	説明
TBS_E_SERVICE_NOT_RUNNING 0x80284008	TBS サービスが実行しておらず、開始できません。
TBS_E_TOO_MANY_TBS_CONTEXTS 0x80284009	開いているコンテキストが多すぎるので、新しいコンテキストを作成できませんでした。
TBS_E_TOO_MANY_RESOURCES 0x8028400A	開いている仮想リソースが多すぎるので、新しい仮想リソースを作成できませんでした。
TBS_E_SERVICE_START_PENDING 0x8028400B	TBS サービスは開始していますが、まだ実行していません。
TBS_E_PPI_NOT_SUPPORTED 0x8028400C	物理プレゼンスインターフェースがサポートされていません。
TBS_E_COMMAND_CANCELED 0x8028400D	コマンドがキャンセルされました。
TBS_E_BUFFER_TOO_LARGE 0x8028400E	入力または出力バッファが大きすぎます。
TBS_E_TPM_NOT_FOUND 0x8028400F	このコンピュータ上に、互換性のある TPM セキュリティデバイスが見つかりません。
TBS_E_SERVICE_DISABLED 0x80284010	TBS サービスが無効になっています。
TBS_E_NO_EVENT_LOG 0x80284011	TCG イベントログが利用できません。
TBS_E_ACCESS_DENIED 0x80284012	呼び出し側に、リクエストされた操作を実行するための適切な権限がありません。
TBS_E_PROVISIONING_NOT_ALLOWED 0x80284013	TPM プロビジョニングアクションが、指定のフラグによって許可されていません。プロビジョニングが成功するには、いくつかのアクションのいずれかが必要になる場合があります。TPM を準備された状態にする TPM 管理コンソール（tpm.msc）アクションが役立ちます。詳細については、Win32_Tpm WMI メソッド「Provision」に関する文書を参照してください。（必要となる可能性のあるアクションには、TPM 所有者認証値のシステムへのインポート、TPM をプロビジョニングし「ForceClear_Allowed」または「PhysicalPresencePrompts_Allowed」のどちらかに対して TRUE を指定するための Win32_Tpm WMI メソッドの呼び出し（追加情報で返される値で示されるとおり）、またはシステム BIOS での TPM の有効化があります）。
TBS_E_PPI_FUNCTION_UNSUPPORTED 0x80284014	このファームウェアの物理プレゼンスインターフェースは、リクエストされたメソッドをサポートしていません。
TBS_E_OWNERAUTH_NOT_FOUND 0x80284015	リクエストされた TPM OwnerAuth 値が見つかりませんでした。

定数 / 値	説明
TBS_E_PROVISIONING_INCOMPLETE 0x80284016	TPM プロビジョニングが完了しませんでした。プロビジョニングを完了するための詳細については、TPM をプロビジョニングするための Win32_Tpm WMI メソッド（「Provision」）を呼び出し、リクエストされた情報をチェックしてください。
TPMAPI_E_INVALID_STATE 0x80290100	コマンドバッファは正しい状態にありません。
TPMAPI_E_NOT_ENOUGH_DATA 0x80290101	コマンドバッファは、リクエストに応えられるだけ十分なデータを含んでいません。
TPMAPI_E_TOO_MUCH_DATA 0x80290102	コマンドバッファは、これ以上データを含められません。
TPMAPI_E_INVALID_OUTPUT_POINTER 0x80290103	1 つまたは複数の出力パラメータが NULL または無効でした。
TPMAPI_E_INVALID_PARAMETER 0x80290104	1 つまたは複数の入力パラメータが無効です。
TPMAPI_E_OUT_OF_MEMORY 0x80290105	リクエストに応えられるだけ十分なメモリが利用できませんでした。
TPMAPI_E_BUFFER_TOO_SMALL 0x80290106	指定のバッファが小さすぎました。
TPMAPI_E_INTERNAL_ERROR 0x80290107	内部エラーが検出されました。
TPMAPI_E_ACCESS_DENIED 0x80290108	呼び出し側に、リクエストされた操作を実行するための適切な権限がありません。
TPMAPI_E_AUTHORIZATION_FAILED 0x80290109	指定した承認情報が無効でした。
TPMAPI_E_INVALID_CONTEXT_HANDLE 0x8029010A	指定のコンテキストが有効ではありませんでした。
TPMAPI_E_TBS_COMMUNICATION_ERROR 0x8029010B	TBS との通信中にエラーが発生しました。
TPMAPI_E_TPM_COMMAND_ERROR 0x8029010C	TPM が予想外の結果を返しました。
TPMAPI_E_MESSAGE_TOO_LARGE 0x8029010D	メッセージは、エンコードスキーマには大きすぎます。
TPMAPI_E_INVALID_ENCODING 0x8029010E	BLOB のエンコードが認識されませんでした。
TPMAPI_E_INVALID_KEY_SIZE 0x8029010F	キーサイズが有効ではありません。

定数 / 値	説明
TPMAPI_E_ENCRYPTION_FAILED 0x80290110	暗号操作が失敗しました。
TPMAPI_E_INVALID_KEY_PARAMS 0x80290111	キーパラメータ構造が有効ではありませんでした。
TPMAPI_E_INVALID_MIGRATION_AUTHORIZATION_BLOB 0x80290112	リクエストされた提供データが有効な移行承認 BLOB ではないようです。
TPMAPI_E_INVALID_PCR_INDEX 0x80290113	指定の PCR インデックスが無効でした。
TPMAPI_E_INVALID_DELEGATE_BLOB 0x80290114	与えられたデータは、有効な委任 BLOB ではないようです。
TPMAPI_E_INVALID_CONTEXT_PARAMS 0x80290115	1 つまたは複数の指定されたコンテキストパラメータが有効ではありませんでした。
TPMAPI_E_INVALID_KEY_BLOB 0x80290116	与えられたデータは、有効なキー BLOB ではないようです。
TPMAPI_E_INVALID_PCR_DATA 0x80290117	指定の PCR データは無効でした。
TPMAPI_E_INVALID_OWNER_AUTH 0x80290118	所有者認証データの形式が無効でした。
TPMAPI_E_FIPS_RNG_CHECK_FAILED 0x80290119	生成されたランダム数は FIPS RNG チェックをパスしません。
TPMAPI_E_EMPTY_TCG_LOG 0x8029011A	TCG イベントログにはデータが含まれていません。
TPMAPI_E_INVALID_TCG_LOG_ENTRY 0x8029011B	TCG イベントログでのエントリが無効です。
TPMAPI_E_TCG_SEPARATOR_ABSENT 0x8029011C	TCG 区切り文字が見つかりません
TPMAPI_E_TCG_INVALID_DIGEST_ENTRY 0x8029011D	TCG ログエントリ内のダイジェスト値がハッシュされたデータに一致しませんでした。
TPMAPI_E_POLICY_DENIES_OPERATION 0x8029011E	リクエストされた操作は、現在の TPM ポリシーによってブロックされました。サポートが必要な場合は、システム管理者に連絡してください。
TBSIMP_E_BUFFER_TOO_SMALL 0x80290200	指定のバッファが小さすぎました。
TBSIMP_E_CLEANUP_FAILED 0x80290201	コンテキストをクリーンアップできませんでした。

定数 / 値	説明
TBSIMP_E_INVALID_CONTEXT_HANDLE 0x80290202	指定のコンテキストハンドルが無効です。
TBSIMP_E_INVALID_CONTEXT_PARAM 0x80290203	無効なコンテキストパラメータが指定されました。
TBSIMP_E_TPM_ERROR 0x80290204	TPM との通信中にエラーが発生しました。
TBSIMP_E_HASH_BAD_KEY 0x80290205	指定のキーのエントリが見つかりませんでした。
TBSIMP_E_DUPLICATE_VHANDLE 0x80290206	指定の仮想ハンドルが、すでに使用されている仮想ハンドルに一致しています。
TBSIMP_E_INVALID_OUTPUT_POINTER 0x80290207	返されたハンドルの場所を示すポインタが NULL または無効でした。
TBSIMP_E_INVALID_PARAMETER 0x80290208	1 つまたは複数のパラメータが無効です。
TBSIMP_E_RPC_INIT_FAILED 0x80290209	RPC サブシステムを初期化できませんでした。
TBSIMP_E_SCHEDULER_NOT_RUNNING 0x8029020A	TBS スケジューラが実行していません。
TBSIMP_E_COMMAND_CANCELED 0x8029020B	コマンドがキャンセルされました。
TBSIMP_E_OUT_OF_MEMORY 0x8029020C	リクエストに応えるだけ十分なメモリがありませんでした。
TBSIMP_E_LIST_NO_MORE_ITEMS 0x8029020D	指定のリストが空か、繰り返しがリストの最後に到達しました。
TBSIMP_E_LIST_NOT_FOUND 0x8029020E	指定のアイテムがリストに見つかりませんでした。
TBSIMP_E_NOT_ENOUGH_SPACE 0x8029020F	TPM には、リクエストされたリソースをロードできるだけ十分な容量がありません。
TBSIMP_E_NOT_ENOUGH_TPM_CONTEXTS 0x80290210	使用されている TPM コンテキストが多すぎます。
TBSIMP_E_COMMAND_FAILED 0x80290211	TPM コマンドが失敗しました。
TBSIMP_E_UNKNOWN_ORDINAL 0x80290212	TBS は、指定の序数を認識していません。

定数 / 値	説明
TBSIMP_E_RESOURCE_EXPIRED 0x80290213	リクエストされたリソースはもはや使用可能ではありません。
TBSIMP_E_INVALID_RESOURCE 0x80290214	リソースタイプは一致しませんでした。
TBSIMP_E_NOTHING_TO_UNLOAD 0x80290215	リソースをアンロードできません。
TBSIMP_E_HASH_TABLE_FULL 0x80290216	新しいエントリをハッシュテーブルに追加できません。
TBSIMP_E_TOO_MANY_TBS_CONTEXTS 0x80290217	開いているコンテキストが多すぎるので、新しい TBS コンテキストを作成できませんでした。
TBSIMP_E_TOO_MANY_RESOURCES 0x80290218	開いている仮想リソースが多すぎるので、新しい仮想リソースを作成できませんでした。
TBSIMP_E_PPI_NOT_SUPPORTED 0x80290219	物理プレゼンスインターフェースがサポートされていません。
TBSIMP_E_TPM_INCOMPATIBLE 0x8029021A	TBS は、システム上に見つかった TPM のバージョンと互換性がありません。
TBSIMP_E_NO_EVENT_LOG 0x8029021B	TCG イベントログが利用できません。
TPM_E_PPI_ACPI_FAILURE 0x80290300	物理プレゼンスコマンドに対する BIOS の応答を取得しようとしているときに、一般的なエラーが検出されました。
TPM_E_PPI_USER_ABORT 0x80290301	ユーザーは TPM 操作リクエストを確認できませんでした。
TPM_E_PPI_BIOS_FAILURE 0x80290302	BIOS の障害により、リクエストされた TPM 操作の正常な実行が妨げられました（たとえば、無効な TPM 操作リクエスト、TPM との BIOS 通信エラー）。
TPM_E_PPI_NOT_SUPPORTED 0x80290303	BIOS は物理プレゼンスインターフェースをサポートしていません。
TPM_E_PPI_BLOCKED_IN_BIOS 0x80290304	物理プレゼンスコマンドは、現在の BIOS 設定によってブロックされました。システム所有者は、コマンドを許可するように BIOS 設定を再設定できる場合があります。
TPM_E_PCP_ERROR_MASK 0x80290400	これは、プラットフォーム暗号化プロバイダエラーを win エラーに変換するためのエラーマスクです。
TPM_E_PCP_DEVICE_NOT_READY 0x80290401	プラットフォーム暗号化デバイスは現在準備できていません。動作できるように完全にプロビジョニングする必要があります。
TPM_E_PCP_INVALID_HANDLE 0x80290402	プラットフォーム暗号化プロバイダに提供されたハンドルが無効です。

定数 / 値	説明
TPM_E_PCP_INVALID_PARAMETER 0x80290403	プラットフォーム暗号化プロバイダに提供されたパラメータが無効です。
TPM_E_PCP_FLAG_NOT_SUPPORTED 0x80290404	プラットフォーム暗号化プロバイダに提供されたフラグがサポートされていません。
TPM_E_PCP_NOT_SUPPORTED 0x80290405	リクエストされた操作は、このプラットフォーム暗号化プロバイダでサポートされていません。
TPM_E_PCP_BUFFER_TOO_SMALL 0x80290406	バッファが非常に小さく、すべてのデータは含められません。バッファに情報が書き込まれていません。
TPM_E_PCP_INTERNAL_ERROR 0x80290407	プラットフォーム暗号化プロバイダで、予想外の内部エラーが発生しました。
TPM_E_PCP_AUTHENTICATION_FAILED 0x80290408	プロバイダオブジェクトを使用する承認が失敗しました。
TPM_E_PCP_AUTHENTICATION_IGNORED 0x80290409	プラットフォーム暗号化デバイスは、辞書攻撃を 抑えるために、プロバイダオブジェクトの承認を無視しました。
TPM_E_PCP_POLICY_NOT_FOUND 0x8029040A	参照ポリシーが見つかりませんでした。
TPM_E_PCP_PROFILE_NOT_FOUND 0x8029040B	参照プロファイルが見つかりませんでした。
TPM_E_PCP_VALIDATION_FAILED 0x8029040C	検証が成功しませんでした。
PLA_E_DCS_NOT_FOUND 0x80300002	データコレクタセットが見つかりませんでした。
PLA_E_DCS_IN_USE 0x803000AA	データコレクタセットまたはその従属関係の 1 つがすでに使用されています。
PLA_E_TOO_MANY_FOLDERS 0x80300045	フォルダが多すぎるため、データコレクタセットを開始できません。
PLA_E_NO_MIN_DISK 0x80300070	データコレクタセットを開始できるだけ十分な空きディスク容量がありません。
PLA_E_DCS_ALREADY_EXISTS 0x803000B7	データコレクタセットがすでに存在しています。
PLA_S_PROPERTY_IGNORED 0x00300100	プロパティ値は無視されます。
PLA_E_PROPERTY_CONFLICT 0x80300101	プロパティ値が競合しています。

定数 / 値	説明
PLA_E_DCS_SINGLETON_REQUIRED 0x80300102	このデータコレクタセットの現在の設定では、ちょうど 1 つのデータコレクタを含むことが必要です。
PLA_E_CREDENTIALS_REQUIRED 0x80300103	現在のデータコレクタセットプロパティをコミットするには、ユーザーアカウントが必要です。
PLA_E_DCS_NOT_RUNNING 0x80300104	データコレクタセットが実行していません。
PLA_E_CONFLICT_INCL_EXCL_API 0x80300105	API の包含 / 除外リストで競合が検出されました。包含リストおよび除外リストの両方に同じ API を指定しないでください。
PLA_E_NETWORK_EXE_NOT_VALID 0x80300106	指定した実行可能パスは、ネットワーク共有または UNC パスを参照しています。
PLA_E_EXE_ALREADY_CONFIGURED 0x80300107	指定した実行可能パスは、すでに API トレーシングに対して設定されています。
PLA_E_EXE_PATH_NOT_VALID 0x80300108	指定した実行可能パスは存在していません。指定したパスが正しいことを確認します。
PLA_E_DC_ALREADY_EXISTS 0x80300109	データコレクタがすでに存在しています。
PLA_E_DCS_START_WAIT_TIMEOUT 0x8030010A	データコレクタセット開始通知の待機がタイムアウトしました。
PLA_E_DC_START_WAIT_TIMEOUT 0x8030010B	データコレクタセットの開始の待機がタイムアウトしました。
PLA_E_REPORT_WAIT_TIMEOUT 0x8030010C	レポート生成ツールの終了の待機がタイムアウトしました。
PLA_E_NO_DUPLICATES 0x8030010D	重複したアイテムは許可されていません。
PLA_E_EXE_FULL_PATH_REQUIRED 0x8030010E	トレースする実行可能ファイルを指定する場合、ファイル名だけではなく、実行可能ファイルへの完全パスを指定する必要があります。
PLA_E_INVALID_SESSION_NAME 0x8030010F	入力したセッション名が無効です。
PLA_E_PLA_CHANNEL_NOT_ENABLED 0x80300110	イベントログチャネル Microsoft-Windows-Diagnosis-PLA/Operational でこの操作を実行できるようにする必要があります。
PLA_E_TASKSCHED_CHANNEL_NOT_ENABLED 0x80300111	イベントログチャネル Microsoft-Windows-TaskScheduler でこの操作を実行できるようにする必要があります。
PLA_E_RULES_MANAGER_FAILED 0x80300112	Rules Manager の実行が失敗しました。

定数 / 値	説明
PLA_E_CABAPI_FAILURE 0x80300113	データを圧縮または抽出しようとしているときにエラーが発生しました。
FVE_E_LOCKED_VOLUME 0x80310000	このドライブは、BitLocker ドライブ暗号化によってロックされています。コントロールパネルからこのドライブをロック解除する必要があります。
FVE_E_NOT_ENCRYPTED 0x80310001	ドライブが暗号化されていません。
FVE_E_NO_TPM_BIOS 0x80310002	BIOS は、TPM と正しく通信しませんでした。BIOS アップグレード手順については、コンピュータの製造元に問い合わせてください。
FVE_E_NO_MBR_METRIC 0x80310003	BIOS はマスターブートレコード（MBR）と正しく通信しませんでした。BIOS アップグレード手順については、コンピュータの製造元に問い合わせてください。
FVE_E_NO_BOOTSECTOR_METRIC 0x80310004	必要な TPM 測定値が欠落しています。コンピュータにブート可能な CD または DVD がある場合は、それを取り外し、コンピュータを再起動して、BitLocker をもう一度オンにします。問題が解決しない場合は、マスターブートレコードが最新であることを確認してください。
FVE_E_NO_BOOTMGR_METRIC 0x80310005	このドライブのブートセクターが BitLocker ドライブ暗号化と互換性がありません。Windows 回復環境の Bootrec.exe ツールを使用して、ブートマネージャ（BOOTMGR）をアップデートまたは修復してください。
FVE_E_WRONG_BOOTMGR 0x80310006	このオペレーティングシステムのブートマネージャが BitLocker ドライブ暗号化と互換性がありません。Windows 回復環境の Bootrec.exe ツールを使用して、ブートマネージャ（BOOTMGR）をアップデートまたは修復してください。
FVE_E_SECURE_KEY_REQUIRED 0x80310007	この操作を実行するには、少なくとも 1 つのセキュアなキー保護機能が必要です。
FVE_E_NOT_ACTIVATED 0x80310008	BitLocker ドライブ暗号化はこのドライブ上で有効になっていません。BitLocker をオンにします。
FVE_E_ACTION_NOT_ALLOWED 0x80310009	BitLocker ドライブ暗号化がリクエストされたアクションを実行できません。この状態は、2 つのリクエストが同時に発行された場合に生じる可能性があります。しばらく待ってから、もう一度アクションを試みてください。
FVE_E_AD_SCHEMA_NOT_INSTALLED 0x8031000A	Active Directory ドメインサービスフォレストには、BitLocker ドライブ暗号化または TPM 情報をホストするために必要な属性とクラスが含まれていません。ドメイン管理者に問い合わせて、必要な BitLocker Active Directory スキーマ拡張がインストールされていることを確認してください。
FVE_E_AD_INVALID_DATATYPE 0x8031000B	Active Directory から取得されたデータのタイプが予想外でした。BitLocker 回復情報が欠落しているか,破損している可能性があります。
FVE_E_AD_INVALID_DATASIZE 0x8031000C	Active Directory から取得されたデータのサイズが予想外でした。BitLocker 回復情報が欠落しているか,破損している可能性があります。

定数 / 値	説明
FVE_E_AD_NO_VALUES 0x8031000D	Active Directory から読み取られた属性には値が含まれていません。BitLocker 回復情報が欠落しているか,破損している可能性があります。
FVE_E_AD_ATTR_NOT_SET 0x8031000E	属性が設定されていませんでした。Active Directory オブジェクトに情報を書き込むことのできるドメインアカウントでログオンしていることを確認してください。
FVE_E_AD_GUID_NOT_FOUND 0x8031000F	Active Directory ドメインサービスで、指定の属性が見つかりませんでした。ドメイン管理者に問い合わせて、必要な BitLocker Active Directory スキーマ拡張がインストールされていることを確認してください。
FVE_E_BAD_INFORMATION 0x80310010	暗号化されたドライブの BitLocker メタデータが有効ではありません。ドライブを修復してアクセスを復元してみることができます。
FVE_E_TOO_SMALL 0x80310011	十分な空き容量がないので、ドライブを暗号化できません。ドライブ上の不要なデータを削除して、空き容量を増やしてから再試行してください。
FVE_E_SYSTEM_VOLUME 0x80310012	システムブート情報を含んでいるので、ドライブを暗号化できません。ブート情報を含むシステムドライブとして使用するための個別のパーティションと、オペレーティングシステムドライブとして使用するための 2 番目のパーティションを作成し、オペレーティングシステムドライブを暗号化してください。
FVE_E_FAILED_WRONG_FS 0x80310013	ファイルシステムがサポートされていないので、ドライブを暗号化できません。
FVE_E_BAD_PARTITION_SIZE 0x80310014	ファイルシステムサイズが、パーティションテーブルのパーティションサイズを上回っています。このドライブは破損しているか、不正に変更されている可能性があります。BitLocker で使用するには、パーティションを再フォーマットする必要があります。
FVE_E_NOT_SUPPORTED 0x80310015	このドライブを暗号化できません。
FVE_E_BAD_DATA 0x80310016	データは有効ではありません。
FVE_E_VOLUME_NOT_BOUND 0x80310017	指定したデータドライブは、現在のコンピュータで自動的にロック解除するように設定されておらず、自動的にロック解除できません。
FVE_E_TPM_NOT_OWNED 0x80310018	BitLocker ドライブ暗号化を使用する前に、TPM を初期化する必要があります。
FVE_E_NOT_DATA_VOLUME 0x80310019	試みた操作は、オペレーティングシステムドライブ上では実行できません。
FVE_E_AD_INSUFFICIENT_BUFFER 0x8031001A	関数に与えられたバッファが、返されたデータを含めるには不十分でした。バッファサイズを増やしてから、関数を再度実行してください。
FVE_E_CONV_READ 0x8031001B	ドライブの変換中に読み取り操作が失敗しました。ドライブは変換されませんでした。BitLocker を再度有効にしてください。

定数 / 値	説明
FVE_E_CONV_WRITE 0x8031001C	ドライブの変換中に書き込み操作が失敗しました。ドライブは変換されませんでした。BitLocker を再度有効にしてください。
FVE_E_KEY_REQUIRED 0x8031001D	1 つまたは複数の BitLocker キー保護機能が必要です。このドライブ上の最後のキーは削除できません。
FVE_E_CLUSTERING_NOT_SUPPORTED 0x8031001E	BitLocker ドライブ暗号化では、クラスタ構成はサポートされていません。
FVE_E_VOLUME_BOUND_ALREADY 0x8031001F	指定したドライブはすでに、現在のコンピュータ上で自動的にロック解除するように設定されています。
FVE_E_OS_NOT_PROTECTED 0x80310020	オペレーティングシステムドライブは、BitLocker ドライブ暗号化で保護されていません。
FVE_E_PROTECTION_DISABLED 0x80310021	BitLocker ドライブ暗号化はこのドライブ上でサスペンドされています。このドライブに対して設定されているすべての BitLocker キー保護機能は、実質的に無効になっており、ドライブは非暗号化（クリア）キーを使用して自動的にロック解除されます。
FVE_E_RECOVERY_KEY_REQUIRED 0x80310022	BitLocker 保護が現在サスペンドされているので、ロックしようとしているドライブには、暗号化に使用できるキー保護機能がありません。BitLocker を再度有効にして、このドライブをロックしてください。
FVE_E_FOREIGN_VOLUME 0x80310023	BitLocker では、TPM を使用してデータドライブを保護することができません。TPM 保護は、オペレーティングシステムドライブにのみ使用できます。
FVE_E_OVERLAPPED_UPDATE 0x80310024	別のプロセスによってアップデート用にロックされていたので、暗号化されたドライブの BitLocker メタデータをアップデートできません。このプロセスを再試行してください。
FVE_E_TPM_SRK_AUTH_NOT_ZERO 0x80310025	TPM のストレージルートキー（SRK）の認証データはゼロでなく、したがって BitLocker と互換性がありません。BitLocker で使用しようとする前に、TPM を初期化してください。
FVE_E_FAILED_SECTOR_SIZE 0x80310026	このセクターサイズでは、ドライブ暗号化アルゴリズムを使用できません。
FVE_E_FAILED_AUTHENTICATION 0x80310027	入力したキーではドライブをロック解除できません。正しいキーを入力したことを確認してから、再試行してください。
FVE_E_NOT_OS_VOLUME 0x80310028	指定したドライブがオペレーティングシステムドライブではありません。
FVE_E_AUTOUNLOCK_ENABLED 0x80310029	このコンピュータに関連した固定データドライブとリムーバブルデータドライブに対して自動ロック解除機能が無効になるまで、BitLocker ドライブ暗号化は、オペレーティングシステムドライブでオフにすることはできません。
FVE_E_WRONG_BOOTSECTOR 0x8031002A	システムパーティションブートセクターは、TPM 測定を実行していません。Windows 回復環境の Bootrec.exe ツールを使用して、ブートセクターをアップデートまたは修復してください。
FVE_E_WRONG_SYSTEM_FS 0x8031002B	BitLocker ドライブ暗号化のオペレーティングシステムドライブを暗号化するには、NTFS ファイルシステムでフォーマットする必要がありま

定数 / 値	説明
	す。ドライブを NTFS に変換してから、BitLocker をオンにしてください。
FVE_E_POLICY_PASSWORD_REQUIRED 0x8031002C	グループポリシー設定では、ドライブを暗号化する前に、回復パスワードが指定されている必要があります。
FVE_E_CANNOT_SET_FVEK_ENCRYPTED 0x8031002D	ドライブ暗号化のアルゴリズムとキーは、以前に暗号化されたドライブ上では設定できません。BitLocker ドライブ暗号化でこのドライブを暗号化するには、以前の暗号化を削除してから BitLocker をオンにしてください。
FVE_E_CANNOT_ENCRYPT_NO_KEY 0x8031002E	暗号化キーが使用できないので、BitLocker ドライブ暗号化は、指定したドライブを暗号化できません。このドライブを暗号化するには、キー保護機能を追加してください。
FVE_E_BOOTABLE_CDDVD 0x80310030	BitLocker ドライブ暗号化が、コンピュータ内でブート可能メディア（CD または DVD）を検出しました。メディアを取り出して、コンピュータを再起動してから、BitLocker を設定してください。
FVE_E_PROTECTOR_EXISTS 0x80310031	このキー保護機能は追加できません。このドライブには、このタイプのキー保護機能は 1 つだけ許可されています。
FVE_E_RELATIVE_PATH 0x80310032	相対パスが指定されたので、回復パスワードファイルが見つかりませんでした。回復パスワードは,完全修飾パスに保存する必要があります。パスでは、コンピュータ上で設定された環境変数を使用できます。
FVE_E_PROTECTOR_NOT_FOUND 0x80310033	指定したキー保護機能がドライブ上に見つかりませんでした。別のキー保護機能を試してください。
FVE_E_INVALID_KEY_FORMAT 0x80310034	入力した回復キーは破損しており、ドライブへのアクセスに使用できません。ドライブへのアクセスを回復するには、回復パスワード、データ回復エージェント、バックアップバージョンの回復キーなどの代替の回復方法を使用する必要があります。
FVE_E_INVALID_PASSWORD_FORMAT 0x80310035	入力された回復パスワードの形式が無効です。BitLocker 回復パスワードは 48 桁です。回復パスワードが正しい形式であることを確認してから、再試行してください。
FVE_E_FIPS_RNG_CHECK_FAILED 0x80310036	ランダム数ジェネレータのチェックテストは失敗しました。
FVE_E_FIPS_PREVENTS_RECOVERY_PASSWORD 0x80310037	FIPS コンプライアンスを必要とするグループポリシー設定により、BitLocker ドライブ暗号化でローカルの回復パスワードを生成することも使用することもできません。FIPS 対応モードで操作する場合は、BitLocker 回復オプションを、USB ドライブに保存された回復キーにすることも、データ回復エージェントを通じた回復キーにすることもできます。
FVE_E_FIPS_PREVENTS_EXTERNAL_KEY_EXPORT 0x80310038	FIPS コンプライアンスを必要とするグループポリシー設定により、回復パスワードを Active Directory に保存できません。FIPS 対応モードで操作する場合は、BitLocker 回復オプションを、USB ドライブに保存された回復キーにすることも、データ回復エージェントを通じた回復キーにすることもできます。グループポリシー設定の構成をチェックしてください。
FVE_E_NOT_DECRYPTED 0x80310039	この操作を完了するために、ドライブを完全に復号化する必要があります。

定数 / 値	説明
FVE_E_INVALID_PROTECTOR_TYPE 0x8031003A	指定したキー保護機能は、この操作に使用できません。
FVE_E_NO_PROTECTORS_TO_TEST 0x8031003B	ハードウェアテストを実行するために、ドライブ上にはキー保護機能が存在していません。
FVE_E_KEYFILE_NOT_FOUND 0x8031003C	USB デバイス上に、BitLocker スタートアップキーも回復パスワードも見つかりませんでした。正しい USB デバイスがあり、USB デバイスがコンピュータのアクティブな USB ポートに差し込まれていることを確認して、コンピュータを再起動した後で再試行してください。問題が解決しない場合は、BIOS アップグレード手順について、コンピュータの製造元に問い合わせてください。
FVE_E_KEYFILE_INVALID 0x8031003D	入力された BitLocker スタートアップキーまたは回復パスワードファイルが破損しているか、無効です。正しいスタートアップキーまたは回復パスワードファイルであることを確認し、再試行してください。
FVE_E_KEYFILE_NO_VMK 0x8031003E	BitLocker 暗号化キーは、スタートアップキーまたは回復パスワードから取得できません。正しいスタートアップキーまたは回復パスワードであることを確認し、再試行してください。
FVE_E_TPM_DISABLED 0x8031003F	TPM が無効です。BitLocker ドライブ暗号化で使用する前に、TPM を有効にし、初期化し、TPM に有効な所有権を与える必要があります。
FVE_E_NOT_ALLOWED_IN_SAFE_MODE 0x80310040	このコンピュータは現在セーフモードで動作しているので、指定したドライブの BitLocker 構成は管理できません。セーフモードの間、BitLocker ドライブ暗号化は回復の目的にのみ使用できます。
FVE_E_TPM_INVALID_PCR 0x80310041	システムブート情報が変更したか、PIN が正しく入力されなかったため、TPM はドライブをロック解除できませんでした。ドライブが不正に変更されておらず、システムブート情報に対する変更は信頼されたソースによって行われたことを確認します。ドライブが安全にアクセスできることを確認した後、BitLocker 回復コンソールを使用してドライブをロック解除し、続いて BitLocker をサスペンドおよび再開して、BitLocker がこのドライブに関連付けるシステムブート情報をアップデートします。
FVE_E_TPM_NO_VMK 0x80310042	BitLocker 暗号化キーを TPM から取得できません。
FVE_E_PIN_INVALID 0x80310043	BitLocker 暗号化キーを TPM および PIN から取得できません。
FVE_E_AUTH_INVALID_APPLICATION 0x80310044	BitLocker ドライブ暗号化が有効になったときから、ブートアプリケーションは変更しています。
FVE_E_AUTH_INVALID_CONFIG 0x80310045	BitLocker ドライブ暗号化が有効になったときから、ブート構成データ（BCD）設定は変更しています。
FVE_E_FIPS_DISABLE_PROTECTION_NOT_ALLOWED 0x80310046	FIPS コンプライアンスを必要とするグループポリシー設定では、非暗号化キーの使用が禁じられているため、このデバイスで BitLocker はサスペンドされません。詳細については、ドメイン管理者に連絡してください。

定数 / 値	説明
FVE_E_FS_NOT_EXTENDED 0x80310047	ファイルシステムがドライブの最後まで拡張していないので、このデバイスは、 BitLocker ドライブ暗号化で暗号化できません。このドライブを再パーティションしてから、 再試行してください。
FVE_E_FIRMWARE_TYPE_NOT_SUPPORTED 0x80310048	BitLocker ドライブ暗号化は、 オペレーティングシステムドライブ上では有効にできません。 BIOS アップグレード手順については、 コンピュータの製造元に問い合わせてください。
FVE_E_NO_LICENSE 0x80310049	このバージョンの Windows には、 BitLocker ドライブ暗号化が含まれていません。 BitLocker ドライブ暗号化を使用するには、 オペレーティングシステムをアップグレードしてください。
FVE_E_NOT_ON_STACK 0x8031004A	重要な BitLocker システムファイルが欠落しているか破損しているため、 BitLocker ドライブ暗号化を使用できません。 Windows スタートアップ修復を使用して、 コンピュータにこれらのファイルを復元します。
FVE_E_FS_MOUNTED 0x8031004B	ドライブの使用中にはドライブをロックできません。
FVE_E_TOKEN_NOT_IMPERSONATED 0x8031004C	現在のスレッドに関連したアクセストークンが偽造トークンではありません。
FVE_E_DRY_RUN_FAILED 0x8031004D	BitLocker 暗号化キーを取得できません。 TPM が有効で、 所有権が取得されていることを確認してください。 このコンピュータに TPM が搭載されていない場合、 USB ドライブが取り付けられ使用可能であることを確認します。
FVE_E_REBOOT_REQUIRED 0x8031004E	BitLocker ドライブ暗号化を続ける前に、 コンピュータを再起動する必要があります。
FVE_E_DEBUGGER_ENABLED 0x8031004F	ブートデバッグが有効である間、 ドライブ暗号化を行えません。 bcdedit コマンドラインツールを使用して、 ブートデバッグをオフにします。
FVE_E_RAW_ACCESS 0x80310050	BitLocker ドライブ暗号化が raw アクセスモードであるときに、 アクションが行われませんでした。
FVE_E_RAW_BLOCKED 0x80310051	このドライブは現在使用中なので、 このドライブで BitLocker ドライブ暗号化は raw アクセスモードに移れません。
FVE_E_BCD_APPLICATIONS_PATH_INCORRECT 0x80310052	BitLocker ドライブ暗号化の完全性保護アプリケーションについてブート構成データ（BCD）で指定したパスが正しくありません。 BCD 設定を確認して修正し、 再試行してください。
FVE_E_NOT_ALLOWED_IN_VERSION 0x80310053	BitLocker ドライブ暗号化は、 コンピュータが事前インストールまたは回復環境で実行しているときに、 限定的なプロビジョニングまたは回復の目的で使用できます。
FVE_E_NO_AUTOUNLOCK_MASTER_KEY 0x80310054	自動ロック解除マスターキーはオペレーティングシステムドライブから使用できませんでした。
FVE_E_MOR_FAILED 0x80310055	システムファームウェアは、 コンピュータが再起動したときに、 システムメモリのクリアを有効にできませんでした。
FVE_E_HIDDEN_VOLUME	非表示のドライブを暗号化できません。

定数 / 値	説明
0x80310056	
FVE_E_TRANSIENT_STATE 0x80310057	ドライブが過渡状態であったため、BitLocker 暗号化キーが無視されました。
FVE_E_PUBKEY_NOT_ALLOWED 0x80310058	このドライブ上では、公開鍵ベースの保護機能は許可されていません。
FVE_E_VOLUME_HANDLE_OPEN 0x80310059	BitLocker ドライブ暗号化はこのドライブ上ですでに操作を実行しています。続行する前にすべての操作を完了してください。
FVE_E_NO_FEATURE_LICENSE 0x8031005A	このバージョンの Windows は、BitLocker ドライブ暗号化のこの機能をサポートしていません。この機能を使用するには、オペレーティングシステムをアップグレードしてください。
FVE_E_INVALID_STARTUP_OPTIONS 0x8031005B	BitLocker スタートアップオプションのグループポリシー設定は競合しており、適用できません。詳細については、システム管理者に連絡してください。
FVE_E_POLICY_RECOVERY_PASSWORD_NOT_ALLOWED 0x8031005C	グループポリシー設定は、回復パスワードの作成を許可していません。
FVE_E_POLICY_RECOVERY_PASSWORD_REQUIRED 0x8031005D	グループポリシー設定は、回復パスワードの作成を必要としています。
FVE_E_POLICY_RECOVERY_KEY_NOT_ALLOWED 0x8031005E	グループポリシー設定は、回復キーの作成を許可していません。
FVE_E_POLICY_RECOVERY_KEY_REQUIRED 0x8031005F	グループポリシー設定は、回復キーの作成を必要としています。
FVE_E_POLICY_STARTUP_PIN_NOT_ALLOWED 0x80310060	グループポリシー設定は、スタートアップ時に PIN の使用を許可していません。別の BitLocker スタートアップオプションを選択してください。
FVE_E_POLICY_STARTUP_PIN_REQUIRED 0x80310061	グループポリシー設定は、スタートアップ時に PIN の使用を必要としています。この BitLocker スタートアップオプションを選択してください。
FVE_E_POLICY_STARTUP_KEY_NOT_ALLOWED 0x80310062	グループポリシー設定は、スタートアップキーの使用を許可していません。別の BitLocker スタートアップオプションを選択してください。
FVE_E_POLICY_STARTUP_KEY_REQUIRED 0x80310063	グループポリシー設定は、スタートアップキーの使用を必要としています。この BitLocker スタートアップオプションを選択してください。
FVE_E_POLICY_STARTUP_PIN_KEY_NOT_ALLOWED0x80310064	グループポリシー設定は、スタートアップキーと PIN の使用を許可していません。別の BitLocker スタートアップオプションを選択してください。
FVE_E_POLICY_STARTUP_PIN_KEY_REQUIRED 0x80310065	グループポリシー設定は、スタートアップキーと PIN の使用を必要としています。この BitLocker スタートアップオプションを選択してください。

定数 / 値	説明
FVE_E_POLICY_STARTUP_TPM_NOT_ALLOWED 0x80310066	グループポリシー設定は、スタートアップ時に TPM のみの使用を許可していません。別の BitLocker スタートアップオプションを選択してください。
FVE_E_POLICY_STARTUP_TPM_REQUIRED 0x80310067	グループポリシー設定は、スタートアップ時に TPM のみの使用を必要としています。この BitLocker スタートアップオプションを選択してください。
FVE_E_POLICY_INVALID_PIN_LENGTH 0x80310068	入力した PIN は、最小長または最大長の要件を満たしていません。
FVE_E_KEY_PROTECTOR_NOT_SUPPORTED 0x80310069	キー保護機能は、現在ドライブ上にある BitLocker ドライブ暗号化のバージョンではサポートされていません。ドライブをアップグレードして、キー保護機能を追加してください。
FVE_E_POLICY_PASSPHRASE_NOT_ALLOWED 0x8031006A	グループポリシー設定は、パスワードの作成を許可していません。
FVE_E_POLICY_PASSPHRASE_REQUIRED 0x8031006B	グループポリシー設定は、パスワードの作成を必要としています。
FVE_E_FIPS_PREVENTS_PASSPHRASE 0x8031006C	FIPS コンプライアンスを必要とするグループポリシー設定により、パスワードを生成することも使用することもできません。詳細については、ドメイン管理者に連絡してください。
FVE_E_OS_VOLUME_PASSPHRASE_NOT_ALLOWED 0x8031006D	パスワードをオペレーティングシステムドライブに追加できません。
FVE_E_INVALID_BITLOCKER_OID 0x8031006E	ドライブ上の BitLocker オブジェクト識別子（OID）が、無効であるか、破損しているようです。manage-BDE を使用して、このドライブ上で OID をリセットしてください。
FVE_E_VOLUME_TOO_SMALL 0x8031006F	ドライブが非常に小さいため、BitLocker ドライブ暗号化を使用して保護できません。
FVE_E_DV_NOT_SUPPORTED_ON_FS 0x80310070	選択した検出ドライブタイプが、ドライブ上のファイルシステムと互換性がありません。BitLocker To Go 検出ドライブは、FAT 形式のドライブで作成する必要があります。
FVE_E_DV_NOT_ALLOWED_BY_GP 0x80310071	選択した検出ドライブタイプは、コンピュータのグループポリシー設定で許可されていません。BitLocker To Go で使用する検出ドライブの作成がグループポリシー設定で許可されていることを確認してください。
FVE_E_POLICY_USER_CERTIFICATE_NOT_ALLOWED 0x80310072	グループポリシー設定では、スマートカードなどのユーザー証明書を、BitLocker ドライブ暗号化とともに使用することを許可していません。
FVE_E_POLICY_USER_CERTIFICATE_REQUIRED 0x80310073	グループポリシー設定では、BitLocker ドライブ暗号化とともに使用するスマートカードなどの有効なユーザー証明書を保有することを必要としています。
FVE_E_POLICY_USER_CERT_MUST_BE_HW 0x80310074	グループポリシー設定では、BitLocker ドライブ暗号化とともにスマートカードベースのキー保護機能を使用することを必要としています。
FVE_E_POLICY_USER_CONFIGURE_FDV_AUTOUNLOCK_NOT_ALLOWED	グループポリシー設定では、BitLocker 保護の固定データドライブが自動的にロック解除されることを許可していません。

定数 / 値	説明
0x80310075	
FVE_E_POLICY_USER_CONFIGURE_RDV_AUTOUNLOCK_NOT_ALLOWED 0x80310076	グループポリシー設定では、BitLocker 保護のリムーバブルデータドライブが自動的にロック解除されることを許可していません。
FVE_E_POLICY_USER_CONFIGURE_RDV_NOT_ALLOWED 0x80310077	グループポリシー設定では、リムーバブルデータドライブ上で BitLocker ドライブ暗号化を構成することを許可していません。
FVE_E_POLICY_USER_ENABLE_RDV_NOT_ALLOWED 0x80310078	グループポリシー設定では、リムーバブルデータドライブ上で BitLocker ドライブ暗号化をオンにすることを許可していません。BitLocker をオンにする必要がある場合は、システム管理者に連絡してください。
FVE_E_POLICY_USER_DISABLE_RDV_NOT_ALLOWED 0x80310079	グループポリシー設定では、リムーバブルデータドライブ上で BitLocker ドライブ暗号化をオフにすることを許可していません。BitLocker をオフにする必要がある場合は、システム管理者に連絡してください。
FVE_E_POLICY_INVALID_PASSPHRASE_LENGTH 0x80310080	パスワードが、最小パスワード長の要件を満たしていません。デフォルトでは、パスワードには少なくとも 8 文字の長さが必要です。組織でのパスワード長の要件については、システム管理者に確認してください。
FVE_E_POLICY_PASSPHRASE_TOO_SIMPLE 0x80310081	パスワードは、システム管理者が設定した複雑さの要件を満たしていません。大文字と小文字、数字、記号を追加してみてください。
FVE_E_RECOVERY_PARTITION 0x80310082	このドライブは、Windows システムリカバリオプション用に予約されているので、暗号化できません。
FVE_E_POLICY_CONFLICT_FDV_RK_OFF_AUK_ON 0x80310083	競合するグループポリシー設定のため、BitLocker ドライブ暗号化をこのドライブに適用できません。ユーザー回復オプションが無効になっているときに、自動的に固定データドライブをロック解除するように BitLocker を設定できません。キー検証が行われた後で BitLocker 保護された固定データドライブを自動的にロック解除する場合は、BitLocker を有効にする前に、システム管理者に設定の競合を解決してもらってください。
FVE_E_POLICY_CONFLICT_RDV_RK_OFF_AUK_ON 0x80310084	競合するグループポリシー設定のため、BitLocker ドライブ暗号化をこのドライブに適用できません。ユーザー回復オプションが無効になっているときに、自動的にリムーバブルデータドライブをロック解除するように BitLocker を設定できません。キー検証が行われた後で BitLocker 保護されたリムーバブルデータドライブを自動的にロック解除する場合は、BitLocker を有効にする前に、システム管理者に設定の競合を解決してもらってください。
FVE_E_NON_BITLOCKER_OID 0x80310085	指定した証明書の拡張キー使用法（EKU）属性では、BitLocker ドライブ暗号化に使用することを許可していません。BitLocker では、証明書に EKU 属性があることは必要ではありませんが、設定されている場合は、BitLocker に対して設定されたオブジェクト ID（OID）に一致する OID に設定されている必要があります。
FVE_E_POLICY_PROHIBITS_SELFSIGNED 0x80310086	グループポリシー設定のため、現在の設定どおりに BitLocker ドライブ暗号化をこのドライブに適用することはできません。ドライブ暗号化に指定した証明書は自己署名証明書です。現在のグループポリシー設定では、自己署名証明書の使用を許可していません。

定数 / 値	説明
	BitLocker を有効にしようとする前に、証明機関から新しい証明書を取得してください。
FVE_E_POLICY_CONFLICT_RO_AND_STARTUP_KEY_REQUIRED 0x80310087	競合するグループポリシー設定のため、BitLocker 暗号化をこのドライブに適用できません。BitLocker で保護されていないドライブへの書き込みアクセスが拒否された場合、USB スタートアップキーの使用を要求できません。BitLocker を有効にしようとする前に、システム管理者にこれらのポリシーの競合を解決してもらってください。
FVE_E_CONV_RECOVERY_FAILED 0x80310088	オペレーティングシステムドライブ上に回復オプションについて競合するグループポリシー設定があるので、BitLocker ドライブ暗号化をこのドライブに適用できません。回復パスワードの生成が許可されていない場合、Active Directory ドメインサービスへの回復情報の保存は要求できません。BitLocker を有効にしようとする前に、システム管理者にこれらのポリシーの競合を解決してもらってください。
FVE_E_VIRTUALIZED_SPACE_TOO_BIG 0x80310089	リクエストされた仮想化サイズが大きすぎます。
FVE_E_POLICY_CONFLICT_OSV_RP_OFF_ADB_ON 0x80310090	オペレーティングシステムドライブ上に回復オプションについて競合するグループポリシー設定があるので、BitLocker ドライブ暗号化をこのドライブに適用できません。回復パスワードの生成が許可されていない場合、Active Directory ドメインサービスへの回復情報の保存は要求できません。BitLocker を有効にしようとする前に、システム管理者にこれらのポリシーの競合を解決してもらってください。
FVE_E_POLICY_CONFLICT_FDV_RP_OFF_ADB_ON 0x80310091	固定データドライブ上に回復オプションについて競合するグループポリシー設定があるので、BitLocker ドライブ暗号化をこのドライブに適用できません。回復パスワードの生成が許可されていない場合、Active Directory ドメインサービスへの回復情報の保存は要求できません。BitLocker を有効にしようとする前に、システム管理者にこれらのポリシーの競合を解決してもらってください。
FVE_E_POLICY_CONFLICT_RDV_RP_OFF_ADB_ON 0x80310092	リムーバブルデータドライブ上に回復オプションについて競合するグループポリシー設定があるので、BitLocker ドライブ暗号化をこのドライブに適用できません。回復パスワードの生成が許可されていない場合、Active Directory ドメインサービスへの回復情報の保存は要求できません。BitLocker を有効にしようとする前に、システム管理者にこれらのポリシーの競合を解決してもらってください。
FVE_E_NON_BITLOCKER_KU 0x80310093	指定した証明書のキー使用法（KU）属性では、BitLocker ドライブ暗号化に使用することを許可していません。BitLocker では、証明書に KU 属性があることは必要ではありませんが、設定されている場合は、Key Encipherment か Key Agreement のどちらかに設定されている必要があります。
FVE_E_PRIVATEKEY_AUTH_FAILED 0x80310094	指定した証明書に関連した秘密キーを承認できません。秘密キーの承認が与えられていなかったか、与えられた承認が無効でした。
FVE_E_REMOVAL_OF_DRA_FAILED 0x80310095	データ回復エージェント証明書の削除は、証明書スナップインを使用して行う必要があります。
FVE_E_OPERATION_NOT_SUPPORTED_ON_VISTA_VOLUME 0x80310096	このドライブは、組織の識別子をサポートしていない Windows Vista および Windows Server 2008 に含まれていたバージョンの BitLocker ドライブ暗号化を使用して暗号化されました。このドライブの組織識別子を指定するには、「manage-bde -upgrade」コマンドを使用して、ドライブ暗号化を最新のバージョンにアップグレードしてください。

定数 / 値	説明
FVE_E_CANT_LOCK_AUTOUNLOCK_ENABLED_VOLUME 0x80310097	このコンピュータ上で自動的にロック解除されるので、ドライブをロックできません。このドライブをロックするには、自動ロック解除保護機能を削除してください。
FVE_E_FIPS_HASH_KDF_NOT_ALLOWED 0x80310098	ECC スマートカード用のデフォルトの BitLocker キー派生関数 SP800-56A は、お使いのスマートカードでサポートされていません。FIPS コンプライアンスを必要とするグループポリシー設定によって、BitLocker は、暗号化に他のキー派生関数を使用できません。FIPS の制限のある環境では、FIPS 対応のスマートカードを使用する必要があります。
FVE_E_ENH_PIN_INVALID 0x80310099	BitLocker 暗号化キーを TPM および拡張 PIN から取得できませんでした。数字だけから成る PIN を使用してみてください。
FVE_E_INVALID_PIN_CHARS 0x8031009A	リクエストされた TPM PIN に無効な文字が含まれています。
FVE_E_INVALID_DATUM_TYPE 0x8031009B	ドライブに保存された管理情報に不明なタイプが含まれていました。古いバージョンの Windows を使用している場合は、最新バージョンからドライブにアクセスしてみてください。
FVE_E_EFI_ONLY 0x8031009C	この機能は、EFI システムでのみサポートされています。
FVE_E_MULTIPLE_NKP_CERTS 0x8031009D	複数のネットワークキー保護機能証明書がシステム上で見つかりました。
FVE_E_REMOVAL_OF_NKP_FAILED 0x8031009E	ネットワークキー保護機能証明書の削除は、証明書スナップインを使用して行う必要があります。
FVE_E_INVALID_NKP_CERT 0x8031009F	無効な証明書が、ネットワークキー保護機能証明書ストアに見つかりました。
FVE_E_NO_EXISTING_PIN 0x803100A0	このドライブは PIN で保護されていません。
FVE_E_PROTECTOR_CHANGE_PIN_MISMATCH 0x803100A1	正しい現在の PIN を入力してください。
FVE_E_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED 0x803100A2	PIN またはパスワードを変更するには、管理者アカウントでログオンする必要があります。リンクをクリックして、管理者として PIN またはパスワードをリセットします。
FVE_E_PROTECTOR_CHANGE_MAX_PIN_CHANGE_ATTEMPTS_REACHED 0x803100A3	BitLocker は、非常に多くのリクエストが失敗した後、PIN およびパスワードの変更を無効にしました。リンクをクリックして、管理者として PIN またはパスワードをリセットします。
FVE_E_POLICY_PASSPHRASE_REQUIRES_ASCII 0x803100A4	システム管理者が、パスワードには印刷可能な ASCII 文字だけが含まれるように要求しています。これには、アクセントのない文字 (A ～ Z、a ～ z)、数字 (0 ～ 9)、空白、演算符号、一般的な句読点、区切り文字、および記号 # $ & @ ^ _ ~ が含まれます。
FVE_E_FULL_ENCRYPTION_NOT_ALLOWED_ON_TP_STORAGE	BitLocker ドライブ暗号化は、シンプロビジョニングされたストレージでの使用済み領域のみの暗号化だけをサポートしています。

定数 / 値	説明
0x803100A5	
FVE_E_WIPE_NOT_ALLOWED_ON_TP_STORAGE 0x803100A6	BitLocker ドライブ暗号化は、シンプロビジョニングされたストレージでの空き領域のワイピングをサポートしていません。
FVE_E_KEY_LENGTH_NOT_SUPPORTED_BY_EDRIVE 0x803100A7	必要な認証キー長がドライブでサポートされていません。
FVE_E_NO_EXISTING_PASSPHRASE 0x803100A8	このドライブはパスワードで保護されていません。
FVE_E_PROTECTOR_CHANGE_PASSPHRASE_MISMATCH 0x803100A9	正しい現在のパスワードを入力してください。
FVE_E_PASSPHRASE_TOO_LONG 0x803100AA	パスワードは 256 文字を超えられません。
FVE_E_NO_PASSPHRASE_WITH_TPM 0x803100AB	TPM 保護機能がドライブ上に存在しているので、パスワードキー保護機能を追加できません。
FVE_E_NO_TPM_WITH_PASSPHRASE 0x803100AC	パスワード保護機能がドライブ上に存在しているので、TPM キー保護機能を追加できません。
FVE_E_NOT_ALLOWED_ON_CSV_STACK 0x803100AD	このコマンドは、指定の CSV ボリュームのコーディネータノードからのみ実行できます。
FVE_E_NOT_ALLOWED_ON_CLUSTER 0x803100AE	このコマンドは、ボリュームがクラスタの一部である場合、そのボリューム上で実行できません。
FVE_E_EDRIVE_NO_FAILOVER_TO_SW 0x803100AF	BitLocker は、グループポリシー設定のため、BitLocker ソフトウェア暗号化の使用に復帰しませんでした。
FVE_E_EDRIVE_BAND_IN_USE 0x803100B0	ドライブのハードウェア暗号化機能がすでに使用されているので、BitLocker でドライブを管理できません。
FVE_E_EDRIVE_DISALLOWED_BY_GP 0x803100B1	グループポリシー設定では、ハードウェアベースの暗号化の使用を許可していません。
FVE_E_EDRIVE_INCOMPATIBLE_VOLUME 0x803100B2	指定したドライブは、ハードウェアベースの暗号化をサポートしていません。
FVE_E_NOT_ALLOWED_TO_UPGRADE_WHILE_CONVERTING 0x803100B3	ディスクの暗号化または復号化中は、BitLocker をアップグレードできません。
FVE_E_EDRIVE_DV_NOT_SUPPORTED 0x803100B4	検出ボリュームは、ハードウェア暗号化を使用したボリュームにはサポートされていません。
FVE_E_NO_PREBOOT_KEYBOARD_DETECTED 0x803100B5	起動前のキーボードが検出されませんでした。ユーザーは、ボリュームをロック解除するために必要な入力を提供できない場合があります。

定数 / 値	説明
FVE_E_NO_PREBOOT_KEYBOARD_OR_WINRE_DETECTED 0x803100B6	Windows 回復環境上のプレブートキーボードが検出されませんでした。ユーザーは、ボリュームをロック解除するために必要な入力を提供できない場合があります。
FVE_E_POLICY_REQUIRES_STARTUP_PIN_ON_TOUCH_DEVICE 0x803100B7	グループポリシー設定では、スタートアップ PIN の作成が必要ですが、このデバイス上ではプレブートキーボードを使用できません。ユーザーは、ボリュームをロック解除するために必要な入力を提供できない場合があります。
FVE_E_POLICY_REQUIRES_RECOVERY_PASSWORD_ON_TOUCH_DEVICE 0x803100B8	グループポリシー設定は、回復パスワードの作成を必要としていますが、プレブートキーボードと Windows 回復環境の両方がこのデバイス上で使用できません。ユーザーは、ボリュームをロック解除するために必要な入力を提供できない場合があります。
FVE_E_WIPE_CANCEL_NOT_APPLICABLE 0x803100B9	空き領域のワイプが現在行われていません。
FVE_E_SECUREBOOT_DISABLED 0x803100BA	セキュアブートが無効になっているので、BitLocker はプラットフォームの完全性にセキュアブートを使用できません。
FVE_E_SECUREBOOT_CONFIGURATION_INVALID 0x803100BB	セキュアブート構成が BitLocker の要件を満たしていないので、BitLocker はプラットフォームの完全性にセキュアブートを使用できません。
FVE_E_EDRIVE_DRY_RUN_FAILED 0x803100BC	お使いのコンピュータは、BitLocker ハードウェアベースの暗号化をサポートしていません。ファームウェアのアップデートについてコンピュータの製造元に確認してください。
FVE_E_SHADOW_COPY_PRESENT 0x803100BD	ボリュームシャドウコピーが含まれているため、ボリューム上で BitLocker を有効にできません。ボリュームを暗号化する前に、ボリュームシャドウコピーをすべて削除してください。
FVE_E_POLICY_INVALID_ENHANCED_BCD_SETTINGS 0x803100BE	拡張ブート構成データのグループポリシー設定に無効なデータが含まれているので、BitLocker ドライブ暗号化をこのドライブに適用できません。BitLocker を有効にしようとする前に、システム管理者にこの無効な構成を解決してもらってください。
FVE_E_EDRIVE_INCOMPATIBLE_FIRMWARE 0x803100BF	この PC のファームウェアが、ハードウェア暗号化をサポートできません。
FVE_E_PROTECTOR_CHANGE_MAX_PASSPHRASE_CHANGE_ATTEMPTS_REACHED 0x803100C0	BitLocker は、非常に多くのリクエストが失敗した後、パスワードの変更を無効にしました。リンクをクリックして、管理者としてパスワードをリセットします。
FVE_E_PASSPHRASE_PROTECTOR_CHANGE_BY_STD_USER_DISALLOWED 0x803100C1	パスワードを変更するには、管理者アカウントでログオンする必要があります。リンクをクリックして、管理者としてパスワードをリセットします。
FVE_E_LIVEID_ACCOUNT_SUSPENDED 0x803100C2	指定した Microsoft アカウントがサスペンドであるため、BitLocker は回復パスワードを保存できません。
FVE_E_LIVEID_ACCOUNT_BLOCKED 0x803100C3	指定した Microsoft アカウントがブロックされているため、BitLocker は回復パスワードを保存できません。

定数 / 値	説明
FVE_E_NOT_PROVISIONED_ON_ALL_VOLUMES 0x803100C4	この PC は、デバイスの暗号化をサポートするようにプロビジョニングされていません。デバイス暗号化ポリシーに準拠するように、すべてのボリュームで BitLocker を有効にしてください。
FVE_E_DE_FIXED_DATA_NOT_SUPPORTED 0x803100C5	非暗号化固定データボリュームが存在しているので、この PC はデバイス暗号化をサポートできません。
FVE_E_DE_HARDWARE_NOT_COMPLIANT 0x803100C6	この PC はデバイス暗号化をサポートするためのハードウェア要件を満たしていません。
FVE_E_DE_WINRE_NOT_CONFIGURED 0x803100C7	WinRE が正しく設定されていないので、この PC はデバイス暗号化をサポートできません。
FVE_E_DE_PROTECTION_SUSPENDED 0x803100C8	ボリューム上で保護は有効ですが、サスペンドになっています。これは、アップデートがシステムに適用されているために起きた可能性があります。再起動後に再試行してください。
FVE_E_DE_OS_VOLUME_NOT_PROTECTED 0x803100C9	この PC は、デバイスの暗号化をサポートするようにプロビジョニングされていません。
FVE_E_DE_DEVICE_LOCKEDOUT 0x803100CA	何度も間違ったパスワードが試みられたため、デバイスロックがトリガされました。
FVE_E_DE_PROTECTION_NOT_YET_ENABLED 0x803100CB	ボリュームで保護が有効になっていません。保護を有効にするには接続済みのアカウントが必要です。すでに接続したアカウントがあるときに、このエラーが表示される場合は、詳細についてイベントログを参照してください。
FVE_E_INVALID_PIN_CHARS_DETAILED 0x803100CC	PIN には、0 から 9 の数字しか含められません。
FVE_E_DEVICE_LOCKOUT_COUNTER_UNAVAILABLE 0x803100CD	お使いの PC 上でカウンタを使用できないので、BitLocker はハードウェアリプレイ保護を使用できません。
FVE_E_DEVICELOCKOUT_COUNTER_MISMATCH 0x803100CE	カウンタの不一致のために、デバイスロックアウト状態の検証が失敗しました。
FVE_E_BUFFER_TOO_LARGE 0x803100CF	入力バッファが大きすぎます。

19

用語集

アクティブ化 - コンピュータが Dell Server に登録され、少なくともポリシーの初期セットを受け取ったときにアクティブ化が実行されます。

Active Directory（AD）：Windows ドメインネットワーク用に Microsoft が開発したディレクトリサービスです。

Application Data Encryption - Application Data Encryption は、保護対象のアプリケーションによって書き込まれたすべてのファイルを、カテゴリ 2 のオーバーライドを使用して暗号化します。つまり、カテゴリ 2 以上の保護を受けているディレクトリ、またはカテゴリ 2 以上の保護を受けている特定の拡張子を持つ場所については、そこにあるファイルを ADE が暗号化することはありません。

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。

キャッシュされた資格情報：キャッシュされた資格情報とは、ユーザーが Active Directory で正しく認証されると PBA データベースに追加される資格情報のことです。ユーザーに関するこの情報は、ユーザーが Active Directory に接続できないとき（例えば、ノートブックを自宅に持ち帰るなど）でもログインできるように保持されます。

共有暗号化 - 共有キーを使用すると、すべての管理対象ユーザーが、暗号化されたファイルが作成されたデバイス上でそれらのファイルにアクセスできるようになります。

非アクティブ化 – 非アクティブ化は、管理コンソールで SED Manager 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 - Encryption 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を保護します。

Encryption External Media アクセスコード - 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 - エンドポイントがネットワークに接続されている、いないにかかわらず、あるいは紛失または盗難に遭ったかどうかにかかわらず、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 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ーとして動作し、一貫して適用される認証、暗号化、および許可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 - コンテキスト、コンピュータ、モバイルデバイス、または外部メディアによって異なります。

暗号化キー – ほとんどの場合、Encryption クライアントはユーザーキーに加え 2 つの別の暗号化キーを使用します。しかし、すべての SDE ポリシーと Secure Windows Credentials ポリシーが SDE キーを使用するという例外があります。Windows ページングファイルの暗号化ポリシーと Windows 休止状態ファイルのセキュア化ポリシーは、独自のキーである General Purpose Key (GPK) を使用します。共有キーを使用すると、すべての管理対象ユーザーが、暗号化されたファイルが作成されたデバイス上でそれらのファイルにアクセスできるようになります。ユーザーキーでは、ファイルを作成したユーザーのみが、ファイルが作成されたデバイス上のみでそれらのファイルにアクセスすることができます。ユーザーローミングキーでは、ファイルを作成したユーザーのみが、任意の Shielded Windows（または Mac）デバイス上でそれらのファイルにアクセスできます。

暗号化スイープ – 含まれるファイルが適切な暗号化状態になるように、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、暗号化の有効と無効を切り替えると、暗号化スイープがトリガされます。

マシンキー - サーバーに暗号化がインストールされている場合、マシンキーにより、サーバーのファイル暗号化キーとポリシーキーが保護されます。マシンキーは、デルサーバ上に保存されます。新しいサーバは、アクティブ化中に Dell Server と証明書を交換し、それ以降の認証イベントでその証明書を使用します。

起動前認証（PBA）- 起動前認証（PBA）は、BIOS または起動ファームウェアの拡張機能としての役割を果たし、信頼された認証レイヤとして、オペレーティングシステム外部のセキュアな耐タンパ環境を保証します。PBA は、ユーザーが正しい資格情報を持っていることを立証するまで、オペレーティングシステムなどをハードディスクから読み取ることができないようにします。

SED Manager - SED Manager 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 Manager 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 Manager 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 - サーバオペレーティングシステムでの暗号化キーの操作とポリシーアップデートの目的で 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。

System Data Encryption（SDE） – SDE は、オペレーティングシステムとプログラムファイルを暗号化するように設計されています。この目的を達成するために、SDE はオペレーティングシステムが起動している間にそのキーを開くことができる必要があります。これは、攻撃者によるオペレーティングシステムの改ざん、またはオフライン攻撃を防ぐためのものです。ユーザーデータは SDE 対象外です。共通キー暗号化およびユーザーキー暗号化は、暗号化キーのロック解除にユーザーパスワードを必要とするため、機密ユーザーデータを対象にしています。SDE ポリシーは、起動プロセスを開始するためにオペレーティングシステムが必要とするファイルを暗号化しません。SDE ポリシーに、起動前認証、またはマスターブートレコードとのインターフェースは、形態にかかわらず必要ありません。コンピュータの起動時、ユーザーログイン前に暗号化されたファイルが使用可能になります（パッチ管理、SMS、バックアップ、およびリカバリツールの有効化のため）。SDE を無効にすると、SDE 暗号化ルールなどの他の SDE ポリシーとは無関係に、関連するユーザーのすべての SDE 暗号化ファイルおよびディレクトリの自動復号化がトリガされます。

Trusted Platform Module（TPM） – TPM は、セキュアストレージ、測定、および構成証明という 3 つの主要機能を備えたセキュリティチップです。Encryption クライアントは、セキュアなストレージ機能のために TPM を使用します。TPM はまた、ソフトウェア資格情報コンテナ用に暗号化されたコンテナも提供できます。

ユーザー暗号化 – ユーザーキーを使用すると、ファイルを作成したユーザーのみが、ファイルが作成されたデバイス上でのみファイルにアクセスできるようになります。Dell Server Encryption を実行しているときは、ユーザー暗号化が共有暗号化に変換されます。リムーバブルメディアデバイスの場合には例外があり、Encryption がインストールされているサーバに外部メディアデバイスが挿入されると、ファイルはユーザーローミングキーで暗号化されます。