Dell Encryption Personal

Installation Guide v11.9

January 2024
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

概要

このガイドでは、Advanced Authentication と Encryption Personal を同時にインストールすることを前提とします。

Encryption Personal

Encryption Personal は、コンピュータを紛失した、またはコンピュータが盗難に遭ったときでも、コンピュータ上のデータを保護することを目的としています。

Encryption Personal は、機密データのセキュリティを確保するためにお使いの Windows コンピュータ上のデータを暗号化します。コンピュータにログインしている間はいつでもデータにアクセスできますが、未許可のユーザーはこの保護対象データにアクセスすることはできません。データはデバイス上で常に暗号化されたままとなりますが、暗号化は透過的であるため、ユーザーがアプリケーションおよびデータを扱う方法を変える必要はありません。

通常、アプリケーションは、ユーザーが作業を進めると同時にデータを復号化します。時折、アプリケーションがファイルを暗号化または復号化しているときに、アプリケーションがそのファイルに同時アクセスしようとすることがあります。この状況が発生した場合、暗号化 / 復号化を待機する、またはキャンセルするオプションを提供するダイアログが 1〜2 秒後に表示されます。待機を選択する場合、アプリケーションは、作業を終えるとすぐにファイルを解放します（通常数秒以内）。

Advanced Authentication

Data Security Console は、ローカル管理者によって設定されたポリシーに基づいて、ユーザーがそれぞれの PBA 資格情報およびセルフリカバリ質問を設定する手順をガイドするインターフェイスです。

Advanced Authentication の使用方法については、Advanced Authentication 管理者設定に関する項および『*Dell Data Security Console User Guide*』（Dell Data Security Console ユーザーガイド）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

この要件には、Encryption Personal のインストールに必要な要件をすべて詳述します。

暗号化

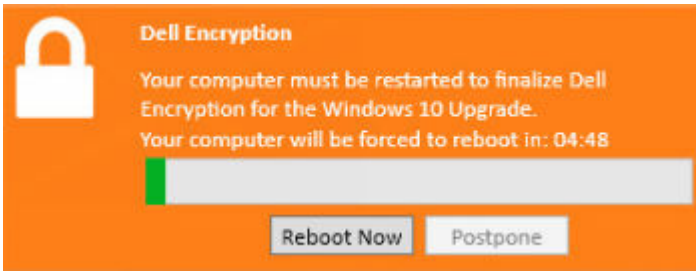
- Encryption Personal を正常にインストールするには資格が必要です。この資格は、Encryption Personal 購入時に提供されます。Encryption Personal を購入する方法に応じて、それに付随する簡単な手順を使用して、資格を手動でインストールすることができます。また、コマンド ラインで資格を入力することもできます。Encryption Personal を Dell Digital Delivery によってインストールした場合、資格のインストールは Dell Digital Delivery サービスによってすでに完了しています（Encryption Enterprise と Encryption Personal では同じバイナリが使用されます。どのバージョンをインストールするかは、資格によって指定されます）。
- Encryption Personal v11.0 以降を Windows 10 で実行している場合、Microsoft および Office 365 アカウントがサポートされます。
- Encryption Personal で Microsoft Live アカウントを有効にするには、KB 記事 124722 を参照してください。
- 暗号化データへのアクセスを保護するため、Windows パスワードが必要です（まだパスワードが存在しない場合）。コンピューター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。パスワードが作成されていない場合、Encryption Personal のアクティブ化が失敗します。
- 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。
- 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。

1. Windows のコントロール パネルに移動します（**スタート** > **コントロール パネル**）。
2. **ユーザー アカウント**アイコンをクリックします。
3. **アカウントのパスワードの作成**をクリックします。
4. 新しいパスワードを入力し、再度パスワードを入力します。
5. 任意でパスワードのヒントを入力します。
6. **パスワードの作成**をクリックします。
7. コンピューターを再起動します。

- 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 SMS 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/アンインストール/アップグレードを開始する前に、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/アンインストール/アップグレード中は、外付け（USB）ドライブの挿入や取り外しを含め、コンピューターに変更を加えないでください。
- 最初の暗号化にかかる時間を短縮するために（または同様にアンインストール時の復号化の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。
- 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 クライアントは、デュアル ブート設定をサポートしていません。これは、もう一方のオペレーティング システムのシステム ファイルが暗号化され、その動作を妨げるおそれがあるためです。
- 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。疑問点や不明点がある場合は、Dell ProSupport にお問い合わせください。
- Encryption クライアントは監査モードをサポートするようになりました。監査モードでは、管理者はサードパーティの SCCM または類似のソリューションを使用してではなく、企業用イメージの一部として、Encryption クライアントを展開できます。企業用イメージに Encryption クライアント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。
- 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 クライアント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。
- 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。

- オペレーティング システムの再インストールもサポートされていません。オペレーティング システムを再インストールするには、ターゲット コンピュータ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。
- 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。
- 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。



動作条件

- Microsoft .Net Framework 4.5.2（またはそれ以降）は、マスター インストーラーおよび子インストーラーに必要です。インストーラーは、Microsoft .Net Framework コンポーネントをインストールしません。

  メモ: FIPS モードを実行する場合は、.Net Framework 4.6（またはそれ以降）が必要です。

- 次のような動作条件がコンピューターにまだインストールされていない場合は、マスター インストーラーによってインストールされます。**子インストーラーを使用する場合**は、Encryption をインストールする前に、こ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 更新プログラム 3 以降再頒布可能パッケージ（x86 または x64） ○ 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。

ハードウェア

- 次の表に、サポートされている最小要件のコンピューター ハードウェアについて詳しく示します。

ハードウェア
○ インテル Pentium または AMD プロセッサー ○ 110 MB の使用可能ディスク領域 ○ 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領域が必要になります。このサイズは、ポリシーとドライブの容量によって異なります。

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

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

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

- 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 の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) **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 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

ローカライズ

- Encryption は複数言語ユーザー インターフェイス準拠で、次の言語でローカライズされています。

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

SED Manager

- IPv6 はサポートされていません。
- ポリシーを適用し、ポリシーの実施を開始できる状態になったら、コンピュータ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。
- SED Manager はマルチドライブ構成ではサポートされません。
- **メモ:**

  RAID と SED の性質上、SED Manager では RAID はサポートされません。SED の［*RAID=On*］には、RAID では、ディスクにアクセスして、SED がロック状態のために利用できない上位セクターの RAID 関連データを読み書きする必要があり、ユーザーがログオンするまで待機してこのデータを読み取ることができないという問題があります。この問題を解決するには、BIOS で SATA の動作を［*RAID=On*］から［*AHCI*］に変更します。オペレーティング システムに AHCI コントローラー ドライバーがプレインストールされていないと、［*RAID=On*］から［*AHCI*］に切り替えるときにオペレーティング システムがクラッシュします。

- 次のような動作条件がコンピューターにまだインストールされていない場合は、マスター インストーラーによってインストールされます。**子インストーラーを使用する場合**は、SED Manager をインストールする前に、こ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 更新プログラム 3 以降再頒布可能パッケージ（x86 または x64）
○ 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 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、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。

  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が SED である必要があります。
  - ターゲット システム内のすべてのディスクが同じブート モードで設定されている必要があります。
  - 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。
- 一部の BIOS バージョンでは、デフォルトで Block SID が有効になっている場合があり、SED Manager を阻害する可能性があります。詳細については、KB 記事 126083 を参照してください。
- 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 Dell Encryption 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。

- **メモ:** 起動前認証ではパスワードが必要です。パスワードは 9 文字以上にすることをお勧めします。

- **メモ:** ［ユーザーの追加］パネルで追加したすべてのユーザーにパスワードが必要です。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。
- 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。

ハードウェア

- 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、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。

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 10 2019 LTSC ■ Windows 10 2021 LTSC ○ Windows 11：Enterprise、Pro v21H2～22H2

認証機能は、起動前認証を有効にしている場合にのみ使用できます。

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 モードおよび起動前認証は、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	

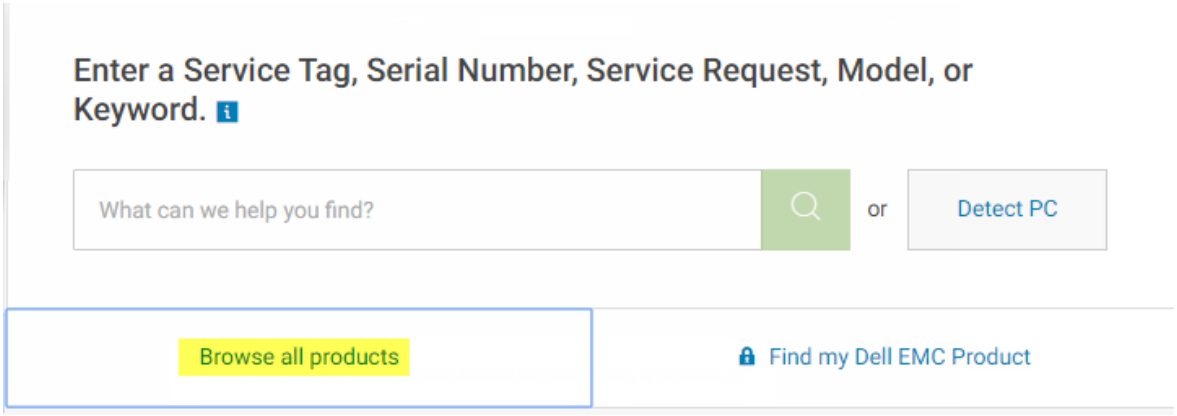
3

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。

   続けて Encryption Personal のインストールを実行します。

4

インストール

Encryption Personal は、マスターインストーラを使用してインストール（推奨）、またはマスターインストーラから子インストーラを抽出してインストールすることができます。いずれの方法でも、Encryption Personal は、ユーザーインタフェース、コマンドラインまたはスクリプト、および組織で使用可能な任意のプッシュテクノロジを使用してインストールできます。

ユーザーは、アプリケーションに関するサポートについては次のヘルプファイルを参照するようにしてください。

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。

- 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` からアクセスできます。
- Advanced Authentication の各機能の使用方法については、*Encryption Personal* 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\Security Tools\Help` からアクセスできます。

資格情報のインポート

Encryption Personal のインストールには、ターゲット コンピューターのレジストリー キーが必要です。このレジストリー キーは、インストール中にコマンド ライン インターフェイスで追加するか、インストールの前に GUI で追加しておきます。

コマンド ライン インターフェイスでレジストリー キーを追加する場合は、「コマンド ラインでのインストール」を参照してください。

GUI でレジストリー キーを追加する場合は、次の手順に従ってください。

1. テキスト エディターを開きます。
2. 次のテキストを追加します。

```
[HKEY_LOCAL_MACHINE\Software\Dell\Dell Data Protection\Entitlement]

"SaEntitlement"="1:PE:{XXXXX-XXX-XXXX-XXX-XXXX-
XXXXXXXXXXXX}:xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX="
```

3. テキスト ファイルに拡張子 `.reg` を付けて保存します。
4. 保存したレジストリー ファイルをダブルクリックして、Encryption Personal の資格情報をインポートします。

インストール方法の選択

クライアントのインストールには 2 種類の方法があります。次の方法の **いずれかひとつ** を選択してください。

- 対話型のインストール - 推奨
- コマンド ラインでのインストール

対話型インストール

Encryption Personal をインストールするには、コンピュータ上の適切な資格がインストーラによって検出される必要があります。適切な資格が見つからない場合は、Encryption Personal をインストールできません。

- マスターインストーラは、複数のクライアントをインストールします。Encryption Personal の場合は、Encryption と SED 管理がインストールされます。
- マスターインストーラログファイルのあるで `C:\ProgramData\Dell\Dell Data Protection\Installer.`

1. 作業を始める前に、必要に応じてインストール先のコンピュータに資格をインストールします。コンピューターに資格を追加する手順は、ライセンス情報を説明する電子メールに記載されています。
2. DDSSetup.exe をローカルコンピュータにコピーします。
3. DDSSetup.exe をダブルクリックしてインストーラを起動します。
4. インストールの前提条件のステータスに関するアラートを示すダイアログが表示されます。これには数分かかります。
5. ようこその画面で次へをクリックします。
6. ライセンス契約を読み、条項に同意して、**次へ** をクリックします。
7. **次へ**をクリックして、Encryption Personal を次のデフォルトの場所にインストールします。 `C:\Program Files\Dell\Dell Data Protection\.`
8. Authentication はデフォルトでインストールされており、選択解除できません。これは、インストーラでは Security Framework として表示されます。

   次へ をクリックします。
9. **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。

   ステータスウィンドウが表示されます。これには数分かかります。
10. [**はい、今すぐコンピューターを再起動します**] を選択し、[**完了**] をクリックします。
11. コンピュータが再起動されたら、Windows の認証を行います。

Encryption Personal および Advanced Authentication のインストールが完了します。

Encryption Personal のセットアップウィザードと構成は、個別に説明します。

Encryption Personal セットアップウィザードと設定が終了したら、Encryption Personal 管理者コンソールを起動します。

このセクションで詳細を複数のインストール作業の残りのとがスキップされる場合があります。「Advanced Authentication と Encryption Personal のセットアップウィザード」に進んでください。

コマンド ラインでのインストール

コマンド ラインを使用して Encryption Personal をインストールするには、最初にマスター インストーラーから子実行可能ファイルを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。完了したら、この項に戻ります。

- 作業を始める前に、必要に応じてインストール先のコンピュータに資格をインストールします。
- **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。
- スイッチ

  コマンド ラインを使用したインストールでは、最初にスイッチを指定する必要があります。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
/s	サイレントモード
/z	InstallScript システム変数 CMDLINE にデータを渡す

- パラメーター：

  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
InstallPath=path to alternate installation location.
FEATURE=PE
ENTITLEMENT=1:PE:{Encryption Personal Entitlement key here} **メモ:** このパラメータは、Encryption Personal で***のみ***使用できます

- コマンド ライン インストールの例

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。

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。

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。

コマンドラインは大文字と小文字を区別します。

- 次の例では、Encryption client をインストール（サイレント インストール、再起動なし、デフォルトの場所の `C:\Program Files\Dell\Dell Data Protection` にインストール）して、資格キーをインストーラーに直接渡します。

  DDPE_XXbit_setup.exe /s /v"ENTITLEMENT=1:PE:{XXXXX-XXX-XXXX-XXX-XXXX-XXXXX-XXXXXXX}:xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX= /l*v c:\Shieldinstall.log /qn /norestart"

- 次の例では、Encryption Personal および Advanced Authentication をインストール（サイレント インストール、再起動なし、デフォルトの場所の `C:\Program Files\Dell\Dell Data Protection` にインストール）します。

  ```
  DDSSetup.exe /s /z"\"FEATURE=PE\""
  ```

- 次の例では、Encryption Personal および Advanced Authentication をインストール（サイレント インストール、再起動なし、代替の場所の `C:\Program Files\Dell\My_New_Folder` にインストール）します。

  ```
  DDSSetup.exe /s /z"\"FEATURE=PE, InstallPath=C:\Program Files\Dell\My_New_Folder\""
  ```

  コンピュータが再起動されたら、Windows の認証を行います。

  Encryption Personal および Advanced Authentication のインストールが完了します。

  Encryption Personal のセットアップウィザードと構成は、個別に説明します。

  Encryption Personal セットアップウィザードと設定が終了したら、Encryption Personal 管理者コンソールを起動します。

  このセクションで詳細を複数のインストール作業の残りのとがスキップされる場合があります。Advanced Authentication と Personal Edition のセットアップウィザードに進んでください。

5

Encryption Personal

Windows のユーザー名とパスワードを使用してログオンします。ユーザーは Windows にシームレスにパスされます。インターフェイスを認識するのに慣れ以外の外観が異なる場合があります。

1. UAC によりアプリケーションを実行するよう求められる場合があります。その場合は、 [はい] をクリックします。
2. 初期インストールを再起動した後、 Advanced Authentication のアクティブ化ウィザードが表示されます。 **次へ** をクリックします。
3. 新しい Encryption 管理者パスワード（EAP）を入力し、再入力します。 **次へ** をクリックします。

   注： Encryption 管理者パスワードは 8 文字以上、127 文字以下にする必要があります。
4. 入力をバックアップの場所には、ネットワークドライブ、またはリムーバブルメディアに保存するためのリカバリ情報とクリックします次 **へを**押します。
5. **適用** をクリックして Advanced Authentication のアクティベーションを開始します。

   Advanced Authentication のアクティブ化ウィザードが終了したら、次の手順に進みます。
6. 通知領域にある Dell Encryption アイコンから Encryption Personal セットアップウィザードを起動します（単独で起動できます）。

   セットアップウィザードは、このコンピュータ上の情報を保護するための暗号化の使用に役立ちます。このウィザードが完了していない場合は、暗号化は開始されます。

   ようこそ画面を読み、 **次へ** をクリックします。
7. ポリシーテンプレートを選択します。ポリシーテンプレートはデフォルトポリシー設定を確立します。

   初期設定を完了すると、ローカル管理コンソールにおける異なるポリシーテンプレートの適用、または選択したテンプレートのカスタム化を簡単に行うことができるようになります。

   次へ をクリックします。
8. Windows パスワードの警告を読み、確認します。この時点で Windows パスワードを作成する場合は、 要件に関する項を参照してください。
9. 8～127 文字の Encryption 管理者パスワード（EAP）を作成して確認します。このパスワードには、英字、数字、および特殊文字を含める必要があります。このパスワードは、Advanced Authentication 用に設定した EAP と同じでも構いませんが、関連していません。**このパスワードを記録して、安全な場所に保管してください。次へ** をクリックします。

   注： Encryption 管理者パスワードは 8 文字以上、127 文字以下にする必要があります。
10. **参照** をクリックして、暗号化キー（LSARecovery_[hostname].exe という名前のアプリケーションでラップされています）をバックアップするネットワークドライブまたはリムーバブルストレージを選択します。

    コンピュータに特定の不具合が生じた場合、これらのキーがデータの回復に使用されます。

    さらに、将来のポリシー変更により、暗号化キーの再バックアップが必要になることもあります。ネットワークドライブまたはリムーバブルストレージが使用可能である場合、暗号化キーのバックアップはバックグラウンドで行われます。しかし、たとえば、バックアップ場所が使用不能な場合（オリジナルのリムーバブルストレージデバイスがコンピュータに挿入されていないなど）、暗号化キーが手動でバックアップされるまで、ポリシー変更は有効になりません。

    メモ: 暗号化キーを手動でバックアップする方法については、ローカル管理コンソールの右上隅にある **［？］ > ［ヘルプ］** を参照するか、または **［スタート］ > ［Dell］ > ［Encryption のヘルプ］** をクリックします。

    次へ をクリックします。
11. 暗号化設定の確認 画面に暗号化設定のリストが表示されます。設定を確認し、設定に問題がなければ **確認** をクリックします。

    コンピュータの設定が開始されます。ステータスバーには、設定の進捗状況が表示されます。
12. **完了** をクリックして設定を完了します。
13. コンピューターが暗号化用に設定されると再起動が必要になります。［**今すぐ再起動**］をクリックします。または、5 回（各 20 分）再起動を延期することができます。

14. コンピュータが再起動されたら、スタートメニューからのローカル管理コンソールを開きますの暗号化ステータスを参照してください。

    暗号化はバックグラウンドで実行されます。ローカルの管理コンソールを開くか閉じることができます。ファイルの暗号化は、いずれの場合でも行われます。コンピュータは、暗号化中も通常どおり使用することができます。

15. スキャンが完了すると、コンピュータが再び再起動します。

    すべての暗号をスイープして、再起動が完了すると、ローカルの管理コンソールを起動してコンプライアンスの状態を確認することができます。ドライブは、「コンプライアンス対応済み」とラベル付けされます。

6

コンソールの設定

デフォルト設定では、管理者とユーザーが、追加の設定を行うことなくアクティブ化後すぐに Advanced Authentication を使用することができます。ユーザーは、Windows パスワードを使用してコンピュータにログオンするときに Advanced Authentication ユーザーとして自動的に追加されますが、デフォルトでは、Windows 多要素認証は有効化されていません。

Advanced Authentication 機能を設定するには、コンピュータの管理者である必要があります。

管理者パスワードおよびバックアップ場所の変更

Advanced Authentication のアクティブ化後、必要に応じて管理者パスワードおよびバックアップ場所を変更することができます。

1. デスクトップショートカットから、管理者として Dell Data Security Console を起動します。
2. **管理者設定** タイルをクリックします。
3. 認証ダイアログで、アクティブ化中にセットアップされた管理者パスワードを入力し、**OK** をクリックします。
4. **管理者設定** タブをクリックします。
5. 管理者パスワードの変更ページでパスワードを変更する場合、入力するパスワードは 8 ～ 32 文字で文字、数字、特殊文字を少なくとも 1 文字ずつ含めるようにします。
6. 確認のためにもう一度パスワードを入力し、**適用** をクリックします。
7. リカバリキーが保存されている場所を変更するには、左ペインで **バックアップ場所の変更** を選択します。
8. バックアップ用の新しい場所を選択し、**適用** をクリックします。

   バックアップファイルは、ネットワークドライブまたはリムーバブルメディアのいずれかに保存する必要があります。バックアップファイルには、このコンピュータのデータを復元するために必要なキーが含まれています。Dell ProSupport がデータの回復をお手伝いするには、このファイルへのアクセス権が必要です。

   リカバリデータは、指定した場所に自動的にバックアップされます。指定した場所を使用できない場合（バックアップ USB ドライブが挿入されていない場合など）は、Advanced Authentication によってデータのバックアップ先を求めるプロンプトが表示されます。暗号化を開始するには、リカバリデータへのアクセスが必要です。

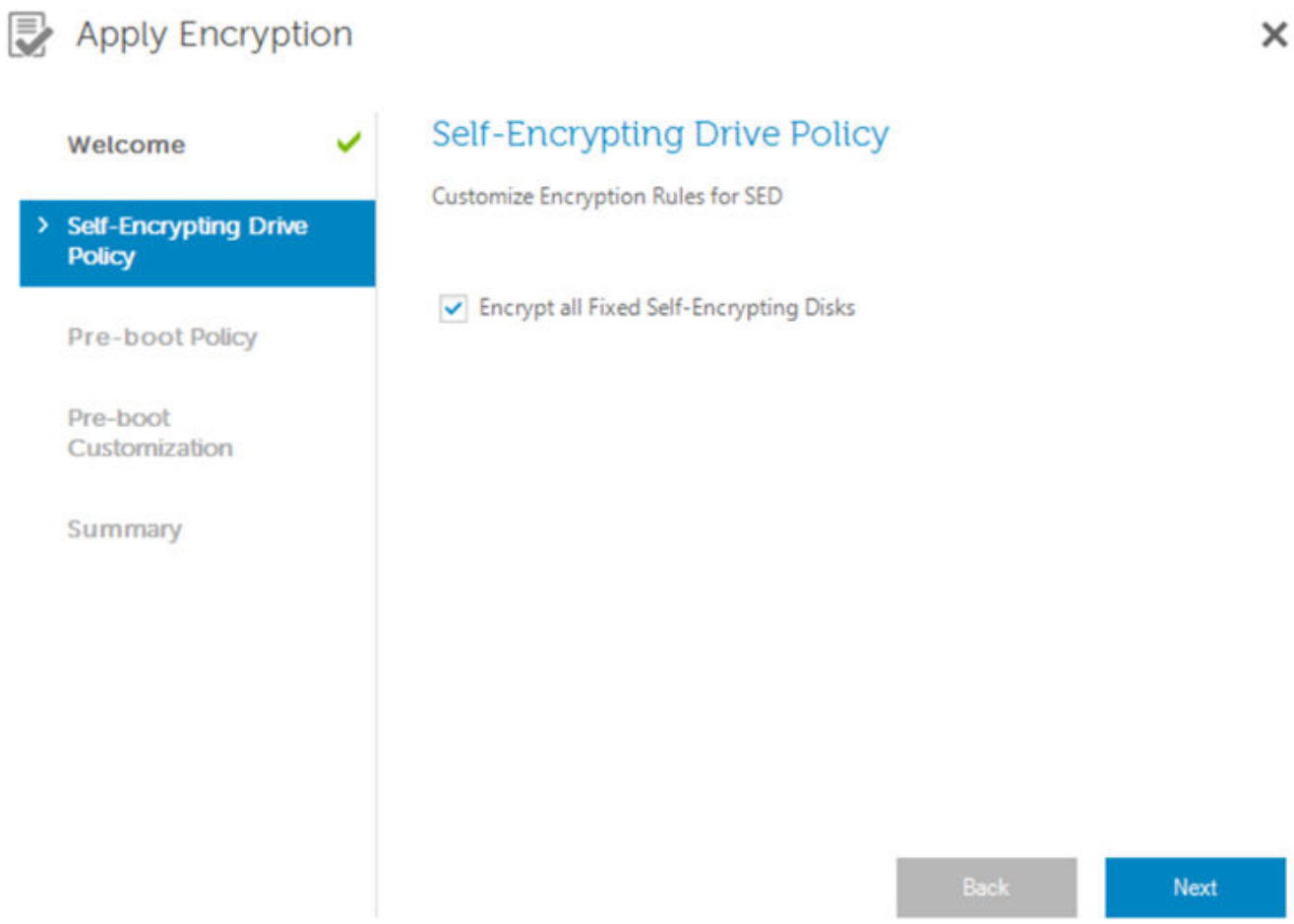
Pre-Boot 認証の設定

PBA は、コンピューターに SED が搭載されている場合に使用できます。PBA は、［Encryption］タブで設定します。SED Manager が SED の所有権を引き継ぐと、PBA が有効になります。

SED 管理を有効にするには、次の手順を実行します。

1. Data Security Console で **管理者設定** タイルをクリックします。
2. バックアップ場所がコンピュータからアクセス可能であることを確認してください。

   バックアップ場所が見つかりません というメッセージが表示され、バックアップ場所が USB ドライブ上にある場合は、ドライブが接続されていないか、ドライブがバックアップ中に使用したスロットとは異なるスロットに接続されています。このメッセージが表示され、バックアップ場所がネットワークドライブ上にある場合は、コンピュータからネットワークにアクセスできません。バックアップ場所の変更が必要な場合は、**管理者設定** タブで **バックアップ場所の変更** を選択し、現行のスロットまたはアクセス可能なドライブに場所を変更します。場所を再度割り当てた後は、数秒で暗号化の有効化プロセスを続行できるようになります。
3. **暗号化** タブをクリックし、**暗号化** をクリックします。
4. ようこそ ページで、**次へ** をクリックします。
5. ［**すべての固定自己暗号化ディスクの暗号化**］を選択してマルチディスクの暗号化を有効にします。



6. 起動前ポリシー ページで次の値を変更または確定し、**次へ** をクリックします。

キャッシュされていないユーザーログインの試行回数	不明なユーザー（これまでコンピュータにログインしたことがない、つまり認証情報がキャッシュされていないユーザー）がログインを試行できる回数です。
キャッシュされたユーザーログインの試行回数	キャッシュされたユーザーがログインを試行できる回数です。
リカバリ質問の回答試行回数	ユーザーが正しい回答の入力を試行できる回数です。
暗号化削除パスワードの有効化	選択して有効にします。
暗号化削除パスワードの入力	フェイルセーフセキュリティメカニズムとして使用される 100 文字までの語句またはコード。起動前認証中にユーザー名またはパスワードのフィールドにこの単語またはコードを入力すると、暗号消去が開始され、セキュアなストレージからキーが削除されます。このプロセスが起動されると、ドライブは回復できなくなります。緊急時のための暗号化削除パスワードが必要ない場合は、このフィールドを空欄のままにしておいてください。 緊急時のための暗号化削除パスワードが必要ない場合は、このフィールドを空欄のままにしておいてください。
情報を記憶する	PBA ログイン 画面で、ユーザーによるログイン情報の記憶の選択を有効または無効にします。

7. 起動前カスタム化 ページで、起動前認証（PBA）画面に表示するカスタムテキストを入力し、**次へ** をクリックします。

起動前タイトルテキスト	このテキストは、PBA 画面の上部に表示されます。このフィールドを空のままにすると、タイトルは表示されません。テキストは改行されないため、17 文字以上入力すると、テキストの一部が表示されない場合があります。
サポート情報テキスト	PBA サポート情報画面に表示されるテキスト。ヘルプデスクやセキュリティ管理者への連絡方法について詳細を含めるには、メッセージをカスタマイズします。このフィールドに何も入力しないと、ユーザーが利用できるサポートの連絡先情報が表示されません。 テキストの改行は文字単位ではなく単語単位で行われます。1 単語で 50 文字以上もあるような場合は、文字列が改行されず、スクロールバーも表示されないため、テキストの一部が表示されません。
法的通知テキスト	このテキストは、ユーザーのデバイスへのログオンが許可される前に表示されます。たとえば、「OK をクリックすることにより、妥当なコンピュータ使用ポリシーへの準拠に同意します」などです。このフィールドにテキストを入力しないと、テキストが全く表示されない、または Ok/ キャンセル ボタンが表示されることになります。テキストの改行は文字単位ではなく単語単位で行われます。例えば、1 単語で 50 文字以上もあるような場合でも改行されず、スクロールバーも表示されないため、テキストの一部が表示されません。

8. サマリ ページで **適用** をクリックします。
9. プロンプトが表示されたら、**シャットダウン** をクリックします。

   暗号化が開始される前に、完全なシャットダウンが必要です。

10. シャットダウン後にコンピュータを再起動してください。

    認証は、Encryption Management Agent によって管理されるようになります。ユーザーは、Windows パスワードを使用して PBA 画面でログインする必要があります。

SED 管理と PBA 設定の変更

初めて暗号化を有効化し、起動前ポリシーとカスタム化を設定した後は、暗号化 タブで次のアクションを使用できるようになります。

- 起動前ポリシーまたはカスタム化の変更 - **暗号化** タブをクリックして **変更** をクリックします。
- アンインストールなど SED 管理を無効にする - ［**復号化**］をクリックします。

最初に SED 管理を有効にして、起動前ポリシーとカスタム化を設定すると、［起動前設定］タブで次のアクションを使用できるようになります。

- 起動前ポリシーまたはカスタマイズの変更 - **起動前設定**タブをクリックし、［**自動暗号化ドライブ ポリシー**］、［**起動前ポリシー**］、または［**起動前カスタマイズ**］を選択します。

ユーザーおよびユーザー認証の管理

ユーザーの追加

Windows ユーザーは、Windows へのログオン時、または資格情報の登録時に自動的に Encryption Personal ユーザーになります。

Data Security Console の ユーザーの追加 タブでドメインユーザーを追加するには、コンピューターがドメインに接続されている必要があります。

1. 管理者設定ツールの左ペインで、**ユーザー** を選択します。
2. ユーザー ページの右上にある **ユーザーの追加** をクリックして、既存の Windows ユーザーの登録処理を開始します。
3. ユーザーの選択 ダイアログが表示されたら、**オブジェクトタイプ** を選択します。
4. ユーザーのオブジェクト名をテキストボックスに入力し、**名前のチェック** をクリックします。
5. 終了したら **OK** をクリックします。

ユーザーの削除

1. 管理者設定ツールの左ペインで、**ユーザー** を選択します。

2. ユーザーを削除する場合は、ユーザーのカラムを選択して **削除** をクリックします。（削除オプションを表示するには、ユーザーカラムの下部までスクロールします。）

ユーザーのすべての登録済み資格情報の削除

1. **管理者設定** タイルをクリックして、パスワードで認証します。
2. **ユーザー** タブをクリックし、削除するユーザーを見つけます。
3. **削除** をクリックします。（remove コマンドは、ユーザーの設定の下部に赤色で表示されます。）

   削除後、ユーザーは再登録しない限り、コンピュータにはログオンできなくなります。

7

マスターインストーラのアンインストール

- 各コンポーネントを個別にアンインストールし、その後でクライアントは、**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。
- 必ずインストールと同じバージョンのクライアントをアンインストールにも使用してください。
- この章では意味を別の章を含む 詳細な 指示子のインストーラのアンインストール方法の。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 クライアントをアンインストールします。
2. Encryption Management Agent をアンインストールします。

ドライバパッケージをアンインストールする必要はありません。

続行を 選択するには、アンインストールの方法を押します。

アンインストール方法の選択

マスターインストーラのアンインストールには 2 つの方法があります。次の**いずれかの**方法を選択します。

- 追加 / 削除プログラムからのアンインストール
- コマンドラインからのアンインストール

対話形式でのアンインストール

1. Windows のコントロールパネルで プログラムのアンインストール に移動し（タスクバーの検索ボックスに**コントロールパネル**と入力し、結果からコントロールパネル を選択します）。
2. **Dell Installer** をハイライト表示して **変更** を左クリックし、セットアップウィザードを起動します。
3. ようこそ画面を読み、**次へ** をクリックします。
4. プロンプトに従ってアンインストールを実行し、**終了** をクリックします。
5. コンピュータを再起動して、Windows にログインします。

   マスターのインストーラがアンインストールされます。

コマンドラインからのアンインストール

- 次の例は、SED クライアントをサイレントアンインストールします。

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

  終了したらコンピュータを再起動します。

  マスターのインストーラがアンインストールされます。

  子インストーラを使用したアンインストールを続行します。

8

子インストーラを使用したアンインストール

- デルは、Data Security Uninstaller を使用して Encryption Personal を削除することをお勧めします。
- 復号とアンインストールを実行するユーザーは、ローカルまたはドメイン管理者である必要があります。コマンドラインでアンインストールする場合は、ドメイン管理者資格が必要です。
- マスターインストーラを使用して Encryption Personal をインストールした場合、「マスターインストーラから子インストーラを抽出する」に記述されているように、アンインストールの前にマスターインストーラから子実行可能ファイルを抽出する必要があります。
- 必ずインストールと同じバージョンのクライアントをアンインストールにも使用してください。
- 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。

Encryption のアンインストール

- **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。

  メモ: アンインストールを実行する前に、すべてのポリシーテンプレートが無効に設定されていることを確認し、正常な復号化のために暗号化された外部メディアを挿入します。

  このビデオを参照すると、ローカル管理コンソールでポリシーテンプレートを変更する手順の詳細を確認できます。
- 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。
-

アンインストール方法の選択

あるは、暗号化クライアントをアンインストールするには 2 つの方法を選択します。 **いずれかの** 次のと

- 対話形式でのアンインストール
- コマンド ラインからのアンインストール

対話形式でのアンインストール

1. Windows のコントロールパネルで プログラムのアンインストール に移動します（タスクバーの検索ボックスに **コントロールパネル** と入力し、結果から **コントロールパネル** を選択します）。
2. **Dell Encryption XX-bit** をハイライト表示し、**変更** を左クリックして Encryption Personal セットアップウィザードを起動します。
3. ようこそ画面を読み、**次へ** をクリックします。
4. Encryption Removal Agent のインストール画面で、次のいずれかを選択します。

   メモ: デフォルトでは、2 番目のオプションが有効になっています。**ファイルの復号化を希望する場合は、選択をオプション 1 に変更するようにしてください。**

   - Encryption Removal Agent - ファイルからキーをインポートする

     SDE、ユーザー、または共通の暗号化の場合、このオプションはファイルを復号化して、Encryption クライアントをアンインストールします。**これは、推奨される選択を押します。**

- Encryption Removal Agent をインストールしない

  このオプションは、暗号化クライアントがアンインストールされます が、ファイルの暗号化されません.このオプションは、 Dell ProSupport の指示に従ったトラブルシューティング目的 **限定** で使用するようにしてください。

  次へ をクリックします。

5. バックアップファイル で、バックアップファイルのネットワークドライブまたはリムーバブルメディアの場所へのパスを入力するか、 **...** をクリックして、場所を参照します。ファイルフォーマットは LSARecovery_[ホスト名].exe です。

   暗号管理者パスワードを入力します。これは、ソフトウェアをインストールしたときのセットアップウィザードのパスワードです。

   次へ をクリックします。

6. *Dell* 復号化エージェントサービスのログオン で **ローカルシステムアカウント** を選択し **完了** をクリックします。
7. プログラムの削除画面で、**削除**をクリックします。
8. 設定の完了画面で、［**終了**］をクリックします。
9. コンピュータを再起動して、 Windows にログインします。

復号化が進行中です。

複合化されるドライブの数、およびこれらのドライブ上のデータの量によっては、復号化処理に数時間かかることがあります。複合化プロセスをチェックするには、 Encryption Removal Agent ステータスのチェックを参照してください。

コマンド ラインからのアンインストール

- コマンドラインのスイッチおよびパラメータは大文字と小文字を区別します。
- 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。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

  %temp%のログイン ユーザー用に一意の子インストーラーのアンインストール ログ ファイルが Windows によって作成されます。このログ ファイルは次の場所に保存されます： `C:\Users\<UserName>\AppData\Local\Temp.`

  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。標準の.msi コマンドを使用してログ ファイルを作成できます。その際には `C:\<any directory>\<any log file name>.log` の形式を使用します。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、コマンド ラインでのアンインストールで「/l*v」（詳細ログ）を使用することはお勧めしません。

- 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。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。
/s	サイレントモード
/x	アン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

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

- Encryption クライアント 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。
- 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： 2 - フォレンジックキーのバンドルを使用してキーを取得する 0 - Encryption Removal Agent をインストールしない
CMGSILENTMODE	サイレントアンインストールのプロパティ 1 - サイレント - /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
DA_KM_PW	ドメイン管理者アカウントのパスワードです。
DA_KM_PATH	キーマテリアルのバンドルをパスします。

- 次の例では、暗号化削除エージェントをインストールせずに暗号化クライアントをアンインストールします。

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=0 CMGSILENTMODE=1
DA_KM_PATH=C:\FullPathToLSA.exe DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
```

- 次の例では、フォレンジックキーのバンドルを使用して暗号化クライアントをアンインストールします。また、フォレンジックキーのバンドルをローカルディスクにコピーし、このコマンドを実行します。

```
DDPE_XXbit_setup.exe /s /x /v"CMG_DECRYPT=2 CMGSILENTMODE=1
DA_KM_PATH=C:\FullPathToForensicKeyBundle DA_KM_PW=password /qn /l C:\ddpe_uninstall.txt"
```

終了したらコンピュータを再起動します。

複合化されるドライブの数、およびこれらのドライブ上のデータの量によっては、復号化処理に数時間かかることがあります。複合化プロセスをチェックするには、Encryption Removal Agent ステータスのチェックを参照してください。

Encryption Management Agent のアンインストール

アンインストール方法の選択

Encryption Management Agent をアンインストールする方法は 2 通りあります。次の**いずれか**を選択します。

- 対話形式でのアンインストール
- コマンド ラインからのアンインストール

対話形式でのアンインストール

1. Windows のコントロールパネルで プログラムのアンインストール に移動します（タスクバーの検索ボックスに **コントロールパネル** と入力し、結果から **コントロールパネル** を選択します）。
2. **Dell Encryption Management Agent** をハイライト表示し、［**変更**］を左クリックしてセットアップ ウィザードを起動します。
3. ようこそ画面を読み、**次へ** をクリックします。

4. プロンプトに従ってアンインストールを実行し、**終了** をクリックします。
5. コンピュータを再起動して、Windows にログインします。

Client Security Framework がアンインストールされました。

コマンド ラインからのアンインストール

- Encryption Management Agent 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 Management Agent\EMAgent_XXbit_setup.exe` で見つけることができます。
- 次の例は、SED 管理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。

9

Data Security アンインストーラ

Encryption Personal 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 - ファイルからキーをインポート**］を選択して、［**次へ**］を選択します。

リカバリキーの場所を参照し、そのファイルのパスフレーズを入力して、**次へ** をクリックします。

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。

10

「ポリシーテンプレートの説明」

Personal Edition ローカル管理コンソールのポリシー上にマウスを置くと、ツールヒントが表示されます。

ポリシー

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
固定ストレージポリシー										
SDE 暗号化有効	True								False	このポリシーは、他のすべての System Data Encryption（SDE）ポリシーに対する「マスターポリシー」となります。このポリシーが False の場合は、他のポリシーの値に関わらず、SDE 暗号化は一切実行されません。 値が True の場合は、他の Policy-Based Encryption ポリシーによって暗号化されなかったすべてのデータが SDE 暗号化ルールポリシーに従って暗号化されることになります。 このポリシーの値の変更には、再起動が必要です。
SDE 暗号化のアルゴリズム	AES256									AES-256 または AES-128
SDE 暗号化ルール										特定のドライブ、ディレクトリ、およびフォルダを暗号化または復号化するために使用する暗号化ルールです。 デフォルト値の変更に関して不明な点がある場合は、カスタマサポートに連絡してサポートを受けてください。
一般設定ポリシー										
暗号化有効	True							False		このポリシーは、すべての一般設定ポリシーに対する「マスタ

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
										ーポリシー」となります。値を False にすると、他のポリシーの値に関わらず、暗号化は一切実行されません。 値を True にすると、すべての暗号化ポリシーが有効になります。 このポリシーの値を変更すると、ファイルを暗号化 / 復号化するための新たなスイープがトリガされます。
共通の暗号化フォルダ										文字列 - それぞれ 500 文字のエントリを最大 100 件（最大 2048 文字） 暗号化される、または暗号化から除外されるエンドポイントドライブ上のフォルダのリストで、エンドポイントへのアクセス権を持つすべての管理対象ユーザーがアクセスできるようになります。 使用可能なドライブ文字は次のとおりです。 # ：すべてのドライブを示します。 f# ：すべての固定（非リムーバブル）ドライブを示します。 r# ：すべてのリムーバブルドライブを示します 重要：ディレクトリ保護を上書きすると、コンピュータが起動不能になったり、ドライブの再フォーマットが必要になったりする可能性があります。 このポリシーとユーザー暗号化フォルダポリシーの両方で同じフォルダが指定された場合は、このポリシーが優先されます。
共通の暗号化アルゴリズム	AES256									AES-256、Rijndael 256、AES 128、Rijndael 128 システムページングファイルは AES-128 を使用して暗号化されます。

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
アプリケーションデータ暗号化リスト	winword.exe excel.exe powerpnt.exe msaccess.exe winproj.exe outlook.exe acrobat.exe visio.exe mspub.exe notepad.exe wordpad.exe winzip.exe winrar.exe onenote.exe onenotem.exe									文字列 - それぞれ 500 文字のエントリを最大 100 件 予期しない、または意図しない結果が発生する可能性があるため、explorer.exe および iexplorer.exe は ADE リストに追加しないことをお勧めします。ただし、explorer.exe は、右クリックメニューを使用してデスクトップ上に新規の Notepad ファイルを作成するために使用されるプロセスです。ADE リストの代わりにファイル拡張子で暗号化を設定すると、より包括的に対象を指定できます。 新規ファイルを暗号化するアプリケーションのプロセス名を、キャリッジリターンで区切ってリストします（パスなし）。ワイルドカードは使用しないでください。 弊社では、システムクリティカルなファイルに書き込みを行うようなアプリケーションまたはインストーラはリストしないことを推奨しています。リストに含めると、重要なシステムファイルが暗号化されて Windows エンドポイントを起動不能にするおそれがあります。 一般的なプロセス名： Outlook.exe、 winword.exe、 powerpnt.exe、 msaccess.exe、 wordpad.exe、 mspaint.exe、excel.exe 以下のハードコーディングされたシステムおよびインストーラプロセス名は、このポリシーに指定しても無視されます。 hotfix.exe、update.exe、 setup.exe、msiexec.exe、 wuauclt.exe、 wmiprvse.exe、 migrate.exe、 unregmp2.exe、 ikernel.exe、wssetup.exe、 svchost.exe

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
アプリケーションデータ暗号化キー	共通									共通またはユーザー アプリケーションデータ暗号化リストで暗号化されたファイルにアクセスできるユーザーと、その場所を指定するキーを選択します。 すべての管理対象ユーザーが、ファイルが作成されたエンドポイント上でファイルにアクセスでき（共通暗号化フォルダと同じアクセスレベル）、共通の暗号化アルゴリズムで暗号化されるようにする場合は共通を選択します。 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エンドポイント上でのみファイルにアクセスでき（ユーザー暗号化フォルダと同じアクセスレベル）、ユーザー暗号化アルゴリズムで暗号化されるようにする場合はユーザーを選択します。 このポリシーに対する変更は、このポリシーによってすでに暗号化されているファイルには影響しません。
Outlook Personal フォルダの暗号化	True							False		True に設定すると、Outlook Personal フォルダが暗号化されます。
一時ファイルの暗号化	True							False		True に設定すると、環境変数 TEMP および TMP に登録されたパスが、ユーザーデータ暗号化キーで暗号化されます。
インターネット一時ファイルの暗号化	True	False								True に設定すると、環境変数 CSIDL_INTERNET_CACHE にリストされたパスが、ユーザーデータ暗号化キーで暗号化されます。 暗号化スイープ時間を短縮するため、クライアントは初期暗号化のための CSIDL_INTERNET_CACHE の内容に加え、このポリシーへのアップデートもクリアします。

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
										このポリシーは、Microsoft Internet Explorer を使用する場合にのみ適用できます。
ユーザープロファイルドキュメントの暗号化	True								False	True に設定すると、次の内容が暗号化されます。 · ユーザープロファイル（C:\Users\jsmith）（ユーザーデータ暗号化キーを使用） · \Users\Public（共通暗号化キーを使用）
Windows ページングファイルの暗号化	True								False	True に設定すると、Windows ページングファイルが暗号化されます。このポリシーに対する変更には、再起動が必要です。
管理対象サービス										文字列 - それぞれ 500 文字のエントリを最大 100 件（最大 2048 文字） このポリシーによりサービスが管理されているときは、ユーザーがログインし、クライアントのロックが解除された後でのみ、サービスが起動します。また、このポリシーによりサービスが管理されているときは、ログオフ中にクライアントがロックされる前に、確実にサービスを停止します。このポリシーによって、サービスが無反応の場合に、ユーザーがログオフできないようにすることも可能です。 構文は、1 行ごとに 1 つのサービス名となります。サービス名に空白を含むことも可能です。 ワイルドカードはサポートされていません。 管理対象外のユーザーがログオンすると、管理対象サービスは起動しません。
暗号化後クリーンアップのセキュア化	3 パス上書き	1 パス上書き							上書きなし	上書きなし、1 パス上書き、3 パス上書き、7 パス上書き このポリシーは、このカテゴリ内のその他のポリシーによって指

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護 (デフォルト)	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
										定されたフォルダが暗号化された後で、オリジナルのファイルの暗号化されていない剰余の処理方法を決定します。 ・上書きなしの場合、剰余は削除されます。この値に設定すると、暗号化処理が最速になります。 ・1 パス上書きの場合、剰余はランダムなデータで上書きされます。 ・3 パス上書きの場合、剰余は 1 と 0 の標準パターンで上書きされた後、その補数で上書きされ、次にランダムなデータで上書きされます。 ・7 パス上書きの場合、剰余は 1 と 0 の標準パターンで上書きされた後、その補数で上書きされ、次にランダムなデータで 5 回上書きされます。この値に設定すると、元のファイルをメモリから回復することが最も難しくなり、暗号化処理が最もセキュアになります。
セキュアな Windows 休止状態ファイル	True					False		True	False	有効にした場合、コンピュータが休止状態に入るときにのみ休止状態ファイルが暗号化されます。コンピュータが休止状態から復帰するとクライアントによって保護が解除され、コンピュータの使用中はユーザーまたはアプリケーションに影響することなく保護が提供されます。
非セキュアな休止状態の防止	True					False		True	False	選択した場合、クライアントは、休止状態データを暗号化できないと、コンピュータの休止状態を許可しません。
ワークステーションのスキャン優先度	高	標準								最高、高、標準、低、最低 暗号化フォルダスキャンの相対的な Windows 優先順位を指定します。

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
ユーザー暗号化フォルダ										文字列 - それぞれ 500 文字のエントリを最大 100 件（最大 2048 文字） ユーザーデータ暗号化キーを使用して暗号化する、または暗号化から除外するエンドポイントハードドライブ上のフォルダのリスト。 このポリシーは、Windows によってハードディスクドライブとして分類されたすべてのドライブに適用されます。タイプがリムーバブルディスクとして表示されるドライブまたはリムーバブルメディアの暗号化にこのポリシーを使用することはできません。代わりに、外部メディアの EMS 暗号化を使用してください。
ユーザー暗号化アルゴリズム	AES256									AES 256、Rijndael 256、AES 128、Rijndael 128 個々のユーザーレベルでのデータの暗号化に使用される暗号化アルゴリズムです。同じエンドポイントのユーザーごとに異なる値を指定できます。
ユーザーデータ暗号化キー	ユーザー	共通		ユーザー	共通				ユーザー	共通またはユーザー 次のポリシーで暗号化されたファイルにアクセスできるユーザーと、その場所を指定するキーを選択します。 · ユーザー暗号化フォルダ · Outlook Personal フォルダの暗号化 · 一時ファイル（\Documents and Settings\username\Local Settings\Temp のみ）の暗号化 · インターネット一時ファイルの暗号化 · ユーザープロファイルドキュメントの暗号化 次を選択します：

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
										· すべての管理対象ユーザーが、ファイルが作成されたエンドポイント上でユーザー暗号化ファイル / フォルダにアクセスすることができ（共通暗号化フォルダと同じアクセスレベル）、共通暗号化アルゴリズムで暗号化されるようにする場合は、共通を選択します。 · 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エンドポイント上のみでそれらのファイルにアクセスすることができ（ユーザー暗号化フォルダと同じアクセスレベル）、ユーザー暗号化アルゴリズムで暗号化されるようにする場合はユーザーを選択します。 ディスクパーティション全体を暗号化する暗号化ポリシーの組み入れを選択する場合は、共通またはユーザーの暗号化ポリシーではなく、デフォルトの SDE 暗号化ポリシーを使用することをお勧めします。これにより、管理対象ユーザーがログインしていない状態でも、暗号化された任意のオペレーティングシステムファイルに確実にアクセスできるようになります。
Hardware Crypto Accelerator（v8.9.1 Encryption クライアントにより v8.3 でのみサポート）										
Hardware Crypto Accelerator（HCA）	False									このポリシーは、その他すべての Hardware Crypto Accelerator（HCA）ポリシーに対する「マスターポリシー」となります。このポリシーが False の場合は、他のポリシーの値に関わらず、HCA 暗号化は一切実行されません。 HCA ポリシーを使用できるのは、Hardware Crypto Accelerator を搭載するコンピュータのみです。
暗号化のターゲットとなるボリューム	すべての固定ボリューム									すべての固定ボリュームまたはシステムボリュームのみ 暗号化のターゲットとなるボリュームを指定します。

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
HCA 暗号化ドライブで使用できるフォレンジックメタデータ	False									True または False True に設定すると、フォレンジックを容易にするためにフォレンジックメタデータがドライブに包含されます。包含されるメタデータ： ● 現在のマシンのマシン ID（MCID） ● 現在の Encryption client インストールのデバイス ID（DCID/SCID） False に設定すると、フォレンジックメタデータはドライブに包含されません。 False から True に変更すると、ポリシーに基づいて再スイープされ、フォレンジックが追加されます。
セカンダリドライブ暗号化のユーザー承認の許可	False									True に設定すると、ユーザーが追加ドライブを暗号化するかどうかを決定することができます。
暗号化アルゴリズム	AES256									AES-256 または AES-128
ポート制御ポリシー										
ポート制御システム	無効									すべてのポート制御システムポリシーを有効または無効にします。このポリシーが無効に設定されている場合、その他のポート制御システムポリシーの値に関わらず、ポート制御システムポリシーは適用されません。 PCS ポリシーを有効にするには、再起動が必要です。 **メモ:** デバイスの操作をブロックすると、デバイス名が空白で表示されます。
ポート：ExpressCard スロット	有効									ExpressCard スロットを介して公開されているポートを有効化、無効化、またはバイパスします。

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
ポート：eSATA	有効									外部 SATA ポートに対するポートアクセスを有効化、無効化、またはバイパスします。
ポート：PCMCIA	有効									PCMCIA ポートに対するポートアクセスを有効化、無効化、またはバイパスします。
ポート：Firewire（1394）	有効									外部 Firewire（1394）ポートに対するポートアクセスを有効化、無効化、またはバイパスします。
ポート：SD	有効									SD カードポートに対するポートアクセスを有効化、無効化、またはバイパスします。
サブクラスストレージ：外部ドライブ制御	ブロック	読み取り専用			完全アクセス			読み取り専用	完全アクセス	クラス：ストレージの子。このポリシーを使用するには、クラス：ストレージを Enabled に設定する必要があります。 このポリシーには、 pc のやり取りします。「Encryption External Media と PCS Interactions」を参照してください。 フルアクセス：外部ドライブポートではデータの読み取り／書き込み制限は適用されません。 読み取り専用：読み取り機能が可能です。データの書き込みは無効です。 ブロック：ポートでは読み取り／書き込み機能がブロックされます。 このポリシーはエンドポイントベースであり、ユーザーポリシーによる上書きはできません。
ポート：メモリ転送デバイス（MTD）	有効									メモリ転送デバイス（MTD）ポートに対するアクセスを有効化、無効化、またはバイパスします。
クラス：ストレージ	有効									次の 3 つのポリシーに対する親です。次の 3 つのサブクラスストレージポリシーを使用するには、このポリシーを有効に

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
										設定します。このポリシーを無効に設定すると、値にかかわらず、3 つのサブクラスストレージポリシーがすべて無効になります。
サブクラスストレージ：光学ドライブ制御	読み取り専用	UDF のみ				完全アクセス		UDF のみ	完全アクセス	クラス：ストレージの子。このポリシーを使用するには、クラス：ストレージを Enabled に設定する必要があります。 フルアクセス：光学ドライブポートではデータの読み取り／書き込み制限は適用されません。 UDF のみ：UDF フォーマット以外のすべてのデータの書き込みをブロックします（CD／DVD 書き込み、ISO 書き込み）。データの読み取りは有効です。 読み取り専用：読み取り機能が可能です。データの書き込みは無効です。 ブロック：ポートでは読み取り／書き込み機能がブロックされます。 このポリシーはエンドポイントベースであり、ユーザーポリシーによる上書きはできません。 ユニバーサルディスクフォーマット（UDF）は ISO/IEC 13346 および ECMA-167 として知られる仕様の実装で、幅広いメディアのコンピュータデータストレージのためのオープンなベンダー中立のファイルシステムです。 このポリシーには、 pc のやり取りします。「Encryption External Media と PCS Interactions」を参照してください。
サブクラスストレージ：フロッピードライブ制御	ブロック	読み取り専用				完全アクセス		読み取り専用	完全アクセス	クラス：ストレージの子。このポリシーを使用するには、クラス：ストレージを Enabled に設定する必要があります。

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
										フルアクセス：フロッピードライブポートではデータの読み取り／書き込み制限は適用されません。 読み取り専用：読み取り機能が可能です。データの書き込みは無効です。 ブロック：ポートでは読み取り／書き込み機能がブロックされます。 このポリシーはエンドポイントベースであり、ユーザーポリシーによる上書きはできません。
クラス：Windows ポータブルデバイス（WPD）	有効									次のポリシーに対する親です。サブクラス Windows ポータブルデバイス（WPD）：ストレージポリシーを使用するには、このポリシーを Enabled に設定します。このポリシーを Disabled に設定すると、値にかかわらず、サブクラス Windows ポータブルデバイス（WPD）：ストレージポリシーが無効になります。 すべての Windows ポータブルデバイスに対するアクセスを制御します。
サブクラス Windows ポータブルデバイス（WPD）：ストレージ	有効									クラス：Windows ポータブルデバイス（WPD）の子 このポリシーを使用するには、クラス：Windows ポータブルデバイス（WPD）を有効に設定する必要があります。 完全アクセス：ポートではデータの読み取り / 書き込み制限は適用されません。 読み取り専用：読み取り機能が可能です。データの書き込みは無効です。 ブロック：ポートでは読み取り／書き込み機能がブロックされます。
クラス：ヒューマンインターフェイスデ	有効									すべてのヒューマンインタフェースデバイスへのアクセスを制御します。

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
バイス（HID）										メモ： USB ポートレベルのブロッキングと HID クラスレベルのブロッキングは、コンピュータシャーシがラップトップまたはノートブックのフォームファクタとして識別できる場合にのみ有効です。コンピュータの BIOS には、シャーシの識別のために依存します。
クラス：その他	有効									その他のクラスの対象とならないすべてのデバイスへのアクセスを制御します。
リムーバブルストレージポリシー										
外部メディアの EMS 暗号化	True					False		True	False	このポリシーは、すべてのリムーバブルストレージポリシーに対する「マスターポリシー」となります。 値を False にすると、他のポリシーの値に関わらず、リムーバブルストレージの暗号化は一切実行されません。 値を True にすると、すべてのリムーバブルストレージ暗号化ポリシーが有効になります。 このポリシーには、 pc のやり取りします。「Encryption External Media と PCS Interactions」を参照してください。
CD/DVD 暗号化の EMS 除外	False								True	False に設定すると、CD/DVD デバイスが暗号化されます。 このポリシーには、 pc のやり取りします。「Encryption External Media と PCS Interactions」を参照してください。
Shield 対象外メディアへの EMS アクセス	ブロック		読み取り専用			完全アクセス		読み取り専用	完全アクセス	ブロック、読み取り専用、完全アクセス このポリシーには、 pc のやり取りします。「Encryption External Media と PCS Interactions」を参照してください。

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護 (デフォルト)	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
										このポリシーがアクセスをブロックするように設定されていると、暗号化されていない限り、リムーバブルストレージにはアクセスできません。 読み取り専用または完全アクセスのいずれかを選択すると、どのリムーバブルストレージを暗号化するかを指定できます。 リムーバブルストレージを暗号化しないことを選択し、このポリシーを完全アクセスに設定すると、リムーバブルストレージに対する完全な読み取り / 書き込みアクセスを持つことになります。 リムーバブルストレージを暗号化しないよう選択し、このポリシーを読み取り専用に設定した場合、暗号化されていないリムーバブルストレージ上の既存ファイルを読み取りまたは削除することはできません。ただし、クライアントはリムーバブルストレージが暗号化されていなければ、そのリムーバブルストレージ上のファイルの編集、またはストレージへのファイルの追加を許可しません。
EMS 暗号化アルゴリズム	AES256									AES-256、Rijndael 256、AES-128、Rijndael 128
外部メディアの EMS スキャン	True	False								True を使用すると、リムーバブルメディアを挿入の都度スキャンすることができます。このポリシーが False であり、外部メディアの EMS 暗号化ポリシーが True になっていると、新規および変更されたファイルのみが暗号化されます。 認証なしにリムーバブルメディアに追加されるすべてのファイルを検出できるように、挿入のたびにスキャンが実行されます。認証が拒否された場合、ファイルはリムーバブルストレージに追加されますが、暗号化されたデータにはアクセスできませ

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
										ん。この場合、追加されたファイルは暗号化されないため、メディアが認証されたタイミングで（暗号化データが機能するように）、追加された可能性のあるすべてのファイルはスキャンされ、暗号化されます。
Shield 対象外デバイス上の暗号化データへの EMS アクセス	True									True に設定すると、エンドポイントが Shield されているかどうかにかかわらず、リムーバブルストレージの暗号化データへのアクセスが許可されます。
EMS デバイスのホワイトリスト										このポリシーでは、リムーバブルメディアの仕様を暗号化の対象から除外することができます。このリストに載っているリムーバブル メディアはいずれも保護されません。PNPDeviceID あたり最大 500 文字で最大 150 台のデバイスです。合計で最大 2048 文字まで使用可能です。 リムーバブルストレージの PNPDeviceID を検索するには、次の手順に従います。 1. リムーバブルストレージデバイスを暗号化されたコンピュータに挿入します。 2. C:\Programdata\Dell\Dell Data Protection\Encryption\EMS の EMSService.log を開きます。 3. 「PNPDeviceID=」を検索します。 例：14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDeviceID = USBSTOR\DISK&VEN_SEAGATE&PROD_USB&REV_0409\2HC015KJ&0 EMS デバイスのホワイトリストのポリシーで、次を指定します。

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
										VEN= ベンダー（例：USBSTOR\DISK&VEN_SEAGATE） PROD= 製品 / モデル名（例：&PROD_USB）。すべての Seagate の USB ドライブ の EMS Encryption からも除外されます。VEN 値（例：USBSTOR\DISK&VEN_SEAGATE）はこの値に先行する必要があります。 REV= ファームウェアのリビジョン（例：&REV_0409）。使用中の特定のモデルも除外します。VEN 値および PROD 値はこの値に先行する必要があります。 シリアル番号（例：\2HC015KJ&0）。このデバイスのみを除外します。VEN 値、PROD 値、および REV 値はこの値に先行する必要があります。 許可される区切り文字：タブ、カンマ、セミコロン、16 進数文字の 0x1E（レコード区切り文字）
EMS パスワードに英字が必要	True									True に設定すると、パスワードに 1 つまたは複数の文字が必要になります。
EMS パスワードに大文字小文字の混在が必要	True	False								Selected に設定すると、パスワードに少なくとも大文字 1 文字および小文字 1 文字が必要になります。
EMS パスワードに必要な文字数	最低 8 文字					6		最低 8 文字		1～40 文字 パスワードに必要とされる最小文字数です。
EMS パスワードに数字が必要	True	False								True に設定すると、パスワードに 1 つまたは複数の数字が必要になります。
EMS パスワード試行	2	3				4		3		1～10

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
の許可回数										ユーザーが正しいパスワードの入力を試行できる回数です。
EMS パスワードに特殊文字が必要	True	False							True	True に設定すると、パスワードに 1 つまたは複数の特殊文字が必要になります。
EMS クールダウン時間遅延	30									0～5000 秒 ユーザーが試行許可回数の初回試行後に、2 回目の試行を行うまで待機する必要がある秒数です。
EMS クールダウン時間増分	30	20				10	30	10		0～5000 秒 アクセスコード入力試行で失敗するたびに以前のクールダウン時間に加算される増分時間です。
EMS 暗号化ルール										特定のドライブ、ディレクトリ、およびフォルダを暗号化または暗号化しないために使用する暗号化ルールです。 合計で 2048 文字まで使用できます。行間にラインを追加するために使用された「空白」および「改行」文字は、使用した文字として計上されます。2048 文字を越えるルールは無視されます。 Firewire、USB、eSATA などのマルチインタフェース接続を内蔵したストレージデバイスでは、デバイスの暗号化に Encryption External Media と暗号化ルール両方の使用が必要となる場合があります。これは、Windows オペレーティングシステムがストレージデバイスを処理する方法がインタフェースタイプに基づいて異なるために必要となります。 「Encryption External Media を使用した iPod の暗号化方法」を参照してください。
Shielded 対象外メデ	True								False	1.44 MB フロッピーディスクなど、55 MB に満たないために

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
ィアに対する アクセスの EMS ブロック										Encryption External Media をホストするストレージ容量が不足しているリムーバブルメディアへのアクセスをブロックします。 EMS およびこのポリシーが True の場合は、すべてのアクセスがブロックされます。EMS Encrypt External Media が True で、かつこのポリシーが False である場合、暗号化非対応リムーバブルメディアからデータを読み取ることはできますが、メディアへの書き込みアクセスはブロックされます。 EMS Encrypt External Media が False である場合、このポリシーに効果はなく、暗号化非対応リムーバブルストレージへのアクセスには影響を及ぼしません。
ユーザーエクスペリエンス制御ポリシー										
更新時の強制再起動	True								False	値を True に設定すると、コンピュータはすぐに再起動して暗号化処理を実行するか、System Data Encryption（SDE）などの、デバイスベースのポリシーに関連して更新を行います。
各再起動の遅延時間の長さ	+5	10				20		15		ユーザーがデバイスベースのポリシーに対する再起動の遅延を選択した場合の遅延時間（分）です。
再起動遅延の許容回数	1					+5		3		ユーザーがデバイスベースポリシーに対する再起動を遅延できる回数です。
ファイル競合通知の抑制	False									このポリシーは、クライアントによるファイルの処理中にアプリケーションがそのファイルへのアクセスを試みた場合に、通知ポップアップをユーザーに表示するかどうかを制御します。
ローカル暗号化処理制御の表示	False		True					False		値を True に設定すると、暗号化 / 復号化を一時停止 / 再開するメニューオプションが通知領域のアイコンに表示さ

ポリシー	固定ドライブおよび外部ドライブのすべてに対する積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
										れます（現在の Encryption の動作によって異なります）。 暗号化の一時停止を許可すると、Encryption client がデータをポリシーに従って完全に暗号化 / 復号化することをユーザーが妨げる恐れがあります。
画面がロックされている場合のみ暗号化処理を許可	False		User-Optional					False		True、False、User-Optional True の場合、ユーザーがアクティブに作業している間は、データの暗号化または復号化が実行されません。クライアントは、画面がロックされている場合にのみデータを処理します。 User-Optional では、通知領域のアイコンにオプションが追加され、ユーザーがこの機能をオンまたはオフにできます。 False を設定すると、ユーザーが作業中であっても、暗号化処理はいつでも実行されます。 このオプションを有効にすると、暗号化または復号化を完了するために必要な時間を大幅に増やすことができます。

テンプレートの説明

固定ドライブおよび外部ドライブのすべてに対する積極的な保護

このポリシーテンプレートは、企業全体における強力なセキュリティとリスク回避を主な目標とする組織のために設計されています。このポリシーは、可用性、および特定のユーザー、グループ、またはデバイスに対する低セキュリティポリシー例外の必要性よりもセキュリティがはるかに重要である場合に最適です。

このポリシーテンプレートでは以下の機能が提供されます。

- 厳しく制限された設定によるより優れた保護。
- システムドライブおよびすべての固定ドライブに対する保護。
- リムーバブルメディアデバイスの全データの暗号化、および暗号化されていないリムーバブルメディアデバイスの使用の防止。
- 読み取り専用の光学ドライブ制御。

PCI 規制の対象

Payment Card Industry Data Security Standard（PCI DSS）は、セキュリティ管理、ポリシー、手順、ネットワークアーキテクチャ、ソフトウェア設計、およびその他の重要な保護手段に対する要件を含む、多面的なセキュリティ規格です。この包括的な規格は、組織が積極的に顧客アカウントデータを保護するためのガイドラインの設定を目的としています。

このポリシーテンプレートでは以下の機能が提供されます。

- システムドライブおよびすべての固定ドライブに対する保護。
- ユーザーに対するリムーバブルメディアデバイスの暗号化のプロンプト表示。
- UDF CD/DVD 限定の書き込み機能。ポート制御設定は、すべての光学ドライブに対する読み取りアクセスを可能にします。

データ漏洩規制の対象

サーベンスオクスリー法では、金融情報の適切な管理が義務付けられています。この情報の多くは電子形式で存在しているため、このデータの保管および転送時には、暗号化が重要な管理要点となります。グラムリーチブライリー法（GLB）（金融サービス近代化法とも呼ばれます）では、暗号化は義務付けられていませんが、ただし、連邦財務審査委員会（FFIEC）では、「金融機関は、機密情報の漏洩および改ざんのリスクを軽減するため、情報の保存時および転送時に暗号化を採用することが望ましい」と推奨しています。カリフォルニア州上院法案 1386（California's Database Security Breach 通知条例）では、組織にコンピュータセキュリティ侵害が発生した場合、影響された個人すべてに通知することを要求して、カリフォルニア州在住者をなりすまし犯罪から保護しようとしています。組織が顧客への通知を回避するための唯一の方法は、セキュリティ侵害が発生する前に個人情報がすべて暗号化されていたことを証明できることです。

このポリシーテンプレートでは以下の機能が提供されます。

- システムドライブおよびすべての固定ドライブに対する保護。
- ユーザーに対するリムーバブルメディアデバイスの暗号化のプロンプト表示。
- UDF CD/DVD 限定の書き込み機能。ポート制御設定は、すべての光学ドライブに対する読み取りアクセスを可能にします。

HIPAA 規制の対象

Health Insurance Portability and Accountability Act（HIPAA）は、医療機関に対して、個人を特定できる医療情報の機密性と整合性を保護するための複数の技術対策の実装を義務付けています。

このポリシーテンプレートでは以下の機能が提供されます。

- システムドライブおよびすべての固定ドライブに対する保護。
- ユーザーに対するリムーバブルメディアデバイスの暗号化のプロンプト表示。
- UDF CD/DVD 限定の書き込み機能。ポート制御設定は、すべての光学ドライブに対する読み取りアクセスを可能にします。

固定ドライブおよび外部ドライブのすべてに対する基本的な保護（デフォルト）

このポリシーテンプレートは、システムのユーザビリティに大きな影響を与えることなく高レベルの保護を提供する推奨設定を提供します。

このポリシーテンプレートでは以下の機能が提供されます。

- システムドライブおよびすべての固定ドライブに対する保護。
- ユーザーに対するリムーバブルメディアデバイスの暗号化のプロンプト表示。
- UDF CD/DVD 限定の書き込み機能。ポート制御設定は、すべての光学ドライブに対する読み取りアクセスを可能にします。

固定ドライブすべてに対する基本的な保護

このポリシーテンプレートでは以下の機能が提供されます。

- システムドライブおよびすべての固定ドライブに対する保護。
- サポートされている任意のフォーマットでの CD/DVD への書き込み機能。ポート制御設定は、すべての光学ドライブに対する読み取りアクセスを可能にします。

  このポリシーテンプレートでは以下の機能は提供されません。

- リムーバブルメディアデバイスに対する暗号化機能。

システムドライブのみに対する基本保護

このポリシーテンプレートでは以下の機能が提供されます。

- システムドライブの保護。このドライブは、通常オペレーティングシステムがロードされる C: ドライブです。
- サポートされている任意のフォーマットでの CD/DVD への書き込み機能。ポート制御設定は、すべての光学ドライブに対する読み取りアクセスを可能にします。

  このポリシーテンプレートでは以下の機能は提供されません。

- リムーバブルメディアデバイスに対する暗号化機能。

外部ドライブに対する基本的な保護

このポリシーテンプレートでは以下の機能が提供されます。

- リムーバブルメディアデバイスの保護。
- UDF CD/DVD 限定の書き込み機能。ポート制御設定は、すべての光学ドライブに対する読み取りアクセスを可能にします。

  このポリシーテンプレートでは以下の機能は提供されません。

- システムドライブ（通常オペレーティングシステムがロードされる C: ドライブ）またはその他固定ドライブに対する保護。

暗号化無効

このポリシーテンプレートでは、暗号化による保護は行われません。このテンプレートを使用する場合は、デバイスをデータの損失や窃盗から守るほかの手段を講じてください。

このテンプレートは、セキュリティへの移行において、アクティブな暗号化なしでの開始を希望する組織に役立ちます。組織がセキュリティ導入に順応していくに従い、個々のポリシーを調整する、または組織の一部または全体に対してより強力なテンプレートを適用することによって、徐々に暗号化を有効にしていくことができます。

11

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。
- マスターのインストーラがインストールに使用されている場合は、クライアントの個別にアンインストールする必要があります。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、次のコマンドを入力します。

   ```
   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\.`

続行をトラブル シューティングしてください。

12

トラブルシューティング

Windows 10 または Windows 11 機能更新プログラムを使用したアップグレード

機能更新プログラムを使用して Windows 10 または Windows 11 をアップグレードするには、KB 記事 125419 の手順に従います。

Dell Encryption のトラブルシューティング

（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 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。

出力	意味
	Common：共通暗号化キー。 WSScan では、Encrypt for Sharing で暗号化されたファイルは報告されません。
KCID	キーコンピュータ ID。 上記の例では、「**7vdlxrsb**」 マッピングされているネットワークドライブをスキャンした場合、KCID はスキャンレポートに表示されません。
UCID	ユーザー ID。 上記の例では、「**_SDENCR_**」 UCID は、そのコンピュータのすべてのユーザーで共有されます。
ファイル	暗号化ファイルのパス。 上記の例では、「**c:\temp\Dell - test.log**」
アルゴリズム	ファイルの暗号化に使用した暗号化アルゴリズム。 上記の例では、「**is still AES256 encrypted**」 Rijndael 128 Rijndael 256 AES-128 AES-256 3DES

Encryption Removal Agent ステータスのチェック

Encryption Removal Agent は、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。
- **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。

Encryption External Media で iPod を暗号化する方法

これらのルールによって、iPod に限らず、すべてのリムーバブルデバイスの上記のフォルダおよびファイルタイプの暗号化が無効または有効になります。ルールを定義するときは注意して行ってください。

- 予期しない結果が発生する可能性があるため、iPod Shuffle の使用はお勧めしません。
- iPod の変更に伴い、この情報も変更される場合があります。このため、Encryption External Media 対応コンピュータでの iPod の使用許可には注意を払うようにしてください。
- iPod 上のフォルダ名は iPod のモデルによって異なるため、すべての iPod モデルのすべてのフォルダ名を対象とする除外ポリシーを作成することをお勧めします。
- Encryption External Media 経由での iPod の暗号化がデバイスを使用不能にしないようにするには、Encryption External Media 暗号化ルールポリシーに次のルールを入力してください。

  -R#:\Calendars

  -R#:\Contacts

  -R#:\iPod_Control

  -R#:\Notes

  -R#:\Photos

- 上記のディレクトリに含まれる特定のファイルタイプを強制的に暗号化することもできます。次のルールを追加すると、以前のルールによって暗号化から除外されたディレクトリに含まれる ppt、pptx、doc、docx、xls、および xlsx ファイルの暗号化が確実になります。

  ^R#:\Calendars;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Contacts;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\iPod_Control;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Notes;ppt.doc.xls.pptx.docx.xlsx

  ^R#:\Photos;ppt.doc.xls.pptx.docx.xlsx

- これらの 5 つのルールを次のルールで置き換えると、iPod、Calendars、Contacts、iPod_Control、Notes、および Photos の任意のディレクトリに含まれる ppt、pptx、doc、docx、xls、および xlsx ファイルが強制的に暗号化されます。

  ^R#:\;ppt.doc.xls.pptx.docx.xlsx

- これらのルールは、次の iPod に対してテストされています。

  第 5 世代 iPod Video 30 GB

  第 2 世代 iPod Nano 2 GB

  第 2 世代 iPod Mini 4 GB

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。

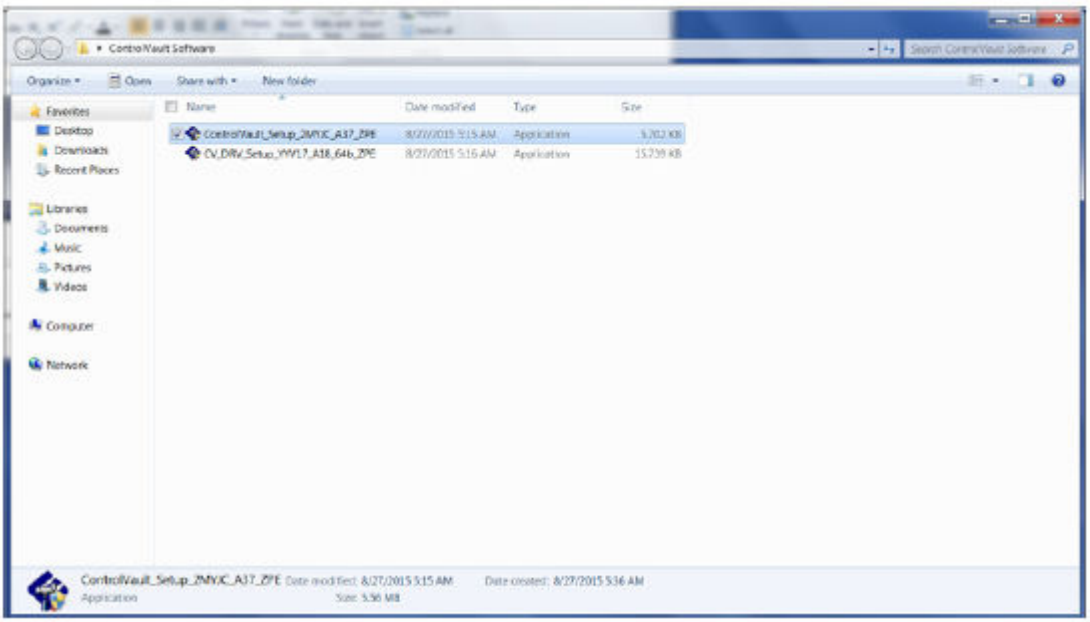
3. **続行** をクリックして開始します。
4. **Ok** をクリックして、ドライバー ファイルをデフォルトの場所である `C:\Dell\Drivers\<New Folder>`に解凍します。
5. **はい** をクリックして新しいフォルダの作成を許可します。
6. 正常に解凍しましたというメッセージが表示されたら **Ok** をクリックします。
7. 抽出後、ファイルが含まれているフォルダが表示されます。表示されない場合は、ファイルを抽出したフォルダに移動します。この場合、フォルダは **JW22F** です。
8. **CVHCI64.MSI** をダブルクリックしてドライ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

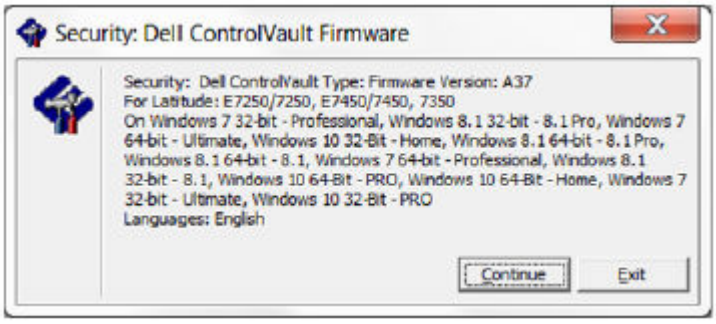
- オペレーティングシステムおよびハードウェアの構成によっては、デバイスマネージャに Dell ControlVault デバイス（およびその他のデバイス）が表示されます。

Dell ControlVault ファームウェアのインストール

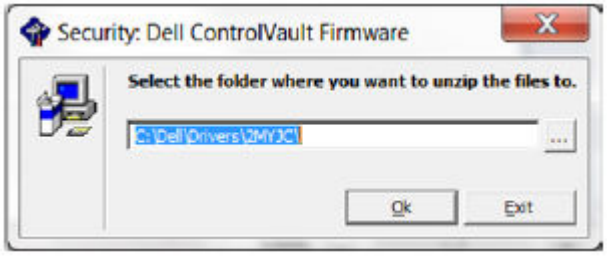
1. ファームウェアのインストールファイルをダウンロードしたフォルダに移動します。



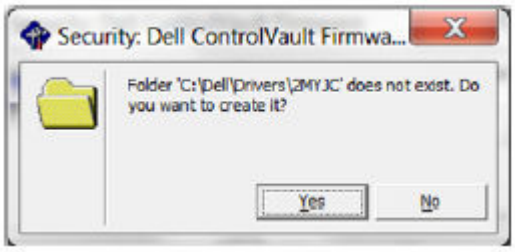
2. Dell ControlVault ファームウェアをダブルクリックして自己解凍形式の実行可能ファイルを実行します。
3. **続行** をクリックして開始します。



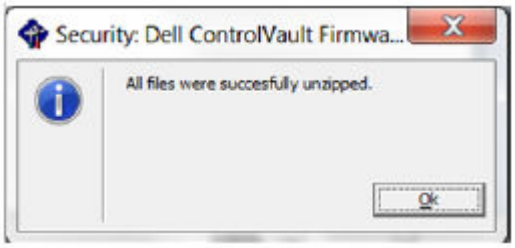
4. **Ok** をクリックして、ドライバー ファイルをデフォルトの場所である `C:\Dell\Drivers\<New Folder>`に解凍します。



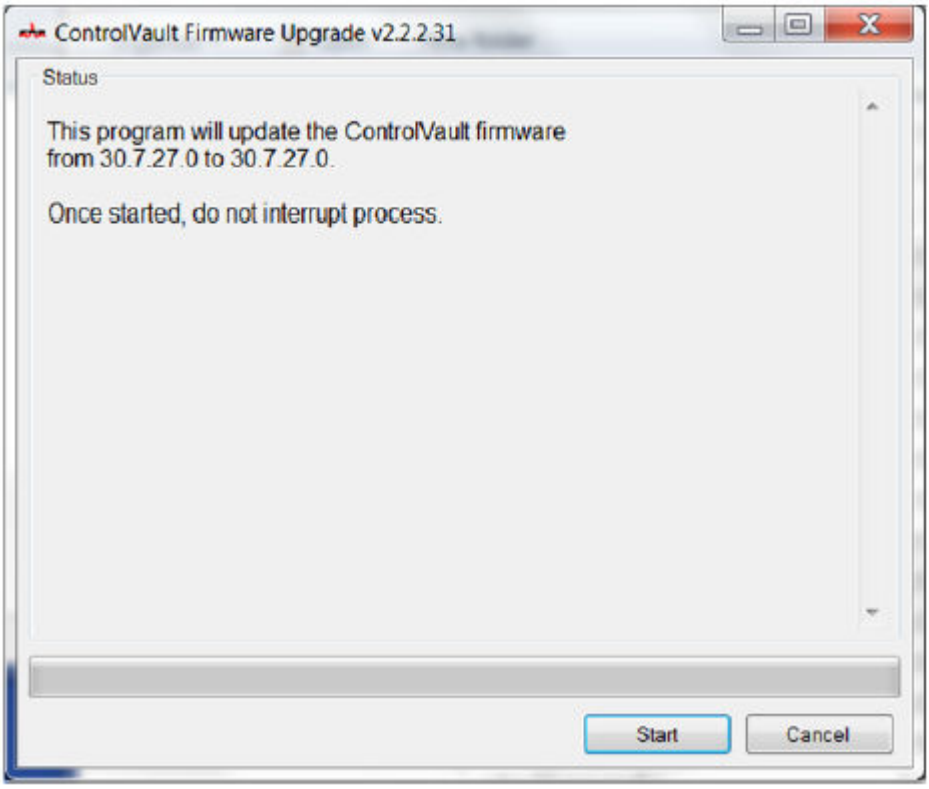
5. **はい** をクリックして新しいフォルダの作成を許可します。



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。

レジストリ設定

この項では、Dell ProSupport で承認された、ローカル クライアント コンピューターのすべてのレジストリー設定について詳細に説明します。

暗号化

（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.`
- 復号化の対象となるコンピューターに次のレジストリー エントリーを作成します。

  [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

Windows ログオンを含むスマート カードの使用

- 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

インストール中に一時ファイルを保持する

- 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 ディレクトリー内のファイル構成の維持を要求するサード パーティー 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 の開始または遅延を決めるユーザー プロンプトのデフォルトの動作の変更

- Encryption クライアントでは、*length of each policy update delay* プロンプトが毎回 5 分間表示されます。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。これを行うには、レジストリを次のレジストリ値に設定します。

  [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]）。

SDUser キーのデフォルト使用の変更

- 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 キーを無効にし、SDE キーを使用してこれらのユーザーディレクトリを暗号化するには、コンピュータ上に次のレジストリエントリを作成します。

  [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。

右クリックのコンテキスト メニューでの Encrypt for Sharing の無効化/有効化

- 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

Encryption Personal のアクティブ化の通知の無効化/有効化

- HKCU\Software\Dell\Dell Data Protection\Encryption

  "HidePasswordPrompt"=DWORD

  1 = Encryption Personal のアクティブ化のパスワード プロンプトを無効にします。

  0 = Encryption Personal のアクティブ化のパスワード プロンプトを有効にします。

Encryption Removal Agent による復号化の最終段階が終了した後の再起動プロンプトの無効化/有効化

- Encryption Removal Agent が復号化プロセスの最終状態を終了した後に、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します。

  HKLM\Software\Dell\Dell Data Protection

  "ShowDecryptAgentRebootPrompt"=DWORD

  デフォルト = 有効

  1 = 有効（プロンプトを表示）

  0 = 無効（プロンプトを非表示）

Advanced Authentication

スマートカードと生体サービス（オプション）

Advanced Authentication がスマート カードおよび生体デバイスに関連付けられているサービスを「自動」起動タイプに変更することを避けるには、サービス起動機能を無効にすることができます。

無効にすると、Authentication は次の 3 つ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。

  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。

- 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。

  [HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

  SmartCardServiceCheck=REG_DWORD:0

  有効化するには 0 に設定します。

  無効化するには 1 に設定します。

Windows ログオンを含むスマート カードの使用

- 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

  続行するには用語集を押します。

- SED 管理でサード パーティー資格情報プロバイダーを無効に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

- 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\

  DWORD: DumpPolicies

  Value=1

  メモ：この変更を有効にするには、再起動が必要です。

- 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

13

用語集

Advanced Authentication - Advanced Authentication 製品では、オプションとしてスマートカードリーダを利用できます。Advanced Authentication は、これらの複数の認証方法の管理を支援し、自己暗号化ドライブ、SSO でのログインをサポートし、ユーザーの資格情報およびパスワードを管理します。

暗号化管理者パスワード（EAP） - EAP は、各コンピュータ固有の管理用パスワードです。このパスワードは、ローカル管理コンソールで行われた設定変更の大部分で必要となります。また、このパスワードは、LSARecovery_[ホスト名].exe ファイルを使用してデータを回復する必要がある場合に必要なパスワードと同じです。このパスワードを記録して、安全な場所に保管してください。

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

暗号化キー – ほとんどの場合、Encryption はユーザー暗号化キーに加え 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。共有暗号化キーを使用すると、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。ユーザー暗号化キーでは、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暗号化キーでは、ファイルを作成したユーザーのみが、任意の暗号化 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。

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。

シングルサインオン（SSO） - SSO は、起動前と Windows ログオンの両方で多因子認証が有効になっているとき、ログオン処理を簡素化します。有効になっている場合、認証は起動前のみで必要となり、ユーザーは Windows に自動的にログオンされます。有効ではない場合は、数回にわたる認証が必要となることがあります。

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 ポリシーでは、起動前認証は必要なく、マスターブートレコードへの干渉は一切行われません。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。