Encryption

システム要件 v10.1

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示しています。

2018 - 11

Rev. A01

目次

1

はじめに

この文書では、Dell Encryption の各種要件を示します。

Dell Encryption に関するドキュメントには、すべて www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals からアクセスできます。

Dell ProSupport へのお問い合わせ

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

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

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

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

2

要件

すべてのクライアント

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 SMS または Dell KACE などの導入ツールによって一時的に割り当てることができます。昇格された権限を持つ非管理者ユーザーはサポートされません。
- インストールまたはアンインストールを開始する前に、重要なデータをすべてバックアップします。
- インストール中は、外付け (USB) ドライブの挿入や取り外しを含め、コンピュータに変更を加えないでください。
- マスターインストーラクライアントが Dell Digital Delivery (DDD) を使用して資格を得る場合は、アウトバウンドポート 443 が Security Management Server/Security Management Server Virtual と通信できるようにしてください。資格機能はポート 443 が (何らかの理由で) ブロックされている場合には機能しません。子インストーラを使用してインストールする場合、DDD は使用されません。
- 必ず www.dell.com/support で、最新の文書およびテクニカルアドバイザリーを定期的に確認してください。

すべてのクライアント - 前提条件

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

  デルの工場から出荷されるすべてのコンピュータには、Microsoft .Net Framework 4.5.2 以降の完全バージョンが事前インストールされています。ただし、Dell ハードウェア上にインストールしていない、または旧型の Dell ハードウェア上で Security Tools をアップグレードしている場合は、インストール / アップグレードの失敗を防ぐため、**Security Tools をインストールする前に**、インストールされている Microsoft .Net のバージョンを確認し、バージョンをアップデートするようにしてください。インストールされている Microsoft .Net のバージョンを検証するには、インストール対象のコンピュータで http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx に記載されている手順を実行します。Microsoft .Net Framework 4.5.2 をインストールするには、https://www.microsoft.com/en-us/download/details.aspx?id=42643 に移動してください。
- マスターインストーラまたは子インストーラの実行可能ファイルに、ControlVault、指紋リーダー、およびスマートカード (下記参照) のドライバとファームウェアは含まれていません。ドライバとファームウェアは最新の状態にしておく必要があります。これらは、http://www.dell.com/support から、お使いのコンピュータモデルを選択してダウンロードできます。認証ハードウェアに基づいて、適切なドライバとファームウェアをダウンロードします。
  - ControlVault
  - NEXT Biometrics Fingerprint ドライバ
  - Validity Fingerprint Reader 495 ドライバ
  - O2Micro スマートカードドライバ

すべてのクライアント - ハードウェア

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

ハードウェア
– Intel Pentium または AMD プロセッサ

ハードウェア

- 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。このサイズは、ポリシーとドライブのサイズによって異なります。

すべてのクライアント - ローカライズ

- Encryption および BitLocker Manager クライアントは複数言語ユーザーインタフェース（MUI）に対応しており、次の言語にローカライズされます。

言語サポート

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

Encryption クライアント

- クライアントコンピュータは、アクティブ化するためにネットワーク接続が必要です。
- 最初の暗号化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。
- 最初の暗号化スイープ中にスリープモードをオフにして、誰も操作していないコンピュータがスリープ状態になるのを防ぎます。スリープ状態のコンピュータでは暗号化は行われません（復号化も行われません）。
- Encryption クライアントは、デュアルブート設定をサポートしていません。これは、もう一方のオペレーティングシステムのシステムファイルが暗号化され、その動作を妨げるおそれがあるためです。
- マスターインストーラでは、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から子インストーラを抽出し、コンポーネントを個々にアップグレードします。
- 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。企業用イメージで Encryption クライアントをインストールする手順については、http://www.dell.com/support/article/us/en/19/SLN304039 を参照してください。
- Encryption クライアントは、McAfee、Symantec クライアント、Kaspersky、および MalwareBytes を使用してテスト済みです。これらのアンチウイルスプロバイダに関しては、アンチウイルススキャンおよび暗号化における互換性を確保するために、ハードコーディングされた除外が設定されています。Encryption クライアントは、Microsoft Enhanced Mitigation Experience Toolkit でもテスト済みです。

  リストに記載のないアンチウイルスプロバイダを組織が使用している場合は、http://www.dell.com/support/article/us/en/19/SLN288353 を参照するか、または Dell ProSupport に連絡してサポートを受けてください。
- TPM は GPK を封印するために使用されます。したがって、Encryption クライアントを実行している場合は、クライアント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前に、BIOS で TPM をクリアする必要があります。
- インプレイスでのオペレーティングシステムのアップグレードは、Encryption クライアントがインストールされている場合ではサポートされていません。Encryption クライアントをアンインストールおよび復号化し、新しいオペレーティングシステムにアップグレードした後、Encryption クライアントを再度インストールしてください。

  さらに、オペレーティングシステムの再インストールもサポートされていません。オペレーティングシステムを再インストールするには、ターゲットコンピュータをバックアップしてからそのコンピュータをワイプし、オペレーティングシステムをインストールした後、確立した回復手順に従って暗号化されたデータを回復してください。

Encryption クライアントの前提条件

- マスターインストーラをコンピュータにすでにインストールされていない場合は Microsoft Visual C++ 2012 アップデート 4 + をインストールします。**子インストーラを使用する場合** は、Encryption クライアント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。

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

Encryption クライアントハードウェア

- 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

Encryption クライアントのオペレーティングシステム

- 次の表では、対応オペレーティングシステムが詳しく説明されています。

Windows オペレーティングシステム (32 ビットと 64 ビット)
– Windows 7 SP1：Enterprise、Professional、Ultimate
– アプリケーション互換テンプレートでの Windows Embedded Standard 7 (ハードウェア暗号化はサポートされていません)
– Windows 8：Enterprise、Pro
– Windows 8.1 Update 0-1：Enterprise Edition、Pro Edition
– Windows Embedded 8.1 Industry Enterprise (ハードウェア暗号化はサポートされていません)
– Windows 10：Education、Enterprise、Pro バージョン 1607 (Anniversary Update/Redstone 1) からバージョン 1803 (April 2018 Update/Redstone 4)
– VMWare Workstation 12.5 以降

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

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

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

メモ:
Encryption External Media をホストするには、外部メディア上の約 55 MB の空き容量に加えて、メディア上に暗号化対象の最大ファイルに等しい空き容量が必要です。

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

- Windows 7 SP1：Enterprise、Professional、Ultimate
- Windows 8：Enterprise、Pro、Consumer
- Windows 8.1 Update 0-1：Enterprise Edition、Pro Edition
- Windows 10：Education、Enterprise、Pro バージョン 1607（Anniversary Update/Redstone 1）からバージョン 1803（April 2018 Update/Redstone 4）

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

- Mac OS Sierra 10.12.4 および 10.12.5
- macOS High Sierra 10.13.5 - 10.13.6
- macOS Mojave 10.14

Server Encryption クライアント

Server Encryption は、サーバーモードで動作しているコンピュータ、特にファイルサーバー上での使用を対象にしています。

- Server Encryption は、Encryption Enterprise および Endpoint Security Suite Enterprise.とのみ互換性があります。
- Server Encryption は次を提供します。
  - ソフトウェアの暗号化は、Microsoft Windows Embedded 8.1 Industry Enterprise
  - リムーバブルメディア暗号化
  - ポート制御

    メモ:
    サーバはポート制御をサポートしている必要があります。

    サーバポート制御システムポリシーは、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と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を使用することができなくなります。

Server Encryption は、次に対して使用します。

- 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、業界をリードするアンチウイルスプロバイダ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間における非互換性を防ぐため、これらのアンチウイルスプロバイダ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。リストにないアンチウイルスプロバイダが組織で使用されている場合は、KB 記事 SLN298707 を参照するか、Dell ProSupport にお問い合わせください。

非対応

Server Encryption は、次での使用は対象外です。

- 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。
- Server Encryption は、Encryption Personal とは互換性がありません。

- Server Encryption は、SED Management または BitLocker Manager クライアントではサポートされません。
- Server Encryption は、分散ファイルシステム（DFS）の一部であるサーバではサポートされません。
- Server Encryption との間の移行はサポートされていません。Encryption External Media から Server Encryption にアップグレードする場合、前の製品を完全にアンインストールしてから Server Encryption を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 ドライブ（RAID および非 RAID）
  - キオスク向けの自動ログオン（Windows 7、8 / 8.1）
  - Microsoft Storage Server 2012
- Server 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。
- インプレイスでのオペレーティングシステムの再インストールがサポートされていません。オペレーティングシステムを再インストールするには、ターゲットコンピュータをバックアップしてからそのコンピュータをワイプし、オペレーティングシステムをインストールした後、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の詳細については、『*Recovery Guide*』（リカバリガイド）を参照してください。

Server Encryption クライアントのハードウェア

最小限のハードウェア要件は、オペレーティングシステムの最小要件を満たしている必要があります。

Server Encryption クライアントのオペレーティングシステム

次の表は、対応オペレーティングシステムの詳しい説明です。

オペレーティングシステム（32 ビットと 64 ビット）

- Windows 7 SP1：Enterprise、Professional、Ultimate
- Windows 8.0：Enterprise、Pro
- Windows 8.1：Enterprise、Pro
- Windows 10：Education、Enterprise、Pro バージョン 1607（Anniversary Update/Redstone 1）からバージョン 1803（April 2018 Update/Redstone 4）

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）

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 2016：Standard Edition、Essentials Edition、Datacenter Edition（Server Core はサポートされません）

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

メモ:
サポートされる UEFI コンピュータでは、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

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。

メモ:
Encryption External Media をホストするには、外部メディア上の約 55 MB の空き容量に加えて、メディア上に暗号化対象の最大ファイルに等しい空き容量が必要です。

Encryption External Media 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 Windows オペレーティングシステム（32 ビットおよび 64 ビット）

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

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

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 Mac オペレーティングシステム（64 ビットカーネル）

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