

Dell Data Protection | Endpoint Security Suite Enterprise

詳細インストールガイド v1.4



メモ、注意、警告

① **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。

© 2017 Dell Inc. 無断転載を禁じます。Dell、EMC、およびその他の商標は、Dell Inc. またはその子会社の商標です。その他の商標は、それぞれの所有者の商標である場合があります。

Dell Data Protection Encryption、Endpoint Security Suite、Endpoint Security Suite Enterprise、および Dell Data Guardian のスイートのドキュメントに使用されている登録商標および商標 (Dell™、Dell のロゴ、Dell Precision™、OptiPlex™、ControlVault™、Latitude™、XPS®、および KACE™)は、Dell Inc. の商標です。Cylance®、CylancePROTECT、および Cylance のロゴは、米国およびその他の国における Cylance, Inc. の登録商標です。McAfee® および McAfee のロゴは、米国およびその他の国における McAfee, Inc. の商標または登録商標です。Intel®、Pentium®、Intel Core Inside Duo®、Itanium®、および Xeon® は米国およびその他の国における Intel Corporation の登録商標です。Adobe®、Acrobat®、および Flash® は、Adobe Systems Incorporated の登録商標です。Authen Tec® および Eikon® は、Authen Tec の登録商標です。AMD® は、詳細設定 Micro Devices, Inc. の登録商標です。Microsoft®、Windows®、および Windows Server®、Internet Explorer®、MS-DOS®、Windows Vista®、MSN®、ActiveX®、Active Directory®、Access®、ActiveSync®、BitLocker®、BitLocker To Go®、Excel®、Hyper-V®、Silverlight®、Outlook®、PowerPoint®、Skydrive®、SQL Serve®、および Visual C++® は、米国および / またはその他の国における Microsoft Corporation の商標または登録商標です。VMware® は、米国およびその他の国における VMware, Inc. の登録商標または商標です。Box® は、Box の登録商標です。DropboxSM は、Dropbox, Inc. のサービスマークです。Google™、Android™、Google™ Chrome™、Gmail™、YouTube®、および Google™ Play は、米国およびその他の国における Google Inc. の商標または登録商標のいずれかです。Apple®、Aperture®、App StoreSM、Apple Remote Desktop™、Apple TV®、Boot Camp™、FileVault™、 iCloud®SM、iPad®、iPhone®、iPhoto®、iTunes Music Store®、Macintosh®、Safari®、および Siri® は、米国またはその他の国あるいはその両方における Apple, Inc. のサービスマーク、商標、または登録商標です。GO ID®、RSA®、および SecurID® は Dell EMC の登録商標です。EnCase™ および Guidance Software® は、Guidance Software の商標または登録商標です。Entrust® は、米国およびその他の国における Entrust®, Inc. の登録商標です。InstallShield® は、米国、中国、欧州共同体、香港、日本、台湾、および英国における Flexera Software の登録商標です。Micron® および RealSSD® は、米国およびその他の国における Micron Technology, Inc. の登録商標です。Mozilla® Firefox® は、米国およびその他の国における Mozilla Foundation の登録商標です。IOS® は同社の商標または米国およびその他の特定の国で Cisco Systems, Inc. の登録商標であり、ライセンスに使用されます。Oracle® および Java® は、Oracle および / またはその関連会社の登録商標です。その他の名称は、それぞれの所有者の商標である場合があります。SAMSUNG™ は、米国およびその他の国における SAMSUNG の商標です。Seagate® は、米国および / またはその他の国における Seagate Technology LLC の登録商標です。Travelstar® は、米国およびその他の国における HGST, Inc. の登録商標です。UNIX® は、The Open Group の登録商標です。VALIDITY™ は、米国およびその他の国における Validity Sensors, Inc. の商標です。VeriSign® およびその他の関連標章は、米国およびその他の国における VeriSign, Inc. またはその関連会社あるいは子会社の商標または登録商標であり、Symantec Corporation にライセンス供与されています。KVM on IP® は、Video Products の登録商標です。Yahoo!® は、Yahoo! Inc. の登録商標ですこの製品は、7-Zip プログラムの一部を使用しています。このソースコードは、7-zip.org に掲載されています。ライセンス供与は、GNU LGPL ライセンス + unRAR 制限 (7-zip.org/license.txt) の対象です。

Endpoint Security Suite Enterprise 詳細インストールガイド

2017 - 04

Rev. A01

1 はじめに.....	7
作業を開始する前に.....	7
このガイドの使用方法.....	7
Dell ProSupport へのお問い合わせ.....	8
2 要件.....	9
すべてのクライアント.....	9
すべてのクライアント - 前提条件.....	9
すべてのクライアント - ハードウェア.....	9
すべてのクライアント - 言語サポート.....	10
Encryption クライアント.....	10
Encryption クライアントの前提条件.....	11
Encryption クライアントハードウェア.....	11
Encryption クライアントのオペレーティングシステム.....	11
外付けメディアシールド (EMS) のオペレーティングシステム.....	12
Server Encryption クライアント.....	12
Server Encryption クライアントの前提条件.....	13
Server Encryption クライアントのハードウェア.....	14
Server Encryption クライアントのオペレーティングシステム.....	14
外付けメディアシールド (EMS) のオペレーティングシステム.....	14
Advanced Threat Prevention クライアント.....	15
Advanced Threat Prevention のオペレーティングシステム.....	15
Advanced Threat Prevention のポート.....	16
BIOS イメージの整合性検証.....	16
SED クライアント.....	17
OPAL ドライバ.....	17
SED クライアントの前提条件.....	17
SED クライアントハードウェア.....	17
SED クライアントのオペレーティングシステム.....	19
Advanced Authentication クライアント.....	19
Advanced Authentication クライアントハードウェア.....	19
Advanced Authentication クライアントのオペレーティングシステム.....	20
BitLocker Manager クライアント.....	20
BitLocker Manager クライアントの前提条件.....	21
BitLocker Manager クライアントのオペレーティングシステム.....	21
認証オプション.....	21
暗号化クライアント.....	22
SED クライアント.....	23
BitLocker Manager.....	24
3 レジストリ設定.....	25

Encryption クライアントのレジストリ設定.....	25
Advanced Threat Prevention クライアントのレジストリ設定.....	29
SED クライアントのレジストリ設定.....	30
Advanced Authentication クライアントのレジストリ設定.....	31
BitLocker Manager クライアントのレジストリ設定.....	32
4 ESSE マスターインストーラを使用したインストール.....	33
ESSE マスターインストーラを使用した対話型のインストール.....	33
ESSE マスターインストーラを使用したコマンドラインによるインストール.....	34
5 ESSE マスターインストーラを使用したアンインストール.....	37
ESSE マスターインストーラのアンインストール.....	37
コマンドラインでのアンインストール.....	37
6 子インストーラを使用したインストール.....	38
ドライバのインストール.....	39
Encryption クライアントのインストール.....	39
コマンドラインでのインストール.....	39
Server Encryption クライアントのインストール.....	41
Server Encryption の対話型インストール.....	42
コマンドラインを使用した Server Encryption のインストール.....	43
Server Encryption のアクティブ化.....	45
Advanced Threat Prevention クライアントのインストール.....	46
コマンドラインでのインストール.....	46
ウェブプロテクションおよびファイアウォールのインストール.....	47
コマンドラインでのインストール.....	48
SED Management と Advanced Authentication クライアントのインストール.....	49
コマンドラインでのインストール.....	49
BitLocker Manager クライアントのインストール.....	50
コマンドラインでのインストール.....	50
7 子インストーラを使用したアンインストール.....	52
ウェブプロテクションおよびファイアウォールのアンインストール.....	53
コマンドラインでのアンインストール.....	53
Encryption および Server Encryption クライアントのアンインストール.....	53
プロセス.....	53
コマンドラインでのアンインストール.....	54
Advanced Threat Prevention のアンインストール.....	55
コマンドラインでのアンインストール.....	55
SED クライアントおよび Advanced Authentication クライアントのアンインストール.....	56
プロセス.....	56
PBA の非アクティブ化.....	56
SED クライアントおよび Advanced Authentication クライアントのアンインストール.....	57
BitLocker Manager クライアントのアンインストール.....	57
コマンドラインでのアンインストール.....	57



8 一般的なシナリオ	58
Encryption クライアント、Advanced Threat Prevention および Advanced Authentication.....	59
SED クライアント (Advanced Authentication を含む) および External Media Shield.....	60
BitLocker Manager および External Media Shield.....	60
BitLocker Manager および Advanced Threat Prevention.....	61
9 Advanced Threat Prevention のためのテナントのプロビジョニング	62
テナントのプロビジョニング.....	62
10 Advanced Threat Prevention エージェント自動アップデートの設定	63
11 ワンタイムパスワード、SED UEFI、および BitLocker のための事前インストール設定	64
TPM の初期化.....	64
UEFI コンピュータ用の事前インストール設定.....	64
UEFI 起動前認証中におけるネットワーク接続の有効化.....	64
レガシーオプション ROM の無効化.....	64
BitLocker PBA パーティションを設定する事前インストール設定.....	65
12 ドメインコントローラでの GPO の設定による資格の有効化	66
13 ESSE マスターインストーラからの子インストーラの抽出	67
14 EE Server に対してアクティブ化した Encryption クライアントをアンインストールするための Key Server の設定	68
サービスパネル - ドメインアカウントのユーザーの追加.....	68
キーサーバーの設定ファイル - EE Server の通信のためのユーザーの追加.....	68
サンプル設定ファイル.....	69
サービスパネル - キーサーバーサービスの再起動.....	69
リモート管理コンソール - フォレンジック管理者の追加.....	70
15 Administrative Download Utility (CMGAd) の使用	71
フォレンジックモードでの Administrative Download Utility の使用.....	71
管理者モードでの Administrative Download Utility の使用.....	72
16 Server Encryption の設定	73
Server Encryption の有効化.....	73
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.....	73
Server Encryption EMS ポリシーの設定.....	74
暗号化されたサーバーインスタンスのサスペンド.....	74
17 トラブルシューティング	76
すべてのクライアントのトラブルシューティング.....	76
Encryption および Server Encryption クライアントのトラブルシューティング.....	76
Windows 10 Anniversary アップデートへのアップグレード.....	76
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.....	76
(オプション) Encryption Removal Agent ログファイルの作成.....	79



TSS バージョンの確認.....	79
EMS と PCS の相互作用.....	79
WSScan の使用.....	79
WSProbe の使用.....	82
Encryption Removal Agent ステータスのチェック.....	83
Advanced Threat Prevention クライアントのトラブルシューティング.....	84
Windows Powershell を使用した製品コードの検索.....	84
Advanced Threat Prevention のプロビジョニングおよびエージェント通信.....	84
BIOS イメージの整合性検証プロセス.....	87
SED クライアントのトラブルシューティング.....	88
初期アクセスコードポリシーの使用.....	88
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.....	89
Dell ControlVault ドライバ.....	90
Dell ControlVault ドライバおよびファームウェアのアップデート.....	90
UEFI コンピュータ.....	91
ネットワーク接続のトラブルシューティング.....	91
TPM および BitLocker.....	92
TPM および BitLocker のエラーコード.....	92
18 用語集.....	122



はじめに

本書では、Advanced Threat Prevention、暗号化クライアント、SED 管理クライアント、Advanced Authentication、および BitLocker Manager のインストールおよび設定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 にあります。

作業を開始する前に

- 1 クライアントを導入する前に、EE Server/VE Server をインストールします。次に示すように、正しいガイドを探し、記載されている手順に従った後、このガイドに戻ります。
 - 『[DDP Enterprise Server インストールおよびマイグレーションガイド](#)』
 - 『[DDP Enterprise Server - Virtual Edition クイックスタートガイドおよびインストールガイド](#)』

希望のポリシーを設定しているかを確認します。? のマークから AdminHelp を参照します。画面の右端にあります。AdminHelp はポリシーの設定および変更、EE Server/VE Server でのオプションを理解するのに役立つよう設計されたページヘルプです。
- 2 『[Advanced Threat Prevention のためのテナントのプロビジョニング](#)』。Advanced Threat Prevention のポリシーの施行がアクティブになる前に、テナントが DDP Server にプロビジョニングされる必要があります。
- 3 本書の「要件」の章をすべて読んでください。
- 4 エンドユーザーにクライアントを導入します。

このガイドの使用法

このガイドは次の順序で使用してください。

- クライアントの必要条件、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、「[ワンタイムパスワード、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 デジタル Delivery (DDD) 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。
- ESSE 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、次を参照してください。
 - [ESSE マスターインストーラを使用した対話型のインストール](#)
 - または [内部接続ポートを編集...](#) のいずれかをクリックします。
 - [ESSE マスターインストーラを使用したコマンドラインによるインストール](#)
- 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 ESSE マスターインストーラから抽出する必要があります。「[ESSE 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。
 - [ドライバのインストール](#) - 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。
 - [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していても、ネットワークから切断していても、紛失していても、盗難されていても、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 クライアントをインストールするには、これらの手順を使用します。



- [Advanced Threat Prevention クライアントのインストール](#) - これらの手順を使用して、Advanced Threat Prevention クライアントをインストールします。これは、アルゴリズムサイエンスおよび機械学習を使用して、既知および不明のサイバー攻撃を識別、分類し、エンドポイントの実行や障害を防止する、次世代のアンチウイルス対策です。
- [ウェブプロテクションおよびファイアウォールのインストール](#) - オプションのウェブプロテクション機能とファイアウォール機能をインストールするには、これらの手順を用います。クライアントファイアウォールは、ルールのリストに従って、すべての受信および発信トラフィックをチェックする、ステートフルファイアウォールです。ウェブプロテクションは、ウェブサイトの評価に基づき、ウェブのブラウジングとダウンロードを監視して脅威を特定し、脅威が検知された場合はアクションを実行します。
- [SED 管理および Advanced 認証クライアントのインストール](#) - これらの手順を使用して SED を管理するための暗号化ソフトウェアをインストールします。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 管理では、すべてのポリシー、ストレージ、および SED 管理を使用すると、すべてのポリシー、ストレージ、および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が保護されないというリスクを軽減します。

Advanced Authentication クライアントは、SED 用の PBA、シングルサインオン(SSO)、指紋やパスワードなどのユーザー資格情報をはじめとする複数の認証方法を管理します。さらに、ウェブサイトおよびアプリケーションにアクセスするための Advanced Authentication 機能を提供します。

- [BitLocker Manager クライアントのインストール](#) - 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 クライアントをインストールする場合にこれらの手順を使用します。

① メモ:

ほとんどのクライアントインストーラは対話形式でインストールできますが、このガイドではインストールについて記述していません。ただし、Advanced Threat Prevention クライアントの子インストーラはコマンドラインでのみインストールできます。

- 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 へのお問い合わせ

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

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

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

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

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。
- ESSE マスターインストーラクライアントが Dell Digital Delivery（DDD）を使用して資格を得る場合は、アウトバウンドポート 443 が EE Server/VE Server と通信できるようにしてください。資格機能はポート 443 が（何らかの理由で）ブロックされている場合には機能しません。子インストーラを使用してインストールする場合、DDD は使用されません。
- 必ず www.dell.com/support で、最新の文書およびテクニカルアドバイザリーを定期的に確認してください。

すべてのクライアント - 前提条件

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

デルの工場から出荷されるすべてのコンピュータには、Microsoft .Net Framework 4.5.2 以降の完全バージョンが事前インストールされています。ただし、Dell ハードウェア上にインストールしていない、または旧型の Dell ハードウェア上で Security Tools をアップグレードしている場合は、インストール / アップグレードの失敗を防ぐため、**Security Tools をインストールする前に**、インストールされている Microsoft .Net のバージョンを確認し、バージョンをアップデートするようにしてください。インストールされている Microsoft .Net のバージョンを検証するには、インストール対象のコンピュータで [http://msdn.microsoft.com/en-us/library/hh925568\(v=vs.110\).aspx](http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx) に記載されている手順を実行します。Microsoft .Net Framework 4.5.2 をインストールするには、<https://www.microsoft.com/en-us/download/details.aspx?id=42643> に進みます。

- ControlVault、指紋リーダー、およびスマートカード（下記参照）のドライバとファームウェアは、ESSE マスターインストーラや子インストーラの実行可能ファイルには含まれていません。ドライバとファームウェアは最新の状態にしておく必要があります。これらは、<http://www.dell.com/support> から、お使いのコンピュータモデルを選択してダウンロードできます。認証ハードウェアに基づいて、適切なドライバとファームウェアをダウンロードします。
 - ControlVault
 - NEXT Biometrics Fingerprint ドライバ
 - Validity Fingerprint Reader 495 ドライバ
 - O2Micro スマートカードドライバ

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

すべてのクライアント - ハードウェア

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



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

すべてのクライアント - 言語サポート

- Encryption、Advanced Threat Prevention、および BitLocker Manager クライアント、複数言語ユーザーインターフェイス (MUI) に対応しており、次の言語をサポートします。リモート管理コンソールに表示されている Advanced Threat Prevention データは英語のみです。

言語サポート

- EN - 英語
 - ES - スペイン語
 - FR - フランス語
 - IT - イタリア語
 - DE - ドイツ語
 - JA - 日本語
 - KO - 韓国語
 - PT-BR - ポルトガル語 (ブラジル)
 - PT-PT - ポルトガル語 (ポルトガル (イベリア))
- SED および Advanced Authentication のクライアントは、複数言語ユーザーインターフェイス (MUI) に対応しており、次の言語をサポートしています。ロシア語、繁体字中国語、または簡体字中国語では、UEFI モードおよび起動前認証はサポートされていません。

言語サポート

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

Encryption クライアント

- クライアントコンピュータは、アクティブ化するためにネットワーク接続が必要です。
- 最初の暗号化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。
- 最初の暗号化スリープ中にスリープモードをオフにして、誰も操作していないコンピュータがスリープ状態になるのを防ぎます。スリープ状態のコンピュータでは暗号化は行われません (復号化も行われません)。
- Encryption クライアントは、デュアルブート設定をサポートしていません。これは、もう一方のオペレーティングシステムのシステムファイルが暗号化され、その動作を妨げるおそれがあるためです。
- Encryption クライアントは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 または類似した暗号化クライアントのソリューションを使用してではなく、企業と同じイメージの一部として、暗号化クライアントを展開することを可能にします。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、<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。

リストにないアンチウイルスプロバイダが組織で使用されている場合は、<http://www.dell.com/support/Article/us/en/19/SLN298707> を参照するか、Contact Dell ProSupport にお問い合わせください。

- 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

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

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

- 次の表は、対応オペレーティングシステムの詳しい説明です。

Windows オペレーティングシステム (32 ビットと 64 ビット)

- Windows 7 SP0-SP1 : Enterprise、Professional、Ultimate
- アプリケーション互換テンプレートでの Windows Embedded Standard 7 (ハードウェア暗号化はサポートされていません)
- Windows 8 : Enterprise、Pro
- Windows 8.1 Update 0-1 : Enterprise Edition、Pro Edition
- Windows Embedded 8.1 Industry Enterprise (ハードウェア暗号化はサポートされていません)
- Windows 10 : Education、Enterprise、Pro
- VMWare Workstation 5.5 以降

① メモ:

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



外付けメディアシールド (EMS) のオペレーティングシステム

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

① メモ:

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

① メモ:

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

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

- Windows 7 SP0-SP1 : Enterprise、Professional、Ultimate、Home Premium
- Windows 8 : Enterprise、Pro、Consumer
- Windows 8.1 Update 0-1 : Enterprise Edition、Pro Edition
- Windows 10 : Education、Enterprise、Pro

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

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

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 Enterprise Edition 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
 - リムーバブルストレージ暗号化
 - ポート制御

① メモ:

サーバーはポート制御をサポートする必要があります。

サーバーポート制御システムポリシーは、例えば、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、保護対象サーバー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、McAfee VirusScan、Symantec クライアント、Kaspersky Anti-Virus、および MalwareBytes Anti-Malware との適合性が検証済みです。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。

- Dell Data Protection サーバー、または Dell Data Protection サーバー用のデータベースを実行しているサーバー
- Server Encryption は Endpoint Security Suite、Personal Edition または Security Tools とは互換性がありません。
- Server Encryption は、SED Management および BitLocker Manager クライアント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。External Media Edition から Server Encryption へのアップグレードでは、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ー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 OS 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アップグレードは、Server Encryption ではサポートされていません。お使いのオペレーティングシステムをアップグレードするには、Server Encryption をアンインストールして復号化し、新しいオペレーティングシステムにアップグレードし、Server Encryption を再インストールします。

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の再インストールが必要な場合は、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 クライアントの前提条件

- Server 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)

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 SP0 ~ SP1 : Home、Enterprise、Professional、Ultimate
- Windows 8.0 : Enterprise、Pro
- Windows 8.1 ~ Windows 8.1 Update 1 : Enterprise Edition、Pro Edition
- Windows 10 : Education Edition、Enterprise Edition、Pro Edition

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 SP2 : Standard Edition、Datacenter Edition (Hyper-V 有りおよび無し)、Enterprise Edition (Hyper-V 有りおよび無し)、Foundation Server Edition
- Windows Server 2008 R2 SP1 : Standard Edition、Datacenter Edition (Hyper-V 有りおよび無し)、Enterprise Edition (Hyper-V 有りおよび無し)、Foundation Edition、Webserver Edition
- Windows Server 2012 : Standard Edition、Essentials Edition、Foundation Edition、Datacenter Edition
- Windows Server 2012 R2 : Standard Edition、Essentials Edition、Foundation Edition、Datacenter Edition
- Windows Server 2016 : Standard Edition、Essentials 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 8 : Enterprise、Pro
- Windows 8.1 ~ Windows 8.1 Update 1 : Enterprise Edition、Pro Edition
- Windows 10 : Education Edition、Enterprise Edition、Pro Edition

① 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。

外付けメディアシールド (EMS) のオペレーティングシステム

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

① メモ:

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

① メモ:

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

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

- Windows 7 SP0-SP1 : Enterprise、Professional、Ultimate、Home Premium
- Windows 8 : Enterprise、Pro、Consumer
- Windows 8.1 Update 0-1 : Enterprise Edition、Pro Edition
- Windows 10 : Education、Enterprise、Pro

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 SP1 以降
- Windows Server 2012 R2

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

- OS X Mavericks 10.9.5
- OS X Yosemite 10.10.5
- OS X El Capitan 10.11.4 および 10.11.5

Advanced Threat Prevention クライアント

- Advanced Threat Prevention クライアントは、コンピュータで Dell Client Security Framework (EMAgent) クライアントが検出されない状態でインストールすることはできません。インストールしようとしても失敗します。
- クライアントを管理している Dell Enterprise Server/VE を 接続モード (デフォルト) で実行しているときに Advanced Threat Prevention のインストールを完了するには、コンピュータのネットワーク接続が必要です。ただし、管理用のデルサーバを 切断モード で実行している場合は、Advanced Threat Prevention をインストールするためのネットワーク接続は **必要ありません**。
- Advanced Threat Prevention 用のテナントをプロビジョニングするには、デルサーバがインターネットに接続されている必要があります。

① | メモ: デルサーバを切断モードで実行しているときは、インターネット接続は必要ありません。

- 切断モードで実行している Dell Enterprise Server/VE によって管理されるクライアントコンピュータでは、オプションの Client Firewall および Web Protection の機能をインストール **しない** ください。
- 他のベンダーのウイルス対策、マルウェア対策およびスパイウェア対策のアプリケーションは、Advanced Threat Prevention クライアントと競合する可能性があります。可能な場合は、これらのアプリケーションをアンインストールしてください。拮抗するソフトウェアに、Windows Defender は含まれません。ファイアウォールアプリケーションは許可されます。

他のウイルス対策、マルウェア対策およびスパイウェア対策のアプリケーションをアンインストールできない場合は、デルサーバの Advanced Threat Protection と該当する他のアプリケーションに除外を追加する必要があります。デルサーバの Advanced Threat Protection に除外を追加する手順については、「<http://www.dell.com/support/article/us/en/04/SLN300970>」を参照してください。他のウイルス対策アプリケーションに追加する除外のリストについては、「<http://www.dell.com/support/article/us/en/19/SLN301134>」を参照してください。

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

- 次の表では、対応オペレーティングシステムが詳しく説明されています。

Windows オペレーティングシステム (32 ビットと 64 ビット)

- Windows 7 SP0-SP1 : Enterprise、Professional、Ultimate
- Windows 8 : Enterprise、Pro
- Windows 8.1 Update 0-1 : Enterprise Edition、Pro Edition



Windows 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
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Advanced Threat Prevention のポート

- Advanced Threat Prevention エージェントは、管理コンソール SaaS プラットフォームによって管理され、管理コンソール SaaS プラットフォームにレポートされます。ポート 443 (https) は通信用に使用され、エージェントがコンソールと通信するために、ファイアウォールで開く必要があります。このコンソールは、Amazon Web サービスによってホストされ、固定 IP がありません。ポート 443 が何らかの理由でブロックされている場合、アンチウイルス署名アップデート (DAT ファイル) をダウンロードできないので、コンピュータに最新の保護が装備されないことがあります。次に示すとおり、クライアントコンピュータが URL にアクセスできることを確認してください。

使用	アプリケーションプロトコル	トランスポートプロトコル	ポート番号	宛先	方向
すべての通信	HTTPS	TCP	443	すべての https トラフィックを *.cylance.com に許可	アウトバウンド

BIOS イメージの整合性検証

BIOS 保証の有効化 ポリシーがリモート管理コンソールで選択されている場合は、Cylance のテナントが BIOS がデル工場出荷時のバージョンから変更されていないか (攻撃ベクターの 1 つ) を確認するために、エンドユーザーシステム上で BIOS ハッシュを検証します。脅威が検出された場合は、通知が DDP をサーバに渡され、IT 管理者はリモート管理コンソールでアラートを受けます。プロセスの概要については、「[BIOS イメージの整合性検証プロセス](#)」を参照してください。

① **メモ:** カスタマイズされた工場出荷時イメージは、BIOS が変更されているため、この機能では使用できません。

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

- Latitude 3470
- Latitude 3570
- Latitude 7275
- Latitude 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7270
- Latitude E7470
- Latitude Rugged 5414
- Latitude Rugged 7214 Extreme
- Latitude Rugged 7414
- OptiPlex 3040
- OptiPlex 3240
- OptiPlex 5040
- OptiPlex 7040
- OptiPlex 7440
- Precision Mobile Workstation 3510
- Precision Mobile Workstation 5510
- VMware Workstation 3620
- VMware Workstation 7510
- VMware Workstation 7710
- Precision Workstation T3420
- Venue 10 Pro 5056
- Venue Pro 5855
- Venue XPS 12 9250
- XPS 13 9350
- XPS 9550

SED クライアント

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

または

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

❗ 重要:

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

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

OPAL ドライバ

- サポートされている OPAL 準拠の SED には、<http://www.dell.com/support> にあるアップデートされた Intel Rapid Storage Technology ドライバが必要です。

SED クライアントの前提条件

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

前提条件

- Visual C++ 2010 SP1 以降再頒布可能パッケージ (x86 および x64)
- Visual C++ 2012 更新プログラム 4 以降再頒布可能パッケージ (x86 および x64)

SED クライアントハードウェア

OPAL 対応の SED

- SED 管理 でサポートされている Opal 準拠 SED の最新のリストについては、KB 記事「<http://www.dell.com/support/article/us/en/19/SLN296720>」を参照してください。



UEFI によりサポートされている Dell コンピュータモデル

- 次の表は、UEFI でサポートされている Dell コンピュータモデルの詳細を説明しています。

Dell コンピュータモデル - UEFI サポート

- | | | | |
|---------------------------------------|-------------------|--|--------------------------------|
| • Latitude 5280 | • Precision M3510 | • Optiplex 3040 ミニタワー、ミニタワー、スモールフォームファクター | • Venue Pro 11 (モデル 5175/5179) |
| • Latitude 5480 | • Precision M4800 | • Optiplex 3046 | • Venue Pro 11 (モデル 7139) |
| • Latitude 5580 | • Precision M5510 | • Optiplex 3050 All-In-One | |
| • Latitude 7370 | • Precision M5520 | • OptiPlex 3050 タワー、スモールフォームファクタ、マイクロ | |
| • Latitude E5270 | • Precision M6800 | • Optiplex 5040 ミニタワー、スモールフォームファクター | |
| • Latitude E5470 | • Precision M7510 | • OptiPlex 5050 タワー、スモールフォームファクタ、マイクロ | |
| • Latitude E5570 | • Precision M7520 | • OptiPlex 7020 | |
| • Latitude E7240 | • Precision M7710 | • Optiplex 7040 Micro、Mini Tower、Small Form Factor | |
| • Latitude E7250 | • Precision M7720 | • OptiPlex 7050 タワー、スモールフォームファクタ、マイクロ | |
| • Latitude E7260 | • Precision T3420 | • Optiplex 3240 All-In-One | |
| • Latitude E7265 | • Precision T3620 | • OptiPlex 5250 All-In-One | |
| • Latitude E7270 | • Precision T7810 | • Optiplex 7440 All-In-One | |
| • Latitude E7275 | | • OptiPlex 7450 All-In-One | |
| • Latitude E7280 | | • OptiPlex 9020 Micro | |
| • Latitude E7350 | | | |
| • Latitude E7440 | | | |
| • Latitude E7450 | | | |
| • Latitude E7460 | | | |
| • Latitude E7470 | | | |
| • Latitude E7480 | | | |
| • Latitude 12 Rugged Extreme | | | |
| • Latitude 12 Rugged タブレット (モデル 7202) | | | |
| • Latitude 14 Rugged Extreme | | | |
| • Latitude 14 Rugged | | | |

① メモ:

認証機能は、適格な [Opal Compliant SED](#) を搭載した、Windows 8、Windows 8.1、および Windows 10 を実行するコンピュータにおいて、UEFI モードでサポートされます。レガシーブートモードは Windows 7、Windows 8、Windows 8.1、および Windows 10 を実行しているその他のコンピュータでサポートされています。

国際キーボード

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

国際キーボードのサポート - UEFI

- DE-CH - ドイツ語 (スイス)
- DE-FR - フランス語 (スイス)

国際キーボードのサポート - UEFI 非対応

- AR - アラビア語 (ラテン文字を使用)
- DE-CH - ドイツ語 (スイス)
- DE-FR - フランス語 (スイス)

SED クライアントのオペレーティングシステム

- 次の表は、対応オペレーティングシステムの詳しい説明です。

Windows オペレーティングシステム (32 ビットと 64 ビット)

- Windows 7 SP0-SP1: Enterprise、Professional (レガシー起動モードではサポートされていますが、UEFI ではサポートされていません)

① メモ:

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

- Windows 8 : Enterprise、Pro
- Windows 8.1 : Enterprise Edition、Pro Edition
- Windows 10 : Education、Enterprise、Pro

Advanced Authentication クライアント

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

ユーザー資格情報の管理に引き続き Microsoft オペレーティングシステムを使用するには、Security Tools Authentication をインストールしないでください。インストールした場合はアンインストールしてください。

- ワンタイムパスワード (OTP) 機能には、TPM が存在し、有効化され、所有されている必要があります。OTP は TPM 2.0 でサポートされていません。TPM の所有権をクリアし、設定するには、<https://technet.microsoft.com> を参照してください。
- SED は、高度な認証または暗号化を提供するために TPM を必要としません。

Advanced Authentication クライアントハードウェア

- 次の表に、サポートされる認証ハードウェアについて詳しく示します。

指紋およびスマートカードリーダー

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

非接触型カード

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

スマートカード

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

① メモ:

ActivIdentity クライアントは事前にロードされていないため、別途インストールする必要があります。

- CSP カード



スマートカード

- 共通アクセスカード (CAC)
 - クラス B/SIPR ネットカード
- 次の表は、SIPR ネットカードでサポートされている Dell コンピュータモデルの詳細を説明しています。

Dell コンピュータモデル - クラス B/SIPR Net カードサポート

- | | | |
|------------------|-------------------|------------------------------|
| • Latitude E6440 | • Precision M2800 | • Latitude 14 Rugged Extreme |
| • Latitude E6540 | • Precision M4800 | • Latitude 12 Rugged Extreme |
| | • Precision M6800 | • Latitude 14 Rugged |

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

Windows オペレーティングシステム

- 次の表では、対応オペレーティングシステムが詳しく説明されています。

Windows オペレーティングシステム (32 ビットと 64 ビット)

- Windows 7 SP0-SP1: Enterprise、Professional、Ultimate
- Windows 8: Enterprise、Pro
- Windows 8.1 Update 0-1: Enterprise Edition、Pro Edition
- Windows 10: Education、Enterprise、Pro

① | **メモ:** Windows 7 では UEFI モードはサポートされていません。

モバイルデバイスオペレーティングシステム

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

Android オペレーティングシステム

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

iOS オペレーティングシステム

- iOS 7.x
- iOS 8.x

Windows Phone オペレーティングシステム

- Windows Phone 8.1
- Windows 10 Mobile

BitLocker Manager クライアント

- BitLocker がまだお使いの環境に導入されていない場合は、「[Microsoft BitLocker の要件](#)」を確認してください。
- PBA パーティションがすでに設定されていることを確認します。PBA パーティションを設定する前に BitLocker Manager がインストールされている場合は、BitLocker を有効にできないため、BitLocker Manager は動作しません。「[BitLocker PBA パーティションを設定するプレインストール構成](#)」を参照してください。

- キーボード、マウス、およびビデオコンポーネントは、コンピュータに直接接続する必要があります。周辺機器の管理に KVM スイッチは使用しないでください。KVM スイッチは、ハードウェアを正しく識別するコンピュータの機能を阻害するおそれがあるためです。
- TPM をオンにして有効にします。BitLocker Manager は TPM の所有権を取得しますが、再起動の必要はありません。ただし、TPM の所有権がすでに存在する場合は、暗号化セットアップ処理が開始されます。再起動する必要はありません。ここでのポイントは、TPM が「所有」され有効化される必要があるという点です。
- 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 クライアントは、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カスタマーに勧めていることから、当社でもこのモードを 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、Server Encryption またはサーバ OS 上の Advanced Threat Prevention ではサポートされません。

BitLocker Manager クライアントの前提条件

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

前提条件

- Visual C++ 2010 SP1 以降再頒布可能パッケージ (x86 および x64)
- Visual C++ 2012 更新プログラム 4 以降再頒布可能パッケージ (x86 および x64)

BitLocker Manager クライアントのオペレーティングシステム

- 次の表では、対応オペレーティングシステムが詳しく説明されています。

Windows オペレーティングシステム

- Windows 7 SP0-SP1: Enterprise、Ultimate (32 ビットと 64 ビット)
- Windows 8: Enterprise (64 ビット)
- Windows 8.1: Enterprise Edition、Pro Edition (64 ビット)
- Windows 10: Education、Enterprise 、 Pro
- Windows Server 2008 R2: Standard Edition 、 Enterprise Edition (64 ビット)
- Windows Server 2012
- Windows Server 2012 R2: Standard Edition、Enterprise Edition (64 ビット)
- Windows Server 2016

認証オプション

- 次の認証オプションには特定のハードウェアが必要です：**指紋、スマートカード、コンタクトレスカード、クラス B/SIPR ネットカード、および UEFI コンピュータでの認証**。次のオプションには次の設定が必要です：**Windows 認証を使用するスマートカード、起動前認証を使用するスマートカード、および ワンタイムパスワード**。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。



暗号化クライアント

非 UEFI

	PBA				Windows 認証					
	パスワード	指紋	接触型スマートカード	OTP	SIPR カード	パスワード	指紋	スマートカード	OTP	SIPR カード
Windows 7 SP0-SP1					X	X ²	X ²	X ¹		X ²
Windows 8					X	X ²	X ²	X ¹		X ²
Windows 8.1 更新プログラム 0 ~ 1					X	X ²	X ²	X ¹		X ²
Windows 10					X	X ²	X ²	X ¹		X ²

1. マスターインストーラでインストールする場合、または子インストーラを使用するときには Advanced Authentication パッケージでインストールする場合に使用可能。

2. 認証ドライバを support.dell.com からダウンロードしたときに使用可能。

UEFI

	PBA - サポートされる Dell コンピュータにあります。				Windows 認証					
	パスワード	指紋	接触型スマートカード	OTP	SIPR カード	パスワード	指紋	スマートカード	OTP	SIPR カード
Windows 7 SP0-SP1										
Windows 8					X	X ²	X ²	X ¹		X ²
Windows 8.1 更新プログラム 0 ~ 1					X	X ²	X ²	X ¹		X ²
Windows 10					X	X ²	X ²	X ¹		X ²

1. マスターインストーラでインストールする場合、または子インストーラを使用するときには Advanced Authentication パッケージでインストールする場合に使用可能。

2. 認証ドライバを support.dell.com からダウンロードしたときに使用可能。



SED クライアント

非 UEFI

	PBA				Windows 認証					
	パスワード	指紋	接触型スマートカード	OTP	SIPR カード	パスワード	指紋	スマートカード	OTP	SIPR カード
Windows 7 SP0-SP1	X ²		X ^{2,3}			X	X ³	X ³	X ¹	X ³
Windows 8	X ²		X ^{2,3}			X	X ³	X ³	X ¹	X ³
Windows 8.1	X ²		X ^{2,3}			X	X ³	X ³	X ¹	X ³
Windows 10	X ²		X ^{2,3}			X	X ³	X ³	X ¹	X ³

1. マスターインストーラでインストールする場合、または子インストーラを使用するときには Advanced Authentication パッケージでインストールする場合に使用可能。
2. 認証ドライバを support.dell.com からダウンロードしたときに使用可能。
3. サポートされる OPAL SED で使用可能。

UEFI

	PBA - サポートされる Dell コンピュータにあります。				Windows 認証					
	パスワード	指紋	接触型スマートカード	OTP	SIPR カード	パスワード	指紋	スマートカード	OTP	SIPR カード
Windows 7										
Windows 8	X ⁴					X	X ²	X ²	X ¹	X ²
Windows 8.1	X ⁴					X	X ²	X ²	X ¹	X ²
Windows 10	X ⁴					X	X ²	X ²	X ¹	X ²

1. マスターインストーラでインストールする場合、または子インストーラを使用するときには Advanced Authentication パッケージでインストールする場合に使用可能。
2. 認証ドライバを support.dell.com からダウンロードしたときに使用可能。
4. サポート対象 UEFI コンピュータ上のサポート対象 OPAL SED で使用可能。



BitLocker Manager

非 UEFI

	PBA ⁵					Windows 認証				
	パスワード	指紋	接触型スマートカード	OTP	SIPR カード	パスワード	指紋	スマートカード	OTP	SIPR カード
Windows 7						X	X ²	X ²	X ¹	X ²
Windows 8						X	X ²	X ²	X ¹	X ²
Windows 8.1						X	X ²	X ²	X ¹	X ²
Windows 10						X	X ²	X ²	X ¹	X ²
Windows Server 2008 R2 (64 ビット)						X		X ²		

1. マスターインストーラでインストールする場合、または子インストーラを使用するときには Advanced Authentication パッケージでインストールする場合に使用可能。

2. 認証ドライバを support.dell.com からダウンロードしたときに使用可能。

5. BitLocker Preboot PIN は、Microsoft 機能によって管理されます。

UEFI

	PBA ⁵ - サポートされる Dell コンピュータにあります。					Windows 認証				
	パスワード	指紋	接触型スマートカード	OTP	SIPR カード	パスワード	指紋	スマートカード	OTP	SIPR カード
Windows 7										
Windows 8						X	X ²	X ²	X ¹	X ²
Windows 8.1						X	X ²	X ²	X ¹	X ²
Windows 10						X	X ²	X ²	X ¹	X ²
Windows Server 2008 R2 (64 ビット)						X		X ²		

1. マスターインストーラでインストールする場合、または子インストーラを使用するときには Advanced Authentication パッケージでインストールする場合に使用可能。

2. 認証ドライバを support.dell.com からダウンロードしたときに使用可能。

5. BitLocker Preboot PIN は、Microsoft 機能によって管理されます。



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。

Encryption クライアントのレジストリ設定

- Dell Server for Enterprise Edition for Windows で自己署名証明書が使用されている場合、クライアントコンピュータで証明書信頼検証を無効のままにしておく必要があります (Enterprise Edition for Windows では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 EE Server/VE 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。
- EE for Windows で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\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

- Windows 認証にスマートカードを使用するには、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。

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

"MSSmartcardSupport"=dword:1

- 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

- インストール中にデフォルトで、システムトレイ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、システムトレイアイコンを非表示にします。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]



"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weep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 クライアントは、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

0 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）。

$(\text{ポリシー更新遅延の許容回数} \times \text{各ポリシーアップデート遅延の長さ}) + (5 \text{ 分} \times [\text{ポリシーアップデート遅延の許容回数} - 1])$

- 次のレジストリ設定を使用して、強制的なポリシー更新のために Encryption クライアントに EE Server/VE Server へのポーリングを行わせませす。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\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。

- 次のレジストリ設定を使用して、最適化されたインベントリを EE Server/VE Server に送信するか、完全なインベントリを EE Server/VE Server に送信するか、アクティブ化されたすべてのユーザーの完全なインベントリを EE Server/VE Server に送信するかのいずれかを、Encryption クライアントに許可します。

- 最適化されたインベントリを EE Server/VE Server に送信する場合：

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\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"OnlySendInvChanges"=REG_DWORD:1

エントリが存在しない場合、最適化されたインベントリが EE Server/VE Server に送信されます。

- 完全なインベントリを EE Server/VE Server に送信する場合：

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\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield]

"OnlySendInvChanges"=REG_DWORD:0

エントリが存在しない場合、最適化されたインベントリが EE Server/VE Server に送信されます。

- 完全なインベントリをアクティブ化されたすべての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。値は資格情報コンテナに保存されるので、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 クライアントは、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 EE Server/VE Server のロードを容易にするために、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。

重要:

スロットアクティブ化の設定は、Dell ProSupport のサポートがないと行えません。時間スロット設定が不適切な場合、多数のクライアントが同時に EE Server/VE Server に対してアクティブ化を試みるという結果を招き、深刻なパフォーマンスの問題が発生する可能性があります。

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。

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

スロットアクティブ化の有効化または無効化

無効 = 0 (デフォルト)

有効 = 1

- [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秒単位の期間。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。

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

すべてのアクティベーション時間スロットが行われた場合の繰り返し内の間隔 (ACTIVATION_SLOT_CALREPEAT)。1 度の間隔だけが許可されます。この設定は 0,<CalRepeat> とする必要があります。0 からのオフセットは予想外の結果を生み出すことがあります。デフォルトの設定は 0,86400 です。7 時間の繰り返しを設定するには、0,25200 を使用します。CALREPEAT は、ユーザーがログインするとアクティブ化されます。

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

そのアクティブ化がスロット化されているユーザーが次回ログインするときに、コンピュータがアクティブ化しようとする前に失われる可能性のあるアクティブ化スロットの数。この即時の試行中にアクティブ化が失敗した場合、クライアントは、スロットアクティブ化試行を再開します。ネットワークの障害のためにアクティブ化が失敗した場合、MISS_THRESHOLD の値を超過していても、ネットワークの再接続時にアクティブ化が試行されます。アクティブ化スロット時間に達する前にユーザーがログアウトした場合、次のログイン時に新しいスロットが割り当てられます。

- [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次の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

- 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次の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=Disabled (default)

1=Enabled

- System Data Encryption (SDE) は、SDE 暗号化ルールポリシー値に基づいて実施されます。SDE 暗号化有効 ポリシーが選択されていると、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。暗号化クライアントがアクティブな SDE ポリシーを含むポリシーアップデートを処理しているとき、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 で暗号化されていないユーザーディレクトリにコピーされた (移動されたものではありません) 暗号化ファイルまたはフォルダにも使用されます。

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。

SDUser の詳細については、www.dell.com/support/article/us/en/19/SLN304916 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=Disabled (default)

1=Enabled

- 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。

Advanced Threat Prevention クライアントのレジストリ設定

- Advanced Threat Prevention プラグインが、LogVerbosity 値への変更がないか HKLM\SOFTWARE\Dell\Dell Data Protection を監視し、変更に応じてクライアントログのレベルを更新するには、次の値を設定します。

[HKLM\SOFTWARE\Dell\Dell Data Protection]

"LogVerbosity"=dword:<以下を参照>

Dump: 0

Fatal: 1

Error 3

Warning 5

Info 10

Verbose 12

Trace 14

Debug 15

レジストリ値は、ATP サービスが開始するとき、または値が変化するたびにチェックされます。レジストリ値がない場合は、ログのレベルの変化はありません。

このレジストリ設定は、Encryption クライアントおよび Client Security Framework を含むその他のコンポーネントのログ冗長性を制御するため、テストまたはデバッグ用途にのみ使用してください。

- 互換性モードは、メモリ保護ポリシーまたはメモリー保護ポリシーとスクリプト制御ポリシーの両方が有効になっている際に、クライアントコンピュータでアプリケーションを実行することを可能にします。互換性モードを有効にするには、クライアントコンピュータ上でレジストリ値を追加する必要があります。

互換性モードを有効にするには、次の手順に従います。

- リモート管理コンソールで、メモリ保護の有効化ポリシーを無効にします。スクリプト制御ポリシーが有効になっている場合は、無効にします。
- CompatibilityMode レジストリ値を追加します。
 - クライアントコンピュータのレジストリエディタを使用して、HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop に移動します。
 - デスクトップ**を右クリックして、**許可**をクリックし、所有権を得て自分自身にフルコントロールを付与します。
 - デスクトップ**を右クリックし、**新規 > バイナリ値**の順に選択します。
 - 名前には、CompatibilityMode と入力します。
 - レジストリの設定を開いて、値を 01 に変更します。
 - OK**をクリックして、レジストリエディタを閉じます。

コマンドでレジストリ値を追加するには、次のコマンドラインオプションのいずれかを使用して、クライアントコンピュータ上で実行することができます。

- (1台のコンピュータの場合) Psexec:

```
psexec -s reg add HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop /v CompatibilityMode /t REG_BINARY /d 01
```

- (複数のコンピュータの場合) Invoke-Command cmdlet:

```
$servers = "testComp1","testComp2","textComp3"
```



```
$credential = Get-Credential -Credential {UserName}\administrator
```

```
Invoke-Command -ComputerName $servers -Credential $credential -ScriptBlock {New-Item -  
Path HKCU:\Software\Cylance\Desktop -Name CompatibilityMode -Type REG_BINARY -Value 01}
```

- c リモート管理コンソールで、メモリ保護の有効化ポリシーを再び有効にします。スクリプト制御ポリシーが前に有効になっていた場合は、再び有効にします。

SED クライアントのレジストリ設定

- SED クライアントとの通信に EE Server/VE Server を使用できない場合の再試行間隔を設定するには、次のレジストリ値を追加します。

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

```
"CommErrorSleepSecs"=dword:300
```

この値は、SED クライアントとの通信に EE Server/VE Server を使用できない場合に、SED クライアントが EE Server/VE Server 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 管理向けの EE Server/VE Server で使用されている場合、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（SED 管理では 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 EE Server/VE 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 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

- Windows 認証にスマートカードを使用するには、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。

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

```
"MSSmartcardSupport"=dword:1
```

- 起動前認証でスマートカードを使用するには、次のレジストリ値をクライアントコンピュータに設定します。また、リモート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。

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

```
"MSSmartcardSupport"=dword:1
```

- 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。

- SED クライアントとの通信に EE Server/VE Server を使用できないときに SED クライアントが EE Server/VE Server との接続を試みる間隔を設定するには、クライアントコンピュータで次の値を設定します。

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

```
"CommErrorSleepSecs"=DWORD Value:300
```



この値は、SED クライアントとの通信に EE Server/VE Server を使用できない場合に、SED クライアントが EE Server/VE Server 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場所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
```

- 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
```

Advanced Authentication クライアントのレジストリ設定

- スマートカードおよびバイOMETリックデバイスに関連付けられているサービスを Advanced Authentication クライアント (Security Tools) 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、Security Tools 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。
- WbioSrv - 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

- Windows 認証にスマートカードを使用するには、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。

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

```
"MSSmartcardSupport"=dword:1
```

- SED 起動前認証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
```

リモート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。



BitLocker Manager クライアントのレジストリ設定

- 自己署名証明書が BitLocker Manager 向けの EE Server/VE 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 EE Server/VE 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



ESSE マスターインストーラを使用したインストール

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

- [ESSE マスターインストーラを使用した対話型のインストール](#)

または [内部接続ポートを編集...](#) のいずれかをクリックします。

- [ESSE マスターインストーラを使用したコマンドラインによるインストール](#)

ESSE マスターインストーラを使用した対話型のインストール

- ESSE マスターインストーラは次の場所にあります。
 - **お使いの Dell FTP アカウントから** - インストールバンドルを DDP-Endpoint-Security-Suite-1.x.x.xxx.zip の中から見つけます。
- これらの手順に従い、ESSE マスターインストーラを使用して Dell Endpoint Security Suite Enterprise を対話形式でインストールします。この方法では、コンピュータごとに製品スイートをインストールします。
 - 1 Dell インストールメディアからを見つめます。それをローカルコンピュータにコピーします。
 - 2 インストーラを起動するには **DDPSuite.exe** をダブルクリックします。これには数分かかる場合があります。
 - 3 ようこそ ダイアログで **次へ** をクリックします。
 - 4 ライセンス契約を読み、その条件に同意して **次へ** をクリックします。
 - 5 **Enterprise Server 名** フィールドに、ターゲットユーザーを管理する EE Server/VE Server の完全修飾ホスト名 (server.organization.com など) を入力します。
Device Server URL フィールドに、クライアントが通信する Device Server (Security Server) の URL を入力します。
場合、フォーマットは https://server.organization.com:**8443**/xapi/(末尾のスラッシュを含む) です。
次へ をクリックします。
 - 6 **次へ** をクリックして、デフォルトの場所である C:\Program Files\Dell\Dell Data Protection\。にこの製品をインストールします。他の場所にインストールすると問題が発生する可能性があるため、**Dell recommends installing in the default location only.**



7 インストールするコンポーネントを選択します。

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

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

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

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

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

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

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

① メモ: Threat Protection および Advanced Threat Prevention は同じコンピュータに共存できません。インストーラによって、両方のコンポーネントの選択が自動的に禁止されます。Threat Protection をインストールする場合、手順については『Endpoint Security Suite 詳細インストールガイド』をダウンロードしてください。

選択が完了したら、次へをクリックします。

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

9 **はい、今すぐコンピュータを再起動します** を選択し、**終了** をクリックします。

インストールが完了しました。

ESSE マスターインストーラを使用したコマンドラインによるインストール

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

スイッチ

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

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

パラメータ

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



パラメータ	説明
SUPPRESSREBOOT	インストールの完了後に自動的に行われる再起動を阻止します。SILENT モードで使用できます。
SERVER	EE Server/VE Server の URL を指定します。
InstallPath	インストールのパスを指定します。SILENT モードで使用できます。
FEATURES	SILENT モードでインストールできるコンポーネントを指定します。 ATP = サーバ OS 上には Advanced Threat Prevention のみ 、ワークステーション OS 上には Advanced Threat Prevention および Encryption。 DE-ATP = サーバ OS 上に Advanced Threat Prevention および Encryption。サーバー OS 上のインストールに対して のみ 使用します。これは、FEATURES パラメータが指定されていない場合のサーバー OS 上のデフォルトのインストールです。 DE = Drive Encryption (Encryption クライアント) のみ 。サーバー OS 上のインストールに対して のみ 使用します。 BLM = BitLocker Manager SED = 自己暗号化ドライブ管理 (EMASgent/Manager、PBA/GPE ドライバ) (ワークステーション OS 上にインストールされる場合のみ使用可能) ATP-WEBFIREWALL = ワークステーション OS 上のクライアントファイアウォールおよびウェブプロテクション DE-ATP-WEBFIREWALL = サーバ OS 上にクライアントファイアウォールおよびウェブプロテクション
	① メモ: Enterprise Edition または v1.4 以前の Endpoint Security Suite Enterprise からのアップグレードの場合、クライアントファイアウォールおよびウェブプロテクションをインストールするために ATP-WEBFIREWALL または DE-ATP-WEBFIREWALL を指定する必要があります。クライアントをインストールする際に、切断モードで実行する Dell Enterprise Server/VE で管理されるようにする場合は、ATP-WEBFIREWALL および DE-ATP-WEBFIREWALL を指定しないでください。
BLM_ONLY=1	SED Management のプラグインを除外するために FEATURES=BLM をコマンドラインに使用する時には、これを使用する必要があります。

コマンドラインの例

- コマンドラインパラメータでは大文字と小文字を区別します。
- (ワークステーション OS 上) この例では、標準ポートで ESSE マスターインストーラを使用して C:\Program Files\Dell\Dell Data Protection\ のデフォルトの場所にすべてのコンポーネントをサイレントインストールし、それが指定した EE Server/VE Server を使用するように設定します。

```
"DDPSuite.exe" -y -gm2 /S /z\"SERVER=server.organization.com\""
```
- (ワークステーション OS 上) この例では、標準ポートで ESSE マスターインストーラ**のみ**を使用して C:\Program Files\Dell\Dell Data Protection\ のデフォルトの場所に Advanced Threat Prevention と Encryption をサイレントインストールし、それが指定した EE Server/VE Server を使用するように設定します。

```
"DDPSuite.exe" -y -gm2 /S /z\"SERVER=server.organization.com, FEATURES=ATP\""
```
- (ワークステーション OS 上) この例では、標準ポートで ESSE マスターインストーラを標準ポートで使用して、再起動なしで、C:\Program Files\Dell\Dell Data Protection\ のデフォルトの場所に Advanced Threat Prevention、Encryption、および SED 管理をサイレントインストールし、それが指定した EE Server/VE Server を使用するように設定します。

```
"DDPSuite.exe" -y -gm2 /S /z\"SERVER=server.organization.com, FEATURES=ATP-SED, SUPPRESSREBOOT=1\""
```
- (ワークステーション OS 上) この例では、標準ポートで ESSE マスターインストーラを使用して C:\Program Files\Dell\Dell Data Protection\ のデフォルトの場所に Advanced Threat Prevention、Encryption、ウェブプロテクション、およびクライアントファイアウォールをサイレントインストールし、それが指定した EE Server/VE Server を使用するように設定します。

```
"DDPSuite.exe" -y -gm2 /S /z\"SERVER=server.organization2.com, FEATURES=ATP-WEBFIREWALL\""
```



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

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

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

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

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

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

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

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



ESSE マスターインストーラを使用したアンインストール

- 各コンポーネントを個別にアンインストールした後で、ESSE マスターインストーラのアンインストールを行う必要があります。クライアントは、**アンインストールの失敗を防止するための特定の順序** でアンインストールする必要があります。
- 子インストーラを取得するには、「[ESSE マスターインストーラからの子インストーラの抽出](#)」に記載されている手順に従います。
- インストールと同じバージョンの ESSE マスターインストーラ（つまりクライアント）をアンインストールにも使用するようしてください。
- 本章では、子インストーラのアンインストール方法の詳細な手順が記された他の章を参照します。本章では、最後の手順である ESSE マスターインストーラのアンインストールのみを説明します。
- クライアントを以下の順序でアンインストールします。
 - [Encryption クライアントのアンインストール](#)。
 - [Advanced Threat Prevention のアンインストール](#)。
 - [SED および Advanced Authentication クライアントのアンインストール](#)（これは、Advanced Threat Prevention がアンインストールされるまでアンインストールできない Dell Client Security Framework をアンインストールします）。
 - [BitLocker Manager クライアントのアンインストール](#)

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。
- 「[ESSE マスターインストーラのアンインストール](#)」に進みます。

ESSE マスターインストーラのアンインストール

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

コマンドラインでのアンインストール

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

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

終了したらコンピュータを再起動します。



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するには、「ESSE マスターインストーラからの子インストーラの抽出」にあるように、まず始めに ESSE マスターインストーラから子実行可能ファイルを抽出する必要があります。
- 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。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\\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と同じ基本的な `.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` スイッチに渡す引数に指定します。

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に `/q` と `/qn` の両方を使用しないでください。「!」および「-」は「/qb」の後にものみ使用してください。

スイッチ	意味
<code>/v</code>	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。
<code>/s</code>	サイレントモード
<code>/x</code>	アンインストールモード
<code>/a</code>	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](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
<code>/q</code>	進行状況ダイアログなし、処理完了後に自動で再起動
<code>/qb</code>	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
<code>/qb-</code>	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
<code>/qb!</code>	キャンセル ボタンなしの進捗状況ダイアログ、再起動のプロンプト表示

オプション	意味
/qb!-	キャンセル ボタンなしの進捗状況ダイアログ、処理完了後に自動で再起動
/qn	ユーザーインターフェースなし
/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、次のドキュメントとヘルプファイルを参照するようにユーザーに指示します。
 - Encryption クライアントの各機能の使用方法については、『Dell Encrypt Help』(Dell Encrypt ヘルプ) を参照してください。このヘルプには、<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\Help からアクセスします。
 - External Media Shield の各機能の使用方法については、『EMS Help』(EMS ヘルプ) を参照してください。このヘルプには、<Install dir>\Program Files\Dell\Dell Data Protection\Encryption\EMS からアクセスします。
 - Advanced Authentication および Advanced Threat Prevention の機能の使用方法については、Endpoint Security Suite Enterprise ヘルプを参照してください。ヘルプには、<Install dir>\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Help からアクセスしてください。

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、ESSE マスターインストーラや子インストーラの実行可能ファイルに含まれません。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 クライアントのインストール

- 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、「Encryption クライアントの要件」を見直します。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、システムトレイで Dell Data Protection アイコンを右クリックし、**ポリシーアップデートのチェック** を選択して、ポリシーをアップデートする必要があります。
- Encryption クライアントインストーラは次の場所にあります。
 - お使いの Dell FTP アカウントから - DDP-Endpoint-Security-Suite-1.x.x.xxx.zip でインストールバンドルを見つけてから、**ESSE 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。

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 サーバの FQDN)

POLICYPROXYHOSTNAME=<RGKName> (デフォルトポリシープロキシの FQDN)



パラメータ

MANAGEDDOMAIN=<MyDomain> (デバイスに対して使用するドメイン)

DEVICESTRIVERURL=<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)

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 systray アイコンを有効化、1 は systray アイコンを無効化)

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。

- 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=30,300 (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=300 (SLOTINTERVAL で設定された上限以上である必要があります。暗号化クライアントが、SLOTINTERVAL に基づいてアクティブ化の試行を行うまでに待機する秒数)

コマンドラインの例

- 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 にインストールする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 DEVICESTRIVERURL=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" DEVICESTRIVERURL="https://server.organization.com:8443/xapi/"
```

- 次の例では、Encryption クライアントおよび Encrypt for Sharing、DDP システムトレイアイコンの非表示、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. にインストールという設定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 DEVICESTRIVERURL=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" DEVICESTRIVERURL="https://server.organization.com:8443/xapi/"  
HIDESYSTRAYICON="1" HIDEOVERLAYICONS="1"
```


① メモ:

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

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

Server Encryption クライアントのインストール

Server Encryption のインストールには、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。

- [Server Encryption の対話型インストール](#)

① メモ:

Server Encryption の対話型インストールは、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み行うことができます。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 Server Encryption のインストール](#)

仮想ユーザーアカウント

- インストールの一部として、Server Encryption を独占的に使用するための**仮想サーバーユーザーアカウント**が作成されます。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 認証は無効化されます。

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ローカルまたはドメインユーザーである必要があります。
- ドメイン管理者が Server Encryption をアクティブ化するという要件を無効にするには、あるいは Server Encryption を非ドメインまたはマルチドメインのサーバー上で実行するには、application.properties ファイル内で 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 DDP Server に基づいて、次のファイルパスに保存されています。

Dell Enterprise Server - <installation folder>/Security Server/conf/application.properties

Virtual Edition - /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。

サーバーポート制御システムポリシーは、例えば、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、保護対象サーバー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 を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) を使用可能な場合、Dell ハードウェア上の GPK を封印するために TPM が使用されます。TPM を使用できない場合、Server Encryption は、Microsoft のデータ保護 API (DPAPI) を使用して汎用キーを保護します。

① メモ:

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、「https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2」を参照してください。

子インストーラの抽出

- Server Encryption では、マスターインストーラ内にあるインストーラのうちの 1 つのみが必要です。Server Encryption をインストールするには、最初に Encryption クライアントの子インストーラ **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。



Server Encryption の対話型インストール

- 次の手順を使用して、Server Encryption を対話形式でインストールします。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 Server Encryption をサーバーにインストールする場合は、**DDPE_XXbit_setup.exe** ファイルをダブルクリックしてインストーラを起動します。

① メモ:

Windows Server 2012 R2 などの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に Server Encryption がインストールされる場合、インストーラはデフォルトでサーバーモードの暗号化をインストールします。

- 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 **次へ** をクリックして Server Encryption をデフォルトの場所にインストールします。

① メモ:

デルでは、デフォルトの場所へのインストールをお勧めしています。デフォルト以外の場所（別のディレクトリ内、D ドライブ上、USB ドライブ上など）にインストールすることは推奨されません。

- 6 **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。
- 7 Dell Enterprise Server の名前 フィールドに、対象ユーザーを管理する Dell Enterprise Server または Virtual Edition の完全修飾ホスト名（*server.organization.com* など）を入力します。
- 8 **管理対象ドメイン** フィールドにドメイン名を入力し（*organization* など）、**次へ** をクリックします。
- 9 **次へ** をクリックして、自動入力済みの **Dell Policy Proxy 情報** ダイアログをスキップします。
- 10 **次へ** をクリックして、自動入力済みの **Dell Device Server 情報** ダイアログをスキップします。
- 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 **設定完了** ダイアログで、**終了** をクリックします。
インストールが完了しました。

① メモ:

インストールのログファイルはアカウントの %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。インストーラのログファイルを見つけるには、名前が 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。そのファイルには、インストーラを実行したときの時間に一致する日時タイムスタンプがあります。

① メモ:

インストールの一部として、Server Encryption を独占的に使用するための**仮想サーバーユーザーアカウント**が作成されます。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 認証は無効化されます。

- 13 コンピュータを再起動します。

① 重要: 作業を保存し、開いているアプリケーションを閉じるための時間が必要な場合にのみ、再起動をスムーズするを選択します。

コマンドラインを使用した Server Encryption のインストール

Server Encryption クライアント - インストーラの場所 : C:\extracted\Encryption

- **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
/s	サイレントモード

パラメータ

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。

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	/!*v [fullpath][filename].log *	SERVERHOSTNAME=<管理サーバー名> SERVERMODE=1 POLICYPROXYHOSTNAME=<RGK 名> MANAGEDDOMAIN=<マイドメイン> DEVICESERVERURL=<Activation Server 名> GKPORT=<新規 GK ポート> MACHINEID=<マシン名> RECOVERYID=<リカバリ ID> REBOOT=ReallySuppress HIDEOVERLAYICONS=1 HIDESYSTRAYICON=1 EME=1

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。
- デフォルト以外の場所 (別のディレクトリ内、C: 以外のドライブ上、USB ドライブ上など) にインストールすることは推奨されません。デルでは、デフォルトの場所へのインストールをお勧めしています。
- 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。
- Dell Activation Server の URL (DEVICESERVERURL) 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、Server Encryption クライアント、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で Server Encryption クライアント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、Server Encryption クライアントをログファイルとデフォルトのパラメータでインストールし (Server Encryption クライアント、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 にインストール)、このコマンドラインが同じサーバー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。

```
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/ /1*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/" /1*v
DDP_ssos-090.log /norestart/qn"
```

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。例えば、`/1*v C:\Logs \DDP_ssos-090.log` では、C:\Logs フォルダにインストールログが作成されます。

コンピュータの再起動

インストール後、コンピュータを再起動します。コンピュータは、できるだけ早く再起動する必要があります。

① 重要:

作業を保存し、開いているアプリケーションを閉じるための時間が必要な場合にのみ、**再起動をスヌーズする**を選択します。


Server Encryption のアクティブ化

- サーバーが組織のネットワークに接続されている必要があります。
- サーバーのコンピュータ名が、リモート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ライブのインタラクティブユーザーが、少なくとも一度はサーバー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、そのサーバーにおいて、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。Server Encryption クライアントは、自動ではアクティブ化を行いません。
- 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**仮想サーバーユーザー**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、仮想サーバーユーザーはリモート管理コンソールに SERVER-USER@<完全修飾サーバー名> 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。

① メモ:

アクティベーション後にサーバーの名前を変更しても、リモート管理コンソールではそのサーバーの表示名は変更されません。ただし、サーバー名が変更された後、Server Encryption クライアントが再度アクティブ化を行うと、新しいサーバー名がリモート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、Server Encryption をアクティブ化するようにユーザーを促します。アクティベーションが完了していない場合は、次の手順に従ってください。

- 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 システムトレイにある Encryption アイコン  を右クリックし、**バージョン情報** をクリックします。
- 3 Encryption がサーバーモードで実行中であることを確認します。
- 4 メニューから **Encryption のアクティブ化** を選択します。
- 5 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。

DDP Server は、マシン ID 用の暗号化キーの発行、**仮想サーバー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ーユーザーアカウントの間に関係を確立します。

- 6 **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。

- 7 暗号化スウィープが完了した後、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。

① メモ:

Windows 資格情報のセキュア化 ポリシーが True に設定されている場合、Server Encryption は Windows 資格情報を含む `\Windows\system32\config` の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 **未選択** である場合であっても暗号化されます。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。



① メモ:

コンピュータの再起動後、共有キーマテリアルの認証には保護対象サーバーのマシンキーが常に必要となります。DDP Server は、資格情報コンテナ内の暗号化キーとポリシーにアクセスするためのロック解除キーを返します。(これらのキーおよびポリシーはサーバー用であり、ユーザー用ではありません)。サーバーのマシンキーなしでは、共有ファイル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、Server Encryption がインストール済みかつ認証済みであり、サーバーモードで動作していることを確認します。Shield ID が**赤色**で表示されている場合、暗号化はまだアクティブ化されていません。

仮想サーバーユーザー

- リモート管理コンソールでは、保護対象サーバーはそのマシン名下にあります。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。各アカウントは、固有の静的ユーザー名と固有のマシン名を持っています。
- 仮想サーバーユーザーアカウントは、Server 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ーの動作に対して透過的です。仮想サーバーユーザーは、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ーユーザーで自動的に認証し、Dell Data Protection サーバーからマシンキーをダウンロードします。

Advanced Threat Prevention クライアントのインストール

- Threat Prevention および Advanced Threat Prevention を**同じコンピュータに格納することはできません**。互換性の問題が発生するので、これらの両方のコンポーネントを同じコンピュータにインストールしないでください。Threat Protection をインストールする場合、手順については『Endpoint Security Suite Advanced Installation Guide』(Endpoint Security Suite 詳細インストールガイド) をダウンロードしてください。
- インストールは特定の順番で実行する必要があります。コンポーネントを適切な順番でインストールしないと、インストールに失敗します。インストーラを次の順番で実行してください。

1 (**ワークステーション OS 上のみ**) \Security Tools - Advanced Threat Prevention には、Dell Client Security Framework コンポーネントが必要です。

(**サーバー OS 上のみ**) Dell Client Security Framework コンポーネント (「**コマンドラインインストール**」を参照)。

2 (**ワークステーション OS 上のみ**) 「\Security Tools\Authentication」- ワークステーション OS 上には、Security Tools と Authentication が一緒にインストールされる必要があります。Authentication は、サーバー OS 上では使用できず、インストールする必要はありません。

3 「**コマンドラインインストール**」に示される Advanced Threat Prevention クライアントです。

- Advanced Threat Prevention クライアントインストーラは、次の場所にあります。

- **お使いの Dell FTP アカウントから** - DDP-Endpoint-Security-Suite-1.x.x.xxx.zip でインストールバンドルを見つけてから、**ESSE 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\Advanced Threat Protection でファイルを見つけます。

- SED および Advanced Authentication クライアントインストーラは次の場所にあります。

- **お使いの Dell FTP アカウントから** - DDP-Endpoint-Security-Suite-1.x.x.xxx.zip でインストールバンドルを見つけてから、**ESSE 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\Security Tools および C:\extracted\Security Tools\Authentication でファイルを見つけます。

① **メモ:** SED および Advanced Authentication クライアントは、ワークステーション OS 上のみインストールすることができ、サーバー OS 上にはインストールできません。

コマンドラインでのインストール

- 基本的な .msi コマンドをインストールに使用することができます。

- 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

ARPSYSTEMCOMPONENT=1 <no entry in the Control Panel Programs list>

REBOOT=ReallySuppress <suppresses the reboot>

FEATURE=BASIC <サーバー OS では**必須** ; オプションでワークステーション OS での使用も可 ; SED Management クライアントと BitLocker Manager インストールを禁止 >

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

- 次の例では、基本的な Dell Client Security Framework コンポーネントを SED Management クライアントも BitLocker Manager もなしでインストールします (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 にインストール)。

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

- 次の例では、サイレントインストール、再起動なし、指定した場所にインストールログファイルとインストールフォルダという設定で Advanced Threat Prevention をインストールします。

```
MSIEXEC.EXE /I "AdvancedThreatProtectionCSFPlugins_x64.msi" /qn REBOOT="ReallySuppress"  
APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Plugins"  
ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer Logs  
\AdvancedThreatProtectionPlugins.msi.log"
```

および

```
AdvancedThreatProtectionAgentSetup.exe /s /norestart REBOOT=ReallySuppress APPFOLDER="C:  
\Program Files\Dell\Dell Data Protection\Advanced Threat Protection" ARPSYSTEMCOMPONENT=1 /l  
"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\AdvancedThreatProtection.log"
```

- ① **メモ:** これらのコンポーネントは、コマンドラインのみを使用してインストールする必要があります。このコンポーネントをインストールするためにダブルクリックすると、製品の非 Dell、非管理下バージョンをインストールしますが、これはサポートされていません。誤ってインストールを行ってしまった場合は、プログラムの追加および削除 に移動してそのバージョンをアンインストールします。

ウェブプロテクションおよびファイアウォールのインストール

- Advanced Threat Prevention および Threat Protection は、**同じコンピュータに共存できません**。互換性の問題が発生するので、これらの両方のコンポーネントを同じコンピュータにインストールしないでください。ただし、Advanced Threat Prevention は、ウェブプロテクションおよびファイアウォールコンポーネントとともにインストールできます。
- インストールは特定の順番で実行する必要があります。コンポーネントを適切な順番でインストールしないと、インストールに失敗します。インストーラを次の順番で実行してください。



- 1 ウェブプロテクションおよびファイアウォール コンポーネントには、暗号化クライアントが必要です。インストールの例については、「コマンドラインの例」に進みます。
- 2 「[コマンドラインでのインストール](#)」の記載に従って、ウェブプロテクションおよびファイアウォールをインストールします。

コマンドラインでのインストール

- 次の表は、**EnsMgmtSdkInstaller.exe** ファイルに使用できるパラメータについての詳細です。

パラメータ	説明
LoadCert	指定のディレクトリに証明書をロードします。

- 次の表は、**setupEP.exe** ファイルに使用できるパラメータについての詳細です。

パラメータ	説明
ADDLOCAL="fw,wc"	インストールするモジュールの指定： fw=クライアントファイアウォール wc=ウェブプロテクション
override "hips"	ホストイントルージョン防止機能をインストールしません
INSTALLDIR	デフォルト以外のインストール場所
nocontentupdate	インストーラに、インストールプロセスの一部として自動的にコンテンツファイルのアップデートを行わないよう指示します。インストール完了後にできる限り早くアップデートのスケジュールを行うことをお勧めします。
nopreservesettings	設定を保存しません。

- 次の表は、**DellThreatProtection.msi** ファイルに使用できるパラメータについての詳細です。

パラメータ	説明
Reboot=ReallySuppress	再起動を抑制します。
ARP	0=プログラムの追加 / 削除にエントリなし 1=プログラムの追加 / 削除にエントリ

- 次の表は、**EnsMgmtSdkInstaller.exe** ファイルに使用できるパラメータについての詳細です。

パラメータ	説明
ProtectProcesses	保護するプロセスのファイル名と場所を指定します。
InstallSDK	指定した場所に SDK をインストールします。
RemoveRightClick	エンドユーザーの右クリックメニューオプションを削除します。
RemoveMcTray	システムトレイを削除します。

コマンドラインの例

\Dell Threat Protection\SDK

- 次のコマンドラインは、証明書デフォルトパラメータをロードします。


```
"Dell Threat Protection\SDK\EnsMgmtSdkInstaller.exe" -LoadCert >"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\McAfeeSDKInstallerBeforeEndPoint.log"
```

① メモ:

アップグレードする場合は、このインストーラをスキップすることができます。

次の操作 :

\Dell Threat Protection\EndPointSecurity

- 次の例では、サイレントモード、クライアントファイアウォール、およびウェブプロテクションのインストール、ホストイントルージョン防止機能のオーバーライド、コンテンツアップデートなし、設定を保存しない、というデフォルトのパラメータでウェブプロテクションおよびクライアントファイアウォールをインストールします。

```
"Dell Threat Protection\EndPointSecurity\EPsetup.exe" ADDLOCAL="fw,wc" /override"hips" /nocontentupdate /nopreservesettings /qn
```

次の操作 :

\Dell Threat Protection\ThreatProtection\WinXXR

- 次の例では、再起動の抑制、ダイアログなし、プログレスバーなし、コントロールパネルプログラムリストにエントリなし、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。

```
"Dell Threat Protection\ThreatProtection\WinXXR\DellThreatProtection.msi" /qn REBOOT=ReallySuppress ARPSYSTEMCOMPONENT=1
```

\Dell Threat Protection\SDK

- 次の例では、Threat Protection SDK をインストールします。

```
"Dell Threat Protection\SDK\EnsMgmtSdkInstaller.exe" -ProtectProcesses "C:\Program Files\Dell\Dell Data Protection\Threat Protection\DellAVAgent.exe" -InstallSDK -RemoveRightClick -RemoveMcTray >"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\McAfeeSDKInstallerAfterEndPoint.log"
```

SED Management と Advanced Authentication クライアントのインストール

- SED クライアントは、v8.x の Advanced Authentication に必要です。
- 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、「[SED 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。
- 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 および Advanced Authentication クライアントインストーラは次の場所にあります。
 - お使いの Dell FTP アカウントから - DDP-Endpoint-Security-Suite-1.x.x.xxx.zip でインストールバンドルを見つけてから、[ESSE 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\Security Tools** および **C:\extracted\Security Tools\Authentication** 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>



パラメータ

SERVERHOST=<securityserver.organization.com>

SERVERPORT=8888

SECURITYSERVERHOST=<securityserver.organization.com>

SECURITYSERVERPORT=8443

ARPSYSTEMCOMPONENT=1 < [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 >

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

\Security Tools

- 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 にインストールという設定で、リモート管理される SED 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：

\Security Tools\Authentication

- 次の例では、サイレントインストール、再起動なし、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"
```

BitLocker Manager クライアントのインストール

- 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、「[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、次の場所にあります。
 - お使いの Dell FTP アカウントから - DDP-Endpoint-Security-Suite-1.x.x.xxx.zip でインストールバンドルを見つけてから、[ESSE 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\Security Tools** 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 < [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>

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"
```



子インストーラを使用したアンインストール

- 各クライアントを個別にアンインストールするには、「ESSE マスターインストーラからの子インストーラの抽出」にあるように、まず始めに ESSE マスターインストーラから子実行可能ファイルを抽出する必要があります。あるいは、管理インストールを実行して .msi を抽出します。
- アンインストールには、インストール時と同じバージョンのクライアントを使用するようにしてください。
- コマンドラインのスイッチおよびパラメータは大文字と小文字を区別します。
- コマンドラインでは、空白などの特殊文字を 1 つ、または複数含む値は、エスケープされた引用符で囲むようにしてください。コマンドラインパラメータでは大文字と小文字を区別します。
- これらのインストーラを使用し、スクリプトインストールやバッチファイルを利用するか、組織で利用できる他のプッシュ技術を活用して、クライアントをアンインストールします。
- ログファイル - Windows はログインしたユーザー用に、固有の子インストーラアンインストールログファイルを C:\Users\\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。/I 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「/!*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、必ずブ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](https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx) を参照してください。

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

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

ウェブプロテクションおよびファイアウォールのアンインストール

ウェブプロテクションおよびファイアウォールがインストールされていない場合は、[Encryption クライアントのアンインストール](#)に進みます。

コマンドラインでのアンインストール

- ESS マスターインストーラから抽出した後は、C:\extracted\Dell Threat Protection\ThreatProtection\WinXXR\DellThreatProtection.msi でウェブプロテクションおよびファイアウォールクライアントインストーラを見つけることができます。
- コントロールパネルでプログラムの追加と削除に移動し、次のコンポーネントをこの順番でアンインストールします。
 - McAfee Endpoint Security Firewall
 - McAfee Endpoint Security Web Control
 - McAfee Agent
- 次の操作：
- 次の例では、ウェブプロテクションおよびファイアウォールをアンインストールします。

```
MSIEXEC.EXE /x "DellThreatProtection.msi"
```

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

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

プロセス

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

- ESSE マスターインストーラから抽出した後、Encryption クライアントインストーラは C:\extracted\Encryption\DDPE_XXbit_setup.exe で見つけることができます。
- 次の表に、アンインストールで使用できるパラメータの詳細を示します。

パラメータ	選択
CMG_DECRYPT	Encryption Removal Agent のインストールタイプを選択するためのプロパティ : 3 - LSAREcovery バンドルを使用 2 - 以前にダウンロードしたフォレンジックキーマテリアルを使用 1 - Dell サーバからキーをダウンロード 0 - Encryption Removal Agent をインストールしない
CMGSILENTMODE	サイレントアンインストールのプロパティ 1 - サイレント 0 - 非サイレント
必須のプロパティ	
DA_SERVER	ネゴシエーションセッションをホストする EE Server の FQHN。
DA_PORT	EE Server 上の要求用ポート (デフォルトは 8050)。
SVCPN	EE Server で Key Server サービスがログオンされている UPN 形式のユーザー名。
DA_RUNAS	キーフェッチリクエストが行われるコンテキストでの SAM 対応形式のユーザー名。このユーザーは、EE Server の Key Server リストに存在している必要があります。
DA_RUNASPWD	runas ユーザーのパスワード。
FORENSIC_ADMIN	アンインストールまたはキーのフォレンジック要求に使用できる Dell サーバ上のフォレンジック管理者アカウント。
FORENSIC_ADMIN_PWD	フォレンジック管理者アカウントのパスワード。



オプションのプロパティ

SVCLOGONUN	パラメータとして Encryption Removal Agent サービスログオンするための UPN 形式のユーザー名。
SVCLOGONPWD	ユーザーとしてログオンするためのパスワード。

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

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

終了したらコンピュータを再起動します。

- 次の例では、Encryption クライアントをアンインストールし、フォレンジック管理者アカウントを使用して暗号化キーをダウンロードします。

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

MSI コマンド :

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

終了したらコンピュータを再起動します。

① 重要:

デルでは、コマンドラインで Administrator パスワードを使用する場合、次のアクションを推奨します

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

① メモ:

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

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

Advanced Threat Prevention のアンインストール

コマンドラインでのアンインストール

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

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

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



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

次の例では Dell Client Security Framework のコンポーネントのみをアンインストールしますが、SED および Advanced Authentication クライアントはアンインストールされません。

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

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

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

プロセス

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

PBA の非アクティブ化

- 1 リモート管理コンソールに Dell 管理者としてログインします。
- 2 左ペインで、**保護と管理 > エンドポイント** をクリックします。
- 3 適切なエンドポイントの種類を選択します。
- 4 表示 > 表示、非表示 または **すべて** を選択します。
- 5 コンピュータのホスト名がわかっている場合は、そのホスト名を **ホスト名** フィールドに入力します。ワイルドカードも使用できます。このフィールドを空白のままにすると、すべてのコンピュータが表示されます。**検索** をクリックします。

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

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

- 6 該当するコンピュータの **詳細** アイコンを選択します。
- 7 上部メニューの **セキュリティポリシー** をクリックします。
- 8 **ポリシーカテゴリ** ドロップダウンメニューから、**自己暗号化ドライブ** を選択します。
- 9 **SED 管理** エリアを展開し、**SED 管理の有効化** ポリシーおよび **PBA のアクティブ化** ポリシーを True から False に変更します。
- 10 **保存** をクリックします。
- 11 左ペインで、**アクション > ポリシーのコミット** をクリックします。
- 12 **変更の適用** をクリックします。

ポリシーが EE Server/VE Server から非アクティブ化対象のコンピュータに反映されるまで待ちます。

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

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

コマンドラインでのアンインストール

- ESSE マスターインストーラから抽出した後は、C:\extracted\Security Tools\EMAgent_XXbit_setup.exe で SED クライアントインストーラを見つけることができます。
- ESSE マスターインストーラから抽出した後は、C:\extracted\Security Tools\Authentication\- 次の例は、SED クライアントをサイレントアンインストールします。

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

終了したらコンピュータをシャットダウンして再起動します。

次の操作：

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

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

終了したらコンピュータをシャットダウンして再起動します。

BitLocker Manager クライアントのアンインストール

コマンドラインでのアンインストール

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

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

終了したらコンピュータを再起動します。



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、「[ESSE マスターインストーラからの子インストーラの抽出](#)」にあるように、まず始めに ESSE マスターインストーラから子実行可能ファイルを抽出する必要があります。
- SED クライアントは、v8.x で Advanced Authentication に必要であり、このため次の例でコマンドラインの一部になっています。
- Advanced Threat Prevention の子インストーラコンポーネントは、コマンドラインのみでインストールする必要があります。このコンポーネントをインストールするためにダブルクリックすると、製品の非 Dell、非管理下バージョンをインストールしますが、これはサポートされていません。誤ってインストールを行ってしまった場合は、プログラムの追加および削除 に移動してそのバージョンをアンインストールします。
- 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\\AppData\Local\Temp. にある %temp% に、ログインしたユーザー用の固有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」の後にも使用してください。

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 クライアントの各機能の使用方法については、『Dell Encrypt Help』(Dell Encrypt ヘルプ) を参照してください。このヘルプには、<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\Help からアクセスします。
- External Media Shield の各機能の使用方法については、『EMS Help』(EMS ヘルプ) を参照してください。このヘルプには、<Install dir>:\Program Files\Dell\Dell Data Protection\Encryption\EMS からアクセスします。
- Advanced Authentication および Advanced Threat Prevention の機能の使用方法については、Endpoint Security Suite Enterprise ヘルプを参照してください。ヘルプには、<Install dir>:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Help からアクセスしてください。

Encryption クライアント、Advanced Threat Prevention および Advanced Authentication

- 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 にインストールという設定で、リモート管理される SED をインストールします。このコンポーネントは、Advanced Threat Prevention で必要とされる Dell Client Security Framework 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、サイレントインストール、再起動なし、指定した場所にインストールログファイルとインストールフォルダという設定で Advanced Threat Prevention をインストールします。

```
MSIEXEC.EXE /I "AdvancedThreatProtectionCSFPlugins_x64.msi" /qn REBOOT="ReallySuppress" APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Plugins" ARPSYSTEMCOMPONENT="1" /! *v "C:\ProgramData\Dell\Dell Data Protection\Installer Logs\AdvancedThreatProtectionPlugins.msi.log"
```

および

```
AdvancedThreatProtectionAgentSetup.exe /s /norestart REBOOT=ReallySuppress APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection" ARPSYSTEMCOMPONENT=1 /! "C:\ProgramData\Dell\Dell Data Protection\Installer Logs\AdvancedThreatProtection.log"
```

- 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 Encryption 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"
```

- 次の例では、**オプション**の機能であるウェブプロテクションおよびファイアウォールをインストールします。
- \Dell Threat Protection\SDK**

次のコマンドラインは、証明書デフォルトパラメータをロードします。

```
EnsMgmtSdkInstaller.exe -LoadCert >"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\McAfeeSDKInstallerBeforeEndPoint.log"
```

メモ:

アップグレードする場合は、このインストーラをスキップすることができます。



次の操作 :

\Dell Threat Protection\EndPointSecurity

- 次の例では、サイレントモード、Threat Protection、クライアントファイアウォール、ウェブプロテクションのインストール、ホストイントルージョン防止機能のオーバーライド、コンテンツアップデートなし、設定を保存しない、というデフォルトのパラメータで オプション機能であるウェブプロテクションおよびファイアウォールをインストールします。

```
"Dell Threat Protection\EndPointSecurity\EPsetup.exe" ADDLOCAL="fw,wc" /override"hps" /nocontentupdate /nopreservesettings /qn
```

次の操作 :

\Dell Threat Protection\ThreatProtection\WinXXR

- 次の例では、再起動の抑制、ダイアログなし、プログレスバーなし、コントロールパネルプログラムリストにエントリなし、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。

```
"DellThreatProtection.msi" /qn REBOOT=ReallySuppress ARPSYSTEMCOMPONENT=1
```

\Dell Threat Protection\SDK

- 次の例では、Threat Protection SDK をインストールします。

```
EngMgmtSdkInstaller.exe -ProtectProcesses "C:\Program Files\Dell\Dell Data Protection\Threat Protection\DellAVAgent.exe" -InstallSDK -RemoveRightClick -RemoveMcTray >"C:\ProgramData\Dell\Dell Data Protection\Installer Logs\McAfeeSDKInstallerAfterEndPoint.log"
```

SED クライアント (Advanced Authentication を含む) および External Media Shield

- 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 にインストールという設定で、リモート管理される SED 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、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、EMS 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"
```

BitLocker Manager および External Media Shield

- 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 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、EMS 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"
```

BitLocker Manager および Advanced Threat Prevention

- 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 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。このコンポーネントは、Advanced Threat Prevention で必要とされる Dell Client Security Framework 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、指定した場所にインストールログファイルとインストールフォルダという設定で Advanced Threat Prevention をインストールします。

```
MSIEXEC.EXE /I "AdvancedThreatProtection_xXX.msi" /qn REBOOT="ReallySuppress"  
ARPSYSTEMCOMPONENT="1" /l*v "C:\ProgramData\Dell\Dell Data Protection\Installer Logs\ATP.log"  
APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection"
```



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

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

前提条件

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

テナントのプロビジョニング

- 1 リモート管理コンソールにログインし、**サービス管理** へ移動します。
- 2 **Advanced Threat Protection サービスのセットアップ** をクリックします。障害がこの時点で発生した場合は、ATP ライセンスをインポートします。
- 3 ライセンスがインポートされると、ガイド付きのセットアップを開始します。**次へ** をクリックして開始します。
- 4 EULA を読んで同意し (チェックボックスはデフォルトでは **オフ** です)、**次へ** をクリックします。
- 5 テナントのプロビジョニングに DDP Server に証明書を提供します。**次へ** をクリックします。Cylance ブランドの既存テナントのプロビジョニングはサポートされていません。
- 6 証明書をダウンロードします。これは、DDP Server との災害シナリオが発生した場合のリカバリに必要です。この証明書は、v9.2「upgrader」を介して自動的にバックアップされません。別のコンピュータで、証明書を安全な場所にバックアップします。証明書のバックアップを確定するために、チェックボックスをオンにして、**次へ** をクリックします。
- 7 セットアップが完了しました。**OK** をクリックします。

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

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

① **メモ:** エージェントの自動アップデートはデルサーバ v9.4.1 以降でサポートされます。

エージェントの自動アップデートの受信

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

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

エージェントの自動アップデート受信の停止

エージェントの自動アップデート受信を停止するには、次の操作を行います。

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



ワンタイムパスワード、SED UEFI、および BitLocker 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。

ワンタイムパスワード (OTP) を使用する場合、このタスクが必要です。

- <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。

- UEFI ファームウェア設定を開始します。
- 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。
- 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。

① 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。

- システム設定 を選択します。
- 統合 NIC を選択します。
- 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。
- 有効 または PXE で有効 を選択します。
- 適用 を選択します。

① 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。
- BitLocker Manager をインストールする **前に** TPM をオンにしてアクティブ化します。BitLocker Manager は 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」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
```

① ヒント:

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。



ドメインコントローラでの GPO の設定による資格の有効化

- お使いのクライアントが Dell Digital Delivery (DDD) から資格を得る場合は、これらの手順に従ってドメインコントローラに GPO を設定し、資格を有効にします (このサーバーは、EE Server/VE Server を実行しているサーバーとは異なる場合があります)。
- ワークステーションは、GPO が適用されている OU のメンバーである必要があります。

メモ:

EE Server/VE Server と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、資格機能は機能しません。

- 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：<EE Server/VE Server の 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。

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

- 1 Dell インストールメディアから、ファイルをローカルコンピュータにコピーします。
- 2 **DDPSuite.exe** ファイルと同じ場所でコマンドプロンプトを開き、次のように入力します。

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

抽出パスは 63 文字を超えられません。

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。詳細については、「要件」を参照してください。

抽出した子インストーラは C:\extracted\ にあります。



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

- 本項では、EE Server 使用時における Kerberos 認証 / 承認との使用のためにコンポーネントを設定する方法について説明します。VE Server では Key Server は使用しません。

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、個別のドメインを経由したりリモート管理コンソール上で許可されます。

- 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ーを対象ドメインに含める必要があります。
- VE Server は Key Server を使用しないので、通常のアンインストールには影響しません。VE Server に対してアクティブ化されている Encryption クライアントがアンインストールされると、Key Server の Kerberos メソッドの代わりに、Security Server を通じた標準的なフォレンジックキーの取得が使用されます。詳細については、「[コマンドラインのアンインストール](#)」を参照してください。

サービスパネル - ドメインアカウントのユーザーの追加

- 1 EE Server で、サービスパネル (スタート > ファイル名を指定して実行 > services.msc > OK) に進みます。
- 2 Key Server を右クリックして、**プロパティ** を選択します。
- 3 ログオン タブを選択し、**このアカウント** : オプションを選択します。

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

ドメインユーザーのパスワードを入力し確認します。

OK をクリックします

- 4 Key Server サービスを再起動します (さらなる操作のため、サービスパネルを開いたままにしておきます)。
- 5 <Key Server インストールディレクトリ> log.txt に移動して、サービスが正しく開始していることを確認します。

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

- 1 <Key Server インストールディレクトリ> に移動します。
- 2 テキストエディタで *Credant.KeyServer.exe.config* を開きます。
- 3 <add key="user" value="superadmin" /> に移動して、「superadmin」の値を、適切なユーザーの名前に変更します。「superadmin」のままとすることもできます。

「superadmin」の形式には、EE Server の認証が受けられる任意の方法を指定できます。SAM アカウント名、UPN、またはドメイン\ユーザー名は容認できます。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、EE 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。その理由は、EE Server で「jdoe」を検索できず、「jdoe」を認証できないためです。マルチドメイン環境では、ドメイン\ユーザー名の形式が容認できますが、UPN が推奨されます。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、EE Server が再起動すると再度暗号化されます。

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

サ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 EE Server
では、形式は 8081/xapi です )]
<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、リモート管理コンソールで選択した
管理者ロールが必要です。「superadmin」の形式には、EE Server の認証が受けられる任意の方法を指定できます。SAM アカウント名、UPN、または
ドメイン\ユーザー名は容認できます。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、EE 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。
その理由は、EE Server で「jdoe」を検索できず、「jdoe」を認証できないためです。マルチドメイン環境では、ドメイン\ユーザー名の形式が容認できま
す。UPN が推奨されます。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" /> [キーを要求できるユーザーをサービスが確認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、必要に応じてリストが更新される前に、どの程度
古いリストまで容認するかが設定されます。]
<add key="epw" value="encrypted value of the password" /> [Security 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 - キーサーバーサービスの再起動

- 1 サービスパネル (スタート > ファイル名を指定して実行 > services.msc > OK) に戻ります。
- 2 Key Server サービスを再起動します。



- 3 <Key Server インストールディレクトリ> log.txt に移動して、サービスが正しく開始していることを確認します。
- 4 サービスパネルを閉じます。

リモート管理コンソール - フォレンジック管理者の追加

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

Administrative Download Utility (CMGAd) の使用

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

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

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

- 1 `cmgad.exe` をダブルクリックして、ユーティリティを起動するか、CMGAd が置かれている場所でコマンドプロンプトを開いて `cmgad.exe -f` (または `cmgad.exe`) と入力します。
- 2 次の情報を入力します (一部のフィールドは事前に入力されている場合があります)。

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

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

パスワード : フォレンジック管理者パスワード

MCID : マシン ID (`machinelD.domain.com` など)

DCID : 16 桁の Shield ID のうち最初の 8 桁

① ヒント:

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

次へ をクリックします。

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

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

次へ をクリックします。

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

- 4 完了したら、**終了** をクリックします。



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

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

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

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

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

ポート番号：デフォルトのポートは 8050 です。

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

MCID：マシン ID（machinelD.domain.com など）

DCID：16 桁の Shield ID のうち最初の 8 桁

① ヒント:

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

次へ をクリックします。

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

パスフレーズを確認します。

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

次へ をクリックします。

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

4 完了したら、**終了** をクリックします。

Server Encryption の設定

Server Encryption の有効化

① メモ:

Server Encryption は、ユーザー暗号化を共有暗号化に変換します。

- 1 Dell リモート管理コンソールで 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** Server 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。

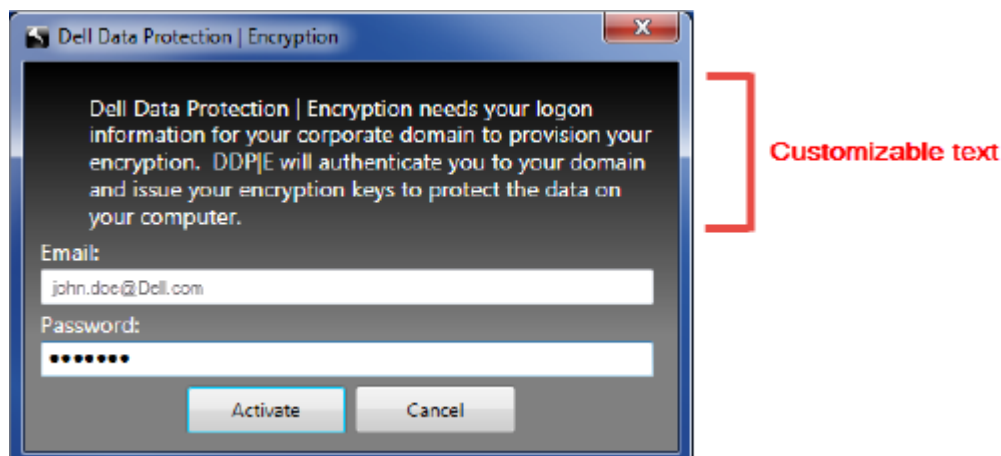
Windows 資格情報のセキュア化ポリシーが**選択されている** (デフォルト) 場合は、\Windows\system32\config ファイルフォルダ内にある Windows 資格情報も含めたすべてのファイルが暗号化されます。Windows 資格情報が暗号化されないようにするには、Windows 資格情報のセキュア化ポリシーを **選択しない** に設定します。Windows 資格情報の暗号化は、SDE 暗号化有効 ポリシーの設定とは無関係に行われます。

- 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

アクティベーションログオン 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。
- ユーザーがシステムトレイにある Encryption アイコンのメニューから Dell Encryption のアクティベーションを選択するとき。



Server Encryption EMS 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 **保護対象サーバー** (Server Encryption がインストール、アクティブ化されているサーバー) で、その保護対象サーバーがリムーバブルデバイスの存在を初めて検知するとき、リムーバブ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。

- EMS ポリシーは、リムーバブルメディアのサーバーへのアクセス、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、保護対象サーバー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、リモート管理コンソールの *Server Encryption* テクノロジグループの下にあります。

Server Encryption と外部メディア

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。Server Encryption はマシンキーでそのデバイスを保護対象サーバーに関連付け、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。その後でリムーバブ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。

① メモ:

Server 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、保護対象サーバー上で使用されるときはブロック、保護対象サーバー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ーに再挿入されると、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ーである場合、所有者 / ユーザーは、開始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 EMS 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 EMS 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。

暗号化されたサーバーインスタンスのサスペンド

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、Server Encryption マシンキーがサスペンドされます。

① 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。

① **重要:**

使用する際は注意が必要です。暗号化されたサーバーインスタンス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ー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。

前提条件

- リモート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は、エンドポイントをサスペンドするのに必要です。
- リモート管理コンソールに管理者がログインしている必要があります。

リモート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。

サーバー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。

① **メモ:**

復帰 ボタンをクリックすると、Server Encryption は再起動後にサーバー上の暗号化されたデータにアクセスできるようになります。



トラブルシューティング

すべてのクライアントのトラブルシューティング

- **ESSE マスターインストーラログファイル**は C:\ProgramData\Dell\Dell Data Protection\Installer にあります。
- Windows は、C:\Users\\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\\AppData\Local\Temp. にある %temp% に作成します。For example, C:\Users\\AppData\Local\Temp\dd_vccredist_amd64_20160109003943.log
- インストール対象のコンピューターにインストールされている Microsoft .Net のバージョンを検証するには、<http://msdn.microsoft.com> の手順に従ってください。

Microsoft .Net Framework 4.5 の完全バージョンをダウンロードするには、<https://www.microsoft.com/en-us/download/details.aspx?id=30653> にアクセスします。

- インストール対象のコンピューターに Dell Access がインストールされている(または過去にされていた)場合は、『[Dell Data Protection | Security Tools Compatibility](#)』(Dell Security Tools 互換性) を参照してください。DDP|A には、この製品スイートへの互換性はありません。

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

Windows 10 Anniversary アップデートへのアップグレード

Windows 10 Anniversary アップデートバージョンへアップグレードするには、次の記事の指示に従います。<http://www.dell.com/support/article/us/en/19/SLN298382>

サーバーオペレーティングシステム上でのアクティベーション

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

初期アクティベーションのトラブルシューティング

初期アクティベーションは、次のときに失敗します。

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

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

ユーザー名とパスワードが一致しません。

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

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

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

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

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

または 内部接続ポートを編集... のいずれかをクリックします。

The operation timed out.

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

可能な解決策

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

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

可能な解決策

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

初期アクティベーションプロセス

次の図は、正常な初期アクティベーションを示します。

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

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

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

初期アクティベーションプロセスは次のとおりです。

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

① メモ:

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

- 6 DDP Server がエンタープライズ資格情報コンテナ (Active Directory またはその同等物) 内の資格情報をチェックして、その資格情報がドメイン管理者資格情報であることを確認します。



- 資格情報を使用して UPN が構築されます。
- その UPN を使用して、DDP Server が仮想サーバーユーザー用の新しいユーザーアカウントを作成し、その資格情報を DDP Server の資格情報コンテナ内に保存します。

仮想サーバーユーザーアカウントは、Encryption クライアントの排他使用用です。サーバーで認証するため、共通暗号化キーを処理するため、およびポリシーアップデートを受信するために使用されます。

メモ:

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

- アクティベーションが成功すると、ユーザーがコンピュータを再起動します。それにより、アクティベーションの第 2 部 (認証とデバイスアクティベーション) が開始されます。

認証とデバイスアクティベーションのトラブルシューティング

デバイスアクティベーションは、次のときに失敗します。

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

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

- バージョン情報 ダイアログを開いて、Server Encryption が認証済みで、サーバーモードになっていることを確認します。
- Shield ID が赤色で表示されている場合、暗号化はまだアクティブ化されていません。
- リモート管理コンソールでは、Server Encryption がインストールされているサーバーのバージョンはサーバー用 Shield としてリストされます。
- ネットワークの障害が原因でマシンキーの取得に失敗した場合、Server Encryption はオペレーティングシステムでネットワーク通知に登録します。
- マシンキーの取得に失敗した場合：
 - 失敗しても、仮想サーバーユーザーのログオンは成功します。
 - 設定した時間間隔でキーの取得を再試行するように、ネットワーク障害時の再試行間隔ポリシーをセットアップします。

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

認証とデバイスアクティベーションのプロセス

次の図は、正常な認証とデバイスアクティベーションを示します。

- 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。
- コンピュータは、自身のデバイスアクティベーションステータスを DDP Server でチェックします。
 - そのコンピュータがまだデバイスアクティブ化されていない場合、DDP Server は、そのコンピュータに MCID、DCID、および信頼証明書を割り当て、そのすべての情報を DDP Server の資格情報コンテナ内に保存します。
 - そのコンピュータがすでにデバイスアクティブ化されている場合、DDP Server は信頼証明書を検証します。
- DDP Server が信頼証明書をサーバーに割り当てた後、そのサーバーはその暗号化キーにアクセスできます。
- 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 > tcspd_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。

EMS と PCS の相互作用

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

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

CD/DVD に書き込まれたデータを暗号化する

- 外部メディアの EMS 暗号化 = True に設定します。
- EMS で CD/DVD 暗号化を除外 = False に設定します。
- サブクラスストレージの設定 : 光学ドライブコントロール = UDF Only に設定します。

WSScan の使用

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

WSScan



- 1 Dell インストールメディアから、スキャン対象の Windows コンピュータに WSScan.exe をコピーします。
- 2 上記の場所でコマンドラインを起動して、コマンドプロンプトに **wsscan.exe** と入力します。WSScan が起動します。
- 3 **詳細設定** をクリックします。
- 4 次のドロップダウンメニューからスキャンしたいドライブの種類を選択します：すべてのドライブ、固定ドライブ、リムーバブルドライブ または CDROM/DVDROM。
- 5 ドロップダウンメニューから該当する暗号化レポートタイプを選択します：暗号化ファイル、非暗号化ファイル、すべてのファイル、または 違反の非暗号化ファイル。
 - 暗号化ファイル - Encryption クライアントをアンインストールするとき、すべてのデータが復号化されていることを確認するために使用します。復号化ポリシーアップデートの発行など、データを復号化するための既存の手順に従います。データを復号化した後は、アンインストール準備として再起動する前に、WSScan を実行してすべてのデータが復号化されていることを確認します。
 - 非暗号化ファイル - 暗号化されていないファイルを特定するために使用します。それらのファイルを暗号化するべきかどうか (Y/N) も示されます。
 - すべてのファイル - すべての暗号化および非暗号化ファイルのリストを表示するために使用します。それらのファイルを暗号化するべきかどうか (Y/N) も示されます。
 - 違反の非暗号化ファイル - 暗号化すべき非暗号化ファイルを特定するために使用します。
- 6 **検索** をクリックします。

または

- 1 **詳細設定** をクリックし、ビューを **シンプル** に切り替えて、特定のフォルダをスキャンします。
- 2 スキャン設定 に移動して、**検索パス** フィールドにフォルダパスを入力します。このフィールドを使用した場合、ドロップダウンボックスの選択は無視されます。
- 3 WSScan の出力をファイルに書き込まない場合は、**ファイルに出力** チェックボックスをオフにします。
- 4 必要に応じて、パスに含まれているデフォルトパスとファイル名を変更します。
- 5 既存のどの WSScan 出力ファイルも上書きしない場合は、**既存のファイルに追加** を選択します。
- 6 出力書式を選択します。
 - スキャンした結果をレポートスタイルのリストで出力する場合は、**レポート書式** を選択します。これがデフォルトの書式です。
 - スプレッドシートアプリケーションにインポートできる書式で出力する場合は、**値区切りファイル** を選択します。デフォルトの区切り文字は「|」ですが、最大 9 文字の英数字、空白、またはキーボード上のパンクチュエーション文字に変更できます。
 - 各値を二重引用符で囲むには、**クオートされる値 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] [-i[v]]] [-d<delimiter>] [-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。



スイッチ	意味
-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。 このモードを使用する場合、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せん。
-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。
-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 暗号化キー。 User : ユーザー暗号化キー。



出力	意味
	<p>Common : 共通暗号化キー。</p> <p>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。</p>
KCID	<p>キーコンピュータ ID。</p> <p>上記の例では、「7vdlxrsb」</p> <p>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。</p>
UCID	<p>ユーザー ID。</p> <p>上記の例では、「_SDENCR_」</p> <p>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。</p>
ファイル	<p>暗号化ファイルのパス。</p> <p>上記の例では、「c:\temp\Dell - test.log」</p>
アルゴリズム	<p>ファイルの暗号化に使用した暗号化アルゴリズム。</p> <p>上記の例では、「is still AES256 encrypted」</p> <p>Rijndael 128</p> <p>Rijndael 256</p> <p>AES 128</p> <p>AES 256</p> <p>3DES</p>

WSProbe の使用

Probing Utility は、EMS ポリシーを除き、すべてのバージョンの Encryption クライアント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、作成される時、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 True 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 True 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、アプリ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、次のように、サービスパネル (スタート > ファイル名を指定して実行 ... > services.msc > OK) の説明エリアにそのステータスを表示します。サービスのステータスをアップデートするために、サービスを定期的に更新します (サービスをハイライト表示 > 右クリック > 更新)。

- SED の非アクティブ化を待機中** – Encryption クライアントはまだインストールされているか、まだ設定されているか、またはその両方です。Encryption クライアントがアンインストールされるまで復号化は開始されません。
- 初期スweep** – サービスは初期スweep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weepは一度だけ実行されます。
- 復号化スweep** – 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weep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weepが完了し、すべてのロックされたファイルが次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weep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weep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weep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weep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、すべて次の再起動で削除されるようにスケジュールされています。

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

Windows Powershell を使用した製品コードの検索

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

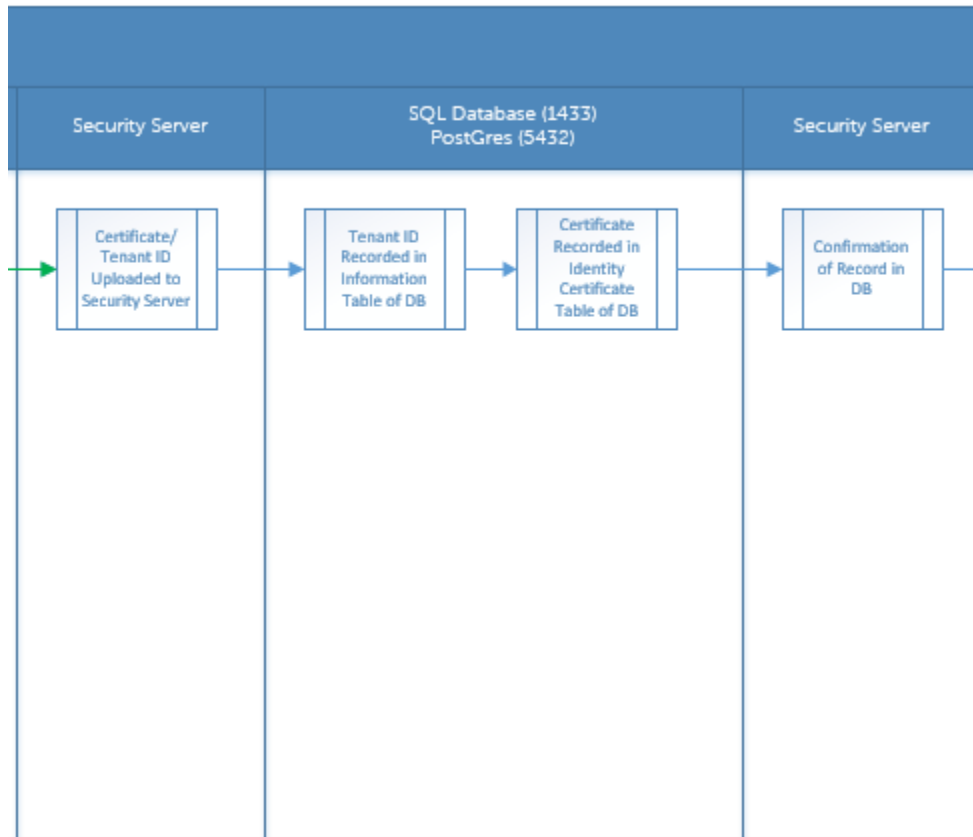
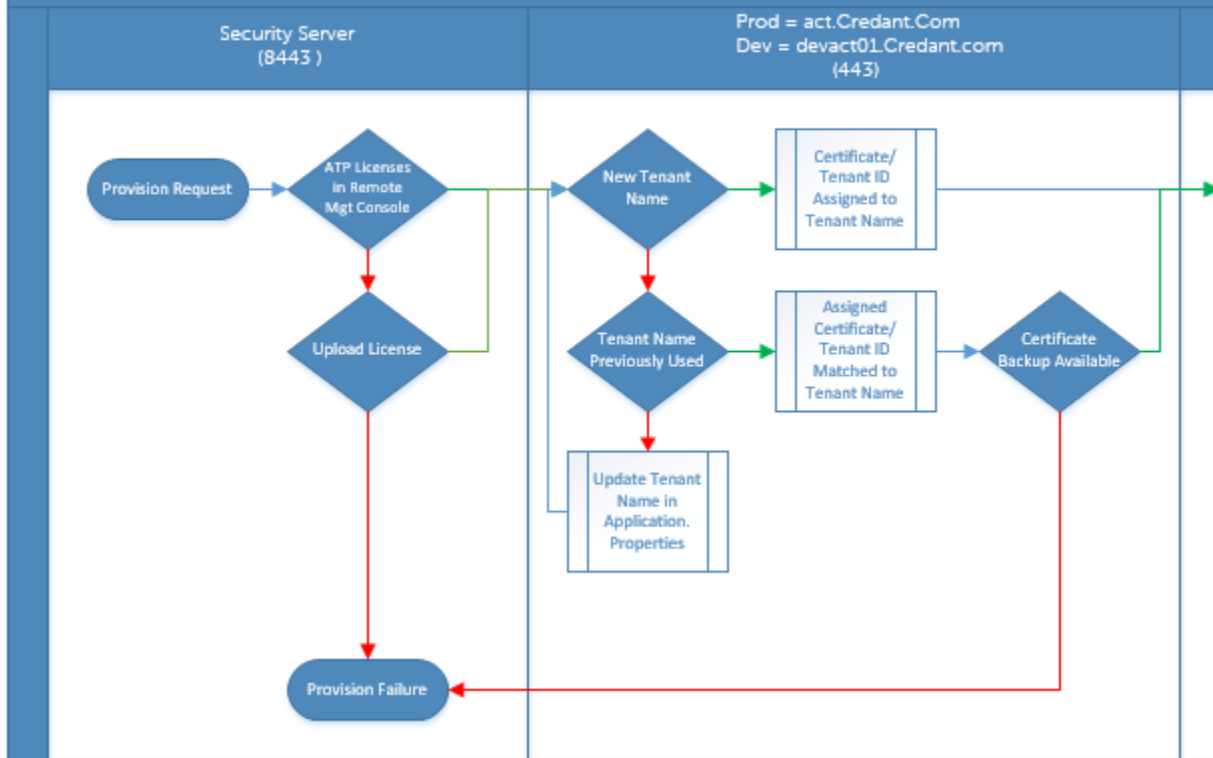
```
Get-WmiObject Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT IdentifyingNumber, Name, LocalPackage
```

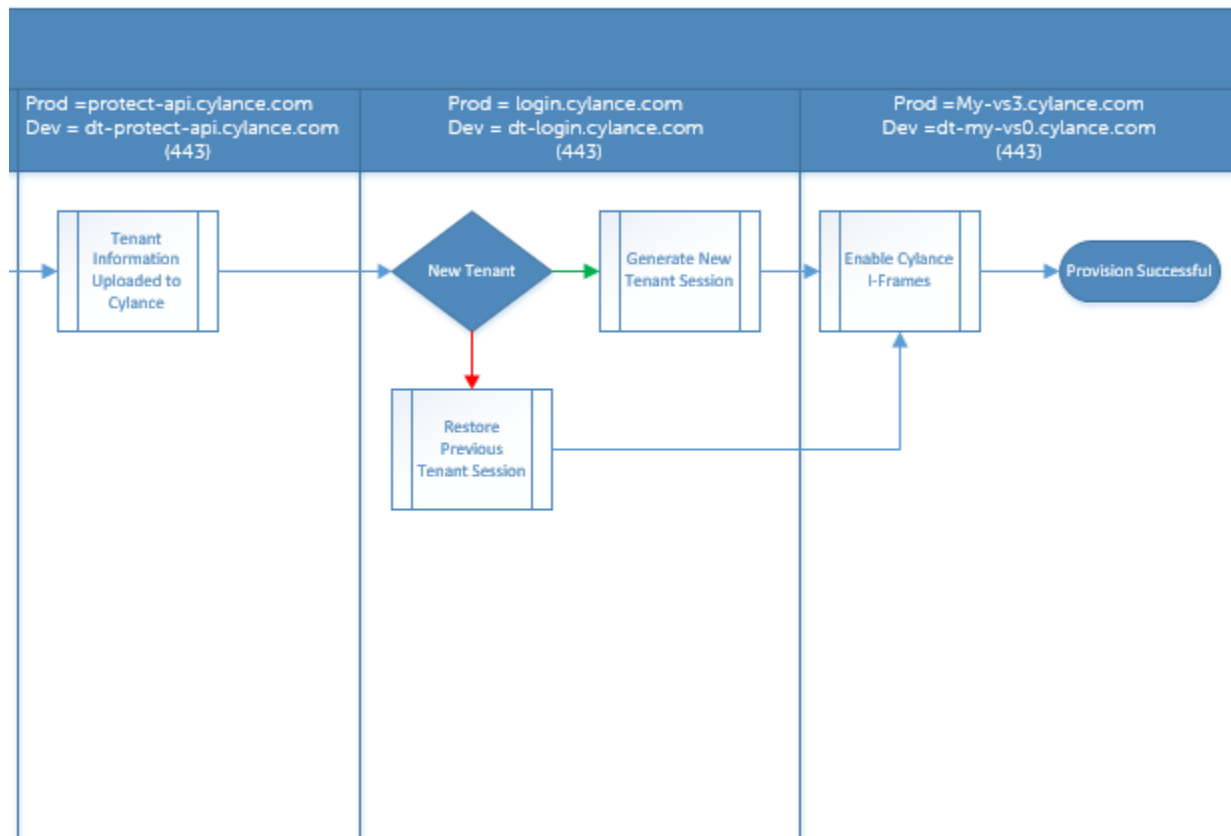
出力結果は、フルパスと .msi ファイル名（変換された 16 進法のファイル名）となります。

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

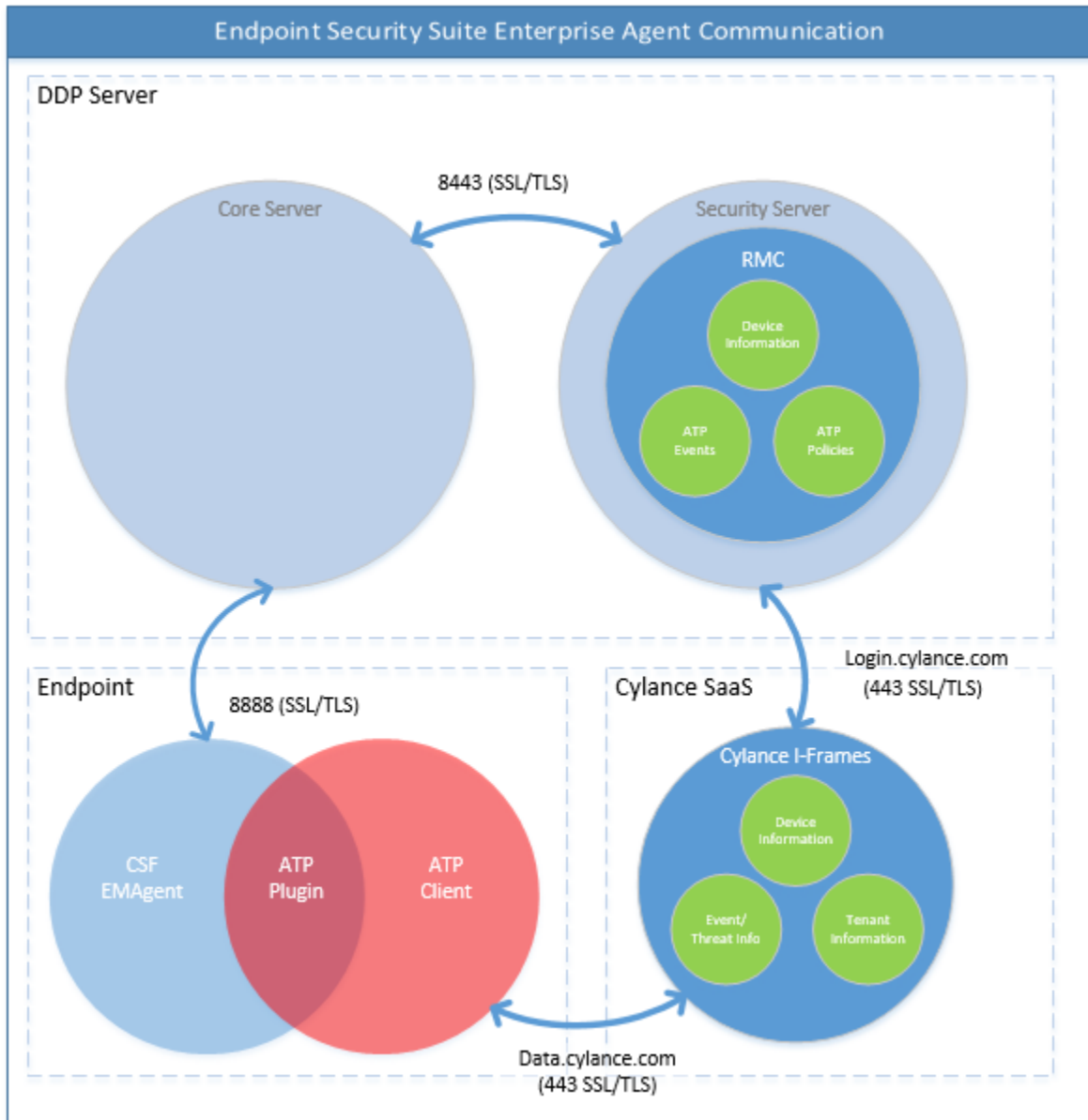
次の図は Advanced Threat Prevention サービスのプロビジョニングプロセスを表しています。

Advanced Threat Protection Service Provisioning Process



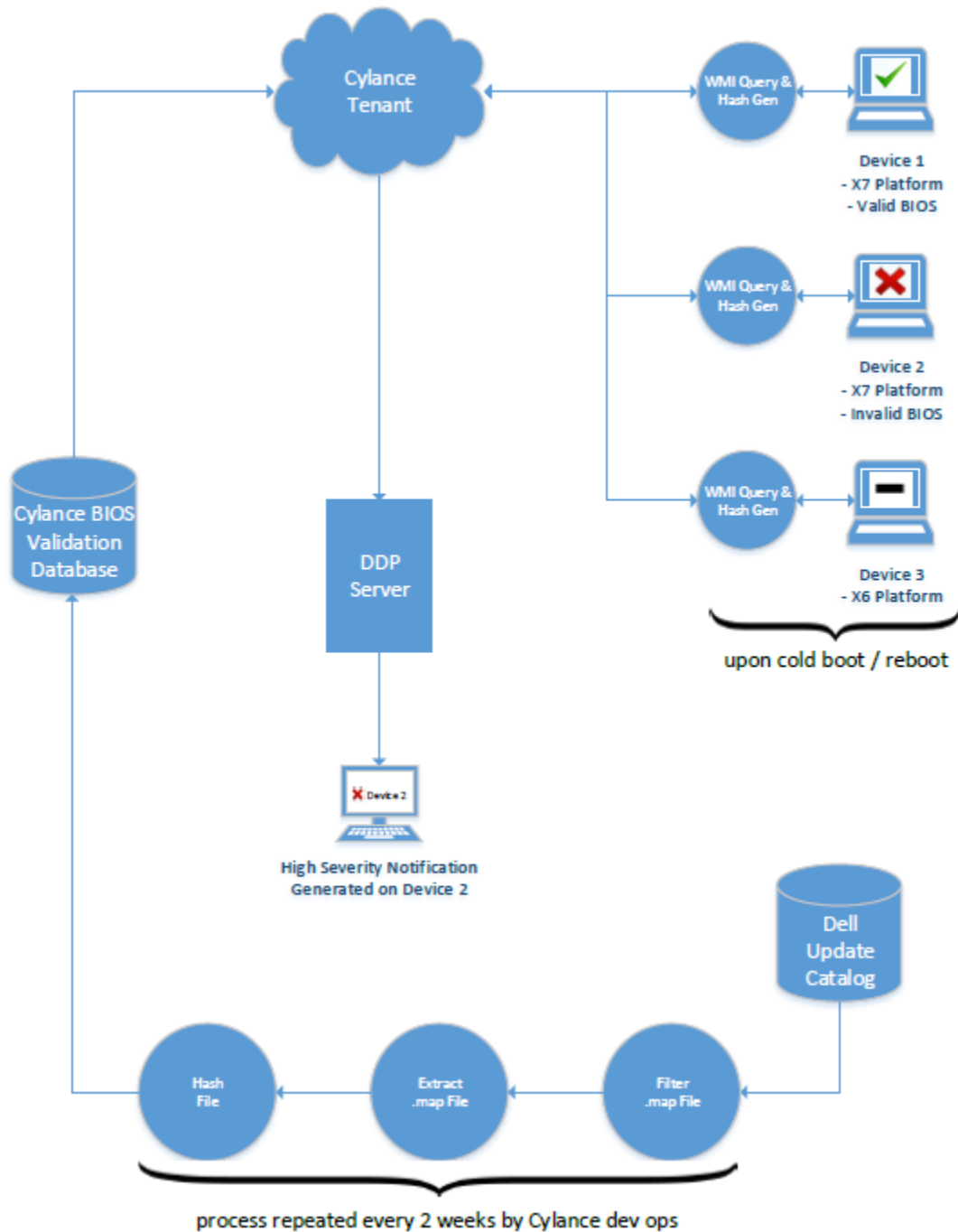


次の図は Advanced Threat Prevention のエージェント通信プロセスを表しています。



BIOS イメージの整合性検証プロセス

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



SED クライアントのトラブルシューティング

初期アクセスコードポリシーの使用

- 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、EE Server/VE Server と AD のどちらにもアクセスできなくなります。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。

安全性の低いログイン方法であるだけでなく、エンドユーザーが初期アクセスコードを使用してアクティブ化される場合、このコンピュータでユーザーがアクティブ化された記録は EE Server/VE Server には残りません。したがって、エンドユーザーがパスワードおよびセルフヘルプ質問の入力に失敗しても、EE Server/VE Server からレスポンスコードを生成することはできません。

- 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。
 - クライアントにネットワークまたは EE Server/VE Server への接続がない。

初期アクセスコードの使用

- 1 リモート管理コンソールで**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、セキュリティコンソールを開き、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 (Credant Manager のみ) 質問 / 回答メッセージに応答します。

青色矢印 をクリックします。

- 12 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かかわらず、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。
 - DDP EE Server/VE Server 接続アイコンが表示されない。ログファイルには、EE Server/VE Server との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、DDP EE Server/VE Server 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 environment

- 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 コンピュータをオンにし、PBA にログインします。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、リアルタイムに書き込まれます。

Dell ControlVault ドライブ

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

工場では Dell コンピュータにインストールされている Dell ControlVault ドライブおよびファームウェアは古いいため、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 のドライブ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 ドライブ (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。

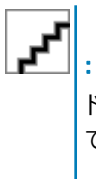
最新のドライブのダウンロード

- 1 [Support.dell.com](https://support.dell.com) に移動します。
- 2 お使いのコンピュータモデルを選択します。
- 3 **ドライブおよびダウンロード** を選択します。
- 4 ターゲットコンピューターの **オペレーティングシステム** を選択します。
- 5 **セキュリティ** カテゴリを展開します。
- 6 Dell ControlVault ドライブ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ブとファームウェアをコピーします。

Dell ControlVault ドライブのインストール

ドライブのインストールファイルをダウンロードしたフォルダに移動します。

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



ドライブ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ブのファイル名は ControlVault_Setup_2MYJC_A37_ZPE.exe です。

続行 をクリックして開始します。

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

はい をクリックして新しいフォルダの作成を許可します。

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

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

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

ようこそ画面で **次へ** をクリックします。

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

完了 オプションを選択して **次へ** をクリックします。

インストール をクリックしてドライバのインストールを開始します。

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

ドライバのインストールの検証

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

Dell ControlVault ファームウェアのインストール

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



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

いくつかのステータスメッセージが表示されます。

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

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

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 モードで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](#)



ユーザ用の事前インストール設定 に概説されているコンピュータ手順が成功し、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ましたが、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	序数が不明または一貫していませんでした。



定数 / 値	説明
0x8028000A	
TPM_E_INSTALL_DISABLED	所有者をインストールする機能が無効です。
0x8028000B	
TPM_E_INVALID_KEYHANDLE	キーハンドルを解釈できません。
0x8028000C	
TPM_E_KEYNOTFOUND	キーハンドルが無効なキーを示しています。
0x8028000D	
TPM_E_INAPPROPRIATE_ENC	受け入れられない暗号化スキーマです。
0x8028000E	
TPM_E_MIGRATEFAIL	移行承認に失敗しました。
0x8028000F	
TPM_E_INVALID_PCR_INFO	PCR 情報を解釈できませんでした。
0x80280010	
TPM_E_NOSPACE	キーをロードする余裕がありません。
0x80280011	
TPM_E_NOSRK	ストレージルートキー (SRK) セットがありません。
0x80280012	
TPM_E_NOTSEALED_BLOB	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。
0x80280013	
TPM_E_OWNER_SET	TPM にはすでに所有者がいます。
0x80280014	
TPM_E_RESOURCES	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。
0x80280015	
TPM_E_SHORTRANDOM	ランダム文字列が短すぎました。
0x80280016	
TPM_E_SIZE	TPM には、操作を実行するための容量がありません。
0x80280017	
TPM_E_WRONGPCRVAL	名前付き PCR 値が現在の PCR 値に一致していません。
0x80280018	
TPM_E_BAD_PARAM_SIZE	コマンドに対する paramSize 引数の値が正しくありません。



定数 / 値	説明
0x80280019	
TPM_E_SHA_THREAD	既存の SHA-1 スレッドがありません。
0x8028001A	
TPM_E_SHA_ERROR	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。
0x8028001B	
TPM_E_FAILEDSELFTEST	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。
0x8028001C	
TPM_E_AUTH2FAIL	2 キー機能での 2 番目のキーの認証が失敗しました。
0x8028001D	
TPM_E_BADTAG	コマンドに送信されたタグ値が正しくありません。
0x8028001E	
TPM_E_IOERROR	TPM への情報の転送中に IO エラーが発生しました。
0x8028001F	
TPM_E_ENCRYPT_ERROR	暗号化プロセスに問題が発生しました。
0x80280020	
TPM_E_DECRYPT_ERROR	復号化プロセスが完了しませんでした。
0x80280021	
TPM_E_INVALID_AUTHHANDLE	無効なハンドルが使用されました。
0x80280022	
TPM_E_NO_ENDORSEMENT	TPM には、保証キー (EK) がインストールされていません。
0x80280023	
TPM_E_INVALID_KEYUSAGE	キーの使用は許可されていません。
0x80280024	
TPM_E_WRONG_ENTITYTYPE	送信されたエンティティタイプは許可されていません。
0x80280025	
TPM_E_INVALID_POSTINIT	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。
0x80280026	
TPM_E_INAPPROPRIATE_SIG	署名データには、追加の DER 情報を含められません。
0x80280027	

定数 / 値	説明
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 physicalPresence 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。
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_NOTRESETTABLE 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。



定数 / 値	説明
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。
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 所有者の制御下であり、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。



定数 / 値	説明
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。
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。



定数 / 値	説明
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トが多すぎます。
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。
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。



定数 / 値	説明
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。

定数 / 値	説明
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。
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ではありません。
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。



定数 / 値	説明
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。
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。



定数 / 値	説明
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。
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せん。
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。



定数 / 値	説明
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、繰り返しがり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。
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イ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。



定数 / 値	説明
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。
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。



定数 / 値	説明
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。
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必要があります。
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。



定数 / 値	説明
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	イベントログチャンネル 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	イベントログチャンネル 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。
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。



定数 / 値	説明
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。
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。

定数 / 値	説明
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、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することができます。
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。
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	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。



定数 / 値	説明
0x8031001D	
FVE_E_CLUSTERING_NOT_SUPPORTED	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。
0x8031001E	
FVE_E_VOLUME_BOUND_ALREADY	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。
0x8031001F	
FVE_E_OS_NOT_PROTECTED	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。
0x80310020	
FVE_E_PROTECTION_DISABLED	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。
0x80310021	
FVE_E_RECOVERY_KEY_REQUIRED	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。
0x80310022	
FVE_E_FOREIGN_VOLUME	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。
0x80310023	
FVE_E_OVERLAPPED_UPDATE	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。
0x80310024	
FVE_E_TPM_SRK_AUTH_NOT_ZERO	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。
0x80310025	
FVE_E_FAILED_SECTOR_SIZE	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。
0x80310026	
FVE_E_FAILED_AUTHENTICATION	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。
0x80310027	
FVE_E_NOT_OS_VOLUME	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。
0x80310028	
FVE_E_AUTOUNLOCK_ENABLED	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。
0x80310029	
FVE_E_WRONG_BOOTSECTOR	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。
0x8031002A	
FVE_E_WRONG_SYSTEM_FS	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。
0x8031002B	

定数 / 値	説明
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。
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。



定数 / 値	説明
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。
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。

定数 / 値	説明
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	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。
0x80310057	
FVE_E_PUBKEY_NOT_ALLOWED	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。
0x80310058	
FVE_E_VOLUME_HANDLE_OPEN	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。
0x80310059	
FVE_E_NO_FEATURE_LICENSE	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。
0x8031005A	
FVE_E_INVALID_STARTUP_OPTIONS	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。
0x8031005B	
FVE_E_POLICY_RECOVERY_PASSWORD_NOT_ALLOWED	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。
0x8031005C	
FVE_E_POLICY_RECOVERY_PASSWORD_REQUIRED	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。
0x8031005D	
FVE_E_POLICY_RECOVERY_KEY_NOT_ALLOWED	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。
0x8031005E	
FVE_E_POLICY_RECOVERY_KEY_REQUIRED	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。
0x8031005F	
FVE_E_POLICY_STARTUP_PIN_NOT_ALLOWED	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。
0x80310060	
FVE_E_POLICY_STARTUP_PIN_REQUIRED	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。
0x80310061	
FVE_E_POLICY_STARTUP_KEY_NOT_ALLOWED	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。
0x80310062	
FVE_E_POLICY_STARTUP_KEY_REQUIRED	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。
0x80310063	
FVE_E_POLICY_STARTUP_PIN_KEY_NOT_ALLOWED	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。
0x80310064	
FVE_E_POLICY_STARTUP_PIN_KEY_REQUIRED	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。
0x80310065	

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。



定数 / 値	説明
FVE_E_POLICY_USER_CONFIGURE_FDVAUTOUNLOCK_NOT_ALLOWED 0x80310075	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。
FVE_E_POLICY_USER_CONFIGURE_RDVAUTOUNLOCK_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_FDVRKOFF_AUKON 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_RDVRKOFF_AUKON 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_SELF_SIGNED 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。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。



定数 / 値	説明
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_FDVRP_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_RDVRP_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する場合があります。
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_ATTEMPT_S_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。

定数 / 値	説明
FVE_E_FULL_ENCRYPTION_NOT_ALLOWED_ON_TP_STORAGE 0x803100A5	BitLocker ドライブ暗号化は、シ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。
FVE_E_WIPE_NOT_ALLOWED_ON_TP_STORAGE 0x803100A6	BitLocker ドライブ暗号化は、シ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。



定数 / 値	説明
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	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_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。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、パスワードの変更が無効になりました。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。

定数 / 値	説明
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。
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 はハードウェアア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。



用語集

アクティブ化 - コンピュータが Dell Enterprise Server/VE 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。

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

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

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

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

EMS Access Code - Dell Enterprise Server/VE 内のこのサービスを使用すると、External Media Shield で保護されているデバイスで、ユーザーがパスワードを忘れてしまい、ログインできなくなった場合に、そのデバイスをリカバリできます。この処理が完了したら、ユーザーはリムーバブルメディアまたは外付けストレージデバイスに設定されたパスワードをリセットできます。

Encryption クライアント – Encryption クライアントは、エンドポイントがネットワークに接続されている、ネットワークから切断されている、または盗難されているかどうかに関わらず、セキュリティポリシーを適用するオンデバイスコンポーネントです。Encryption クライアントは、エンドポイントに信頼できるコンピュー

タ環境を作成しながら、デバイスのオペレーティングシステム上のレイヤとして動作し、一貫して適用される認証、暗号、および承認を提供して機密情報を最大限に保護します。

エンドポイント - Dell Enterprise Server/VE によって管理されるコンピュータまたはモバイルハードウェアデバイス。

暗号化キー - 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こ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こ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) デバイス上でこれらのファイルにアクセスできます。

暗号化スweep - 暗号化スweepは、含まれるファイルが適切な暗号化状態になるように、管理下のエンドポイントで暗号化するフォルダをスキャンするプロセスです。通常のファイル作成および名前変更操作では、暗号化スweepはトリガされません。次のように、暗号化スweepが行われる可能性のある場合と、その結果生じるスweep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weep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weepされます。- その後、特定のポリシー変更があると、スweep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weepをトリガします。さらに、暗号化の有効化と無効化を切り替えると、暗号化スweepがトリガされます。

ワンタイムパスワード (OTP) - ワンタイムパスワードは、一度しか使用できないパスワードで、有効時間が限定されています。OTP には、TPM が存在し、有効化され、所有されている必要があります。OTP を有効にするには、Security Console および Security Tools Mobile アプリを使用して、モバイルデバイスをコンピュータとペアリングします。Security Tools Mobile アプリは、Windows ログオン画面でのコンピュータへのログオンに使用されるパスワードをモバイルデバイス上に生成します。コンピュータへのログオンに OTP を使用しなかった場合は、ポリシーに基づき、パスワードの期限が切れたときに、またはパスワードを忘れたときに、OTP 機能を使用してコンピュータへのアクセスを回復することができます。OTP 機能は、認証またはリカバリのいずれかに使用できますが、両方には使用できません。生成されたパスワードが一度しか使用できず、短時間で失効するため、OTP セキュリティは他の認証手法よりも優れています。

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。

スクリプト制御 - スクリプト制御は、悪意のあるスクリプトが実行されないようにブロックすることによってデバイスを保護します。

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

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

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 暗号化を無効にすると、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。TPM は、BitLocker Manager およびワンタイムパスワード機能の使用にも必須です。



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。外部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。

