

Dell Data Protection | Personal Edition

インストールガイド v8.13



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。

Personal Edition Installation Guide (Personal Edition のインストールガイド)

2017 - 04

Rev. A01

1 Personal Edition 7.....	6
Personal Edition.....	6
Security Tools.....	6
Dell ProSupport へのお問い合わせ.....	6
2 Personal Edition 7.....	7
暗号化クライアント.....	7
暗号化クライアント 13.....	8
Mac クライアントハードウェア.....	8
暗号化クライアントのオペレーティングシステム.....	8
External Media Shield (EMS) 対応のオペレーティングシステム.....	9
暗号化クライアントの言語サポート.....	9
Advanced Authentication クライアント -.....	10
Advanced Authentication クライアント 20.....	10
詳細な認証クライアントオペレーティングシステム.....	11
詳細な認証クライアントの言語サポート.....	11
3 ソフトウェアのダウンロード.....	13
4 Personal Edition のインストール 20.....	15
インストール方法の選択.....	15
マスターインストーラ - 推奨を使用した Personal Edition をインストールします。.....	15
子のインストーラを使用した Personal Edition をインストールします。.....	17
5 セキュリティツールおよび Personal Edition セットアップウィザード.....	20
6 Security Tools 管理者の設定.....	22
管理者パスワードおよびバックアップ場所の変更.....	22
認証の設定オプション.....	22
サインインオプションの設定.....	22
Password Manager 認証の設定.....	24
リカバリ質問の設定.....	24
指紋スキャン認証の設定.....	25
ワンタイムパスワード認証の設定.....	25
スマートカード登録の設定.....	26
詳細な許可の設定.....	26
ユーザー認証の管理.....	26
新規ユーザーの追加.....	27
ユーザー資格情報の登録または変更.....	27
1つの登録済み資格情報の削除.....	28
ユーザーのすべての登録済み資格情報の削除.....	28

7 子インストーラを使用したアンインストール.....	29
インストール方法の選択.....	29
からの追加 / 削除プログラムをアンインストールします.....	29
コマンドラインからのアンインストール.....	29
8 子インストーラを使用したアンインストール.....	31
Encryption クライアントのアンインストール.....	31
インストール方法の選択.....	31
高度な認証をアンインストールします。.....	33
インストール方法の選択.....	33
Client Security Framework のアンインストール.....	34
インストール方法の選択.....	34
9 「ポリシーテンプレートの説明」.....	35
ポリシー.....	35
テンプレートの説明.....	52
固定ドライブおよび外部ドライブのすべてに対する積極的な保護.....	52
PCI 規制の対象.....	53
データ漏洩規制の対象.....	53
HIPAA 規制の対象.....	53
固定ドライブおよび外部ドライブのすべてに対する基本的な保護 (デフォルト)	53
固定ドライブすべてに対する基本的な保護.....	54
システムドライブのみに対する基本保護.....	54
外部ドライブに対する基本的な保護.....	54
暗号化無効.....	54
10 ワンタイムパスワードのための事前インストール設定.....	55
TPM の初期化.....	55
11 マスターインストーラからの子インストーラの抽出.....	56
12 トラブルシューティング 61.....	57
Encryption クライアントのトラブルシューティング.....	57
Windows 10 Anniversary アップデートへのアップグレード.....	57
(オプション) Encryption Removal Agent ログファイルの作成.....	57
TSS バージョンの確認.....	58
EMS と PCS の相互作用.....	58
WSScan の使用.....	58
Encryption Removal Agent ステータスのチェック.....	60
EMS を使用した iPod の暗号化方法.....	60
Dell ControlVault ドライバ.....	61
Dell ControlVault ドライバおよびファームウェアのアップデート.....	61
レジストリ設定.....	62
暗号化クライアント.....	63

Advanced Authentication クライアント -.....	64
13 用語集.....	66



Personal Edition 7

本ガイドは、Security Tools が Personal Edition と共にインストールされることを前提としています。

Personal Edition

Personal Edition は、コンピューターを紛失した、またはコンピューターが盗難された時でさえも、コンピューター上のデータを保護することを目的としています。

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

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

Security Tools

セキュリティツールの目的は、インを高度な認証をサポートするための、エンドツーエンドのセキュリティのソリューションを提供することです。

セキュリティツールにより、Windows 認証においてパスワード、指紋リーダー、スマートカード (非接触型と接触型の両方) のみならず、自己登録、ワンタイムパスワード (OTP)、ワンステップログオン (シングルサインオン [SSO]) を使用できる多要素認証がサポートされます。

DDP Security Console は、管理者によって設定されたポリシーに基づいて、ユーザーがそれぞれの資格情報およびセルフリカバリ質問を設定する手順をガイドする Security Tools のインタフェースです。

Administrator Settings ツールは管理者権限を持つユーザーが使用できるツールで、認証ポリシーとリカバリオプションのセットアップ、ユーザーの管理、および詳細設定を行う他、Windows ログオン用にサポートされている資格情報に固有の設定を行うためにも使用されます。

Security Tools アプリケーションの使用方法を学ぶには、[Security Tools 管理者設定の実行](#)および『*Dell Console User Guide*』(Dell Console ユーザーガイド)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。

Personal Edition 7

これらの Personal Edition のインストールに必要な要件の詳細すべてをします。

暗号化クライアント

- Personal Edition が必要とする権利を正常にインストールします。この資格は、DDP|PE ご購入時に提供されます。Personal Edition のご購入方法によっては、資格を手動で入力する必要がある場合があります。その場合は、資格に付いている簡単な手順に従って入力してください。Personal Edition が Dell Digital Delivery によってインストールされている場合は、資格のインストールは Dell Digital Delivery サービスがすでに完了しています。(同じバイナリの Enterprise Edition および Personal Edition 用に使用されます。[使用資格をインストールするにはどのバージョンのインストーラを指示します])
- Windows パスワードの作成 - 暗号化データへのアクセスを保護するため、Windows パスワードの作成が強く推奨されます (まだパスワードが存在しない場合)。コンピュータにパスワードを作成すると、他のユーザーがパスワードなしでユーザーアカウントにログインすることを防止できます。
 - に進み、Windows のコントロールパネル (**スタート > コントロールパネル**)。
 - ユーザーアカウント** アイコンをクリックします。
 - アカウントのパスワードの作成** をクリックします。
 - 新しいパスワードを入力し、再度パスワードを入力します。
 - 任意でパスワードのヒントを入力します。
 - パスワードの作成** をクリックします。
 - コンピュータを再起動します。
- 導入中は、IT ベストプラクティスに従う必要があります。これには、初期テスト向けの管理されたテスト環境や、ユーザーへの時間差導入が含まれますが、それらに限定されるものではありません。
- インストール、アップグレード、アンインストールを実行するユーザーアカウントは、ローカルまたはドメイン管理者ユーザーである必要があります。これは、Microsoft SMS 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。
- 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。
- 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)。
- 暗号化クライアントは、デュアルブート設定をサポートしていません。これは、もう一方のオペレーティングシステムのシステムファイルが暗号化され、その動作を妨げるおそれがあるためです。
- マスターインストーラでは、v8.0 より前のコンポーネントからのアップグレードはサポートされていません。マスターインストーラから子インストーラを抽出し、コンポーネントを個々にアップグレードします。疑問点や不明点がある場合は、Dell ProSupport にお問い合わせください。
- Encryption クライアントは監査モードをサポートするようになりました。監査モード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。企業イメージに Encryption クライアントをインストールする方法に関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。
- 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。
- 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 も使用してテスト済みです。



リストに記載のないアンチウイルスプロバイダを組織が使用している場合は、KB 記事 SLN298707 (現在参照不可) を参照するか、または Dell ProSupport に連絡してサポートを受けてください。

- 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。

- 必ず定期的にチェックします www.dell.com/support に は最新のマニュアルや技術アドバイザリー用です。

暗号化クライアント 13

- Microsoft .Net Framework 4.5.2 (またはそれ以降) は、マスターインストーラおよび子インストーラクライアントに必要です。

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 (またはそれ以降) が事前インストールされています。ただし、デルハードウェア上にインストールしていない場合、または旧型のデルハードウェア上でクライアント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、**クライアント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) の指示に従います。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。

- マスターインストーラをコンピュータにすでにインストールされていない場合は Microsoft Visual C++ 2012 アップデート 4 + をインストールします。**子インストーラを使用する場合は**、Encryption クライアントをインストールする前に、このコンポーネントをインストールする必要があります。

前提条件

- Visual C++ 2012 更新プログラム 4 以降再頒布可能パッケージ (x86 および x64)
- Microsoft SQL Server Compact 3.5 SP2 (x86 および x64)

Mac クライアントハードウェア

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

ハードウェア

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

- 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。

オプションの組み込みハードウェア

- TPM 1.2 または 2.0

暗号化クライアントのオペレーティングシステム

- 次の表では、対応オペレーティングシステムが詳しく説明されています。

Windows オペレーティングシステム (32 ビットと 64 ビット)

- Windows 7 SP0、SP1 : (Enterprise、Professional、Ultimate)

Windows オペレーティングシステム (32 ビットと 64 ビット)

- 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 の場合 : Enterprise 、 Pro
- Windows 8.1 アップデート 0 ~ 1、次の 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 を教育、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。

External Media Shield (EMS) 対応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 の場合 : Enterprise 、 Pro 、 Consumer
- Windows 8.1 アップデート 0 ~ 1、次の Enterprise Edition 、 Pro Edition
- Windows 10 を教育、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

暗号化クライアントの言語サポート

- Encryption クライアントは複数言語ユーザーインターフェイス (MUI) 対応で、次の言語をサポートしています。

言語サポート

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



Advanced Authentication クライアント -

- Advanced Authentication を使用する場合、ユーザーは、Dell Data Protection | 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す。クリアするに設定し、TPM の所有権を、を参照してください https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2..

Advanced Authentication クライアント 20

- 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
- Dell 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

- PKCS 11 のスマートカードを使用して、[ACTIVIDENTITY クライアント

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
 - 共通アクセスカード (CAC)
 - クラス B / SIPR Net カード
- Dell 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 (以下に示すとおり)、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、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。
 - Dell 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。Dell ControlVault ドライバのインストール手順は、「

- 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 コンピュータのモデル - クラス B / SIPR Net カードのサポート

- Latitude E6440
- Precision M2800
- Latitude 14 Rugged Extreme
- Precision M4800
- Latitude 12 Rugged Extreme

詳細な認証クライアント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 の場合: Enterprise、Pro
- Windows 8.1 アップデート 0 ~ 1、次の Enterprise Edition、Pro Edition
- Windows 10 を教育、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

詳細な認証クライアントの言語サポート

- Advanced Authentication クライアントおよび Security Tools は、多言語ユーザーフェース (MUI) に対応しており、次の言語をサポートします。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
- KO - 韓国語
- ZH-CN - 中国語 (簡体字)
- ZH-TW - 中国語 (繁体字)



言語サポート

- DE - ドイツ語
- ES - スペイン語
- JA - 日本語
- 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))
- RU - ロシア語

続行を [入手するにはソフトウェア](#)を押します。

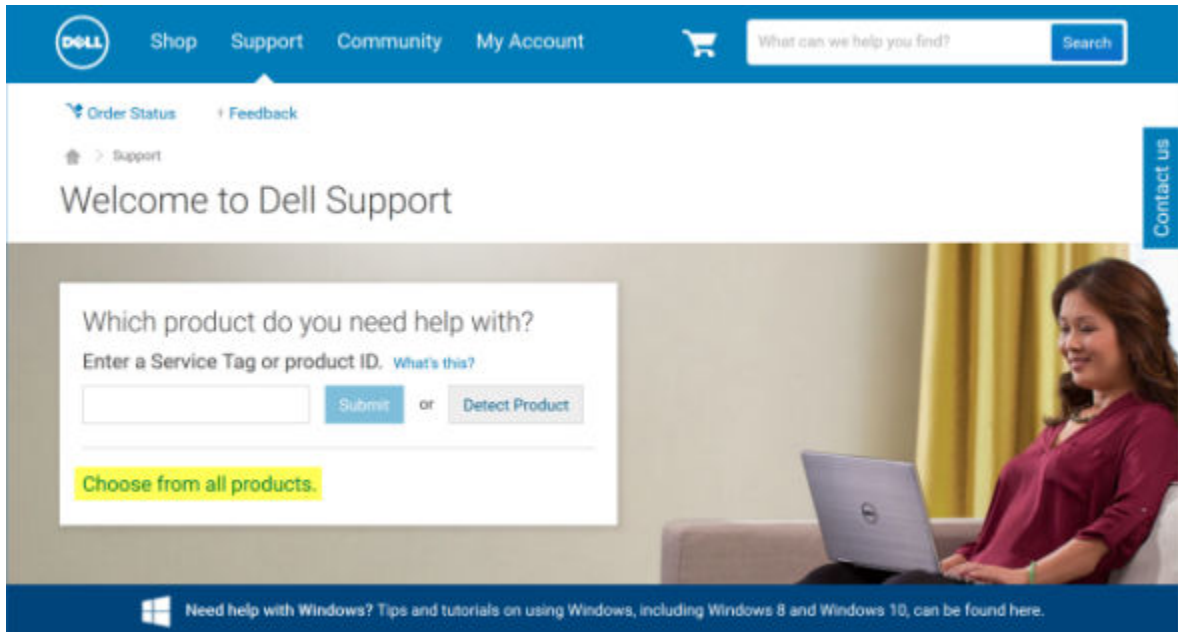


ソフトウェアのダウンロード

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

dell.com/support にアクセスして手順を開始します。

- 1 デルサポート Web ページで、**すべての製品から選択** を選択します。



- 2 製品のリストから **ソフトウェアおよびセキュリティ** を選択します。
- 3 ソフトウェアおよびセキュリティ セクションで、**エンドポイントセキュリティソリューション** を選択します。
一度行った選択はその後 Web サイトに記憶されます。
- 4 Dell Data Protection 製品を選択します。
例：

Dell Encryption

Dell Endpoint Security Suite

Dell Endpoint Security Suite Enterprise

- 5 **ドライバおよびダウンロード** を選択します。
- 6 目的のクライアントのオペレーティングシステムの種類を選択します。
- 7 一致項目で **Dell Data Protection (4 ファイル)** を選択します。これは一例ですので、実際には内容が一部異なる場合があります。たとえば、選択対象は 4 ファイルではない場合もあります。





- Support topics & articles
- Drivers & downloads
- Manuals

Optimize your system with drivers and updates. 1

View all available updates for Windows 10, 64-bit. [Change OS](#)

- Apple Mac OS
- VMware ESXi 5.1
- VMware ESXi 5.5
- VMware ESXi 6.0
- Windows 10, 32-bit
- Windows 10, 64-bit
- Windows 7, 32-bit
- Windows 7, 64-bit
- Windows 8, 32-bit
- Windows 8, 64-bit
- Windows 8.1, 32-bit
- Windows 8.1, 64-bit
- Windows Server 2003
- Windows Server 2003 x64
- Windows Server 2008 R2
- Windows Server 2008 x64
- Windows Server 2008 x86
- Windows Server 2012 R2

Looking for a different OS? [View the list of Dell supported operating systems](#)

Refine your results:

Category

Importance

Contact us

- ダウンロードまたは **My Download List #XX に追加** を選択します。
続行するには [Personal Edition](#) をインストールします。



Personal Edition のインストール 20

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

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 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 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。
- 詳細認証の各機能の使用方法については、「[」および「](#)」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。

インストール方法の選択

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

- マスターインストーラ - 推奨を使用した Personal Edition をインストールします。
- 子のインストーラを使用した Personal Edition をインストールします。

マスターインストーラ - 推奨を使用した Personal Edition をインストールします。

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

Dell Data Protection Installer は、複数のクライアントをインストールするため、一般的にマスターインストーラと呼ばれています。Personal Edition の場合は、暗号化クライアントした高度な認証クライアントをインストールします。

マスターインストーラユーザーインタフェースを使用してインストールする場合、Personal Edition は 1 度に 1 台のコンピュータにしかインストールできません。

マスターインストーラログファイルのあるで C:\programdata C:\program データ保護 \ インストーラです。

インストール方法を 1 つ選択してください。

[ユーザーインタフェースを使用したインストール](#)

[コマンドラインを使用したインストール](#)

ユーザーインタフェースを使用したインストール

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

それをローカルコンピュータにコピーします。

setup.exe をダブルクリックして、インストーラを起動します。

前提条件のインストールステータスを警告するダイアログが表示されます。これには数分かかります。



ようこそ画面で次へをクリックします。

ライセンス契約を読み、条項に同意して、**次へ** をクリックします。

Personal Edition をデフォルトの場所 C:\Program Files\Dell\Dell Data Protection にインストールするには、**次へ** をクリックします

セキュリティツールはデフォルトではインストールされ、選択解除します。これは、インストーラでは Security Framework として表示されます。詳細な認証はデフォルトではインストールされ、選択解除します。

次へ をクリックします。

インストール をクリックしてインストールを開始します。

ステータスウィンドウが表示されます。これには数分かかります。

[はい] を選択し、たいのマイコンピュータを今再起動) をクリックし、**完了** を押します。

コンピュータが再起動されたら、Windows の認証を行います。

Personal Edition および Security Tools のインストールが完了しました。

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

パーソナル・エディションセットアップウィザードと設定が終了したら、セキュリティツール管理者コンソールを起動します。

このセクションで詳細を複数のインストール作業の残りのとがスキップされる場合があります。続行するに [セキュリティツールおよび Personal Edition のセットアップ・ウィザード](#) を押します。

コマンドラインを使用したインストール

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

スイッチ

コマンドラインインストールには、まず最初にスイッチを指定する必要があります。次の表に、インストールで使用できるスイッチの詳細を示します。

スイッチ	意味
-y -gm2	Self-Extractor にデータを渡す
/S	サイレントモード
/z	InstallScript システム変数 CMDLINE にデータを渡す

パラメータ

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

代替インストール先への InstallPath=path。

機能 = PE

コマンドラインインストールの例

これらの例では再起動について書かれていませんが、最終的に再起動が必要になります。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。

空白などの特殊文字を 1 つ、または複数含む値は、エスケープされた引用符で囲むようにしてください。

コマンドラインは大文字と小文字を区別します。

次の例では、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 Personal Edition および Security Tools をインストールします。

```
DDPSetup.exe -y -gm2 /S /z "\"FEATURE=PE\""
```



次の例では、サイレントインストール、再起動なし、代替場所の C:\Program Files\Dell\My_New_Folder にインストールという設定で Personal Edition および Security Tools をインストールします。

```
DDPSetup.exe -y -gm2 /S /z "\"FEATURE=PE, InstallPath=C:\Program Files\Dell\My_New_Folder\""
```

コンピュータが再起動されたら、Windows の認証を行います。

Personal Edition および Security Tools のインストールが完了しました。

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

パーソナル・エディションセットアップウィザードと設定が終了したら、セキュリティツール管理者コンソールを起動します。

このセクションで詳細を複数のインストール作業の残りのとがスキップされる場合があります。続行するに [セキュリティツールおよび Personal Edition のセットアップ・ウィザード](#)を押します。

子のインストーラを使用した Personal Edition をインストールします。

子インストーラを使用して Personal Edition をインストールするには、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。「[マスターインストーラからの子インストーラの抽出](#)」を参照してください。完了したら、この項に戻ります。

コマンドラインでのアンインストール

コマンドラインのスイッチおよびパラメータは大文字と小文字を区別します。

コマンドラインで空白などの特殊文字を 1 つ、または複数含む値は、エスケープされた引用符で囲むようにしてください。

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 が作成する一意の子インストーラは、インストールのログファイルは、ユーザーがログインして %TEMP% にある C: ¥ Users ¥ UserName [<< -> ¥ AppData ¥ Local ¥ Temp とします

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。標準の .msi コマンドを使用して作成します。ログファイルで使用 /!*v c:\ [<< \n **すべてのディレクトリは c:\> <Quit を任意のログファイル名 -> ログインしてください。**

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で、/q と /qn の両方を使用しないでください。を使用してだけです！ および - /qb を指定した後です。

スイッチ	意味
/v	*.exe 内の .msi に変数を渡します。
/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	の再起動の進行状況] ダイアログで [キャンセル] ボタンを要求されます
/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!-	進捗状況ダイアログなしの キャンセル ボタンは、プロセスの完了後に、自体が再起動
/qn	ユーザーインタフェースなし

ドライバのインストール

Dell ControlVault、指紋リーダー、およびスマートカードのドライバとファームウェアは、マスターインストールまたは子インストールの実行ファイルには**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、<http://www.dell.com/support> で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。

Dell 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。

次の操作：

詳細な認証クライアントをインストールします

ユーザーは、Windows 資格情報を使用して PBA にログインします。

探しているファイルは、**C:\extracted\Security Tools** および **C:\extracted\Security Tools\Authentication** にあります。

コマンドラインインストールの例

\Security Tools

次の例では、サイレントインストール、再起動なし、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 Security Framework をインストールします。

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



SED クライアントは、v8.x の Advanced Authentication に必要です。

次の操作：

DDP | Security Tools Authentication

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 Security Tools をインストールします。

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

次の操作：

Encryption Client のインストール 67



暗号化クライアント 自分の組織が EnTrust または Verisign などのルート認証局によって署名された証明書を使用している場合は、暗号化クライアントレビューの要件。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。

ファイルは **C:\extracted\Encryption** にあります。

コマンドラインインストールの例

次の例では、オーバーレイアイコンを非表示、ダイアログなし、進捗状況バーなし、再起動なしという設定で Personal Edition、Encrypt for Sharing をインストールします。

```
DDPE_XXbit_setup.exe /s /v"HIDEOVERLAYICONS=1 REBOOT=ReallySuppress /qn"
```

コンピュータが再起動されたら、Windows の認証を行います。

Personal Edition および Security Tools のインストールが完了しました。Personal Edition のセットアップウィザードと構成は個別に説明します。

続行するに [セキュリティツール](#)および [Personal Edition のセットアップ・ウィザード](#)を押します。



セキュリティツールおよび Personal Edition セットアップウィザード

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

- 1 Uac ではアプリケーションを実行するよう求められる場合があります。その場合は、[はい] をクリックします。
- 2 初期インストールを再起動した後、次のセキュリティツールのアクティブ化) ウィザードが表示されます。次へ をクリックします。
- 3 新しい暗号化の管理者パスワード) を入力します。入力し再次へ をクリックします。
- 4 入力をバックアップの場所には、ネットワークドライブ、またはリムーバブルメディアに保存するためのリカバリ情報とクリックします次へ を押します。
- 5 **[適用] をクリックします**。ST アクティベーションを開始します。
- 6 [セキュリティツールをアクティベーションウィザードが終了すると、システムトレイにあるのアイコン。ddp から Personal Edition セットアップウィザードを起動します (上で独自の it 起動) があります。
セットアップウィザードは、このコンピュータ上の情報を保護するための暗号化の使用に役立ちます。このウィザードが完了していない場合は、暗号化は開始されます。

ようこそ画面を読み、次へ をクリックします。

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

次へ をクリックします。

- 8 Windows パスワードの警告を読み、確認します。この時点で Windows パスワードを作成する場合は、「
- 9 では、9-32 文字の暗号管理者パスワード eap を作成し、確認します。このパスワードには、英字、数字、および特殊文字を含める必要があります。このパスワードは、セキュリティツール用に設定して、eap と同じで構いません。そのに関連していませんこのパスワードを記録して、安全な場所に保管してください。次へ をクリックします。
- 10 **[参照] をクリックします**。ネットワークドライブまたはリムーバブルストレージは、暗号化キー (が exe アプリケーションという LSARecovery]_ [ホスト名] でラップされています。 \n する) を選択します。
コンピュータに特定の不具合が生じた場合、これらのキーがデータの回復に使用されます。

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

- ① **メモ:** 暗号化キーを手動でバックアップする方法については、ローカル管理コンソールの右上隅にある「> ヘルプ」を参照して、ローカルの管理コンソールの右上隅で、またはをクリックして スタート > すべてのプログラム > Dell > Dell Data Protection > [暗号化] > [暗号化のヘルプ] を押します。

次へ をクリックします。

- 11 暗号化設定の確認 画面に暗号化設定のリストが表示されます。設定を確認し、設定に問題がなければ **確認** をクリックします。
コンピュータの設定が開始されます。ステータスバーには、設定の進捗状況が表示されます。
- 12 **[完了] をクリックし** て設定を完了します。
- 13 再起動がコンピュータの暗号化用に設定すると必要があります。をクリックして **今すぐ再起動する** か、各 5X T20 分再起動を延期することができます。

- 14 コンピュータが再起動されたら、スタートメニューからのローカル管理コンソールを開きますの暗号化ステータスを参照してください。
暗号化はバックグラウンドで実行されます。ローカルの管理コンソールを開くか閉じることができます。ファイルの暗号化は、いずれの場合でも行われます。コンピュータは、暗号化中も通常どおり使用することができます。
- 15 スキャンが完了すると、コンピュータは複数回再起動します。
すべての暗号をスweepして、再起動が完了すると、ローカルの管理コンソールを起動してコンプライアンスの状態を確認することができます。ドライブは、コンプライアンス]で「でラベル付けされます。

[Security Tools 管理者設定の実行](#)に進みます。



Security Tools 管理者の設定

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

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

管理者パスワードおよびバックアップ場所の変更

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

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

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

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

認証の設定オプション

管理者設定認証 タブのコントロールでは、ユーザーサインインオプションを設定し、それぞれの設定をカスタマイズすることができます。

① **メモ:** TPM が存在せず、所有も有効化もされていない場合、ワンタイムパスワードはリカバリ オプション下に表示されません。

サインインオプションの設定

サインインオプション ページでは、ログオンポリシーを設定することができます。デフォルトでは、すべての対応資格情報が使用可能なオプション にリストされます。


サインインオプションを設定するには、次の手順を実行します。

左ペインの 認証 で、**サインインオプション** を選択します。

セットアップするロールを選択するには、**サインインオプションの適用先** : リストで、**ユーザー** または **管理者** 役割を選択します。このページで行った変更は、いずれも選択した役割のみに適用されます。

認証用に 使用可能なオプション を設定します。

デフォルトで、各認証方法は他の認証方法との組み合わせではなく、単独で使用されるように設定されています。デフォルトは、次の方法で変更できます。

認証オプションの組み合わせをセットアップするには、使用可能なオプション で  をクリックして、第 1 認証方法を選択します。使用可能なオプション ダイアログで、第 2 認証方法を選択して **OK** をクリックします。

例えば、ログオン資格情報として指紋とパスワードの両方を要求することができます。ダイアログで、指紋認証で使用する必要がある第 2 認証方法を選択します。

各認証方法を単独で使用できるようにするには、使用可能なオプション ダイアログで第 2 認証方法を **なし** のままにし、**OK** をクリックします。

サインインオプションを削除するには、サインインオプション ページの 使用可能なオプション の下で **X** をクリックしてその方法を削除します。

認証方法の新しい組み合わせを追加するには、**オプションの追加** をクリックします。

ロックアウトした場合にユーザーがコンピュータへのアクセスを回復するためのリカバリオプションを設定します。

ユーザーがコンピュータへのアクセスを回復するために質問と回答の一連を定義できるようにするには、**リカバリ質問** を選択します。

リカバリ質問を使用できないようにするには、このオプションの選択を解除します。

ユーザーがモバイルデバイスを使用してアクセスを回復できるようにするには、**ワンタイムパスワード** を選択します。ワンタイムパスワード (OTP) がリカバリ方法として選択されているときは、Windows ログオン画面でのサインインオプションとしては使用できません。

ログオンに OTP 機能を使用するには、リカバリオプションでそのオプションの選択を解除します。リカバリ方法としての選択が解除されると、少なくとも一名のユーザーが OTP に登録している限り、OTP オプションが Windows ログオンページに表示されます。



管理者は、ワンタイムパスワードの用途 (認証またはリカバリ) を制御できます。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。この設定は、サインインオプション フィールドの サインインオプションの適用先 での選択に応じて、コンピュータの全ユーザーまたは全管理者のどちらかに影響します。

ワンタイムパスワード オプションがリカバリオプション の下にリストされていない場合、お使いのコンピュータ設定はそのオプションをサポートしません。詳細については [要件](#) を参照してください。

ログオン資格情報を紛失したり忘れてしまった場合に、ユーザーがヘルプデスクに連絡することを必須とするには、リカバリオプション の下のリカバリ質問およびワンタイムパスワードの両方のボックスからチェックマークを外します。

ユーザーが認証資格情報を登録できる期間を設定するには、**猶予期間** を選択します。

猶予期間機能では、設定されたサインインオプションの執行を開始する日付を設定することができます。サインインオプションが執行される日付よりも前にサインインオプションを設定して、ユーザーの登録を許可する期間を設定します。デフォルトでは、ポリシーが即時に執行されます。

サインインオプションの執行日付を 即時 から変更するには、**猶予期間** ダイアログでドロップダウンメニューをクリックし、**指定日** を選択します。日付フィールドの右側の下矢印をクリックしてカレンダーを表示し、カレンダーで日付を選択します。ポリシーの執行は、選択した日付の午前 12 時 1 分ごろに開始されます。

次の Windows ログオン時に必要な資格情報を登録するためのリマインダをユーザーに表示する (デフォルト) または定期的なリマインダをセットアップすることもできます。その場合は、ユーザーのリマインダ ドロップダウンリストから、リマインダの間隔を選択します。



ユーザーに表示されるリマインダは、リマインダがトリガされたときにユーザーが Windows ログオン画面にいるか、Windows セッション中であるかに応じて若干異なります。リマインダは、起動前認証ログオン画面には表示されません。

猶予期間中の機能



指定した猶予期間中は、ユーザーが変更されたサインオンオプションを満たすために必要とされる最小限の資格情報をまだ登録していない場合、ログオンするたびに追加の資格情報通知が表示されます。メッセージの内容は、登録に使用可能な資格情報が他にもあります になります。

追加の資格情報が登録可能でも、それらが必須ではないという場合、このメッセージはポリシー変更後に一度だけ表示されます。

通知をクリックすると、状況に応じて次の操作が行われます。

資格情報が何も登録されていない場合は、管理者ユーザーによるコンピュータ関連の設定を可能にし、最も一般的な資格情報を登録する機能をユーザーに提供するセットアップウィザードが表示されます。

初回資格情報登録の後には、通知をクリックして DDP セキュリティコンソールにセットアップウィザードを表示します。

猶予期間期限切れ後の機能

どのような場合でも、猶予期間の期限が切れると、ユーザーはサインオンオプションによって必要とされる資格情報を登録せずにログオンすることができなくなります。ユーザーがサインオンオプションを満たさない資格情報または資格情報の組み合わせでログオンしようとすると、Windows ログオン画面の上にセットアップウィザードが表示されます。

ユーザーが必要な資格情報を正常に登録した場合は、Windows にログインされます。

必要な資格情報を正常に登録しなかった、またはウィザードをキャンセルした場合、ユーザーは Windows ログオン画面に戻ります。

選択された役割の設定を保存するには、**適用** をクリックします。

Password Manager 認証の設定

Password Manager ページでは、Password Manager マネージャーへのユーザーの認証方法を設定することができます。

Password Manager 認証を設定するには、次の手順を実行します。


左ペインの 認証 で、**Password Manager** を選択します。

セットアップするロールを選択するには、**サインオンオプションの適用先** : リストで、**ユーザー** または **管理者** 役割を選択します。このページで行った変更は、いずれも選択した役割のみに適用されます。

オプションで **認証を必須としない** チェックボックスを選択して、選択されたユーザー役割が、Password Manager に保管されている資格情報を用いてすべてのソフトウェアアプリケーションおよびインターネットウェブサイト自動的にログオンできるようにします。

認証用に 使用可能なオプション を設定します。

デフォルトで、各認証方法は他の認証方法との組み合わせではなく、単独で使用されるように設定されています。デフォルトは、次の方法で変更できます。

認証オプションの組み合わせをセットアップするには、使用可能なオプション で  をクリックして、第 1 認証方法を選択します。使用可能なオプション ダイアログで、第 2 認証方法を選択して **OK** をクリックします。

例えば、ログオン資格情報として指紋とパスワードの両方を要求することができます。ダイアログで、指紋認証で使用する必要がある第 2 認証方法を選択します。

各認証方法を単独で使用できるようにするには、使用可能なオプション ダイアログで第 2 認証方法を **なし** のままにし、**OK** をクリックします。

サインオンオプションを削除するには、サインオンオプション ページの 使用可能なオプション の下で **X** をクリックしてその方法を削除します。

認証方法の新しい組み合わせを追加するには、**オプションの追加** をクリックします。

選択した役割の設定を保存するには、**適用** をクリックします。



: 元の値に設定を復元するには、**デフォルト ボタン**を選択します。

リカバリ質問の設定

リカバリ質問 ページでは、ユーザーが個人用のリカバリ質問および回答を定義するときに、どの質問を提示するかを選択することができます。リカバリ質問を使用することにより、ユーザーは、パスワードの期限が切れた、またはパスワードを忘れた場合に、コンピュータへのアクセスを回復できるようになります。

リカバリ質問を設定するには、次の手順を実行します。

左ペインの 認証 で、**リカバリ質問** を選択します。

リカバリ質問 ページでは、少なくとも 3 つの事前定義済みリカバリ質問を選択します。

オプションとして、ユーザーが質問を選択するリスト内に最大 3 つのカスタム質問を追加できます。

リカバリ質問を保存するには、**適用** をクリックします。

指紋スキャン認証の設定

指紋スキャン認証を設定するには、次の手順を実行します。

左ペインの 認証 で、**指紋** を選択します。

登録 で、ユーザーが登録できる指の最少数および最大数を設定します。

指紋スキャン感度を設定します。

感度を下げると、許容可能な差異と不正スキャン受入の可能性が増加します。最高設定では、システムが正当な指紋を拒否する可能性があります。感度設定を上げると、他人受入率が 1 / 10,000 スキャンまで低下します。

指紋リーダーのバッファからすべての指紋のスキャンと資格情報登録を削除するには、**リーダーのクリア** をクリックします。これにより、現在追加しているデータのみが削除されます。前のセッションで保管されたスキャンおよび登録内容は削除されません。

設定を保存するには、**適用** をクリックします。

ワンタイムパスワード認証の設定



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。TPM の設定方法については、「ワンタイムパスワードのインストール前の設定」を参照してください。

ワンタイムパスワード機能を使用するには、モバイルデバイス上の Security Tools Mobile アプリケーションを使用してワンタイムパスワードを生成し、コンピュータにそのパスワードを入力します。パスワードは 1 度しか使用できず、有効期限も限定されています。

セキュリティをさらに向上させるため、管理者は、パスワードを必須とすることによってモバイルアプリケーションのセキュリティを確保することができます。

モバイルデバイス ページでは、モバイルデバイスのセキュリティをさらに向上させる設定と、ワンタイムパスワードを設定できます。

ワンタイムパスワード認証を設定するには、次の手順を実行します。

左ペインにある 認証 で **モバイルデバイス** を選択します。

ユーザーが Security Tools Mobile アプリケーションにアクセスするときに、パスワードの入力を必須にする場合は、**パスワードを必須にする** を選択します。



モバイルデバイスをコンピュータに登録した後で パスワードを必須にする ポリシーを有効化すると、すべてのモバイルデバイスの登録が解除されます。ユーザーは、このポリシーを有効化した後、モバイルデバイスを再登録する必要があります

パスワードを必須にする チェックボックスが選択されている場合、ユーザーは、Security Tools Mobile アプリにアクセスするために、使用しているモバイルデバイスをロック解除する必要があります。モバイルデバイスにデバイスロックがない場合、パスワードが必要になります。

ワンタイムパスワード (OTP) の長さを選択するには、**ワンタイムパスワードの長さ** で、必須とするパスワード文字数を選択します。

ユーザーがワンタイムパスワードを正しく入力するための試行回数を選択するには、**許可されるユーザーサインイン試行回数** で **5 ~ 30** の数値を選択します。

最大試行回数に到達すると、ユーザーがモバイルデバイスを再登録するまで、OTP 機能が無効化されます。



デルでは、ワンタイムパスワードに加え、その他の追加認証方法を少なくともひとつセットアップすることをお勧めします。



スマートカード登録の設定

DDP|Security Tools は、接触型および非接触型の 2 種類のスマートカードをサポートしています。

接触型カードでは、カードを挿入するスマートカードリーダーが必要です。接触型カードとの互換性があるのは、ドメインコンピュータのみです。CAC および SIPRNet カードは、どちらも接触型カードです。これらのカードの高度な機能性のため、ユーザーがログオンするには、カード挿入後に証明書の選択が必要となります。

非接触型カードは、非ドメインコンピュータ、およびドメイン仕様で設定されたコンピュータによってサポートされています。

ユーザーは、ユーザーアカウントごとに 1 枚の接触型スマートカードを登録するか、アカウントごとに複数の非接触型カードを登録することができます。

スマートカードは起動前認証ではサポートされません。



複数のカードが登録されたアカウントからひとつのスマートカード登録を削除するときは、すべてのカードが同時に登録解除されます。

スマートカード登録を設定するには、次の手順を実行します。

管理者設定ツールの認証 タブで **スマートカード** を選択します。

詳細な許可の設定

詳細 をクリックして、詳細エンドユーザーオプションを変更します。詳細 では、ユーザーに対して、資格情報の自己登録をオプションとして許可、またはユーザー自身の登録済み資格情報の変更をオプションとして許可し、ワンステップログオンを有効にできます。

次のチェックボックスを選択または選択解除します。

ユーザーに資格情報の登録を許可する - このチェックボックスはデフォルトで選択されています。ユーザーは、管理者の介入なしで資格情報を登録することが許可されます。このチェックボックスの選択を解除すると、管理者による資格情報の登録が必要になります。

ユーザーに登録済み資格情報の変更を許可する - このチェックボックスはデフォルトで選択されています。これが選択されていると、ユーザーは、管理者の介入なしでそれぞれの登録済み資格情報を変更および削除することが許可されます。このチェックボックスの選択を解除すると、一般ユーザーは資格情報を変更または削除できなくなり、管理者が変更または削除する必要があります。



ユーザーの資格情報を登録するには、管理者設定 ツールの ユーザー ページに移動し、ユーザーを選択して登録 をクリックします。

ワンステップログオンを許可する - ワンステップログオンとは、シングルサインオン (SSO) のことです。このチェックボックスはデフォルトで選択されています。この機能を有効にすると、ユーザーが資格情報を入力する必要があるのは、起動前認証 画面のみとなります。ユーザーは、Windows に自動的にログオンされます。このチェックボックスを選択解除すると、ユーザーは複数回ログオンする必要が生じる場合があります。



このオプションは、ユーザーに資格情報の登録を許可する 設定が選択されていない限り、選択できません。

終了したら **適用** をクリックします。

ユーザー認証の管理

管理者設定認証 タブのコントロールでは、ユーザーログオンオプションを設定し、それぞれの設定をカスタマイズすることができます。

ユーザー認証を管理するには、次の手順を実行します。

- 1 **管理者設定** タイルを管理者としてクリックします。
- 2 **ユーザー** タブをクリックしてユーザーを管理し、ユーザー登録ステータスを表示します。このタブでは、次の操作を実行することができます。

- 新規ユーザーの登録
- 資格情報の追加または変更
- ユーザーの資格情報の削除

① **メモ:**

サインイン および **セッション** には、ユーザーの登録ステータスが表示されます。

サインイン ステータスが **OK** のときは、ユーザーがログオンするために必要なすべての登録が完了しています。**セッション** ステータスが **OK** のときは、ユーザーが Password Manager を使用するために必要なすべての登録が完了しています。

どちらのステータスが **いいえ** になっている場合でも、ユーザーは追加の登録作業を完了する必要があります。どの登録がまだ必要かを確認するには、**管理者設定** ツールを選択し、**ユーザー** タブを開きます。灰色のチェックマークボックスは、登録が完了していないことを示します。または、**登録** タイルをクリックし、**ステータス** タブで必要な登録がリストされている **ポリシー** 列を見直します。

新規ユーザーの追加



新しい Windows ユーザーは、Windows にログオン、または資格情報を登録するときに自動で追加されます。

既存の Windows ユーザーの登録プロセスを開始するには、**ユーザーの追加** をクリックします。

ユーザーの選択 ダイアログが表示されたら、**オブジェクトタイプ** を選択します。

ユーザーのオブジェクト名をテキストボックスに入力し、**名前のチェック** をクリックします。

終了したら **OK** をクリックします。

登録ウィザードが開きます。

続いて **ユーザー資格情報の登録または変更** に移動して指示を表示します。

ユーザー資格情報の登録または変更

管理者は、ユーザーの代理としてユーザーの資格情報を登録または変更できますが、リカバリ質問やユーザーの指紋のスキャンなど、いくつかの登録アクティビティにはユーザーの参加が必要です。

ユーザー資格情報を登録または変更するには、次の手順を実行します。

管理者設定 で **ユーザー** タブをクリックします。

ユーザー ページで **登録** をクリックします。

ようこそ ページで **次へ** をクリックします。

認証が必要です ダイアログでユーザーの Windows パスワードを使用してログインし、**OK** をクリックします。

ユーザーの Windows パスワードを変更するには、パスワード ページで新規パスワードを入力して確認し、**次へ** をクリックします。

パスワードの変更をスキップするには、**スキップ** をクリックします。ウィザードでは、資格情報を登録しない場合、その資格情報をスキップすることができます。前のページに戻るには、**戻る** をクリックします。

各ページの手順に従って、適切なボタン (**次へ**、**スキップ**、**戻る**) をクリックします。

サマリ ページで登録した資格情報を確認し、登録が完了したら **適用** をクリックします。

資格情報登録 ページに戻って変更を行うには、変更するページが表示されるまで **戻る** をクリックします。


資格情報の登録または変更の詳細については、『コンソールユーザーガイド』を参照してください。




1つの登録済み資格情報の削除

管理者設定 タイルをクリックします。

ユーザー タブをクリックし、変更するユーザーを見つけます。

削除する資格情報の緑色のチェックマーク上にカーソルを合わせます。チェックマークが  に変わります。

 シンボルをクリックしてから **はい** をクリックして削除を確認します。



:これがユーザーの唯一の登録済み資格情報である場合は、この方法で削除することはできません。さらに、この方法でパスワードを削除することもできません。ユーザーのコンピュータへのアクセスを完全に削除するには、remove コマンドを使用してください。

ユーザーのすべての登録済み資格情報の削除

管理者設定 タイルをクリックします。

ユーザー タブをクリックし、削除するユーザーを見つけます。

削除 をクリックします。(remove コマンドは、ユーザーの設定の下部に赤色で表示されます。)

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

子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、その後でクライアントは、**アンインストールの失敗を防止するために特定の順序**でアンインストールする必要があります。
- 手順の説明をに **抽出**します。マスターインストーラから子インストーラの子インストーラを入手します。
- 必ずインストールと同じバージョンのクライアントをアンインストールにも使用してください。
- この章では意味を別の章を含む **詳細な** 指示子のインストーラのアンインストール方法の。この章で説明している手順の最後で **のみ**、マスターインストーラをアンインストールします。

クライアントを以下の順序でアンインストールします。

- 1 Encryption クライアントのアンインストール 74
- 2 DDP | Client Security Framework
- 3 **詳細な認証をアンインストールしてください。**

ドライバパッケージをアンインストールする必要はありません。

続行を **選択**するには、**アンインストールの方法**を押します。

インストール方法の選択

あるがマスターインストーラをアンインストールするには 2 つの方法を選択します。 **いずれかの** 次のと

- からの追加 / 削除プログラムをアンインストールします
- コマンドラインからのアンインストール

からの追加 / 削除プログラムをアンインストールします

移動をアンインストールするプログラムで、Windows のコントロールパネル (**スタート > コントロールパネル > プログラムと機能を > アンインストールするプログラム**)。)

Dell Data Protection Installer をハイライト表示して **変更** を左クリックし、セットアップウィザードを起動します。

ようこそ画面を読み、**次へ** をクリックします。

プロンプトに従ってアンインストールを実行し、**終了** をクリックします。

コンピュータを再起動して、Windows にログインします。

マスターのインストーラがアンインストールされます。

コマンドラインからのアンインストール

次の例は、SED クライアントをサイレントアンインストールします。

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

終了したらコンピュータを再起動します。

マスターのインストーラがアンインストールされます。



子インストーラを使用したアンインストールを続行します。



子インストーラを使用したアンインストール

- 復号とアンインストールを実行するユーザーは、ローカルまたはドメイン管理者ユーザーである必要があります。コマンドラインでアンインストールする場合は、ドメイン管理者の資格情報が必要です。
- マスターのインストーラで Personal Edition をインストールする場合は、子の実行可能ファイルを最初にアンインストールする前に、マスターインストーラから抽出する必要があります。に示すように、[マスターインストーラから子のインストーラを解凍します](#)。
- 必ずインストールと同じバージョンのクライアントをアンインストールにも使用してください。
- 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。
- ファイルのロックが原因で復号化エラーが発生する可能性を最小限に抑えるために、すべてのプロセスおよびアプリケーションをシャットダウンします。

Encryption クライアントのアンインストール

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

インストール方法の選択

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

[ユーザーインターフェースを使用したアンインストール](#)

[コマンドラインからのアンインストール](#)

ユーザーインターフェースを使用したアンインストール

移動をアンインストールするプログラムで、Windows のコントロールパネル ([スタート > コントロールパネル > プログラムと機能を > アンインストールするプログラム](#))。).

Encryption をハイライト表示し、**変更** を左クリックして Personal Edition セットアップウィザードを起動します。

ようこそ画面を読み、**次へ** をクリックします。

Encryption Removal Agent のインストール画面で、次のいずれかを選択します。



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

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

Sde、ユーザー、または共通の暗号化のため、このオプションは、暗号化クライアントファイルをアンインストールします。複合化します。これは、**推奨される選択を押します**。

Encryption Removal Agent をインストールしない



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

次へ をクリックします。

バックアップファイル テキストボックスで、バックアップファイルのネットワークドライブまたはリムーバブルストレージの場所へのパスを入力、またはファイルフォーマットは LSARecovery_[ホスト名].exe です。

[パスワード] テキストボックスに、暗号化の管理者パスワードを入力します。これは、ソフトウェアをインストールするとき、セットアップウィザードで設定したパスワードです。

次へ をクリックします。

にある Dell 復号をエージェントサービスとしてログオン] 画面には、2 つのオプションがあります。**ローカルシステムアカウント** を選択します。**終了** をクリックします。

[プログラムの削除画面で、削除をクリックします。

設定完了 画面で

コンピュータを再起動して、Windows にログインします。

復号化が進行中です。

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

コマンドラインからのアンインストール

コマンドラインのスイッチおよびパラメータは大文字と小文字を区別します。

コマンドラインで空白などの特殊文字を 1 つ、または複数含む値は、エスケープされた引用符で囲むようしてください。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 が作成する一意の子のインストーラのアンインストールログファイル用のユーザーがログインして %TEMP% にある C: ¥ Users ¥ UserName [<< -> ¥ AppData ¥ Local ¥ Temp とします

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。標準の .msi コマンドを使用して作成します。ログファイルで使用 /! c:\ [<< \n **すべてのディレクトリは c:\> <Quit を任意のログファイル名 -> ログインしてください。**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、特に断りがない限り、コマンドラインでのアン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で、/q と /qn の両方を使用しないでください。を使用してください！ および - /qb を指定した後です。

スイッチ	意味
/v	setup.exe 内の .msi に変数を渡します。
/s	サイレントモード
/x	アンインストールモード

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

Encryption クライアントインストーラは、マスターインストーラから抽出された後、C:\extracted\Encryption\DDPE_XXbit_setup.exe にあります。次の表に、アンインストールで使用できるパラメータの詳細を示します。

パラメータ	選択
CMG_DECRYPT	Encryption Removal Agent のインストールタイプを選択するためのプロパティ : 2 - フォレンジックキーのバンドルを使用してキーを取得する 0 - Encryption Removal Agent をインストールしない
CMGSILENTMODE	サイレントアンインストールのプロパティ 1 - サイレント 0 - 非サイレント
Da_customize KM (CLEAR_PW)	フォレンジック管理者アカウントのパスワード。
Da_customize KM _ パス	キーマテリアルのバンドルをパスします。

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

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

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

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

終了したらコンピュータを再起動します。

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

高度な認証をアンインストールします。

インストール方法の選択

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

ユーザーインタフェースを使用したアンインストール



コマンドラインからのアンインストール

ユーザーインターフェースを使用したアンインストール

移動をアンインストールするプログラムで、Windows のコントロールパネル (**スタート > コントロールパネル > プログラムと機能を > アンインストールするプログラム**)。

Security Tools Authentication をハイライト表示して **変更** を左クリックし、セットアップウィザードを起動します。

ようこそ画面を読み、**次へ** をクリックします。

管理者パスワードを入力します。

プロンプトに従ってアンインストールを実行し、**終了** をクリックします。

コンピュータを再起動して、Windows にログインします。

Security Tools Authentication がアンインストールされました。

コマンドラインからのアンインストール

マスターインストーラから抽出された高度な認証クライアントインストーラを配置するには、C: ¥ \ セキュリティツール ¥ 認証 ¥ [<< x64 または x86 -> X:\setup.exe 解凍してください。

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。

続行するには、[ポリシーとテンプレートの説明](#)。

Client Security Framework のアンインストール

インストール方法の選択

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

[ユーザーインターフェースを使用したアンインストール](#)

[コマンドラインからのアンインストール](#)

ユーザーインターフェースを使用したアンインストール

移動をアンインストールするプログラムで、Windows のコントロールパネル (**スタート > コントロールパネル > プログラムと機能を > アンインストールするプログラム**)。

Client Security Framework をハイライト表示して **変更** を左クリックし、セットアップウィザードを起動します。

ようこそ画面を読み、**次へ** をクリックします。

プロンプトに従ってアンインストールを実行し、**終了** をクリックします。

コンピュータを再起動して、Windows にログインします。

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

コマンドラインからのアンインストール

Cloud Edition クライアントインストーラは、マスターインストーラから抽出された後、C:\extracted\Cloud\Cloud_。

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。

「ポリシーテンプレートの説明」

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

ポリシー

ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての基本的な保護 (デフォルト)	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
------	----------------------------	------------------	------------	--------------------	------------------------------------	---------------------	--------------------	------------------	-------	----

固定ストレージポリシー

SDE 暗号化有効	True								False	このポリシーは、他のすべての System Data Encryption (SDE) ポリシーに対する「マスターポリシー」となります。このポリシーが False の場合は、他のポリシーの値に関わらず、SDE 暗号化は一切実行されません。 値が True の場合は、他の Intelligent Encryption ポリシーによって暗号化されなかったすべてのデータが SDE 暗号化ルールポリシーに従って暗号化されることになります。 このポリシーの値の変更には、再起動が必要です。
SDE 暗号化アルゴリズム	AES256									AES 256、AES 128、3DES
SDE 暗号化ルール										特定のドライブ、ディレクトリ、およびフォルダを暗号化または復号化するために使用する暗号化ルールです。 デフォルト値の変更に関して不明な点がある場合は、カスタムサポートに連絡してサポートを受けてください。

一般設定ポリシー



ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての積極的な保護 (デフォルト)	固定ドライブすべての基本的な保護	システムドライブのみに対する基本的保護	外部ドライブに対する基本的な保護	暗号化無効	説明
暗号化有効	True							False		<p>このポリシーは、すべての一般設定ポリシーに対する「マスターポリシー」となります。値を False にすると、他のポリシーの値に関わらず、暗号化は一切実行されません。</p> <p>値を True にすると、すべての暗号化ポリシーが有効になります。</p> <p>このポリシーの値を変更すると、ファイルを暗号化 / 復号化するための新たなスイープがトリガされます。</p>
共通の暗号化フォルダ										<p>文字列 - それぞれ 500 文字のエントリを最大 100 件 (最大 2048 文字)</p> <p>暗号化される、または暗号化から除外されるエンドポイントドライブ上のフォルダのリストで、エンドポイントへのアクセス権を持つすべての管理対象ユーザーがアクセスできるようにします。</p> <p>使用可能なドライブ文字は次のとおりです。</p> <p># : すべてのドライブを示します。</p> <p>f# : すべての固定 (非リムーバブル) ドライブを示します。</p> <p>すべてのリムーバブルドライブを示します</p> <p>重要 : ディレクトリ保護を上書きすると、コンピュータが起動不能になったり、ドライブの再フォーマットが必要になったりする可能性があります。</p> <p>このポリシーとユーザー暗号化フォルダポリシーの両方で同じフォルダが指定された場合は、このポリシーが優先されます。</p>
共通の暗号化アルゴリズム	AES256									<p>AES 256、Rijndael 256、AES 128、Rijndael 128、3DES</p> <p>システムページングファイルは AES 128 を使用して暗号化されます。</p>



ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての積極的な保護 (デフォルト)	固定ドライブすべての積極的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
アプリケーションデータ暗号化リスト	winword.exe excel.exe powerpnt.exe msaccess.exe winproj.exe outlook.exe acrobat.exe visio.exe mspub.exe notepad.exe wordpad.exe winzip.exe winrar.exe onenote.exe onenotem.exe									<p>文字列 - それぞれ 500 文字のエントリを最大 100 件</p> <p>予期しない、または意図しない結果が発生する可能性があるため、explorer.exe および iexplorer.exe は ADE リストに追加しないことをお勧めします。ただし、explorer.exe は、右クリックメニューを使用してデスクトップ上に新規の Notepad ファイルを作成するために使用されるプロセスです。ADE リストの代わりにファイル拡張子で暗号化を設定すると、より包括的に対象を指定できます。</p> <p>新規ファイルを暗号化するアプリケーションのプロセス名を、キャリッジリターンで区切ってリストします (パスなし)。ワイルドカードは使用しないでください。</p> <p>弊社では、システムクリティカルなファイルに書き込みを行うようなアプリケーションまたはインストーラはリストしないことを推奨しています。リストに含めると、重要なシステムファイルが暗号化されて Windows エンドポイントを起動不能にするおそれがあります。</p> <p>一般的なプロセス名 :</p> <p>Outlook.exe、winword.exe、frontpg は \n し、Setup.exe、powerpnt.exe exe、msaccess.exe exe、wordpad、setup.exe、mspaint は、setup.exe、Excel の Explorer.exe</p> <p>以下のハードコーディングされたシステムおよびインストーラプロセス名は、このポリシーに指定しても無視されます。</p> <p>Hotfix.exe、setup.exe をクリックし、setup.exe、msiexec.exe wuauclt は、setup.exe、wmiprvse.exe を更新して、setup.exe を実行するには、a2 unregmp は、setup.exe ikernel は、setup.exe wssetup は、</p>



ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての積極的な保護 (デフォルト)	固定ドライブすべての基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
アプリケーション共通 ンデータ暗 号化キー										<p>setup.exe svchost setup.exe を移行するには</p> <p>共通またはユーザー</p> <p>アプリケーションデータ暗号化リストで暗号化されたファイルにアクセスできるユーザーと、その場所を指定するキーを選択します。</p> <p>すべての管理対象ユーザーが、ファイルが作成されたエンドポイント上でそれらファイルにアクセスすることができます (共通暗号化フォルダと同じアクセスレベル)。共通の暗号化アルゴリズムで暗号化されるようにする場合は共通を選択します。</p> <p>ファイルを作成したユーザーのみが、ファイルが作成されたエンドポイント上のみでそれらのファイルにアクセスすることができます (ユーザー暗号化フォルダと同じアクセスレベル)。ユーザー暗号化アルゴリズムで暗号化されるようにする場合はユーザーを選択します。</p> <p>このポリシーに対する変更は、このポリシーによってすでに暗号化されているファイルには影響しません。</p>
Outlook Personal フォルダの暗号化	True							False		True に設定すると、Outlook Personal フォルダが暗号化されません。
一時ファイルの暗号化	True							False		True に設定すると、環境変数 TEMP および TMP に登録されたパスが、ユーザーデータ暗号化キーで暗号化されます。
インターネット一時ファイルの暗号化	True	False								<p>True に設定すると、環境変数 CSIDL_INTERNET_CACHE にリストされたパスが、ユーザーデータ暗号化キーで暗号化されません。</p> <p>暗号化スweep時間を短縮するため、クライアントは初期暗号化のための CSIDL_INTERNET_CACHE の</p>



ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての積極的な保護 (デフォルト)	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本的保護	外部ドライブに対する基本的な保護	暗号化無効	説明
										内容に加え、このポリシーへのアップデートもクリアします。
										このポリシーは、Microsoft Internet Explorer を使用する場合にのみ適用できます。
ユーザープロファイルの暗号化	True								False	True に設定すると、次の内容が暗号化されます。 <ul style="list-style-type: none"> ・ ユーザープロファイル (C:\Users\jsmith)(ユーザーデータ暗号化キーを使用) ・ Windows 7 の \Users\Public (共通暗号化キーを使用)
Windows ページングファイルの暗号化	True								False	True に設定すると、Windows ページングファイルが暗号化されます。このポリシーに対する変更には、再起動が必要です。
管理対象サービス										文字列 - それぞれ 500 文字のエントリを最大 100 件 (最大 2048 文字) サービスがこのポリシーによって管理されているときは、ユーザーがログインし、クライアントのロックが解除された後でのみ、サービスが起動されます。また、このポリシーは、ログオフ中にクライアントがロックされる前に、このポリシーによって管理されているサービスが停止されることを確実にします。このポリシーは、サービスが無反応の場合におけるユーザーログオフを防ぐことも可能です。 構文は、1 行ごとに 1 つのサービス名となります。サービス名では空白がサポートされています。 ワイルドカードはサポートされていません。 管理対象外のユーザーがログオンすると、管理対象サービスは起動しません。
暗号化後クリーンアップのセキュア化	3 パス上書き	1 パス上書き								上書きなし 上書きなし、1 パス上書き、3 パス上書き、7 パス上書き



ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての積極的な保護 (デフォルト)	固定ドライブすべての基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
										<p>このポリシーは、このカテゴリ内のその他のポリシーによって指定されたフォルダが暗号化された後で、オリジナルのファイルの暗号化されていない剰余の処理方法を決定します。</p> <ul style="list-style-type: none"> ・上書きなしの場合、剰余は削除されます。この値に設定すると、暗号化処理が最速になります。 ・1パス上書きの場合、剰余はランダムなデータで上書きされます。 ・3パス上書きの場合、剰余は1と0の標準パターンで上書きされた後、その補数で上書きされ、次にランダムなデータで上書きされます。 ・7パス上書きの場合、剰余は1と0の標準パターンで上書きされた後、その補数で上書きされ、次にランダムなデータで5回上書きされます。この値に設定すると、元のファイルをメモリから回復することが最も難しくなり、暗号化処理が最もセキュアになります。
Windows 休止状態ファイルのセキュア化	True				False		True	False		有効にした場合、コンピュータが休止状態に入るときにのみ休止状態ファイルが暗号化されます。コンピュータが休止状態から復帰すると Shield によって保護が解除され、コンピュータの使用中にユーザーまたはアプリケーションに影響することなく保護が提供されます。
非セキュアな休止状態の防止	True				False		True	False		選択した場合、クライアントは、休止状態データを暗号化できないと、コンピュータの休止状態を許可しません。
ワークステーションのスキューン優先度	高	標準								最高、高、標準、低、最低 暗号化フォルダスキャンの相対的な Windows 優先順位を指定します。
ユーザー暗号化フォルダ										文字列 - それぞれ 500 文字のエントリを最大 100 件 (最大 2048 文字)

ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての積極的な保護 (デフォルト)	固定ドライブすべての基本的な保護	システムドライブのみに対する基本的な保護	外部ドライブに対する基本的な保護	暗号化無効	説明
										<p>ユーザーデータ暗号化キーを使用して暗号化する、または暗号化から除外するエンドポイントハードドライブ上のフォルダのリスト。</p> <p>このポリシーは、Windows によってハードディスクドライブとして分類されたすべてのドライブに適用されます。タイプがリムーバブルディスクとして表示されるドライブまたは外部メディアの暗号化にこのポリシーを使用することはできません。代わりに、外部メディアの EMS 暗号化を使用してください。</p>
ユーザー暗号化アルゴリズム	AES256									<p>AES 256、Rijndael 256、AES 128、Rijndael 128、3DES</p> <p>個々のユーザーレベルでのデータの暗号化に使用される暗号化アルゴリズムです。同じエンドポイントのユーザーごとに異なる値を指定できます。</p>
ユーザーデータ暗号化キー	ユーザー	共通			ユーザー	共通			ユーザー	<p>共通またはユーザー</p> <p>次のポリシーで暗号化されたファイルにアクセスできるユーザーと、その場所を指定するキーを選択します。</p> <ul style="list-style-type: none"> ・ユーザー暗号化フォルダ ・ Outlook Personal フォルダの暗号化 テンポラリー・ファイル (¥ Documents and Settings ¥ username ¥ Local Settings ¥ temp のみ) を暗号化する ・ インターネット一時ファイルの暗号化 ・ ユーザープロファイルドキュメントの暗号化 <p>次を選択します。</p> <ul style="list-style-type: none"> ・ すべての管理対象ユーザーが、ファイルが作成されたエンドポイント上でユーザー暗号化ファイル / フォルダにアクセスすることができ (共通暗号化フォルダと同じアク



ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての積極的な保護 (デフォルト)	固定ドライブすべての基本的な保護	システムドライブのみに対する基本的保護	外部ドライブに対する基本的な保護	暗号化無効	説明
------	----------------------------	------------------	------------	--------------------	------------------------------------	------------------	---------------------	------------------	-------	----

セスレベル)、共通の暗号化アルゴリズムで暗号化されるようにする場合は共通を選択します。

・ファイルを作成したユーザーのみが、ファイルが作成されたエンドポイント上のみでそれらのファイルにアクセスすることができ(ユーザー暗号化フォルダと同じアクセスレベル)、ユーザー暗号化アルゴリズムで暗号化されるようにする場合はユーザーを選択します。

ディスクパーティション全体を暗号化する暗号化ポリシーの組み入れを選択する場合は、共通またはユーザーの暗号化ポリシーではなく、デフォルトの SDE 暗号化ポリシーを使用することをお勧めします。これにより、管理対象ユーザーがログインしていない状態でも、暗号化された任意のオペレーティングシステムファイルに確実にアクセスできるようになります。

Hardware Crypto Accelerator (v8.9.1 Encryption クライアントにより v8.3 でのみサポート)

Hardware Crypto Accelerator (HCA) False

このポリシーは、その他すべての Hardware Crypto Accelerator (HCA) ポリシーに対する「マスターポリシー」となります。このポリシーが False の場合は、他のポリシーの値に関わらず、HCA 暗号化は一切実行されません。

HCA ポリシーを使用できるのは、Hardware Crypto Accelerator を搭載するコンピュータのみです。

暗号化のターゲットとなるボリューム すべての固定ボリューム

すべての固定ボリュームまたはシステムボリュームのみ

暗号化のターゲットとなるボリュームを指定します。

HCA 暗号化ドライブで使用できるフォレンジックメタデータ False

True または False

True に設定すると、フォレンジックを容易にするためにフォレンジックメタデータがドライブに包含されません。包含されるメタデータ:

- 現在のマシンのマシン ID (MCID)



ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての積極的な保護 (デフォルト)	固定ドライブすべての基本的な保護	システムドライブのみに対する基本的な保護	外部ドライブに対する基本的な保護	暗号化無効	説明
セカンダリドライブ暗号化のユーザー承認の許可	False									<ul style="list-style-type: none"> 現在の Shield インストールのデバイス ID (DCID/SCID) <p>False に設定すると、フォレンジックメタデータはドライブに包含されません。</p> <p>False から True に変更すると、HCA ポリシーに基づいて再スリープされ、フォレンジックが追加されます。</p> <p>True に設定すると、ユーザーが追加ドライブを暗号化するかどうかを決定することができます。</p>
暗号化アルゴリズム	AES256									AES 256 または AES 128
ポート制御ポリシー										
ポート制御システム	無効									<p>すべてのポート制御システムポリシーを有効または無効にします。このポリシーが無効に設定されている場合、その他のポート制御システムポリシーに関わらず、ポート制御システムポリシーは適用されません。</p> <p>メモ： PCS ポリシーを有効にするには、再起動が必要です。</p>
ポート： ExpressCard スロット	有効									ExpressCard スロットを介して公開されているポートを有効化、無効化、またはバイパスします。
ポート： eSATA	有効									外部 SATA ポートに対するポートアクセスを有効化、無効化、またはバイパスします。
ポート： PCMCIA	有効									PCMCIA ポートに対するポートアクセスを有効化、無効化、またはバイパスします。
ポート： Firewire (1394)	有効									外部 Firewire (1394) ポートに対するポートアクセスを有効化、無効化、またはバイパスします。
ポート： SD	有効									SD カードポートに対するポートアクセスを有効化、無効化、またはバイパスします。



ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての積極的な保護 (デフォルト)	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本的な保護	外部ドライブに対する基本的な保護	暗号化無効	説明
サブクラス ストレージ: 外部ドライブ制御	ブロック	読み取り専用			完全アクセス			読み取り専用	完全アクセス	<p>クラス: ストレージの子。このポリシーを使用するには、クラス: ストレージを Enabled に設定する必要があります。</p> <p>このポリシーには、pc のやり取りします。EMS および PCS との相互作用を参照してください。</p> <p>フルアクセス: 外部ドライブポートではデータの読み取り / 書き込み制限は適用されません。</p> <p>読み取り専用: 読み取り機能が可能です。データの書き込みは無効です。</p> <p>ブロック: ポートでは読み取り / 書き込み機能がブロックされます。</p> <p>このポリシーはエンドポイントベースであり、ユーザーポリシーによる上書きはできません。</p>
ポート: メモリ転送デバイス (MTD)	有効									メモリ転送デバイス (MTD) ポートに対するアクセスを有効化、無効化、またはバイパスします。
クラス: ストレージ	有効									次の 3 つのポリシーに対する親です。次の 3 つのサブクラスストレージポリシーを使用するには、このポリシーを有効に設定します。このポリシーを無効に設定すると、値にかかわらず、3 つのサブクラスストレージポリシーがすべて無効になります。
サブクラス ストレージ: 光学ドライブ制御	読み取り専用	UDF のみ			完全アクセス			UDF のみ	完全アクセス	<p>クラス: ストレージの子。このポリシーを使用するには、クラス: ストレージを Enabled に設定する必要があります。</p> <p>フルアクセス: 光学ドライブポートではデータの読み取り / 書き込み制限は適用されません。</p> <p>UDF のみ: UDF フォーマット以外のすべてのデータの書き込みをブロックします (CD / DVD 書き込み、ISO 書き込み)。データの読み取りは有効です。</p>



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



ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての積極的な保護 (デフォルト)	固定ドライブすべての基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
サブクラス Windows ポータブルデバイス (WPD) : ストレージ	有効									すべての Windows ポータブルデバイスに対するアクセスを制御します。 クラス : Windows ポータブルデバイス (WPD) の子 このポリシーを使用するには、クラス : Windows ポータブルデバイス (WPD) を有効に設定する必要があります。 完全アクセス : ポートではデータの読み取り / 書き込み制限は適用されません。 読み取り専用 : 読み取り機能が可能です。データの書き込みは無効です。 ブロック : ポートでは読み取り / 書き込み機能がブロックされます。
クラス : ヒューマンインターフェイスデバイス (HID)	有効									すべてのヒューマンインターフェイスデバイスへのアクセスを制御します。 メモ : USB ポートレベルのブロッキングと HID クラスレベルのブロッキングは、コンピュータシャーシがラップトップまたはノートブックのフォームファクタとして識別できる場合にのみ有効です。コンピュータの BIOS には、シャーシの識別のために依存します。
クラス : その他	有効									その他のクラスの対象とならないすべてのデバイスへのアクセスを制御します。
リムーバブルストレージポリシー										
外部メディアの EMS 暗号化	True				False		True	False		このポリシーは、すべてのリムーバブルストレージポリシーに対する「マスターポリシー」となります。値を False にすると、他のポリシーの値に関わらず、リムーバブルストレージの暗号化は一切実行されません。 値を True にすると、すべてのリムーバブルストレージ暗号化ポリシーが有効になります。



ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての積極的な保護 (デフォルト)	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本的な保護	外部ドライブに対する基本的な保護	暗号化無効	説明
CD/DVD 暗号化の EMS 除外	False								True	このポリシーには、pc のやり取りします。EMS および PCS との相互作用を参照してください。 False に設定すると、CD/DVD デバイスが暗号化されます。 このポリシーには、pc のやり取りします。EMS および PCS との相互作用を参照してください。
Shield 対象 外メディアへの EMS アクセス	ブロック		読み取り専用		完全アクセス		読み取り専用	完全アクセス		ブロック、読み取り専用、完全アクセス このポリシーには、pc のやり取りします。EMS および PCS との相互作用を参照してください。 このポリシーがアクセスをブロックするように設定されていると、暗号化されていない限り、リムーバブルストレージにはアクセスできません。 読み取り専用または完全アクセスのいずれかを選択すると、どのリムーバブルストレージを暗号化するかを指定できます。 リムーバブルストレージを暗号化しないことを選択し、このポリシーを完全アクセスに設定すると、リムーバブルストレージに対する完全な読み取り / 書き込みアクセスを持つこととなります。 リムーバブルストレージを暗号化しないよう選択し、このポリシーを読み取り専用を設定した場合、暗号化されていないリムーバブルストレージ上の既存ファイルは読み取りまたは削除できません。ただし、クライアントはリムーバブルストレージが暗号化されていないならば、そのリムーバブルストレージ上のファイルの編集、またはストレージへのファイルの追加を許可しません。
EMS 暗号化アルゴリズム	AES256									AES 256、Rijndael 256、AES 128、Rijndael 128、3DES



ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての積極的な保護 (デフォルト)	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
外部メディアの EMS スキャン	True	False								<p>True に設定すると、リムーバブルストレージが挿入されるたびに EMS でリムーバブルストレージのスキャンを行うことが可能になります。</p> <p>このポリシーが False であり、外部メディアの EMS 暗号化ポリシーが True になっていると、EMS は新規および変更されたファイルのみを暗号化します。</p> <p>挿入されるたびにスキャンが行われるため、EMS はリムーバブルストレージに追加されたファイルを認証なしで検出できます。認証を拒否した場合はリムーバブルストレージにファイルを追加できませんが、暗号化データにはアクセスできません。この場合、追加されたファイルは暗号化されません。このため、次回暗号化データでの作業のためにリムーバブルメディアに対して認証を行うときに、EMS がそのメディアをスキャンし、暗号化なしで追加された可能性があるファイルすべてを暗号化します。</p>
Shield 対象外デバイス上の暗号化データへの EMS アクセス	True									<p>True に設定すると、エンドポイントが Shield されているかどうかにかかわらず、リムーバブルストレージの暗号化データへのアクセスが許可されます。</p>
EMS デバイスのホワイトリスト										<p>このポリシーでは、外部メディアデバイスの仕様を EMS 暗号化の対象から除外することができます。このリストに載っている外部メディアデバイスはいずれも保護されません。PNPDeviceID あたり最大 500 文字で最大 150 台のデバイスです。合計で最大 2048 文字まで使用可能です。</p> <p>リムーバブルストレージの PNPDeviceID を検索するには、次の手順に従います。</p> <ol style="list-style-type: none"> 1 リムーバブルストレージデバイスを Shield されたコンピュータに挿入します。 2 C:\Programdata\Dell\Dell Data Protection\Encryption\EMS の



ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての積極的な保護 (デフォルト)	固定ドライブすべての積極的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
										<p>EMSService.log を開きません。</p> <p>3 「PNPDeviceID=」を検索します。</p> <p>例 : 14.03.18 18:50:06.834 [!] [Volume "F:\"] PnPDeviceID = USBSTOR \DISK&VEN_SEAGATE& PROD_USB&REV_0409\ 2HC015KJ&0</p> <p>EMS デバイスのホワイトリストのポリシーで、次を指定します。</p> <p>VEN= ベンダー (例 : USBSTOR \DISK&VEN_SEAGATE)</p> <p>PROD= 製品 / モデル名 (例 : &PROD_USB)。すべての Seagate の USB ドライブ の EMS Encryption から除外され ます。VEN 値 (例 : USBSTOR \DISK&VEN_SEAGATE)はこの 値に先行する必要があります。</p> <p>REV= ファームウェアのリビジョン (例 : &REV_0409)。使用中の 特定のモデルも除外します。VEN 値および PROD 値はこの値に先 行する必要があります。</p> <p>シリアル番号 (例 : \2HC015KJ&0)。このデバイスの みを除外します。VEN 値、 PROD 値、および REV 値はこの 値に先行する必要があります。</p> <p>許可される区切り文字 : タブ、カンマ、セミコロン、16 進数文字の 0x1E (レコード区切り文字)</p>
EMS パスワードに英字が必要	True									True に設定すると、パスワードに 1 つまたは複数の文字が必要になります。
EMS パスワードに大文字小文字の混在が必要	True	False								Selected に設定すると、パスワードに少なくとも大文字 1 文字および小文字 1 文字が必要になります。



ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての積極的な保護 (デフォルト)	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本的な保護	外部ドライブに対する基本的な保護	暗号化無効	説明
EMS パスワードに必要な文字数	最低 8 文字				6			最低 8 文字		1~40 文字 パスワードに必要なとされる最小文字数です。
EMS パスワードに数字が必要	True	False								True に設定すると、パスワードに 1 つまたは複数の数字が必要になります。
EMS パスワード試行の許可回数	2	3			4			3		1~10 ユーザーが正しいパスワードの入力を試行できる回数です。
EMS パスワードに特殊文字が必要	True	False							True	True に設定すると、パスワードに 1 つまたは複数の特殊文字が必要になります。
EMS クールダウン時間遅延	30									0~5000 秒 ユーザーが試行許可回数の初回試行後に、2 回目の試行を行うまで待機する必要がある秒数です。
EMS クールダウン時間増分	30	20			10	30	10			0~5000 秒 アクセスコード入力試行で失敗するたびに以前のクールダウン時間に加算される増分時間です。
EMS 暗号化ルール										特定のドライブ、ディレクトリ、およびフォルダを暗号化または暗号化しないために使用する暗号化ルールです。 合計で 2048 文字まで使用できます。行間にラインを追加するために使用された「空白」および「改行」文字は、使用した文字として計上されます。2048 文字を越えるルールは無視されます。 Firewire、USB、eSATA などのマルチインタフェース接続を内蔵したストレージデバイスでは、エンドポイントの暗号化に EMS と暗号化ルール両方の使用が必要となる場合があります。これは、Windows オペレーティングシステムがストレージデバイスを処理する方法がインタフェースタイプに基づいて異なるために必要となります。

ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての積極的な保護 (デフォルト)	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本的な保護	外部ドライブに対する基本的な保護	暗号化無効	説明
Shielded 対象外メディアに対するアクセスの EMS ブロック	True								False	<p>す。EMS を使用した iPod の暗号化方法を参照してください。</p> <p>1.44MB フロッピーディスクなど、17 MB に満たないために Removable Media Shield をホストするストレージ容量が不足しているリムーバブルストレージへのアクセスをブロックします。</p> <p>すべてのアクセスを外部メディアを暗号化します。このポリシーは、両方の true の場合はブロックされます。外部メディアの暗号化が True で、かつこのポリシーが False である場合、暗号化非対応リムーバブルストレージからデータを読み取ることはできますが、メディアへの書き込みアクセスはブロックされます。</p> <p>外部メディアの暗号化が False である場合、このポリシーに効果はなく、暗号化非対応リムーバブルストレージへのアクセスには影響を及ぼしません。</p>
ユーザーエクスペリエンス制御ポリシー										
更新時の強制再起動	True								False	<p>値を True に設定すると、コンピュータはすぐに再起動して暗号化処理を実行するか、System Data Encryption (SDE) などの、デバイスベースのポリシーに関連して更新を行います。</p>
各再起動の遅延時間の長さ	5	10			20			15		<p>ユーザーがデバイスベースのポリシーに対する再起動の遅延を選択した場合の遅延時間 (分) です。</p>
再起動遅延の許容回数	1				5			3		<p>ユーザーがデバイスベースポリシーに対する再起動を遅延できる回数です。</p>
ファイル競合通知の抑制	False									<p>このポリシーは、クライアントによるファイルの処理中にアプリケーションがそのファイルへのアクセスを試みた場合に、通知ポップアップをユーザーに表示するかどうかを制御します。</p>



ポリシー	固定ドライブおよび外部ドライブのすべての積極的な保護	PCI (Regulation)	データ漏洩規制の対象	HIPAA (Regulation)	固定ドライブおよび外部ドライブのすべての積極的な保護 (デフォルト)	固定ドライブすべてに対する基本的な保護	システムドライブのみに対する基本保護	外部ドライブに対する基本的な保護	暗号化無効	説明
ローカル暗号化処理制御の表示	False		True					False		<p>値を True に設定すると、暗号化 / 復号化を一時停止 / 再開するメニューオプションがシステムトレイアイコンに表示されます(現在の Shield の動作によって異なります)。</p> <p>① メモ: 重要: 暗号化の一時停止を許可すると、Shield がデータをポリシーに従って完全に暗号化 / 復号化することをユーザーが妨げる恐れがあります。</p>
画面がロックされている場合のみ暗号化処理を許可	False		User-Optional					False		<p>True、False、User-Optional</p> <p>True の場合、ユーザーがアクティブに作業している間は、データの暗号化または復号化が実行されません。Shield は、画面がロックされている場合にのみデータを処理します。</p> <p>User-Optional では、システムトレイアイコンにオプションが追加され、ユーザーがこの機能をオンまたはオフにできます。</p> <p>False を設定すると、ユーザーが作業中であっても、暗号化処理はいつでも実行されます。</p> <p>このオプションを有効にすると、暗号化または復号化を完了するために必要な時間が大幅に増加します。</p>

テンプレートの説明

固定ドライブおよび外部ドライブのすべての積極的な保護

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

このポリシーテンプレートでは以下の機能が提供されます。

厳しく制限された設定によるより優れた保護。

システムドライブおよびすべての固定ドライブに対する保護。

リムーバブルストレージデバイスの全データの暗号化、および暗号化されていないリムーバブルストレージデバイスの使用の防止。
読み取り専用の光学ドライブ制御。

PCI 規制の対象

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

このポリシーテンプレートでは以下の機能が提供されます。

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

データ漏洩規制の対象

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

このポリシーテンプレートでは以下の機能が提供されます。

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

HIPAA 規制の対象

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

このポリシーテンプレートでは以下の機能が提供されます。

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

固定ドライブおよび外部ドライブのすべてに対する基本的な保護 (デフォルト)

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



このポリシーテンプレートでは以下の機能が提供されます。

システムドライブおよびすべての固定ドライブに対する保護。

ユーザーに対するリムーバブルストレージデバイスの暗号化のプロンプト表示。

UDF CD/DVD 限定の書き込み機能。ポート制御設定は、すべての光学ドライブに対する読み取りアクセスを可能にします。

固定ドライブすべてに対する基本的な保護

このポリシーテンプレートでは以下の機能が提供されます。

システムドライブおよびすべての固定ドライブに対する保護。

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

このポリシーテンプレートでは以下の機能は提供されません。

リムーバブルストレージデバイスに対する暗号化機能。

システムドライブのみに対する基本保護

このポリシーテンプレートでは以下の機能が提供されます。

システムドライブの保護。このドライブは、通常オペレーティングシステムがロードされる C: ドライブです。

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

このポリシーテンプレートでは以下の機能は提供されません。

リムーバブルストレージデバイスに対する暗号化機能。

外部ドライブに対する基本的な保護

このポリシーテンプレートでは以下の機能が提供されます。

リムーバブルストレージデバイスの保護。

UDF CD/DVD 限定の書き込み機能。ポート制御設定は、すべての光学ドライブに対する読み取りアクセスを可能にします。

このポリシーテンプレートでは以下の機能は提供されません。

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

暗号化無効

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

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

[ワンタイムパスワードの事前インストール設定](#) に続行します。

ワンタイムパスワードのための事前インストール設定

これらの Personal Edition の機能を必要とする設定する **前に**、インストールを開始します。

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。



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。
- マスターのインストーラがインストールに使用されている場合は、クライアントの個別にアンインストールする必要があります。このプロセスを使用します。アンインストール用にインストールできるように使用でき、マスタインストーラからクライアントを抽出します。

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

```
DDPSetup.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。参照を [要件](#) の詳細については。

抽出した子インストーラは C:\extracted\ に格納されます。

続行をトラブル [シューティング](#) してください。

トラブルシューティング 61

Windows 10 Anniversary Update へのアップグレード

Encryption とともにインストールされたコンピュータは、特別に設定された Windows 10 アップグレードパッケージを使用して、Windows 10 Anniversary Update にアップグレードする必要があります。設定されているバージョンのアップグレードパッケージは、Dell Data Protection が暗号化ファイルへのアクセスを管理して、アップグレードプロセス中にそれらのファイルを危害から保護することを確実にします。

Windows 10 Anniversary バージョンに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>

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>

(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 > tcsd_win32.exe と移動します。ファイルを右クリックして、**プロパティ** を選択します。**詳細** タブでファイルのバージョンを確認します。

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) も示されません。
 - 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 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	<p>ファイルの暗号化に使用した暗号化の種類。</p> <p>SysData : SDE 暗号化キー。</p> <p>User : ユーザー暗号化キー。</p> <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>



出力	意味
	AES 256
	3DES

Encryption Removal Agent ステータスのチェック

Encryption Removal Agent は、次のように、サービスパネル (スタート > ファイル名を指定して実行 ... > services.msc > OK) の説明 エリアにそのステータスを表示します。サービスのステータスをアップデートするために、サービスを定期的に更新します (サービスをハイライト表示 > 右クリック > 更新)。

- **SED の非アクティブ化を待機中** – Encryption クライアントはまだインストールされているか、まだ設定されているか、またはその両方です。Encryption クライアントがアンインストールされるまで復号化は開始されません。
- **初期ス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。
- **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。

EMS を使用した iPod の暗号化方法

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

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

-R#:\Calendars

-R#:\Contacts

-R#:\iPod_Control

-R#:\Notes

-R#:\Photos



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

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

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

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

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

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

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

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

- これらのルールは、次の iPod に対してテストされています。

第 5 世代 iPod Video 30 GB

第 2 世代 iPod Nano 2 GB

第 2 世代 iPod Mini 4 GB

Dell ControlVault ドライバ

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

工場では Dell コンピュータにインストールされている Dell ControlVault ドライバおよびファームウェアは古いため、次の手順の順序にしたがってアップデートする必要があります。

クライアントのインストールの際に、Dell ControlVault のドライバをアップデートするためにインストールを終了することを促すエラーメッセージが表示された場合、このメッセージは無視してクライアントのインストールを続行します。Dell ControlVault ドライバ（およびファームウェア）はクライアントのインストールが完了した後にアップデートすることができます。

最新のドライバのダウンロード

- 1 Support.dell.com に移動します。
- 2 お使いのコンピュータモデルを選択します。
- 3 **ドライバおよびダウンロード** を選択します。
- 4 ターゲットコンピューターの **オペレーティングシステム** を選択します。
- 5 **セキュリティ** カテゴリを展開します。
- 6 Dell ControlVault ドライバをダウンロードして保存します。
- 7 Dell ControlVault ファームウェアをダウンロードして保存します。
- 8 必要に応じて、ターゲットコンピュータにドライバとファームウェアをコピーします。

Dell ControlVault ドライバのインストール

ドライバのインストールファイルをダウンロードしたフォルダに移動します。

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



ドライバを先にインストールします。本文書の作成時におけるドライバのファイル名は ControlVault_Setup_2MYJC_A37_ZPE.exe です。



続行 をクリックして開始します。

Ok をクリックして、ドライバファイルを C:\Dell\Drivers\

はい をクリックして新しいフォルダの作成を許可します。

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

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

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

ようこそ画面で **次へ** をクリックします。

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

完了 オプションを選択して **次へ** をクリックします。

インストール をクリックしてドライバのインストールを開始します。

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

ドライバのインストールの検証

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

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。

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

暗号化クライアント

Encryption Removal Agent のログファイルを作成します (オプション)。

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

スマート Windows ログを持つカードで使します。

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
```

インストール中に一時ファイルを保持する

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

[プロンプトをユーザのデフォルトの動作を開始しますまたは遅延の暗号化の変更

[暗号化クライアントを表示するには、長さの各ポリシーの更新遅延の各時間が5分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）。

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

SDUser キーのデフォルト使用の変更

System Data Encryption (SDE) は、SDE 暗号化ルールポリシー値に基づいて実施されます。SDE 暗号化の有効化ポリシーが選択されている場合、追加のディレクトリがデフォルトで保護されます。詳細については、AdminHelp で「SDE 暗号化ルール」を検索してください。Encryption 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デフォルトで、SDE キー（デバイスキー）ではなく、SDUser キー（ユーザーキー）を使用して暗号化されます。SDUser キーは、SDE で暗号化されないユーザーディレクトリにコピーされる（移動ではない）ファイルまたはフォルダを暗号化するためにも使用されます。

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

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Credant\CMGShield]
```

```
"EnableSDUserKeyUsage"=dword:00000000
```

このレジストリキーが存在しないか、0 以外に設定されていると、これらのユーザーディレクトリを暗号化するために、SDUser キーが使用されます。

Advanced Authentication クライアント -

スマートカードとバイOMETリックサービス（オプション）

Security Tools が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「自動」起動タイプに変更することを避けるには、サービス起動機能を無効にすることができます。

無効化すると、Security Tools は次の 3 つのサービスの起動を試行しなくなります。

SCardSvr - コンピュータが読み取るスマートカードへのアクセスを管理します。このサービスが停止されると、コンピュータはスマートカードを読み取ることができなくなります。このサービスが無効化されると、このサービスに確実に依存するサービスの開始が失敗するようになります。

SCPolicySvc - スマートカード取り外し時にユーザーのデスクトップをロックするようシステムを設定することができます。

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。

また、この機能を無効化すると、実行されていない必須サービスに関連する警告も抑制されます。

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

```
[HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]
```

```
SmartCardServiceCheck=REG_DWORD:0
```

有効化するには 0 に設定します。

無効化するには 1 に設定します。

スマート Windows ログを持つカードで使⽤します。

Windows 認証にスマートカードを⽤するには、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

続⾏を⽤語 [集](#)を押します。



用語集

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

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

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

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

暗号化ス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、Shielded 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が行われる可能性がある場合と、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、認証または回復のどちらかに使用できますが、両方に使用することはできません。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、ハードディスクからオペレーティングシステムなどを何も読み取ることができないようにします。

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

System Data Encryption (SDE) – SDE は、オペレーティングシステムとプログラムファイルを暗号化するように設計されています。この目的を達成するために、SDE はオペレーティングシステムが起動している間にそのキーを開くことができる必要があります。これは、攻撃者によるオペレーティングシステムの改ざん、またはオフライン攻撃を防ぐためのものです。ユーザーデータは SDE 対象外です。共通キー暗号化およびユーザーキー暗号化は、暗号化キーのロック解除にユーザーパスワードを必要とするため、機密ユーザーデータを対象にしています。SDE ポリシーは、起動プロセスを開始するためにオペレーティングシステムが必要とするファイルを暗号化しません。SDE ポリシーでは、起動前認証は必要なく、マスターブートレコードへの干渉は一切行われません。コンピュータの起動時、ユーザーログイン前に暗号化されたファイルが使用可能になります(パッチ管理、SMS、バックアップ、およびリカバリツールの有効化のため)。SDE 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、ソフトウェアボルトの暗号化されたコンテナも提供します。TPM は、ワンタイムパスワード機能の使用にも必須です。

