Dell Data Protection | Security Tools

Security Tools のインストールガイド

Dell Data Protection | Security Tools インストールガイド

インストール ガイド v1.12

DELL EMC

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その危険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。

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。EnCaseTM™ 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。VALIDITYTM™ 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。

2017- 02

Rev. A01

目次

1

はじめに

Dell Data Protection | Security Tools は、Dell コンピュータの管理者とユーザーにセキュリティと個人情報保護を提供します。DDP | Security Tools は、Dell Latitude、Optiplex、Precision コンピュータ、および特定の Dell XPS ノートブックに事前インストールされています。DDP | Security Tools を*再インストール*する必要がある場合は、本ガイドの手順に従ってください。追加サポートについては、www.dell.com/support > Endpoint Security Solutions を参照してください。

概要

DDP | Security Tools は、高度な認証サポートの他、起動前認証 (PBA) のサポート、および自己暗号化ドライブの管理機能を提供するために設計されたエンドツーエンドのセキュリティソリューションです。

DDP | Security Tools は、パスワード、指紋リーダー、および「非接触型」と「接触型」両方のスマートカードを使用した Windows 認証のための多要素サポートに加え、自己登録、ワンステップログオン (シングルサインオン (SSO))、およびワンタイムパスワード (OTP) も提供します。

管理者は、エンドユーザーが Security Tools を使用できるようにする前に、たとえば、起動前認証および認証ポリシーの有効化など、DDP Security Console の 管理者設定 ツールを使用して Security Tools 機能を設定することが推奨されます。ただし、デフォルト設定では、管理者およびユーザーが、インストールおよびアクティブ化後すぐに Security Tools を開始できるようになっています。

DDP Security Console

DDP Security Console は、ユーザーが、管理者が設定したポリシーに基づいて、それぞれの資格情報の登録および管理し、セルフリカバリ質問を設定することができる Security Tools インタフェースです。ユーザーは、次の Security Tools アプリケーションにアクセスできます。

- Encryption ツールでは、ユーザーがコンピュータのドライブの暗号化ステータスを表示することができます。
- Enrollments ツールにより、ユーザーは、資格情報のセットアップと管理、セルフリカバリ質問の設定、および資格情報登録のステータスの表示を行うことが可能になります。これらの権限は、管理者が設定したポリシーに基づきます。
- Password Manager では、ユーザーがウェブサイト、Windows アプリケーション、およびネットワークリソースにログオンするために必要なデータを自動的に入力し、送信することができます。また、Password Manager はユーザーにアプリケーションを介してログオンパスワードを変更する機能も提供し、Password Manager によって維持されているログオンパスワードが対象リソースのパスワードと同期化されていることを確実にします。

管理者設定

管理者設定ツールは、コンピュータの全ユーザーに対して Security Tools を設定するために使用されるツールで、管理者が認証ポリシーのセットアップ、ユーザーの管理、および Windows ログオンで使用できる資格情報の設定を行うことを可能にします。

管理者設定ツールを使用することにより、管理者は、暗号化と起動前認証 (PBA) の有効化、PBA ポリシーの設定、および PBA 画面テキストのカスタマイズを行うことができます。

続けて 要件 に移動します。

2

要件

- DDP | Security Tools は、Dell Latitude、Optiplex、Precision コンピュータ、および特定の Dell XPS ノートブックに事前インストールされており、次の最小要件を満たしています。DDP | Security Tools の再インストールが必要になった場合は、お使いのコンピュータが引き続きこれらの要件を満たしていることを確認してください。詳細については、www.dell.com/support > Endpoint Security Solutions for more information を参照してください。
- Windows 8.1 を自己暗号化ドライブのドライブ 1 にインストールしないでください。Windows 8.1 はリカバリパーティションドライブ 0 を作成しますが、これは起動前認証を破損するため、このオペレーティングシステム設定はサポートされていません。その代わりに、Windows 8.1 はドライブ 0 として設定されたドライブにインストールするか、任意のドライブにイメージとして回復させてください。
- DDP | Security Tools はダイナミックディスクをサポートしていません。
- 自己暗号化ドライブが搭載されているコンピュータで Hardware Crypto Accelerator を使用することはできません。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ないことにご注意ください。この非対応構成は、アフターマーケット構成となります。
- DDP | Security Tools はマルチブートディスク設定をサポートしていません。
- クライアント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 の TPM (Trusted Platform Module) をクリアします。
- 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。

ドライバ

- サポートされている Opal 準拠 SED には、次の場所にあるアップデート済みの Intel Rapid Storage Technology ドライバが必要です。http://www.dell.com/support/drivers/us/en/19/DriverDetails/Product/latitude-e6440-laptop?driverId=1KX2H&osCode=W764&fileId=3356216042&languageCode=en&categoryId=SA

> **メモ:**
>
> **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、ブルースクリーンになります。**

クライアントの前提条件

- Security Tools には、Microsoft .Net 4.5 (またはそれ以降) が必要です。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 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。Microsoft .Net Framework 4.5 の完全バージョンをインストールするには、https://www.microsoft.com/en-us/download/details.aspx?id=30653 に移動します。

  インストールされている .Net のバージョンを検証するには、インストール対象のコンピュータで http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx に記載されている手順を実行します。
- お使いの認証ハードウェアのドライバとファームウェアが、コンピュータ上で最新状態になっている必要があります。Dell コンピュータ向けのドライバおよびファームウェアを入手するには、http://www.dell.com/support/home/us/en/19/Products/?app=drivers に進み、お使いのコンピュータのモデルを選択してください。お使いの認証ハードウェアに基づいて、次をダウンロードします。
  - NEXT Biometrics Fingerprint ドライバ
  - Validity FingerPrint Reader 495 ドライバ
  - O2Micro Smartcard ドライバ
  - Dell ControlVault

  その他のハードウェアベンダーでは、独自のドライバが必要になる場合があります。

このコンポーネントは、コンピュータにインストールされていない場合、インストーラによってインストールされます。

前提条件

- Microsoft Visual C++ 2012 アップデート 4 以降の再頒布可能パッケージ/ (x86/x64)

ソフトウェア

Windows オペレーティングシステム

次の表では、サポートされているソフトウェアの詳細を説明します。

Windows オペレーティングシステム (32 ビットと 64 ビット)

- Microsoft Windows 7 SP0 ~ SP1
  - Enterprise
  - Professional

  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。
- Microsoft Windows 8
  - Enterprise
  - Pro
  - Windows 8 （ Consumer ）

  メモ: Opal Compliant SED モデルおよび Dell コンピュータモデル - UEFI サポート とで使用する際に、Windows 8 は UEFI モードでサポートされます。
- Microsoft Windows 8.1 - 8.1 Update 1
  - Enterprise Edition
  - Pro Edition

  メモ: Opal Compliant SED モデルおよび Dell コンピュータモデル - UEFI サポート とで使用する際に、Windows 8.1 は UEFI モードでサポートされます。
- Microsoft Windows 10 ~ Version 1511 (November Update/Threshold 2)
  - Education Edition
  - Enterprise Edition
  - Pro Edition

メモ: Opal Compliant SED モデルおよび Dell コンピュータモデル - UEFI サポート とで使用する際に、Windows 10 は UEFI モードでサポートされます。

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。

モバイルデバイスオペレーティングシステム

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

モバイルデバイスオペレーティングシステム

- 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

ハードウェア

認証

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。

認証

指紋リーダー

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

  メモ: 外部指紋リーダーを使用するときは、その特定リーダーに必要な最新ドライバをダウンロードしてインストールする必要があります。

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

  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。
- 共通アクセスカード (CAC)

  メモ: 複数の証明書を持つ CAC では、ログオン時にユーザーがリストから正しい証明書を選択します。
- CSP カード
- クラス B / SIPR Net カード

次の表は、SIPR ネットカードでサポートされている De l l 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
- Latitude E6540
- Precision M2800
- Precision M4800
- Precision M6800
- Latitude 14 Rugged Extreme
- Latitude 12 Rugged Extreme
- Latitude 14 Rugged

Dell コンピュータモデル - UEFI サポート

認証機能は、適格な Opal Compliant SED を搭載した、Microsoft Windows 8、Microsoft Windows 8.1、および Microsoft Windows 10 を実行する特定の Dell コンピュータにおいて、UEFI モードでサポートされます。Legacy ブートモードは Microsoft Windows 7、Microsoft Windows 8、icrosoft Windows 8.1、および Microsoft 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。

次の表は、UEFI でサポートされている De l l 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 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7240
- Latitude E7250
- Latitude E7260
- Latitude E7265
- Latitude E7270
- Latitude E7275
- Latitude E7350
- Latitude E7440
- Latitude E7450
- Latitude E7460
- Latitude E7470
- Latitude 12 Rugged Extreme
- Latitude 12 Rugged タブレット (モデル 7202)
- Latitude 14 Rugged Extreme
- Latitude 14 Rugged
- Precision M3510
- Precision M4800
- Precision M5510
- Precision M6800
- Precision M7510
- Precision M7710
- Precision T3420
- Precision T3620
- Precision T7810
- Optiplex 3040 マイクロ、ミニタワー、スモールフォームファクター
- Optiplex 3046
- OptiPlex 3050 All-In-One
- OptiPlex 3050 タワー、スモールフォームファクタ、マイクロ
- Optiplex 5040 ミニタワー、スモールフォームファクター
- OptiPlex 5050 タワー、スモールフォームファクタ、マイクロ
- OptiPlex 7020
- Optiplex 7040 マイクロ、ミニタワー、スモールフォームファクター
- OptiPlex 7050 タワー、スモールフォームファクタ、マイクロ
- Optiplex 3240 All-In-One
- OptiPlex 5250 All-In-One
- Optiplex 7440 All-In-One
- OptiPlex 7450 All-In-One
- OptiPlex 9020 マイクロ
- Venue Pro 11 (モデル 5175/5179)
- Venue Pro 11(モデル 7139)

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。

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。一部のモデルでは PBA ログオン画面が表示され、別のモデルには Windows ログオン画面が表示されます。どちらのログオン画面も等しく安全です。

メモ:

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。

レガシーオプション ROM を無効にするには、次の手順を実行します。

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。

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。

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)

言語サポート

DDP | Security Tools は複数言語ユーザーインタフェース (MUI) 対応で、次の言語をサポートしています。

メモ:

UEFI コンピューターではロシア語、繁体字中国語、簡体字中国語での PBA ローカライゼーション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

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**

ワンタイムパスワード機能には、TPM が存在し、有効化され、所有されている必要があります。詳細については、「所有権のクリアと TPM のアクティブ化」を参照してください。OTP は TPM 2.0 でサポートされていません。

以下の表では、ハードウェアと構成の要件を満たした Security Tools で使用できる認証オプションをオペレーティングシステム別に示しています。

非 UEFI

	PBA				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[1]					X	X	X	X	X
Windows 8	X[1]					X	X	X	X	X
Microsoft Windows 8.1 - Windows 8.1 アップデート 1	X[1]					X	X	X	X	X
Windows 10	X[1]					X	X	X	X	X

1. 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[2]					X	X	X	X	X
Microsoft Windows 8.1 - Windows 8.1 アップデート 1	X[2]					X	X	X	X	X
Windows 10	X[2]					X	X	X	X	X

2. 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。

相互運用性

Dell Data Protection | Access のプロビジョニング解除とアンインストール

お使いのコンピュータに DDP|A が現在インストールされている、または過去にインストールされていた場合は、Security Tools をインストールする **前に** DDP|A 管理対象ハードウェアのプロビジョニングを解除してから DDP|A をアンインストールする必要があります。DDP|A を使用したことがない場合は、DDP|A を単純にアンインストールした後でインストールプロセスを再開することができます。

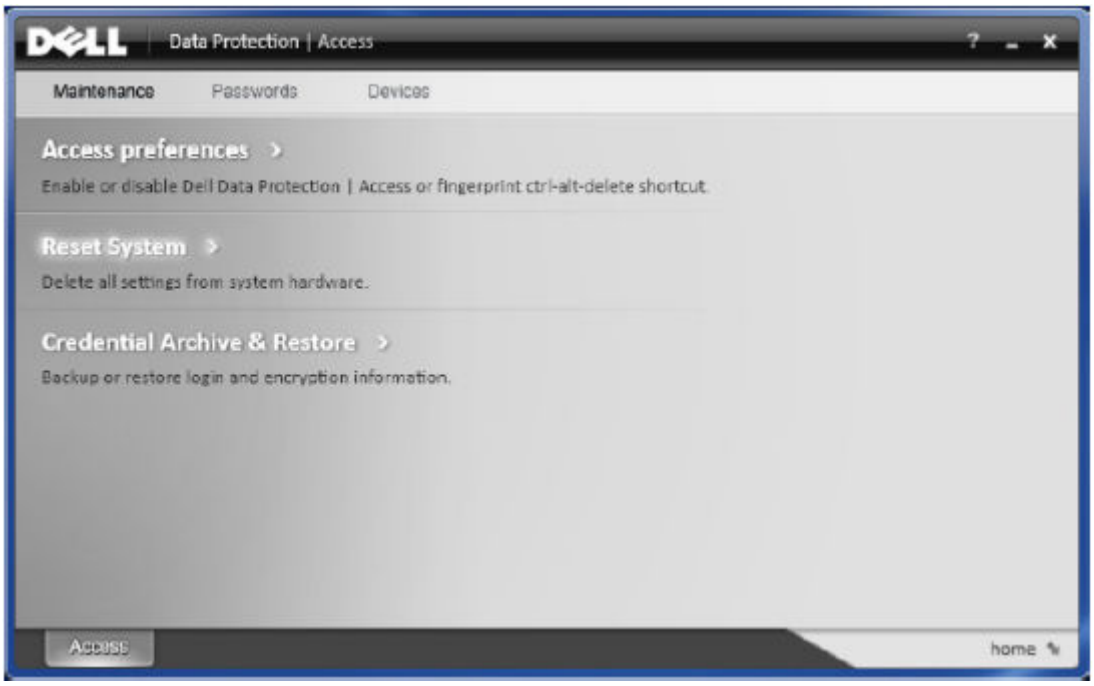
DDP|A 管理対象ハードウェアのプロビジョニング解除には、指紋リーダー、スマートカードリーダー、BIOS パスワード、TPM、自己暗号化ドライブが含まれます。

メモ: DDP|E 暗号化製品を実行している場合は、暗号化スイープを停止または一時停止します。Microsoft BitLocker を実行している場合は、暗号化ポリシーを一時中断してください。DDP|A をアンインストールし、Microsoft BitLocker ポリシーの一

時中断を解除したら、http://technet.microsoft.com/en-us/library/cc753140.aspx に記載されている手順に従って TPM を初期化します。

DDP|A 管理対象ハードウェアのプロビジョニング解除

1. DDP|A を起動して**詳細** タブをクリックします。



2. **システムのリセット** を選択します。これには、ユーザーの身元確認のため、プロビジョニングされた資格情報の入力が必要になります。DDP|A が資格情報を確認すると、DDP|A は次のアクションを実行します。
   - プロビジョニングされたすべての資格情報を Dell ControlVault から削除する（存在する場合）
   - Dell ControlVault 所有者パスワードを削除する（存在する場合）
   - プロビジョニングされたすべての指紋を内蔵指紋リーダーから削除する（存在する場合）
   - すべての BIOS パスワード（BIOS システム、BIOS 管理者、HDD の各パスワード）を削除する
   - Trusted Platform Module をクリアする
   - DDP|A 資格情報プロバイダを削除する

     コンピュータのプロビジョニングが解除されると、DDP|A がそのコンピュータを再起動し、Windows のデフォルト資格情報プロバイダを復元します。

DDP|A のアンインストール

認証ハードウェアのプロビジョニングが解除されたら、DDP|A をアンインストールしてください。

1. DDP|A を起動して、システムのリセット を実行します。

   これにより、すべての DDP|A 管理対象資格情報とパスワードが削除され、Trusted Platform Module（TPM）がクリアされます。
2. **アンインストール** をクリックしてインストーラを起動します。
3. アンインストールが完了したら **はい** をクリックして再起動します。

   メモ: DDP|A を削除すると SED のロックも解除され、起動前認証が削除されます。

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。

所有権のクリアと TPM のアクティブ化

TPM の所有権をクリアし、設定するには、https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2 を参照してください。

インストールおよびアクティベーションを に進みます。

3

インストールとアクティブ化

本項では、ローカルコンピュータでの DDP | Security Tools のインストールを詳しく説明します。DDP | Security Tools をインストールしてアクティブ化するには、コンピュータに管理者としてログオンしている必要があります。

メモ:

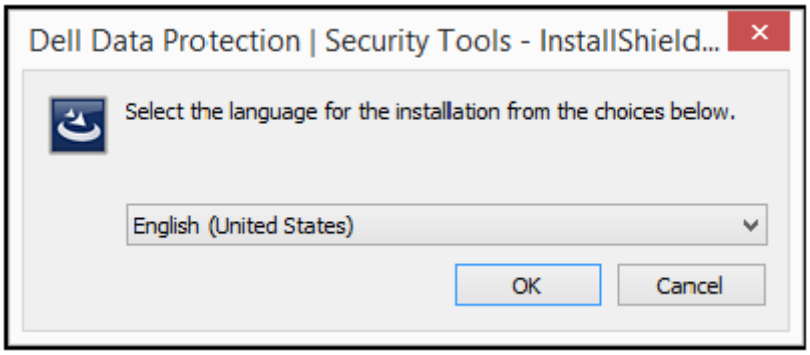
インストール中は、外付け（USB）ドライブの挿入や取り外しを含め、コンピュータに変更を加えないでください。

DDP | Security Tools のインストール

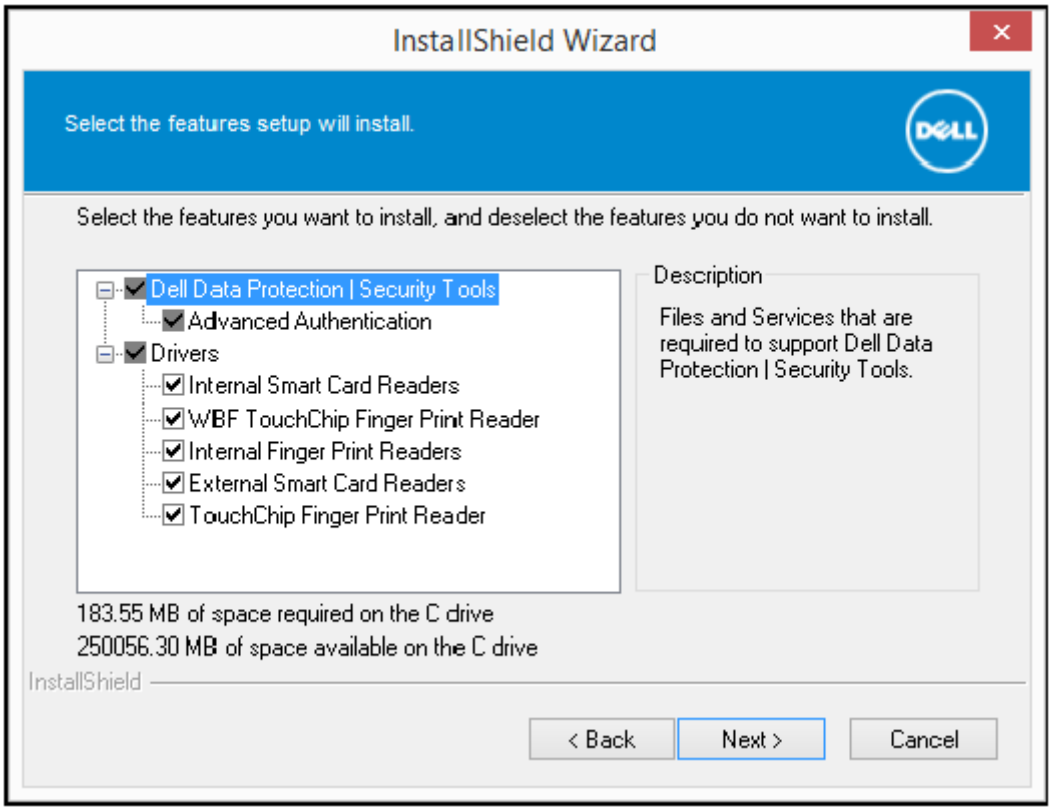
Security Tools をインストールするには、次の手順を実行します。

1. DDP | Security Tools インストールメディアにあるインストールファイルを見つけます。それをローカルコンピュータにコピーします。

   メモ: **インストールメディアは、www.dell.com/support > Endpoint Security Solutions にあります。**
2. 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。
3. 適切な言語を選択して、**OK** をクリックします。



4. ようこそ 画面が表示されたら **次へ** をクリックします。
5. 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。
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 Security Tools をインストールします。**選択します**



7. **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。
8. インストールの完了後はコンピュータの再起動が必要です。**はい** を選択して再起動してから、**終了** をクリックします。

   インストールが完了しました。

DDP | Security Tools のアクティブ化

DDP Security Console を初めて実行して 管理者設定 を選択すると、アクティブ化プロセス全体をガイドするアクティブ化ウィザードが表示されます。

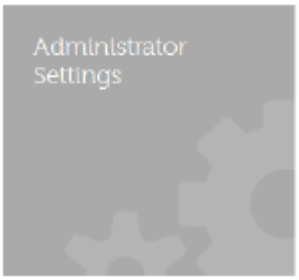
DDP Security Console は、まだアクティブ化されていなくても、エンドユーザーによる実行が可能です。エンドユーザーが、管理者が DDP | Security Tools をアクティブ化して設定をカスタマイズする前に DDP Security Console を使用する最初の人物である場合は、デフォルトの値が使用されます。

Security Tools をアクティブ化するには、次の手順を実行します。

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。

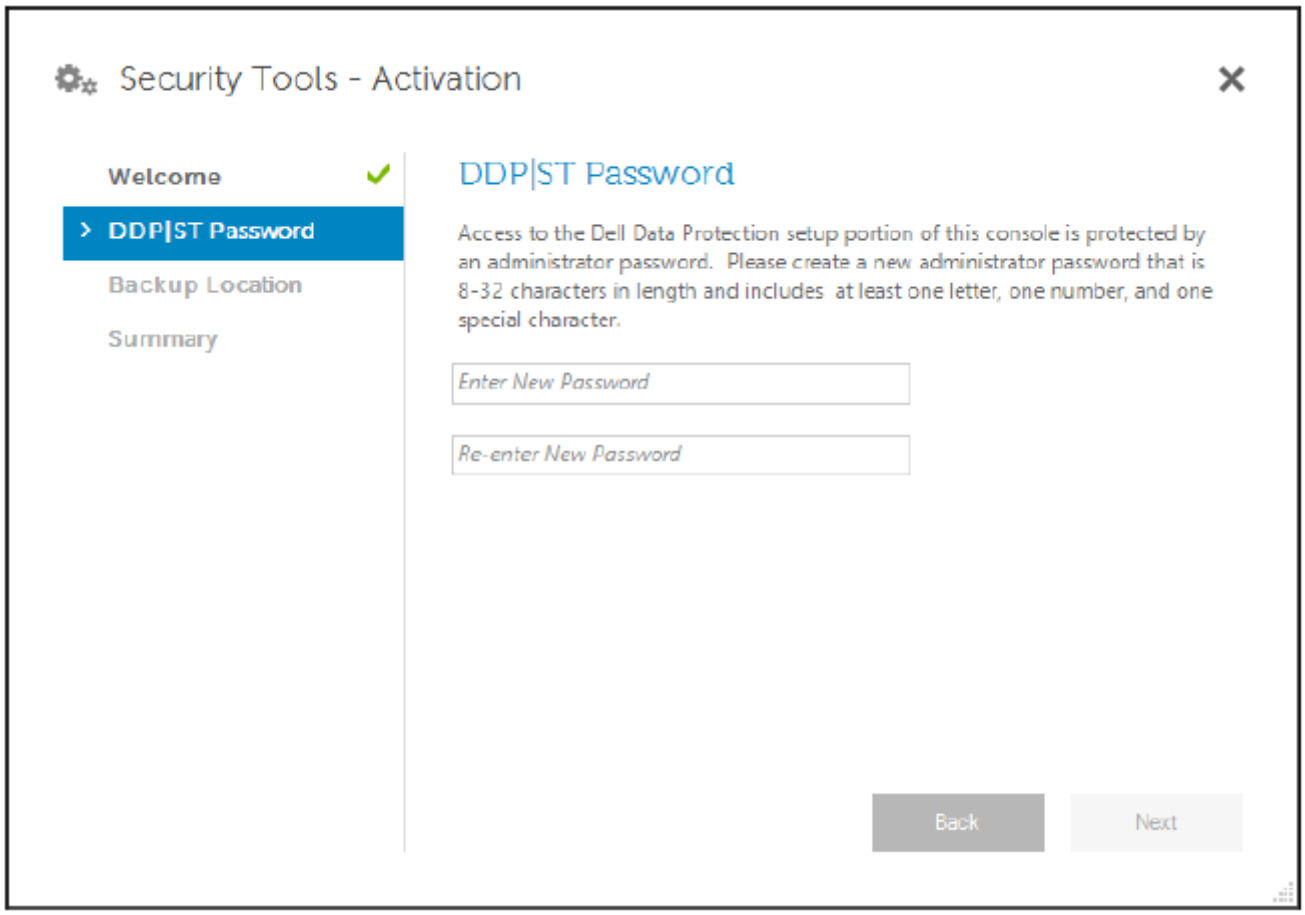
メモ: 標準の Windows アカウントで一般ユーザーとしてログインした場合、管理者設定 ツールの起動には UAC 昇格が必要です。一般ユーザーは、最初は管理者資格情報を入力してツールにログオンし、2 回目は、プロンプトが表示されたときに管理者のパスワード (管理者設定 に保管されているパスワード) を入力します。

2. **管理者設定** タイルをクリックします。



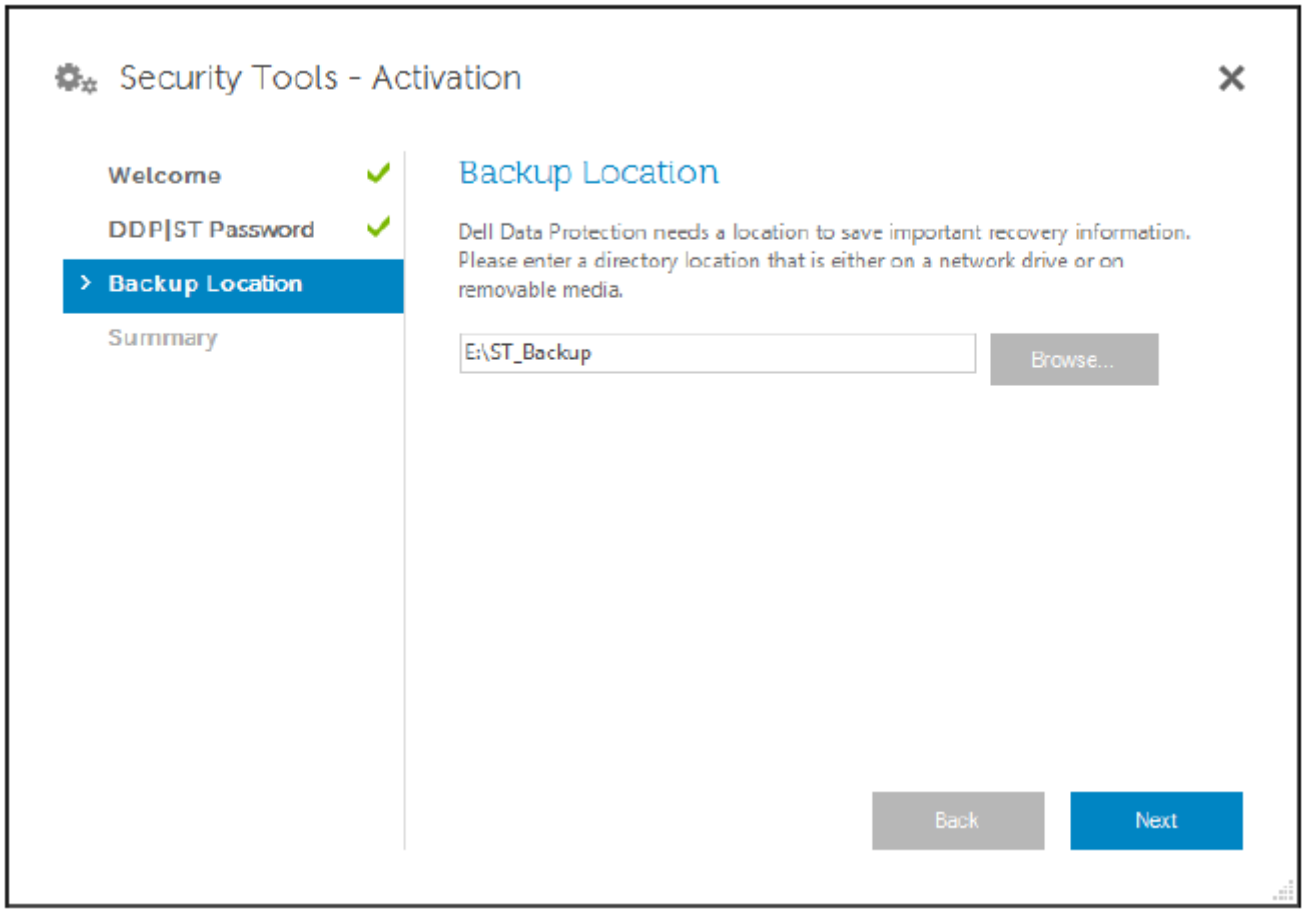
3. ようこそ ページで、**次へ** をクリックします。
4. DDP | Security Tools パスワードを作成し、**次へ** をクリックします。

   DDP | Security Tools 管理者のパスワードは、Security Tools の設定前に作成する必要があります。このパスワードは、管理者設定ツールを実行するときに常時必要となります。パスワードの長さは 8 ~ 32 文字で、少なくとも 1 つの文字、1 つの数字、および 1 つの特殊文字を含む必要があります。



5. **バックアップの場所** でバックアップファイルが書き込まれる場所を指定し、**次へ** 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。デルサポート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。場所が使用不可の場合 (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、DDP | Secruity Tools がデータをバックアップする場所を求めるプロンプトを表示します。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。



6. サマリ ページで **適用** をクリックします。

   Security Tools のアクティブ化が完了しました。

   管理者およびユーザーは、Security Tools 機能をデフォルトの設定に基づいて即時に活用できるようになります。

4

管理者向けのタスクの設定

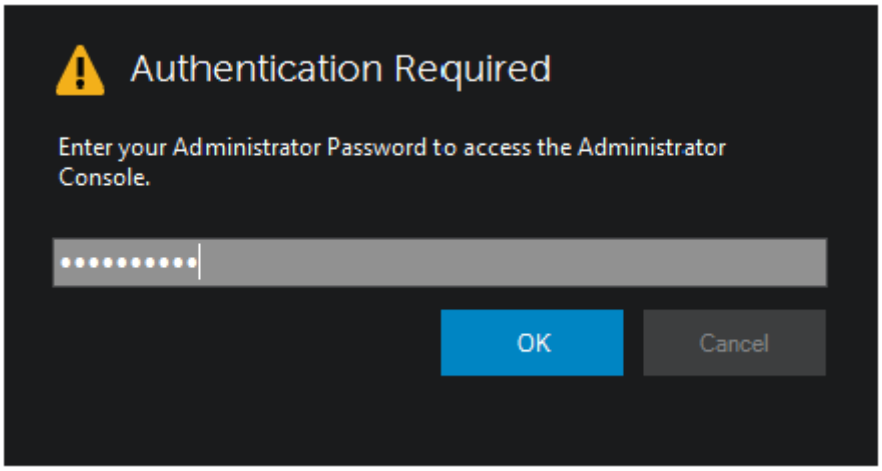
Security Tools デフォルト設定では、管理者とユーザーが、追加の設定を行うことなくアクティブ化後すぐに Security Tools を使用することができます。ユーザーは、Windows パスワードを使用してコンピュータにログオンするときに Security Tools ユーザーとして自動的に追加されますが、デフォルトでは、Windows 多要素認証は有効化されていません。また、暗号化および起動前認証もデフォルトで無効になっています。

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。

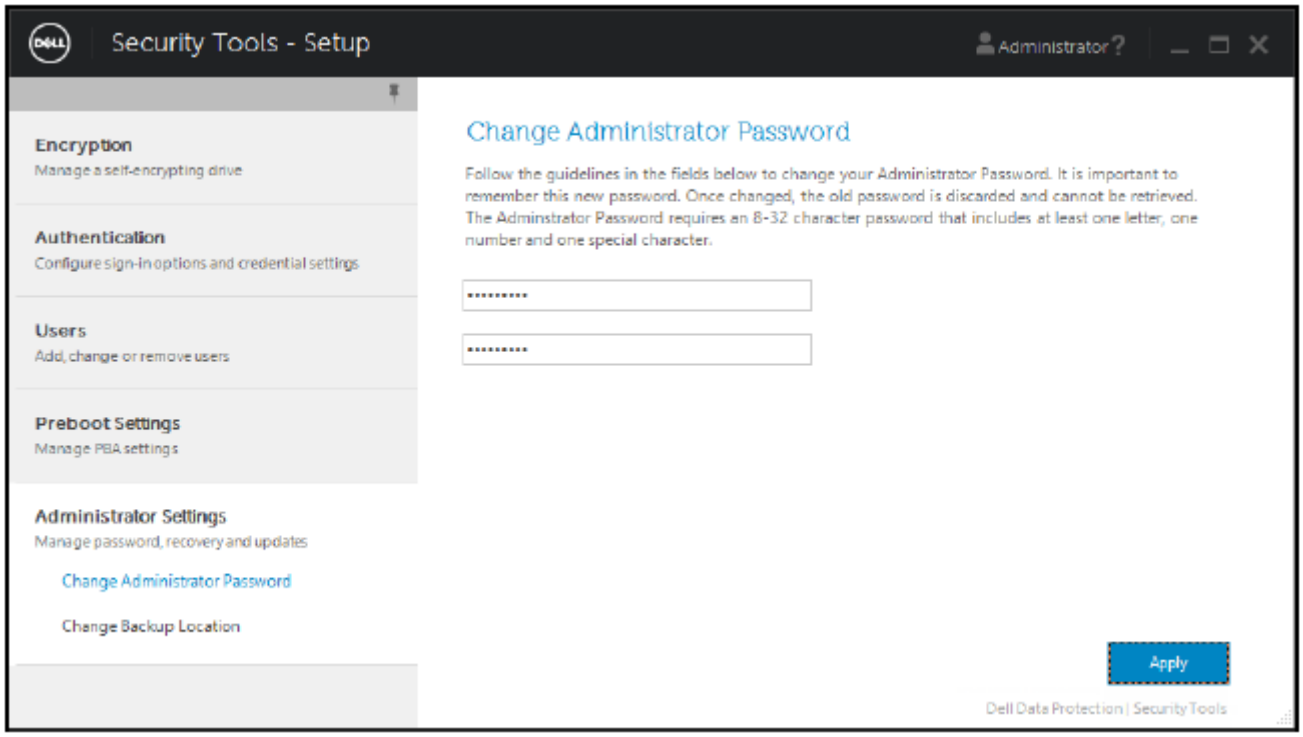
管理者パスワードおよびバックアップ場所の変更

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。



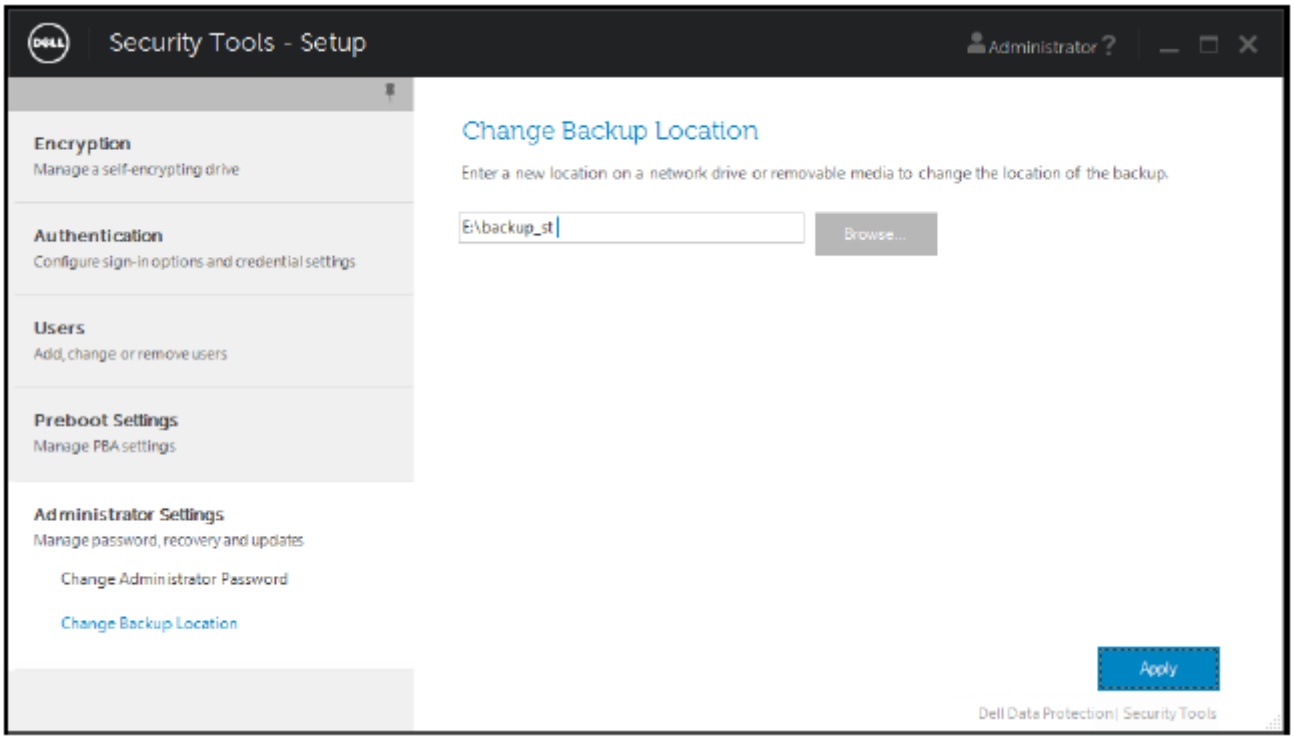
4. **管理者設定** タブをクリックします。
5. 管理者パスワードの変更 ページで、パスワードを変更したい場合、8 ~ 32 文字で少なくとも 1 つの文字、1 つの数字、1 つの特殊文字を含む新しいパスワードを入力します。



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。



暗号化と起動前認証の設定

お使いのコンピュータが自己暗号化ドライブ (SED) を備えている場合、暗号化および起動前認証 (PBA) が使用できます。どちらも 暗号化 タブから設定しますが、これは、自己暗号化ドライブ (SED) がコンピュータに搭載されている場合にのみ表示されます。暗号化または PBA のどちらかを有効化すると、もう一方も有効化されます。

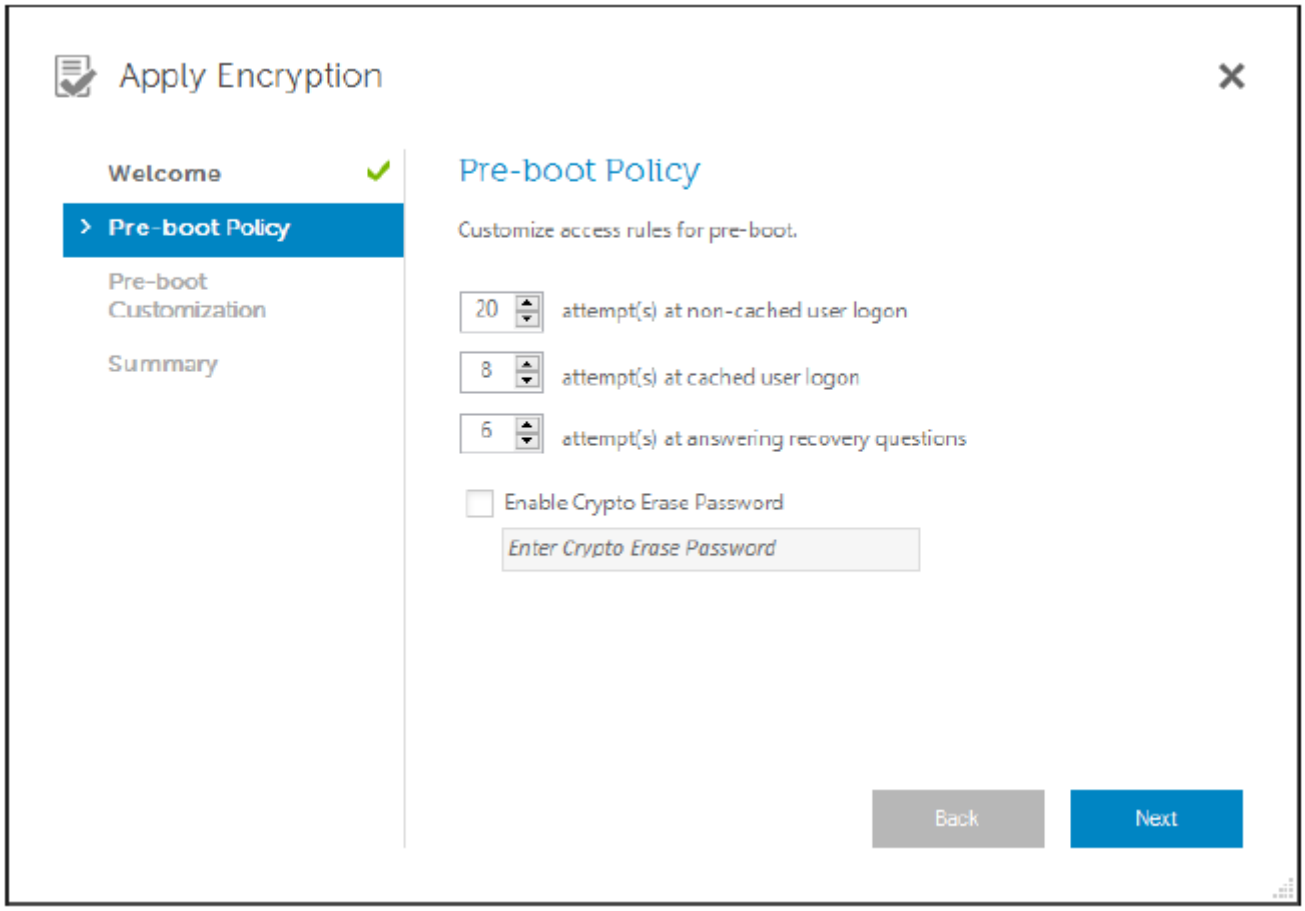
デルでは、パスワードを紛失した場合にそれを回復できるように、暗号化および PBA を有効にする前に、リカバリオプションとしてリカバリ質問を登録して有効化することをお勧めします。詳細については、「サインインオプションの設定」を参照してください。

暗号化および起動前認証を設定するには、次の手順を実行します。

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

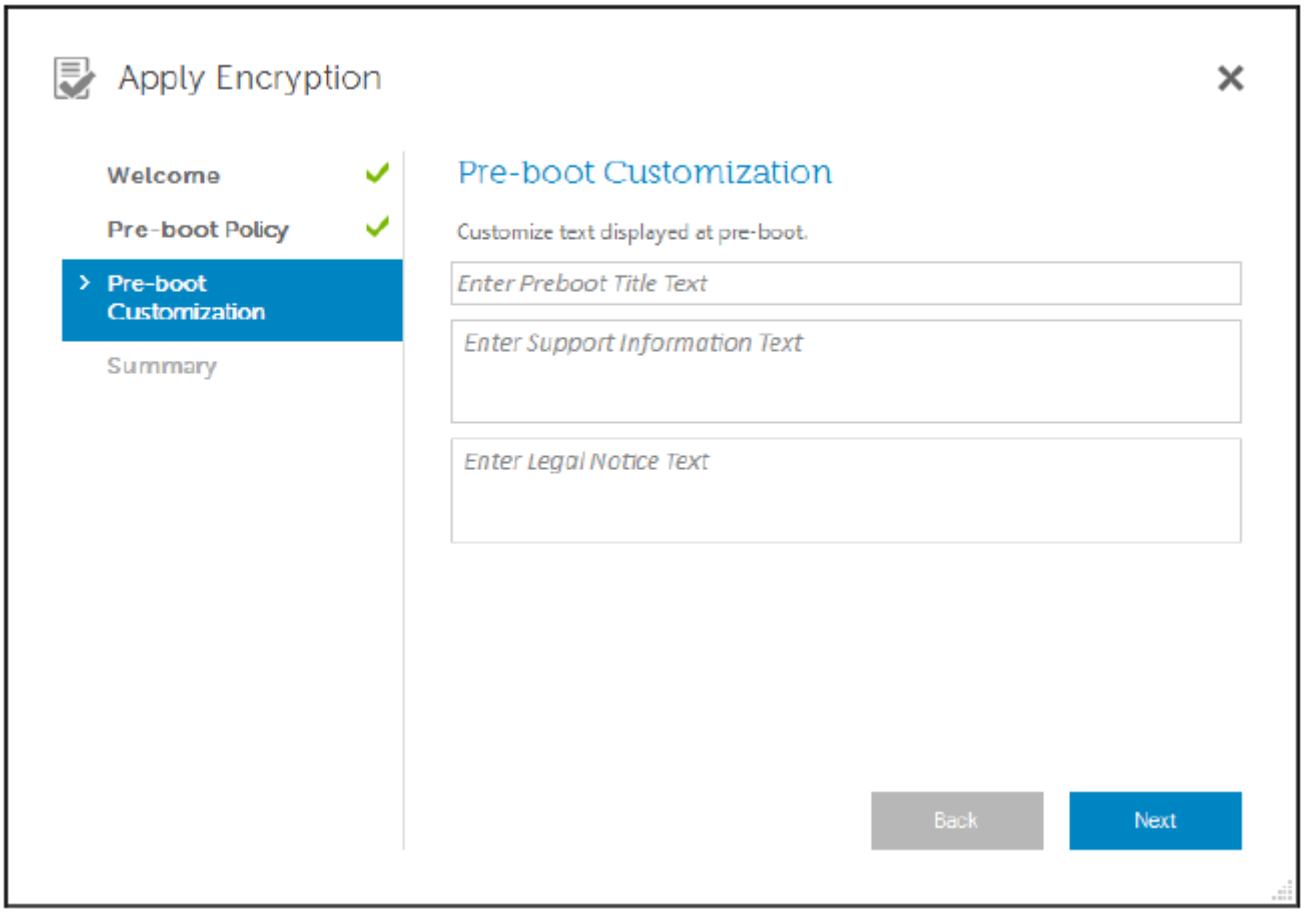
   メモ: 暗号化が有効化されているときに「バックアップ場所が見つかりません」というメッセージが表示され、バックアップ場所が USB ドライブ上にある場合は、ドライブが接続されていない、またはドライブがバックアップ中に使用したスロットとは異なるスロットに接続されています。このメッセージが表示され、バックアップ場所がネットワークドライブ上にある場合は、コンピュータからネットワークにアクセスできません。バックアップ場所の変更が必要な場合は、管理者設定 タブで バックアップ場所の変更 を選択し、現行のスロットまたはアクセス可能なドライブに場所を変更します。場所を再度割り当てた後は、数秒で暗号化の有効化プロセスを続行できるようになります。
3. **暗号化** タブをクリックし、**暗号化** をクリックします。
4. ようこそ ページで、**次へ** をクリックします。
5. 起動前ポリシーページで次の値を変更または確定し、**次へ** をクリックします。

キャッシュされていないユーザーログインの試行回数	不明なユーザー (これまでコンピュータにログインしたことがない、つまり資格情報がキャッシュされていないユーザー)がログインを試行できる回数です。
キャッシュされたユーザーログインの試行回数	キャッシュされたユーザーがログインを試行できる回数です。
リカバリ質問の回答試行回数	ユーザーが正しい回答の入力を試行できる回数です。
暗号化削除パスワードの有効化	選択して有効にします。
暗号化削除パスワードの入力	フェイルセーフセキュリティメカニズムとして使用される 100 文字までの語句またはコード。PBA 認証中にユーザー名またはパスワードのフィールドにこの単語またはコードを入力すると、すべてのユーザーに対する認証トークンが削除され、SED がロックされます。その後は、管理者しかデバイスを強制的にロック解除できません。 緊急時のための暗号化削除パスワードが必要ない場合は、このフィールドを空欄のままにしておいてください。



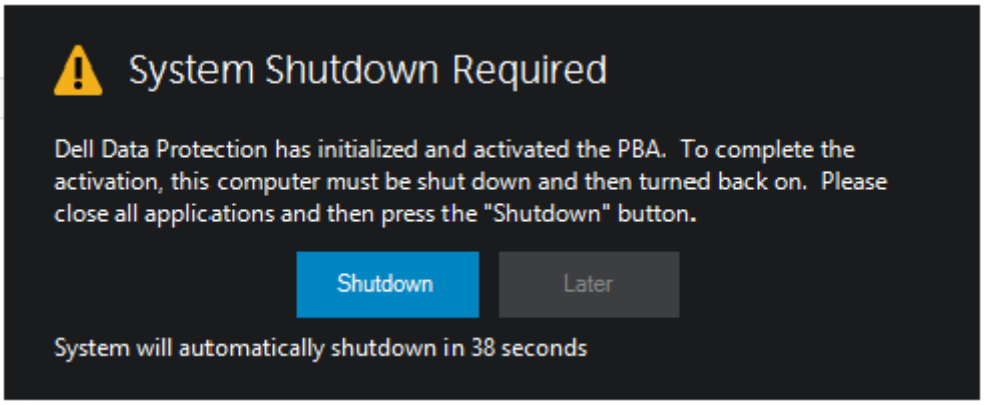
6. 起動前カスタマイズ ページで、起動前認証 (PBA) 画面に表示するカスタムテキストを入力し、**次へ** をクリックします。

起動前タイルテキスト	このテキストは、PBA 画面の上部に表示されます。このフィールドを空のままにすると、タイトルは表示されません。テキストは改行されないため、18 文字以上入力すると、テキストの一部が表示されない場合があります。
サポート情報テキスト	このテキストは、PBA サポート情報 ページに表示されます。Dell は、ヘルプデスクやセキュリティ管理者への連絡方法についての具体的な指示をメッセージに含めるようにカスタマイズすることを推奨します。このフィールドに何も入力しないと、ユーザーが利用できるサポートの連絡先情報が表示されません。テキストの改行は文字単位ではなく単語単位で行われます。例えば、1 単語で 50 文字以上もあるような場合でも改行されず、スクロール バーも表示されないため、テキストの一部が表示されません。
法的通知テキスト	このテキストは、ユーザーのデバイスへのログオンが許可される前に表示されます。たとえば、「OK をクリックすると、容認されているコンピュータの使用ポリシーを遵守することに同意します。」などです。このフィールドにテキストを入力しないと、テキストなし、または OK / キャンセル ボタンが表示されることになります。テキストの改行は文字単位ではなく単語単位で行われます。例えば、1 単語で 50 文字以上もあるような場合でも改行されず、スクロール バーも表示されないため、テキストの一部が表示されません。



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

   暗号化が開始される前に、完全なシャットダウンが必要です。



9. シャットダウン後にコンピュータを再起動してください。

   認証は、今では Security Tools で管理されています。ユーザーは、Windows パスワードを使用して起動前認証画面でログインする必要があります。

暗号化および起動前認証設定の変更

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

- 起動前ポリシーまたはカスタム化の変更 - **暗号化** タブをクリックして **変更** をクリックします。
- SED の複合化 (たとえば、アンインストールのためのもの) - **複合化** をクリックします。

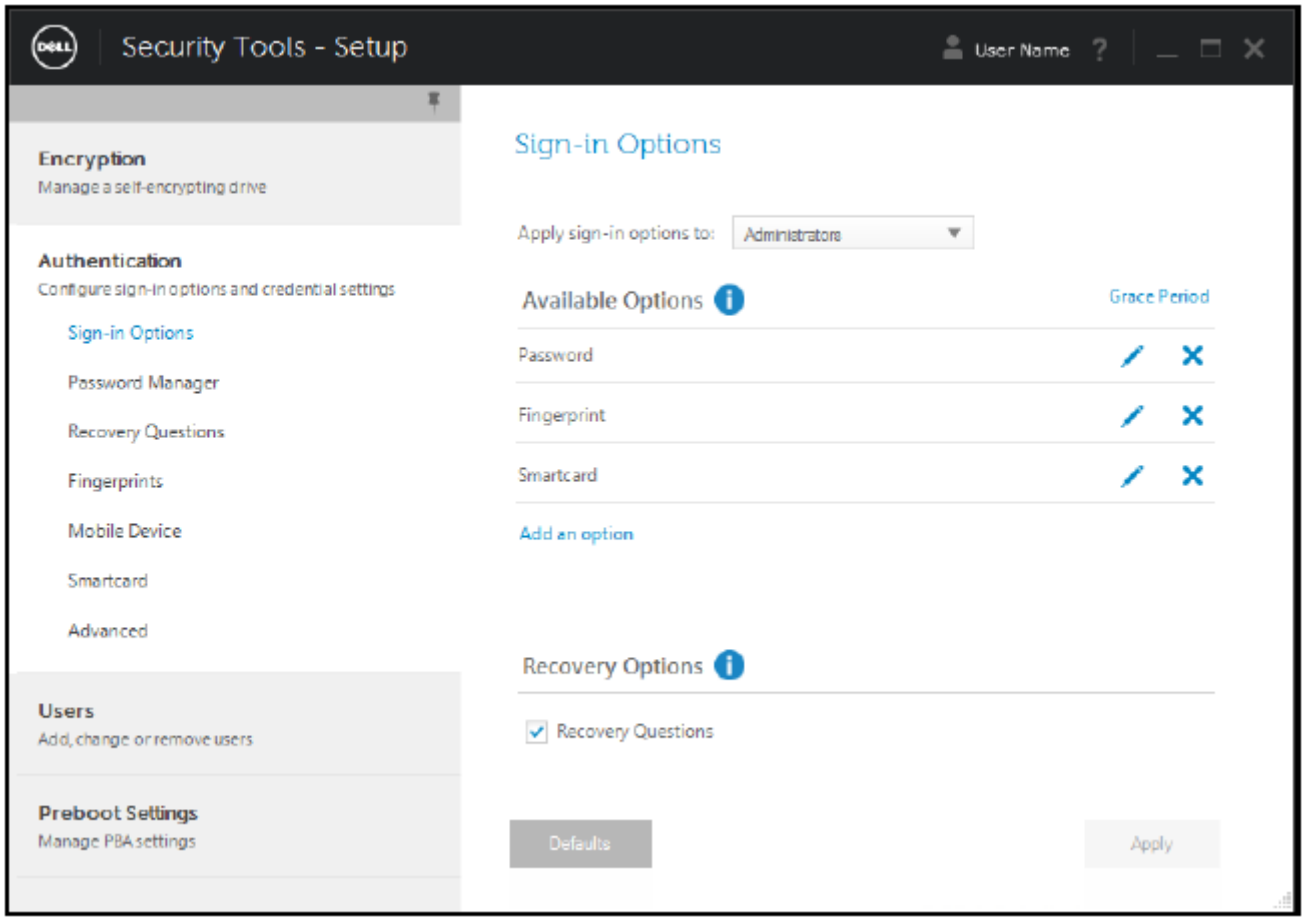
初めて暗号化を有効化し、起動前ポリシーとカスタム化を設定した後は、起動前設定 タブで次のアクションを使用できるようになります。

- 起動前ポリシーまたはカスタム化の変更 - **起動前設定** タブをクリックして **起動前のカスタム化** または **起動前のログオンポリシー** のいずれかを選択します。

アンインストールの指示については、「アンインストールタスク」を参照してください。

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。



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。

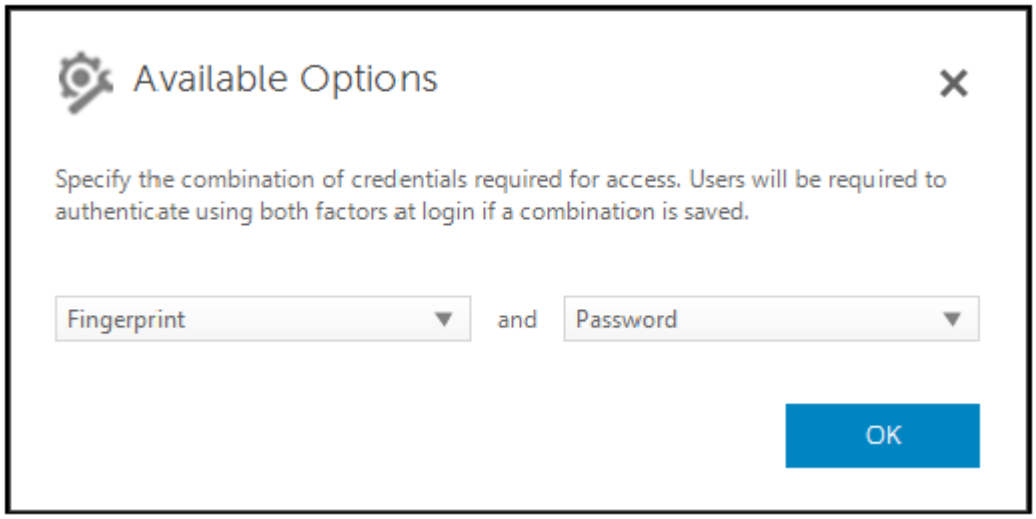
サインインオプションを設定するには、次の手順を実行します。

1. 左ペインの 認証 で、**サインインオプション** を選択します。
2. 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。
3. 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。

4. 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。

     メモ: 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。
5. 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。

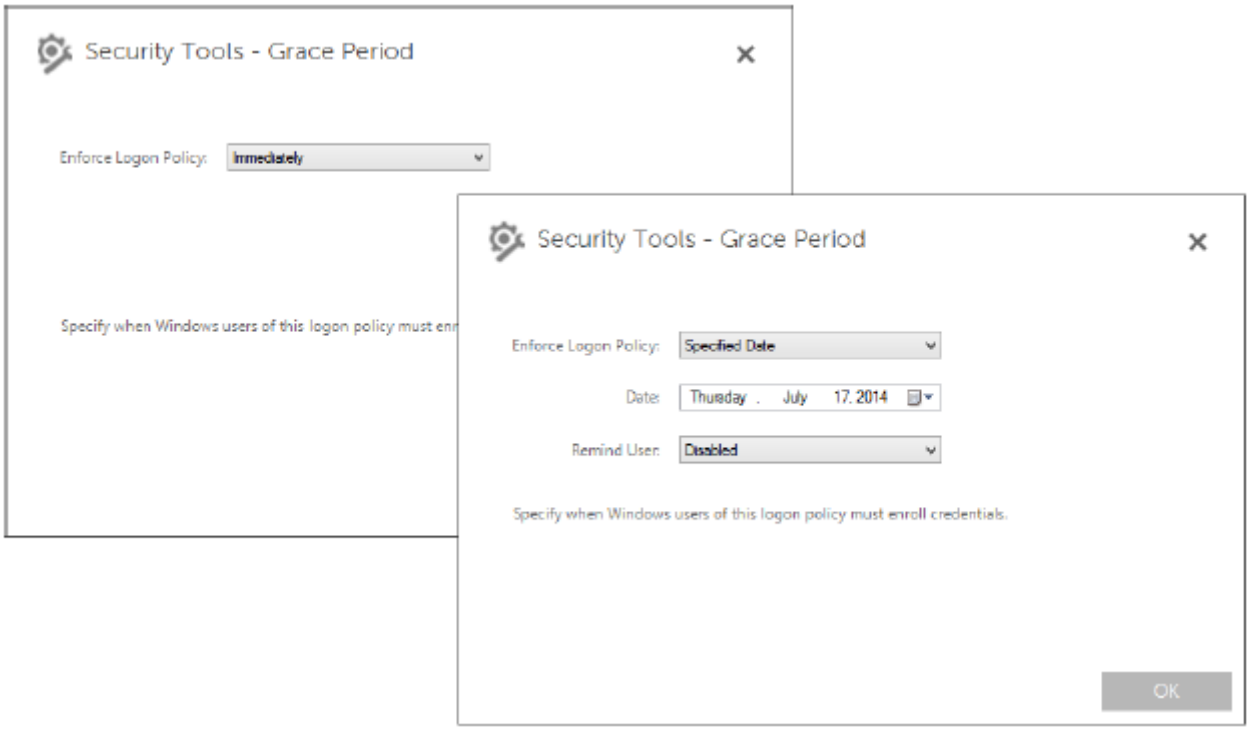
   猶予期間機能では、設定されたサインインオプションの執行を開始する日付を設定することができます。サインインオプションが執行される日付よりも前にサインインオプションを設定して、ユーザーの登録を許可する期間を設定します。デフォルトでは、ポリシーが即時に執行されます。

   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。

   次回の 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ド* 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。

   メモ:

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、ユーザーはサインイ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。ユーザーがサインイ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。

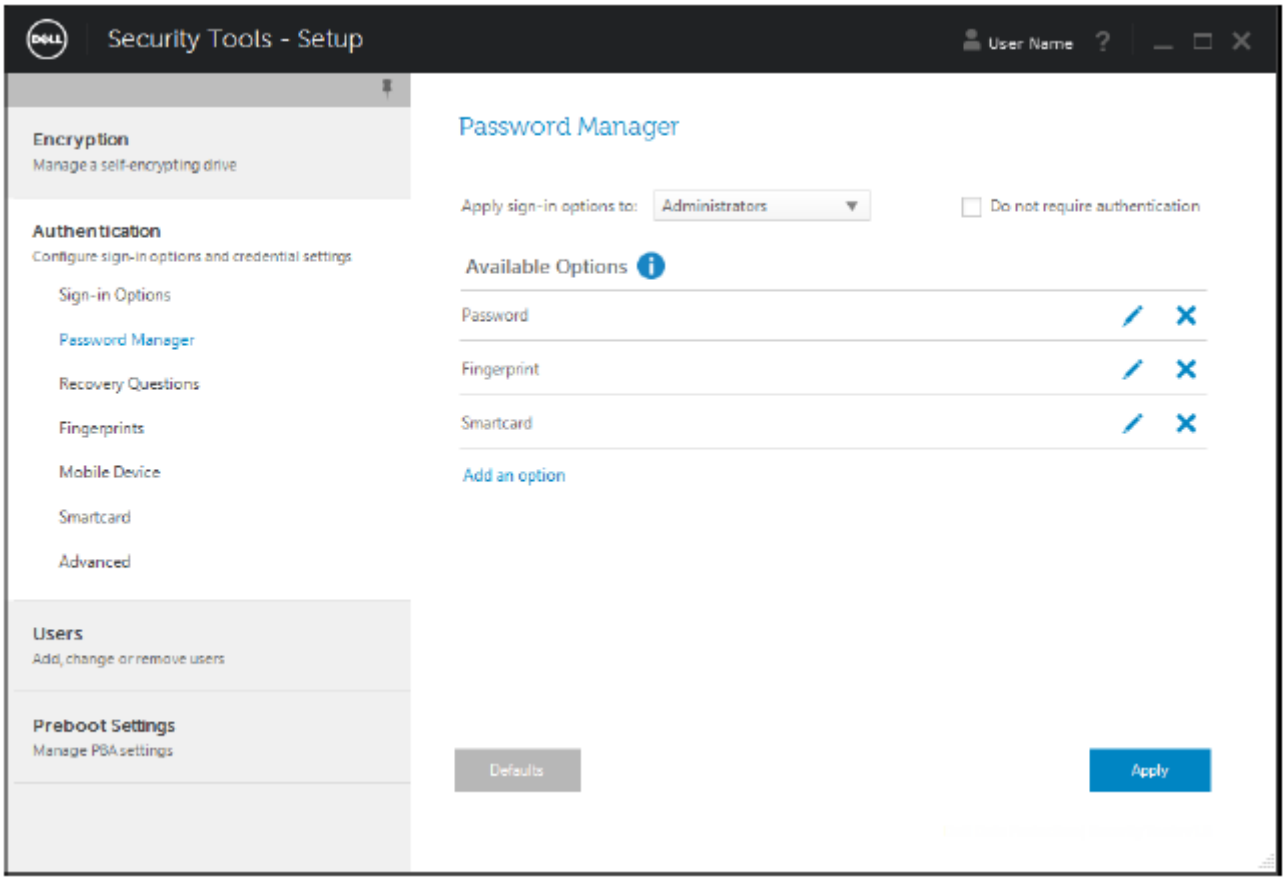
6. 選択された役割の設定を保存するには、**適用** をクリックします。

Password Manager 認証の設定

Password Manager ページでは、Password Manage 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。

1. 左ペインの 認証 で、**Password Manager** を選択します。
2. 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。
3. 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に自動的にログオンできるようにします。

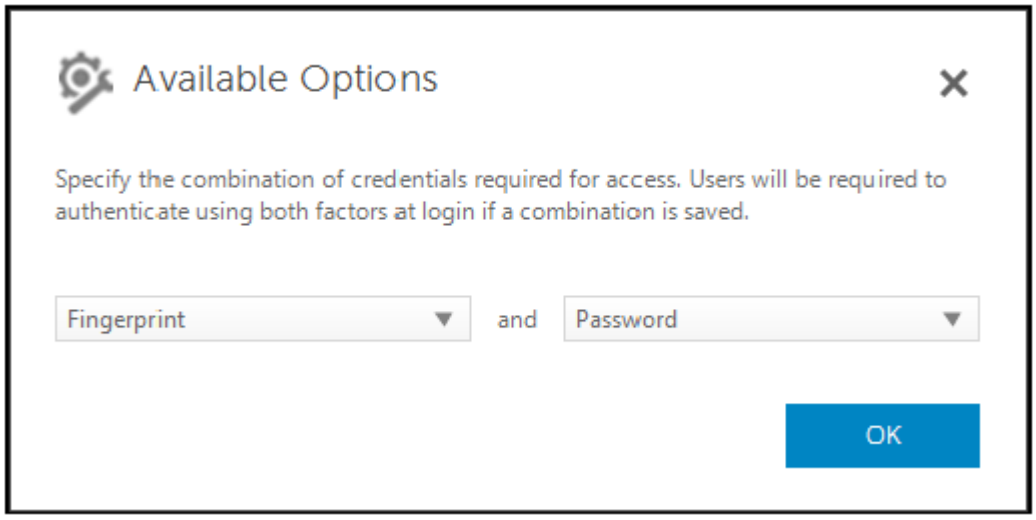


4. 認証用に 使用可能なオプション を設定します。

   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。

5. 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。

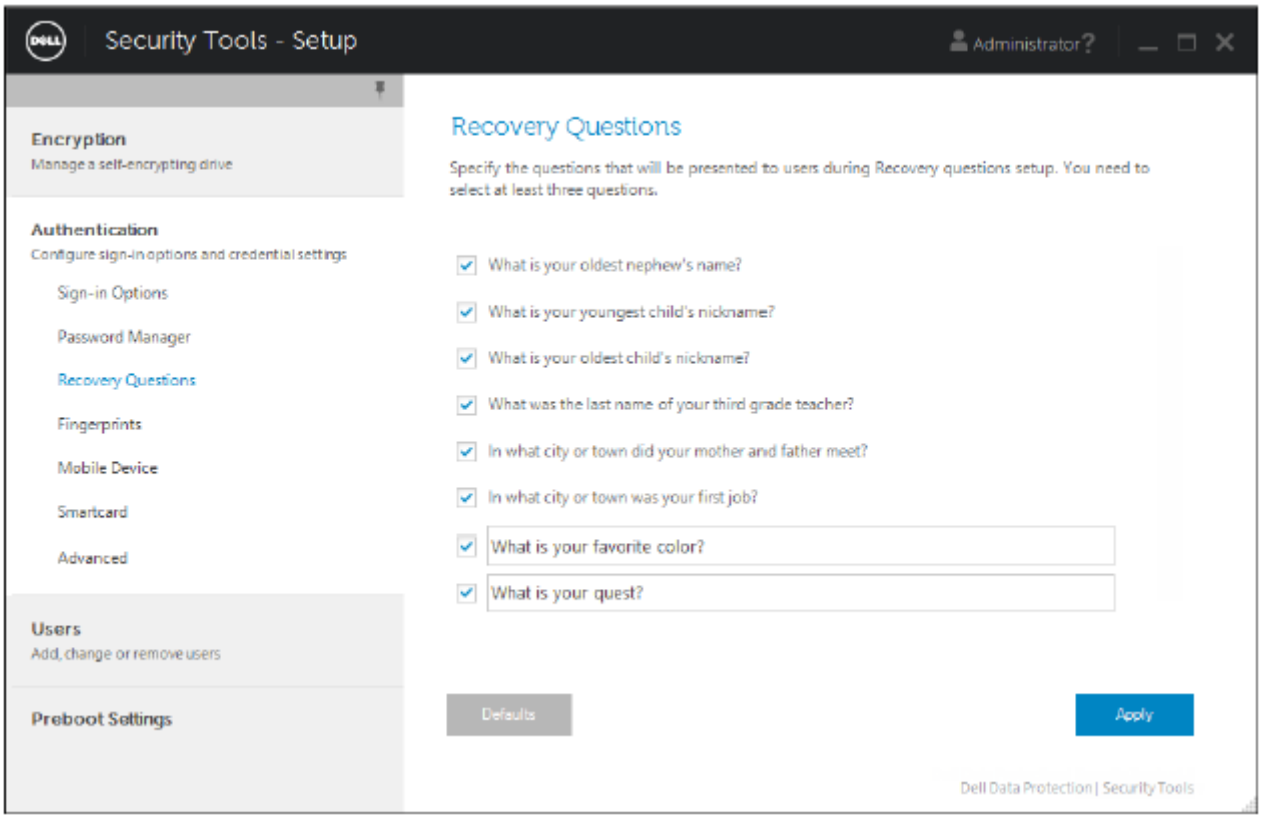
メモ: **元の値に設定を復元するには、デフォルト ボタンを選択します。**

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。

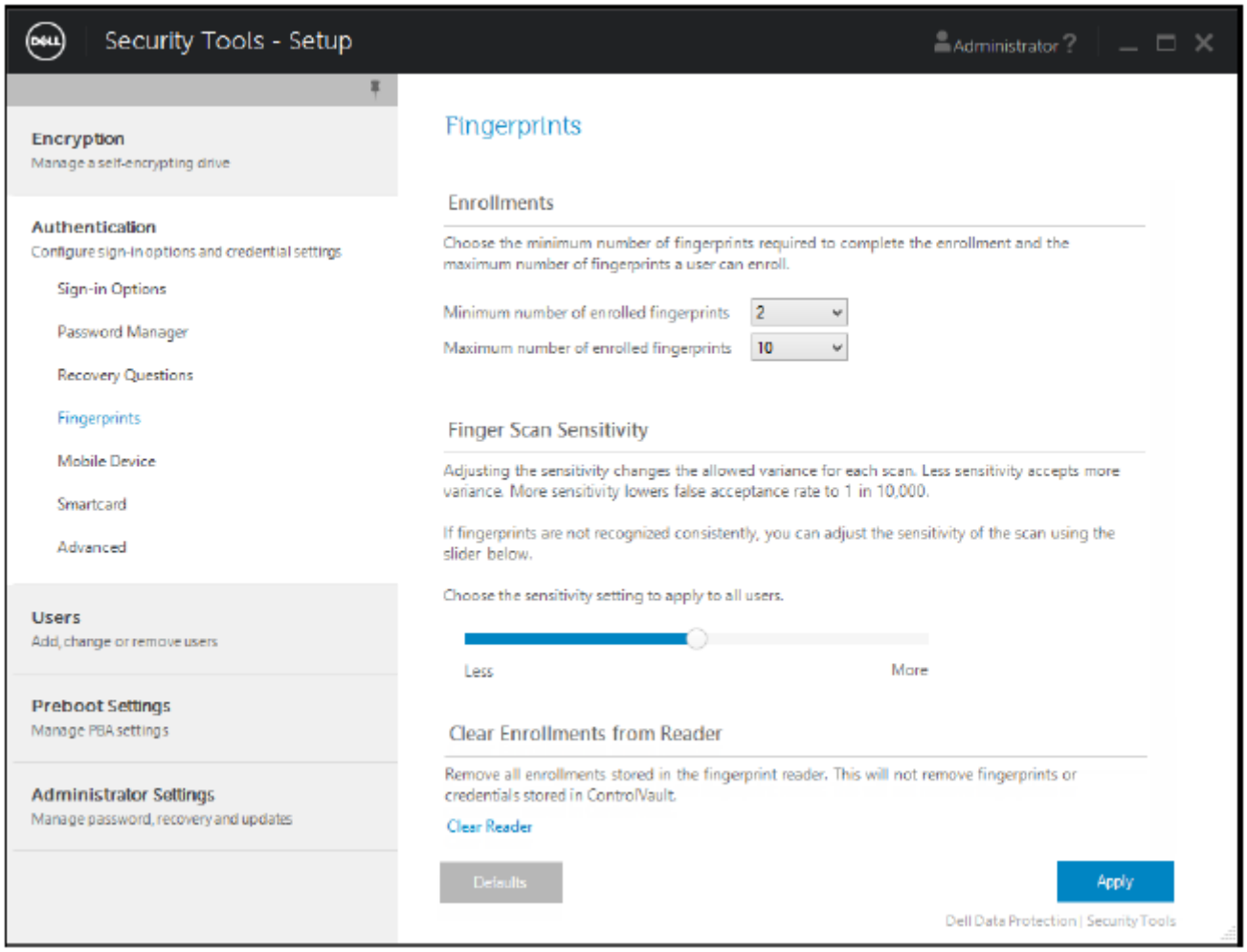
1. 左ペインの 認証 で、**リカバリ質問** を選択します。
2. リカバリ質問 ページでは、少なくとも 3 つの事前定義済みリカバリ質問を選択します。
3. オプションとして、ユーザーが質問を選択するリスト内に最大 3 つのカスタム質問を追加できます。
4. リカバリ質問を保存するには、**適用** をクリックします。



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。

1. 左ペインの 認証 で、**指紋** を選択します。
2. 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。



3. 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。
4. 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。
5. 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。

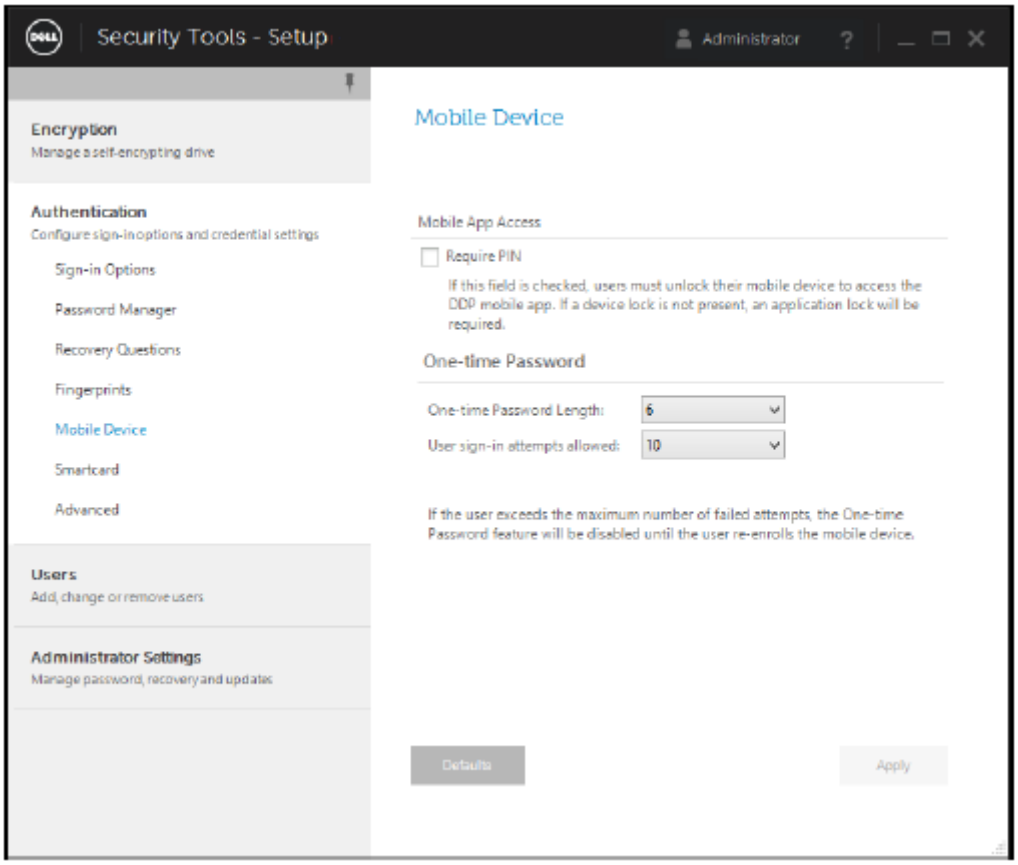
モバイルデバイス ページでは、モバイルデバイスのセキュリティをさらに向上させる設定と、ワンタイムパスワードを設定できます。

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。

1. 左ペインにある 認証 で **モバイルデバイス** を選択します。
2. 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。

   メモ: 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。



3. 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。
4. 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、ユーバ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。

   メモ: 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。

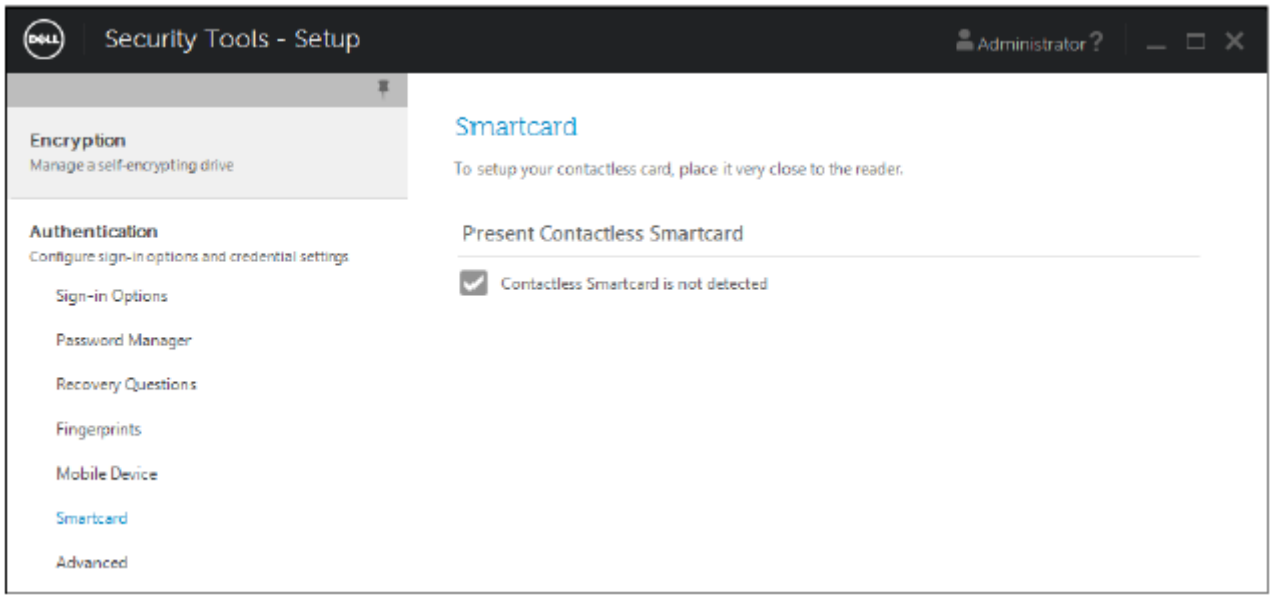
接触型カードでは、カードを挿入するスマートカードリーダーが必要です。接触型カードとの互換性があるのは、ドメインコンピュータのみです。CAC および SIPRNet カードは、どちらも接触型カードです。これらのカードの高度な機能性のため、ユーザーがログオンするには、カード挿入後に証明書の選択が必要となります。

- 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。

メモ: 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。

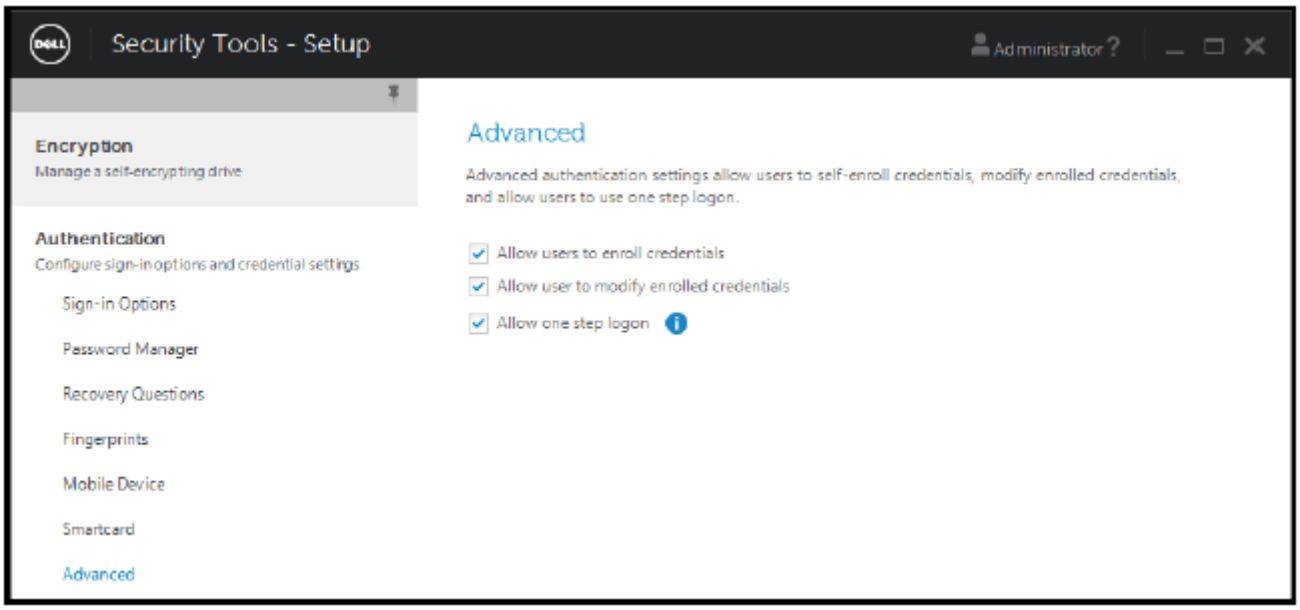
スマートカード登録を設定するには、次の手順を実行します。

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

1. **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。



2. 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。

   メモ: 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。

メモ: 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。

3. 終了したら **適用** をクリックします。

スマートカードとバイオメトリックサービス (オプション)

Security Tools がスマートカードおよびバイオメトリックデバイスに関連付けられているサービスを「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。
- WbioSrvc - Windows 生体認証サービスは、クライアントアプリケーションに対し、生体認証ハードウェアやサンプルに直接アクセスすることなく、生体認証データの取得、比較、操作、および保存する機能を提供します。このサービスは特権 SVCHOST プロセスでホストされます。

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

自動サービス起動の無効化

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。

1. **Regedit** を実行します。
2. 次のレジストリエントリを探します。

   [HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

   SmartCardServiceCheck=REG_DWORD:0

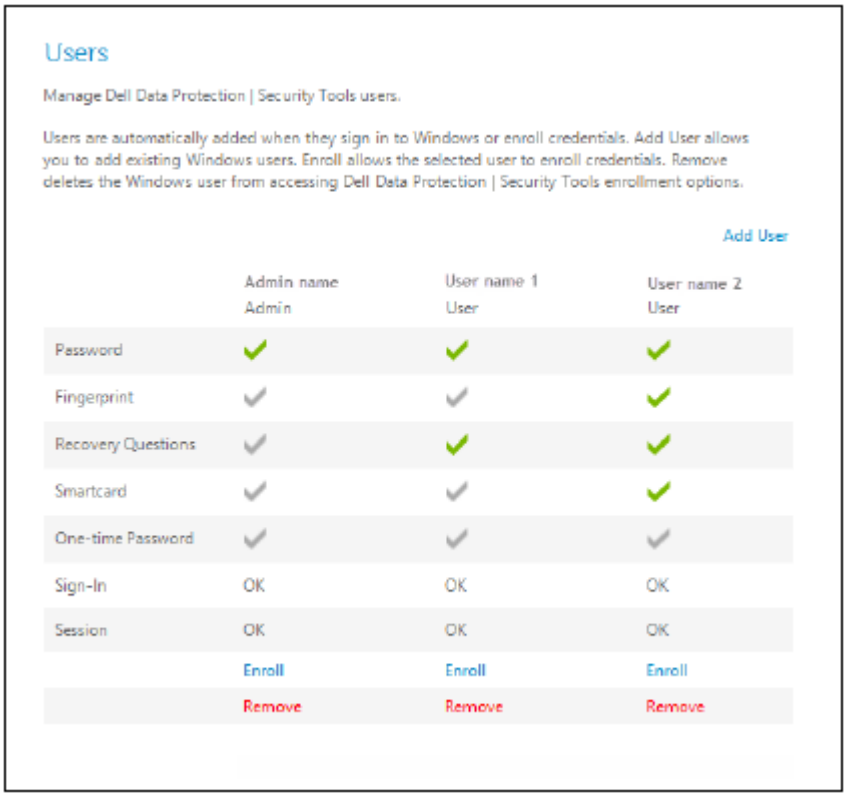
   有効化するには 0 に設定します。無効化するには 1 に設定します。

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



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。

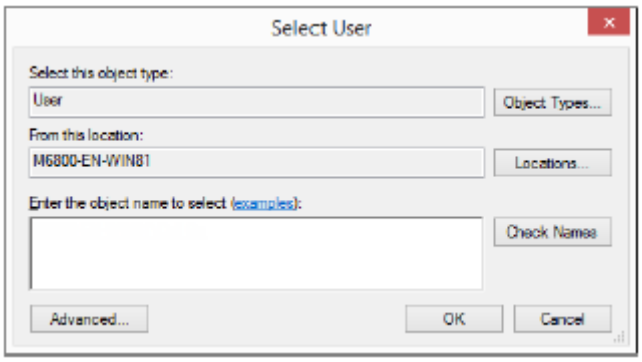
サインイン ステータスが OK のときは、ユーザーがログオンするために必要なすべての登録が完了しています。セッション ステータスが OK のときは、ユーザーが Password Manager を使用するために必要なすべての登録が完了しています。

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

メモ: 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。

1. 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。
2. *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。



3. 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。

4. 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。

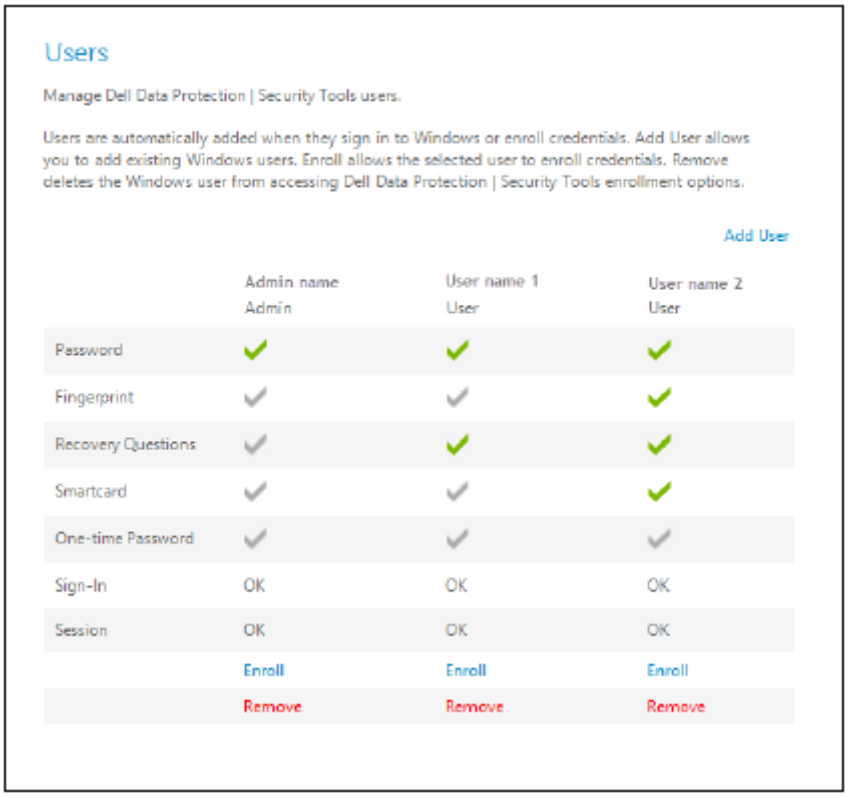
   続いて ユーザー資格情報の登録または変更 に移動して指示を表示します。

ユーザー資格情報の登録または変更

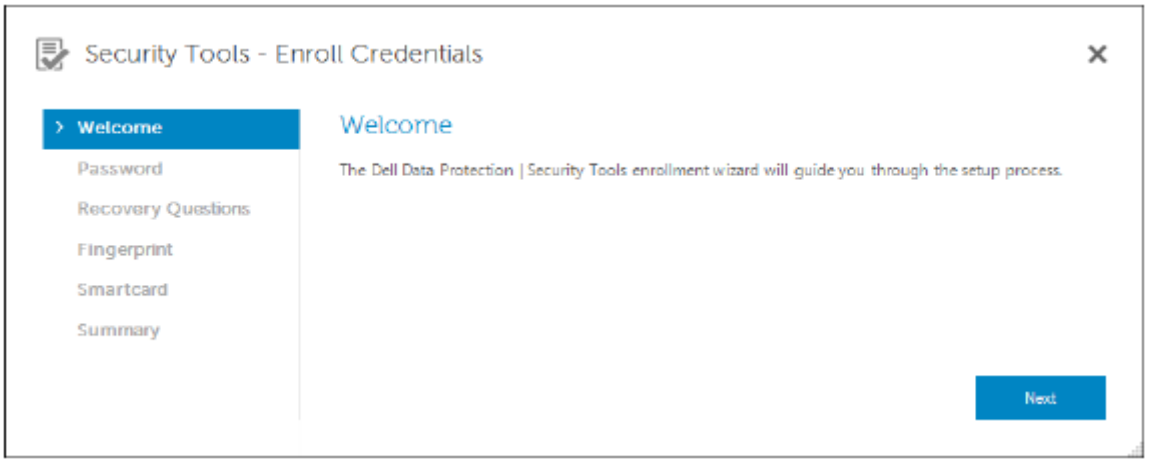
管理者は、ユーザーの代理としてユーザーの資格情報を登録または変更できますが、リカバリ質問やユーザーの指紋のスキャンなど、いくつかの登録アクティビティにはユーザーの参加が必要です。

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。

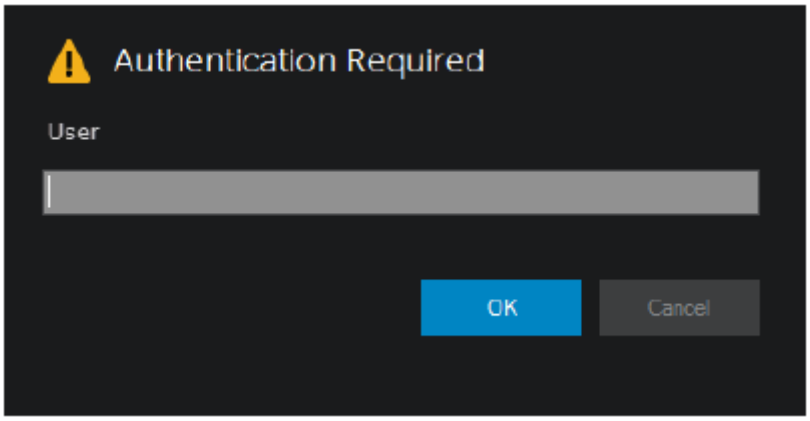
1. 管理者設定 で **ユーザー** タブをクリックします。
2. ユーザー ページで **登録** をクリックします。



3. ようこそ ページで **次へ** をクリックします。



4. 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。



5. 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。
6. 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。
7. 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。

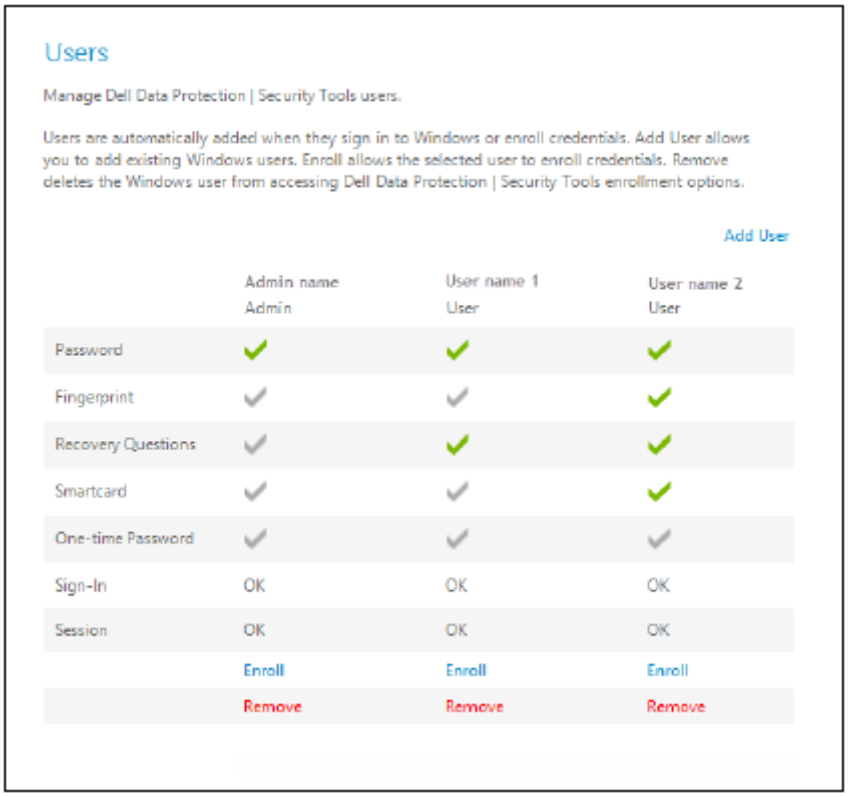
   資格情報登録 ページに戻って変更を行うには、変更するページが表示されるまで **戻る** をクリックします。

   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

1. **管理者設定** タイルをクリックします。
2. **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。
3. 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。
4. ⊗ 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。

   メモ: 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

1. **管理者設定** タイルをクリックします。
2. **ユーザー** タブをクリックし、削除するユーザーを見つけます。
3. **削除** をクリックします。(remove コマンドは、ユーザーの設定の下部に赤色で表示されます。)
   削除後、ユーザーは再登録しない限り、コンピュータにはログオンできなくなります。

5

アンインストールタスク

DDP | Security Tools をアンインストールするには、少なくとも **ローカル管理者** ユーザーである必要があります。

DDP | Security Tools のアンインストール

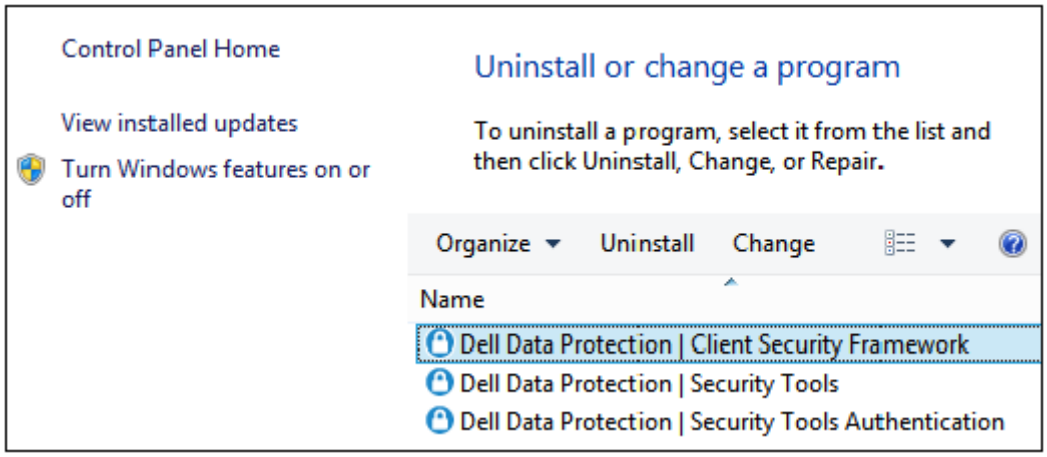
アプリケーションは、次の順序でアンインストールする必要があります。

1. DDP | Client Security Framework
2. DDP | Security Tools 認証
3. DDP | Security Tools

自己暗号化ドライブ搭載のコンピュータをお持ちの場合 は、次の手順に従ってアンインストールを行います。

1. SED のプロビジョニング解除：
   a) 管理者設定 から、**暗号化** タブをクリックします。
   b) **複合化** をクリックして暗号化を無効にします。
   c) SED が暗号化解除されたら、コンピュータを再起動します。
2. Windows コントロールパネルで **プログラムのアンインストール** に移動します。

   メモ: スタート > コントロールパネル > プログラムと機能 > プログラムのアンインストール。



3. **Client Security Framework** をアンインストールし、コンピュータを再起動します。
4. Windows コントロールパネルから、**Security Tools Authentication** をアンインストールします。

   ユーザーデータを保持するかどうかを尋ねるメッセージが表示されます。

   Security Tools を再インストールする予定の場合は、**はい** をクリックします。それ以外の場合は、**いいえ** をクリックします。

   アンインストールの完了後、コンピュータを再起動します。

5. Windows コントロールパネルから、**Security Tools** をアンインストールします。

   このアプリケーションとそのコンポーネントを完全にアンインストールするかどうかを尋ねるメッセージが表示されます。

   はい をクリックします。

   *アンインストール完了*ダイアログが表示されます。
6. **はい、今すぐコンピュータを再起動します** をクリックし、**完了** をクリックします。
7. コンピュータが再起動され、アンインストールが完了します。

6

リカバリ

リカバリオプションは、ユーザー資格情報の期限が切れた、または紛失した場合に使用することができます。

- **ワンタイムパスワード（OTP）:** ユーザーは、登録済みモバイルデバイス上で Security Tools Mobile を使用して OTP を生成し、アクセスを回復させるために Windows ログオン画面でこの OTP を入力します。このオプションは、コンピュータ上でモバイルデバイスを Security Tools に登録した場合に限り、使用可能です。リカバリのために OTP 機能を使用するには、ユーザーがコンピュータへのログオンに OTP を使用していない必要があります。

  メモ: ワンタイムパスワード（OTP）機能には TPM が存在し、有効化および所有されている必要があります。「所有権のクリアと TPM のアクティブ化」の指示に従います。OTP 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。詳細については、「サインオンオプションの設定」を参照してください。

- **リカバリ質問:** ユーザーは、一連の個人的な質問に正しく回答してコンピュータへのアクセスを回復させます。このオプションは、管理者がリカバリ質問を設定および有効化しており、ユーザーがリカバリ質問を登録した場合にのみ使用可能です。このオプションは、起動前認証画面および Windows ログオン画面の両方からコンピュータへのアクセスを回復させるために使用できます。

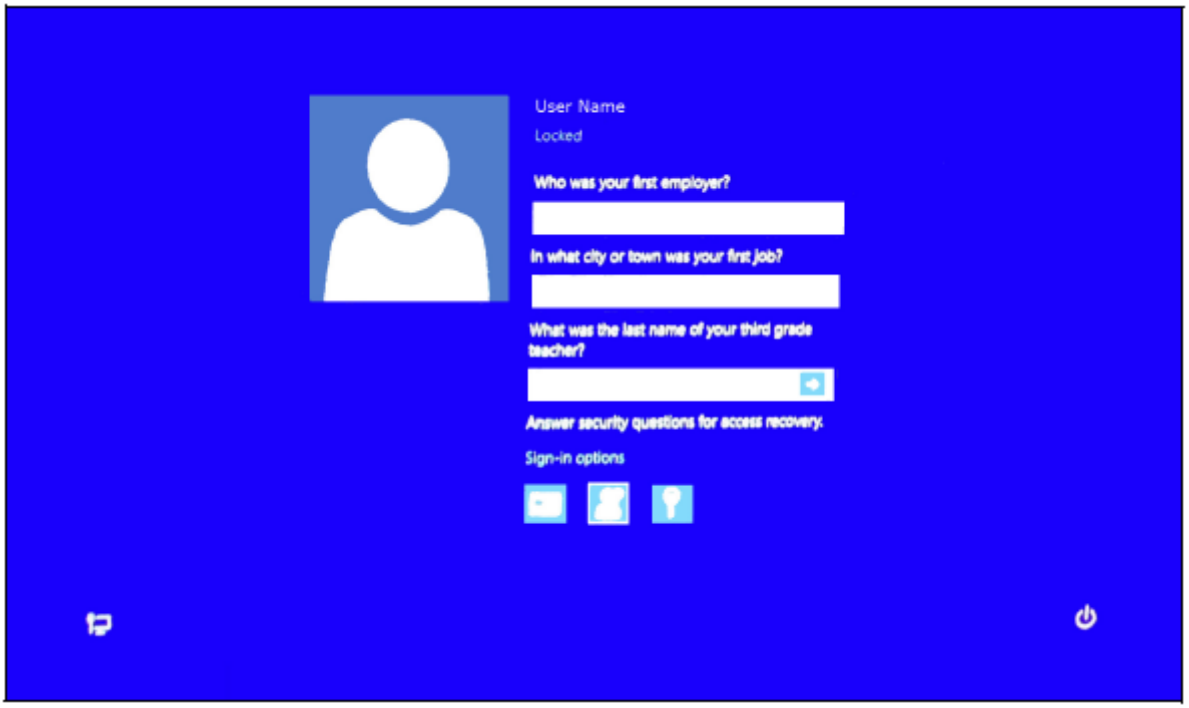
どちらのリカバリ方法でも、リカバリ質問の登録、またはコンピュータ上でのモバイルデバイスの Security Tools への登録のいずれかによってリカバリ準備を整えておく必要があります。

セルフリカバリ、Windows ログオンリカバリ質問

Windows ログオン画面でアクセスを回復させるためのリカバリ質問に回答するには、次の手順を実行します。

1. リカバリ質問を使用するには、**アカウントにアクセスできませんか?** をクリックします。

   登録時に選択したリカバリ質問が表示されます。



2. 回答を入力し、**OK** をクリックします。

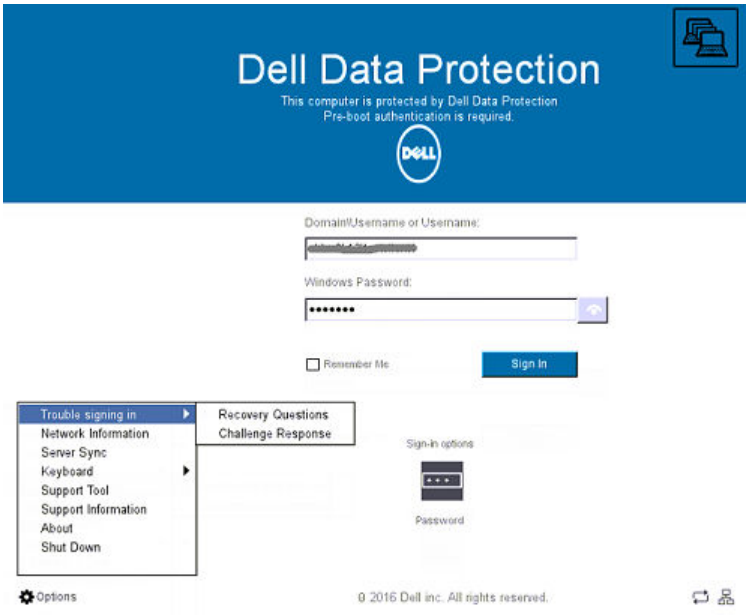
   質問に対する回答を正しく入力すると、アクセスリカバリ モードになります。この後の動作は、失敗した資格情報の内容によって異なります。

   - 正しい Windows パスワードの入力に失敗すると、パスワードの変更 画面が表示されます。
   - 指紋の認識が失敗すると、指紋を再登録できる 指紋登録 ページが表示されます。

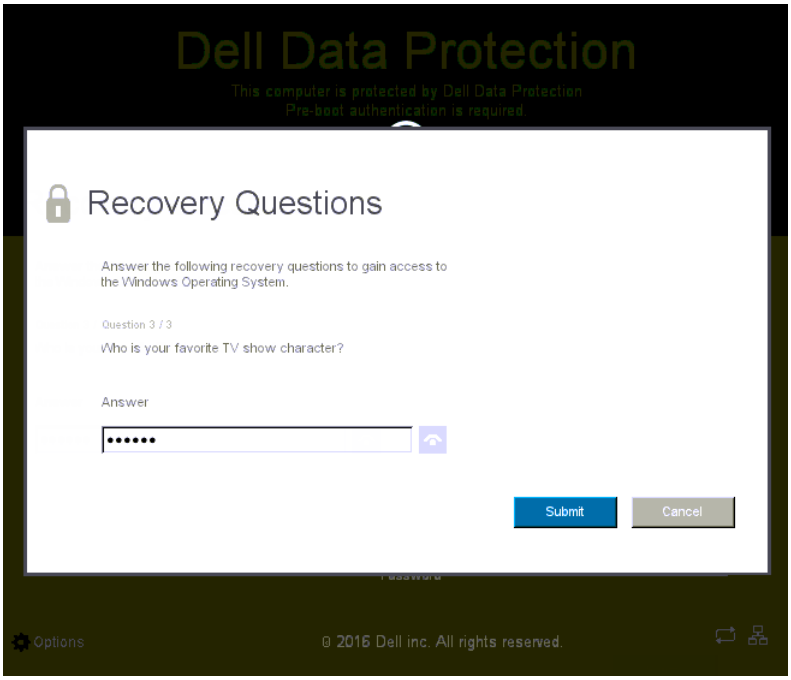
セルフリカバリ、PBA リカバリ質問

起動前認証画面でアクセスを回復させるためのリカバリ質問に回答するには、次の手順を実行します。

1. ユーザー名を入力します。
2. 画面の左下隅で **オプション**、**サインインできない場合** の順にクリックします。



3. Q&A ダイアログが表示されたら、初回サインイン時にリカバリ質問に登録したときに提供した回答を入力します。



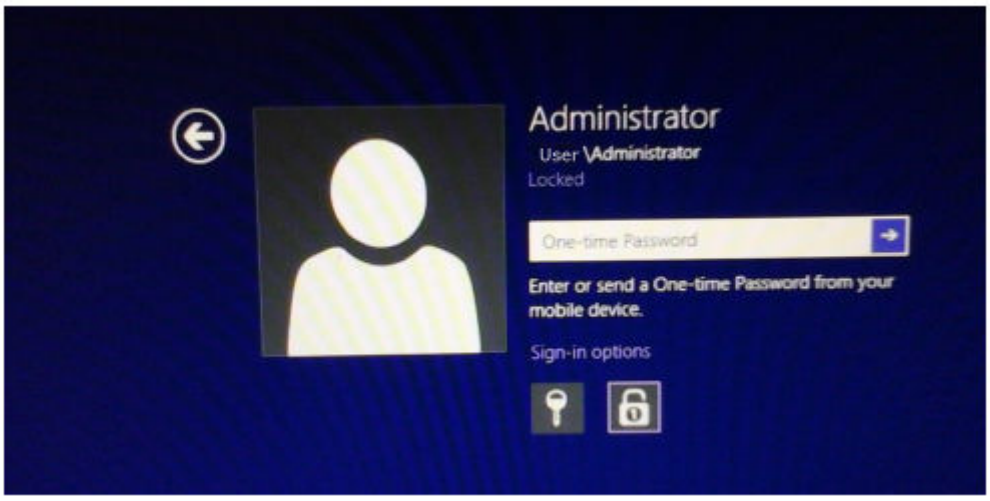
セルフリカバリ、ワンタイムパスワード

この手順では、例えば Windows パスワードの期限が切れた、パスワードを忘れた、またはログオンの最大許容回数を超過した場合に、ワンタイムパスワード (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方法を説明します。ワンタイムパスワード (OTP) オプションは、ユーザーがモバイルデバイスを登録した場合、または、OTP が Windows への最後のログオンに使用されていない場合に限り、使用可能です。

メモ: ワンタイムパスワード機能には TPM が存在し、有効化および所有されている必要があります。OTP は Windows 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。管理者は、リカバリまたは認証のいずれかのために OTP を許可するポリシーを設定する、またはこの機能を無効化することができます。

コンピュータへのアクセスを回復するために OTP を使用するには、次の手順を実行します。

1. Windows ログオン画面で OTP アイコン を選択します。



2. モバイルデバイスで Security Tools Mobile アプリを開き、パスワードを入力します。
3. アクセスするコンピュータを選択します。

   モバイルデバイスにコンピュータ名が表示されない場合は、次のいずれかの状態が存在する可能性があります。

   - モバイルデバイスがアクセスしたいコンピュータに登録またはペアリングされていない。

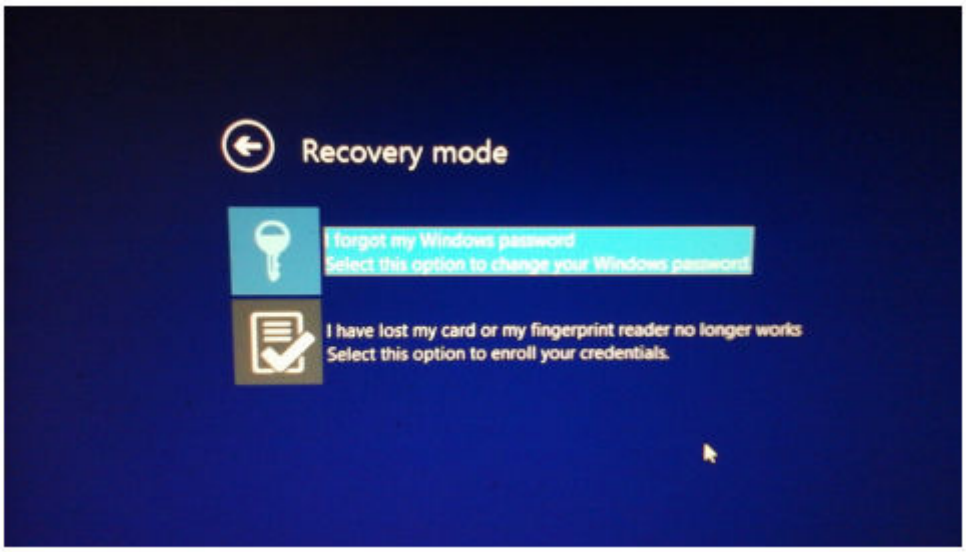
- 複数 Windows ユーザーアカウントを持っている場合は、アクセスしようとしているコンピュータ上に DDP | Security Tools がインストールされていないか、コンピュータとモバイルデバイスのペアリングに使用したアカウントとは異なるユーザーアカウントにログオンしようとしているかのいずれかです。

4. **ワンタイムパスワード** をタップします。

   モバイルデバイス画面にパスワードが表示されます。

   メモ: 必要であれば、更新シンボル をクリックして新しいコードを取得します。最初 2 回の OTP 更新後、別の OTP を生成できるようになるまでに 30 秒の遅延が発生します。コンピュータとモバイルデバイスは、両方が同時に同じパスワードを認識できるように同期化されている必要があります。パスワードを急速に連続して作成しようとすると、コンピュータとモバイルデバイスが非同期状態となり、OTP 機能が失敗する原因となります。この問題が発生した場合は、2 つのデバイスが再度同期化されるまで 30 秒程待ってから、再試行してください。

5. コンピュータの Windows ログオン画面で、モバイルデバイスに表示されているパスワードを入力し、**Enter** を押します。
6. コンピュータのリカバリ モード画面で、**Windows パスワードを忘れた** を選択し、画面上の手順に従ってパスワードをリセットします。



7

用語集

プロビジョニング解除 - プロビジョニング解除により、PBA データベースが削除され、PBA が非アクティブ化されます。プロビジョニング解除を有効にするには、シャットダウンが必要です。

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ことがあります。

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、ソフトウェアボー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。