Dell Data Protection

Security Tools Installation Guide v1.12

February 2017
Rev. A01

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

Introduction

Dell Data Protection | Security Tools provides security and identity protection to Dell computer administrators and users. DDP | Security Tools is pre-installed on all Dell Latitude, Optiplex, and Precision computers and on select Dell XPS notebooks. Should you need to *reinstall* DDP | Security Tools, follow the instructions in this guide. For additional support, see www.dell.com/support > Endpoint Security Solutions.

Overview

DDP | Security Tools is an end-to-end security solution designed to provide advanced authentication support, as well as support for Preboot Authentication (PBA) and management of self-encrypting drives.

DDP | Security Tools provides multi-factor support for Windows authentication with passwords, fingerprint readers, and smart cards - both "contactless" and "contacted" - as well as self-enrollment, One-Step Logon (Single Sign-On [SSO]), and One-time Passwords (OTP).

Before making Security Tools available to end users, administrators may want to configure Security Tools features, using the DDP Security Console's Administrator Settings tool, for example, to enable Preboot Authentication and authentication policies. However, default settings allow administrators and users to begin using Security Tools immediately after installation and activation.

DDP Security Console

The DDP Security Console is the Security Tools interface through which users can enroll and manage their credentials and configure self-recovery questions, based on policy set by the administrator. Users can access these Security Tools applications:

- The Encryption tool allows users to view the encryption status of the computer's drives.
- The Enrollments tool allows users to set up and manage credentials, configure self-recovery questions, and view the status of their credential enrollment. These privileges are based on policy set by the administrator.
- Password Manager allows users to automatically fill in and submit data required to log on to websites, Windows applications, and network resources. Password Manager also provides the capability for a user to change their logon passwords through the application, ensuring that passwords maintained by Password Manager are kept in sync with those of the targeted resource.

Administrator Settings

The Administrator Settings tool is used to configure Security Tools for all users of the computer, allowing the administrator to set up authentication policies, manage users, and configure which credentials can be used for Windows logon.

With the Administrator Settings tool, the administrator can enable encryption and Preboot Authentication (PBA), as well as configure PBA policies and customize PBA screen text.

Continue to Requirements.

2

Requirements

- DDP | Security Tools is pre-installed on all Dell Latitude, Optiplex, and Precision computers and on select Dell XPS notebooks, and meets the following minimum requirements. Should you need to reinstall DDP | Security Tools, ensure that your computer still meets these requirements. See www.dell.com/support > Endpoint Security Solutions for more information.
- Windows 8.1 should not be installed on drive 1 on self-encrypting drives. This operating system configuration is not supported because Windows 8.1 creates a recovery partition drive 0 which in turn, breaks Preboot Authentication. Instead, either install Windows 8.1 on the drive configured as drive 0, or restore Windows 8.1 as an image to any of the drives.
- DDP | Security Tools does not support dynamic disks.
- Computers equipped with self-encrypting drives cannot be used with Hardware Crypto Accelerators. Incompatibilities exist that prevent the provisioning of the HCA. Note that Dell does not sell computers with self-encrypting drives that support the HCA module. This unsupported configuration would be an after-market configuration.
- DDP | Security Tools does not support multiboot disk configuration.
- Before installing a new operating system on the client, clear the Trusted Platform Module (TPM) in the BIOS.
- An SED does not require a TPM to provide Advanced Authentication or encryption.

Drivers

- Supported Opal compliant SEDs require updated Intel Rapid Storage Technology Drivers, located at http://www.dell.com/support/drivers/us/en/19/DriverDetails/Product/latitude-e6440-laptop?driverId=1KX2H&osCode=W764&fileId=3356216042&languageCode=en&categoryId=SA

NOTE:

Due to the nature of RAID and SEDs, SED management does not support RAID. The issue with "RAID=On" with SEDs is that RAID requires access to the disk to read and write RAID-related data at a high sector not available on a locked SED from start and cannot wait to read this data until after the user is logged on. Change the SATA operation in the BIOS from "RAID=On" to "AHCI" to resolve the issue. If the operating system does not have the AHCI controller drivers pre-installed, the operating system will blue screen when switched from "RAID=On" to "AHCI."

Client Prerequisites

- The full version of Microsoft .Net Framework 4.5 (or later) is required for Security Tools. All computers shipped from the Dell factory are pre-installed with the full version of Microsoft .Net Framework 4.5. However, if you are not installing on Dell hardware or are upgrading Security Tools on older Dell hardware, you should verify which version of Microsoft .Net is installed and update the version, prior to installing Security Tools to prevent installation/upgrade failures. To install the full version of Microsoft .Net Framework 4.5, go to https://www.microsoft.com/en-us/download/details.aspx?id=30653

  To verify the version of .Net installed, follow these instructions on the computer targeted for installation: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx
- Drivers and firmware for your authentication hardware must be up-to-date on your computer. To obtain drivers and firmware for Dell computers, go to http://www.dell.com/support/home/us/en/19/Products/?app=drivers and select your computer model. Based on your authentication hardware, download the following:
  - NEXT Biometrics Fingerprint Driver
  - Validity FingerPrint Reader 495 Driver
  - O2Micro Smartcard Driver
  - Dell ControlVault

  Other hardware vendors may require their own drivers.

The installer installs this component if not already installed on the computer:

Prerequisites
• Microsoft Visual C++ 2012 Update 4 or later Redistributable Package (x86/x64)

Software

Windows Operating Systems

The following table details supported software.

Windows Operating Systems (32- and 64-bit)
• Microsoft Windows 7 SP0-SP1 - Enterprise - Professional **NOTE: Legacy Boot mode is supported on Windows 7. UEFI is not supported on Windows 7.**
• Microsoft Windows 8 - Enterprise - Pro - Windows 8 (Consumer) **NOTE: Windows 8 is supported with UEFI Mode when used with Opal Compliant SEDs and Dell Computer Models - UEFI Support.**
• Microsoft Windows 8.1 - 8.1 Update 1 - Enterprise Edition - Pro Edition **NOTE: Windows 8.1 is supported with UEFI Mode when used with Opal Compliant SEDs and Dell Computer Models - UEFI Support.**
• Microsoft Windows 10 through Version 1511 (November Update/Threshold 2) ○ Education Edition ○ Enterprise Edition ○ Pro Edition **NOTE: Windows 10 is supported with UEFI Mode when used with Opal Compliant SEDs and Dell Computer Models - UEFI Support.**

Mobile Device Operating Systems

The following mobile operating systems are supported with Security Tools One-time Password feature.

Mobile Device Operating Systems
Android Operating Systems
• 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 Operating Systems
• iOS 7.x • iOS 8.x

Mobile Device Operating Systems
Windows Phone Operating Systems
• Windows Phone 8.1 • Windows 10 Mobile

Hardware

Authentication

The following table details supported authentication hardware.

Authentication
Fingerprint Readers
• Validity VFS495 in Secure Mode
• Broadcom Control Vault Swipe Reader
• UPEK TCS1 FIPS 201 Secure Reader 1.6.3.379
• Authentec Eikon and Eikon To Go USB Readers **NOTE: When using an external fingerprint reader, you must download and install the latest drivers required for your specific reader.**
Contactless Cards
• Contactless Cards using Contactless Card Readers built-in to specified Dell laptops
Smart Cards
• PKCS #11 Smart cards using the ActivIdentity client **NOTE: The ActivIdentity client is not pre-loaded and must be installed separately.**
• Common Access Cards (CAC) **NOTE: With multi-cert CACs, at logon, the user selects the correct certificate from a list.**
• CSP Cards
• Class B/SIPR Net Cards

The following table details Dell computer models supported with SIPR Net cards.

Dell Computer Models - Class B/SIPR Net Card Support		
• Latitude E6440 • Latitude E6540	• Precision M2800 • Precision M4800 • Precision M6800	• Latitude 14 Rugged Extreme • Latitude 12 Rugged Extreme • Latitude 14 Rugged

Dell Computer Models - UEFI Support

Authentication features are supported with UEFI mode on select Dell computers running Microsoft Windows 8, Microsoft Windows 8.1, and Microsoft Windows 10 with qualified Opal Compliant SEDs. Other computers running Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 8.1, and Microsoft Windows 10 support Legacy Boot mode.

The following table details Dell computer models supported with UEFI.

Dell Computer Models - UEFI Support			
• 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 Tablet (Model 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 Micro, Mini Tower, Small Form Factor • Optiplex 3046 • OptiPlex 3050 All-In-One • OptiPlex 3050 Tower, Small Form Factor, Micro • Optiplex 5040 Mini Tower, Small Form Factor • OptiPlex 5050 Tower, Small Form Factor, Micro • OptiPlex 7020 • Optiplex 7040 Micro, Mini Tower, Small Form Factor • OptiPlex 7050 Tower, Small Form Factor, Micro • Optiplex 3240 All-In-One • OptiPlex 5250 All-In-One • Optiplex 7440 All-In-One • OptiPlex 7450 All-In-One • OptiPlex 9020 Micro	• Venue Pro 11 (Models 5175/5179) • Venue Pro 11 (Model 7139)
NOTE: Authentication features are supported with UEFI mode on these computers running Windows 8, Windows 8.1, and Windows 10 with qualified Opal Compliant SEDs. Other computers running Windows 7, Windows 8, Windows 8.1, and Windows 10 support Legacy Boot mode.			

NOTE: On a supported UEFI computer, after selecting Restart from the main menu, the computer restarts and then displays one of two possible logon screens. The logon screen that appears is determined by differences in computer platform architecture. Some models display the PBA logon screen; other models display the Windows logon screen. Both logon screens are equally secure.

NOTE:

Ensure that the Enable Legacy Option ROMs setting is disabled in the BIOS.

To disable Legacy Option ROMs:

1. Restart the computer.
2. As it is restarting, press **F12** repeatedly to bring up the UEFI computer's boot settings.
3. Press the down arrow, highlight the **BIOS Settings** option, and press **Enter**.
4. Select **Settings** > **General** > **Advanced Boot Options**.
5. Clear the **Enable Legacy Option ROMs** checkbox and click **Apply**.

Opal Compliant SEDs

For the most up-to-date list of Opal compliant SEDs supported with the SED management, refer to this KB article: http://www.dell.com/support/article/us/en/19/SLN296720.

International Keyboards

- The following table lists international keyboards supported with Preboot Authentication on UEFI and non-UEFI computers.

International Keyboard Support - UEFI
○ DE-CH - Swiss German
○ DE-FR - Swiss French

International Keyboard Support - Non-UEFI
○ AR - Arabic (using Latin letters)
○ DE-CH - Swiss German
○ DE-FR - Swiss French

Language Support

DDP | Security Tools is Multilingual User Interface (MUI) compliant and supports the following languages.

NOTE:

PBA localization is not supported in Russian, Traditional Chinese, or Simplified Chinese on UEFI computers..

Language Support	
• EN - English	• KO - Korean
• FR - French	• ZH-CN - Chinese, Simplified
• IT - Italian	• ZH-TW - Chinese, Traditional/Taiwan
• DE - German	• PT-BR - Portuguese, Brazilian
• ES - Spanish	• PT-PT - Portuguese, Portugal (Iberian)
• JA - Japanese	• RU - Russian

Authentication Options

The following authentication options require specific hardware: Fingerprints, Smart Cards, Contactless Cards, Class B/SIPR Net Cards, and **authentication on UEFI computers**.

The One-time Password feature requires that a TPM is present, enabled, and owned. For more information, see Clear Ownership and Activate the TPM. OTP is not supported with TPM 2.0.

The following tables show authentication options available with Security Tools, by operating system, when hardware and configuration requirements are met.

Non-UEFI										
	PBA					Windows Authentication				
	Password	Fingerprint	Contacted Smart card	OTP	SIPR Card	Password	Fingerprint	Smart card	OTP	SIPR Card
Windows 7 SP0-SP1	X[1]					X	X	X	X	X
Windows 8	X[1]					X	X	X	X	X
Windows 8.1-Windows 8.1 Update 1	X[1]					X	X	X	X	X
Windows 10	X[1]					X	X	X	X	X
1. Available with a supported Opal SED.										

UEFI										
	PBA - on supported Dell computers					Windows Authentication				
	Password	Fingerprint	Contacted Smart card	OTP	SIPR Card	Password	Fingerprint	Smart card	OTP	SIPR Card
Windows 7										
Windows 8	X[2]					X	X	X	X	X
Windows 8.1-Windows 8.1 Update 1	X[2]					X	X	X	X	X
Windows 10	X[2]					X	X	X	X	X
2. Available with a supported OPAL SED on supported UEFI computers.										

Interoperability

Deprovision and Uninstall Dell Data Protection | Access

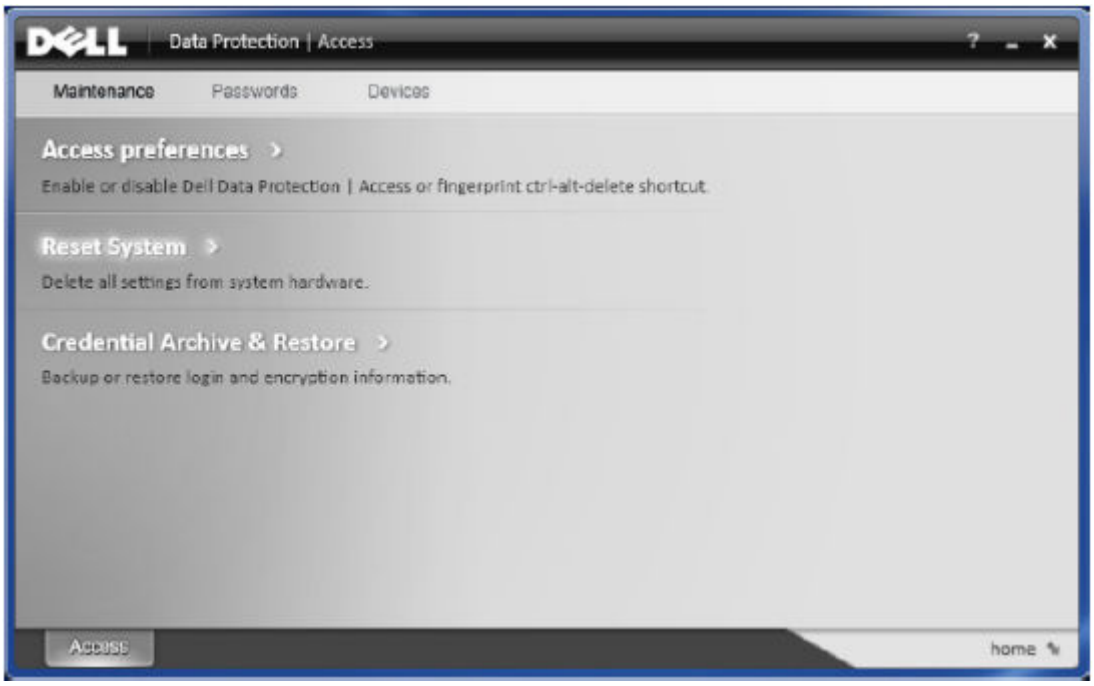
If DDP|A is installed now or has been installed in the past on your computer, **before** installing Security Tools, you must deprovision the DDP|A-managed hardware and then uninstall DDP|A. If DDP|A has not been used, you may simply uninstall DDP|A and restart the installation process.

Deprovisioning DDP|A-managed hardware includes the fingerprint reader, smart card reader, BIOS passwords, TPM, and the Self-Encrypting Drive.

NOTE: If running DDP|E encryption products, stop or pause an encryption sweep. If running Microsoft BitLocker, suspend the encryption policy. Once DDP|A is uninstalled and Microsoft BitLocker policy is unsuspended, initialize the TPM by following the instructions located at http://technet.microsoft.com/en-us/library/cc753140.aspx.

Deprovision DDP|A-Managed Hardware

1. Launch DDP|A and click the **Advanced** tab.



2. Select **Reset System**. This will require that you enter any provisioned credentials to verify your identity. After DDP|A verifies the credentials, DDP|A will perform the following actions:
   - Remove all provisioned credentials from Dell ControlVault (if present)
   - Remove Dell ControlVault owner password (if present)
   - Remove all provisioned fingerprints from integrated fingerprint reader (if present)
   - Remove all BIOS passwords (BIOS System, BIOS Admin, and HDD passwords)
   - Clear the Trusted Platform Module
   - Remove the DDP|A Credential Provider

   Once the computer is deprovisioned, DDP|A restarts the computer to restore the Windows default credential provider.

Uninstall DDP|A

Once the authentication hardware is deprovisioned, uninstall DDP|A.

1. Launch DDP|A and perform a Reset System.

   This will remove all DDP|A managed credentials and passwords and will clear the Trusted Platform Module (TPM).

2. Click **Uninstall** to launch the installer.
3. When the uninstall finishes, click **Yes** to restart.

NOTE: Removing DDP|A will also unlock the SED and remove the Preboot Authentication.

Initialize the TPM

- You must be a member of the local Administrators group, or equivalent.
- The computer must be equipped with a compatible BIOS and a TPM.

This task is required if using One-time Password (OTP).

- Follow the instructions located at http://technet.microsoft.com/en-us/library/cc753140.aspx.

Clear Ownership and Activate the TPM

To clear and set ownership of the TPM, see https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2.

Proceed to Installation and Activation.

3

Installation and Activation

This section details installing DDP | Security Tools on a local computer. To install and activate DDP | Security Tools, you must be logged on to the computer as an administrator.

NOTE:

During installation, do not make any changes to the computer, including inserting or removing external (USB) drives.

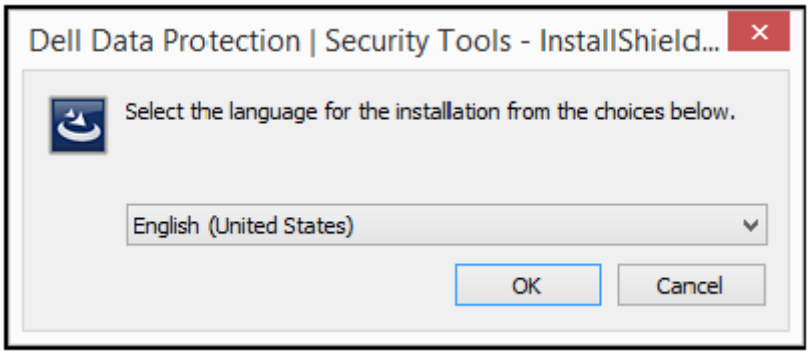
Install DDP | Security Tools

To install Security Tools:

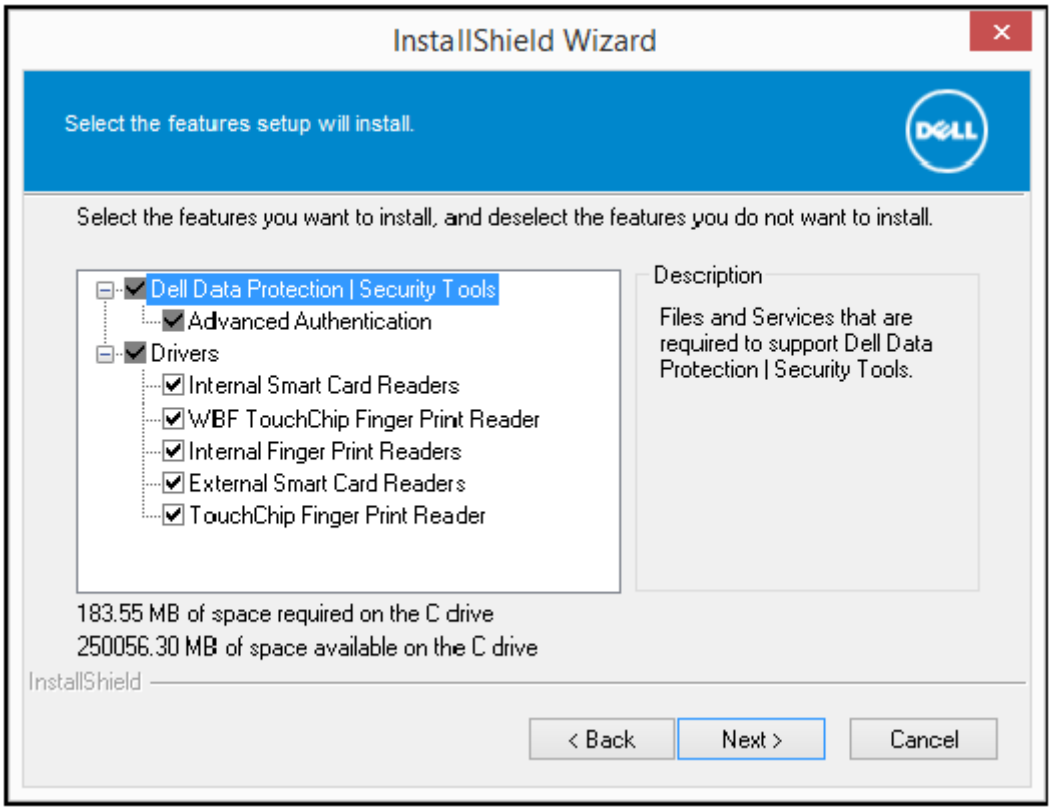
1. Locate installation file in the DDP | Security Tools installation media. Copy it to the local computer.

   NOTE: The installation media can be located at www.dell.com/support > Endpoint Security Solutions.

2. Double-click the file to launch the installer.
3. Select the appropriate language and click **OK**.



4. Click **Next** when the Welcome page displays.
5. Read the license agreement, agree to the terms, and click **Next**.
6. Click **Next** to install Security Tools in the default location of `C:\Program Files\Dell\Dell Data Protection. Select`



7. Click **Install** to begin the installation.
8. Once the installation is complete, a computer restart is required. Select **Yes** to restart and then click **Finish**.

   Installation is complete.

Activate DDP | Security Tools

The first time that you run the DDP Security Console and select Administrator Settings, the Activation wizard walks you through the Activation process.

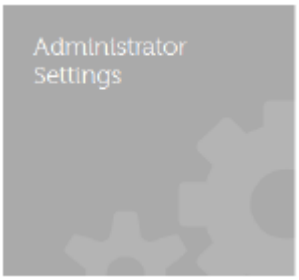
If the DDP Security Console isn't activated yet, an end user can still run it. When an end user is the first person to use the DDP Security Console before an administrator has activated DDP | Security Tools and customized the settings, the default values will be used.

To activate Security Tools:

1. As an administrator, launch Security Tools from the Desktop shortcut.

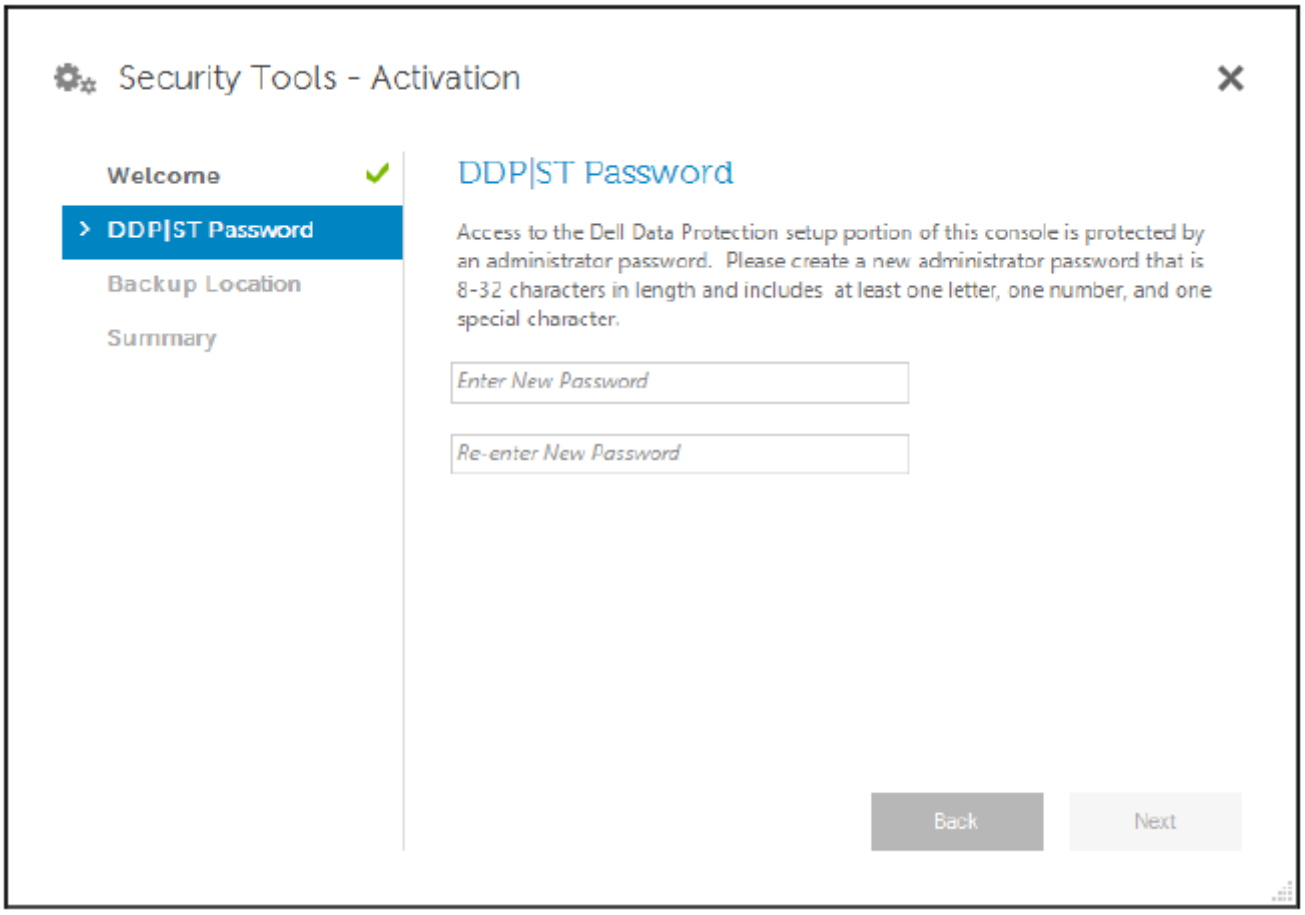
NOTE: If logged in as a regular user (using a standard Windows account), the Administrator Settings tool requires UAC elevation to launch. The regular user will first enter administrator credentials to log on to the tool and a second time, when prompted, he enters the administrator's password (the password stored in Administrator Settings).

2. Click the **Administrator Settings** tile.



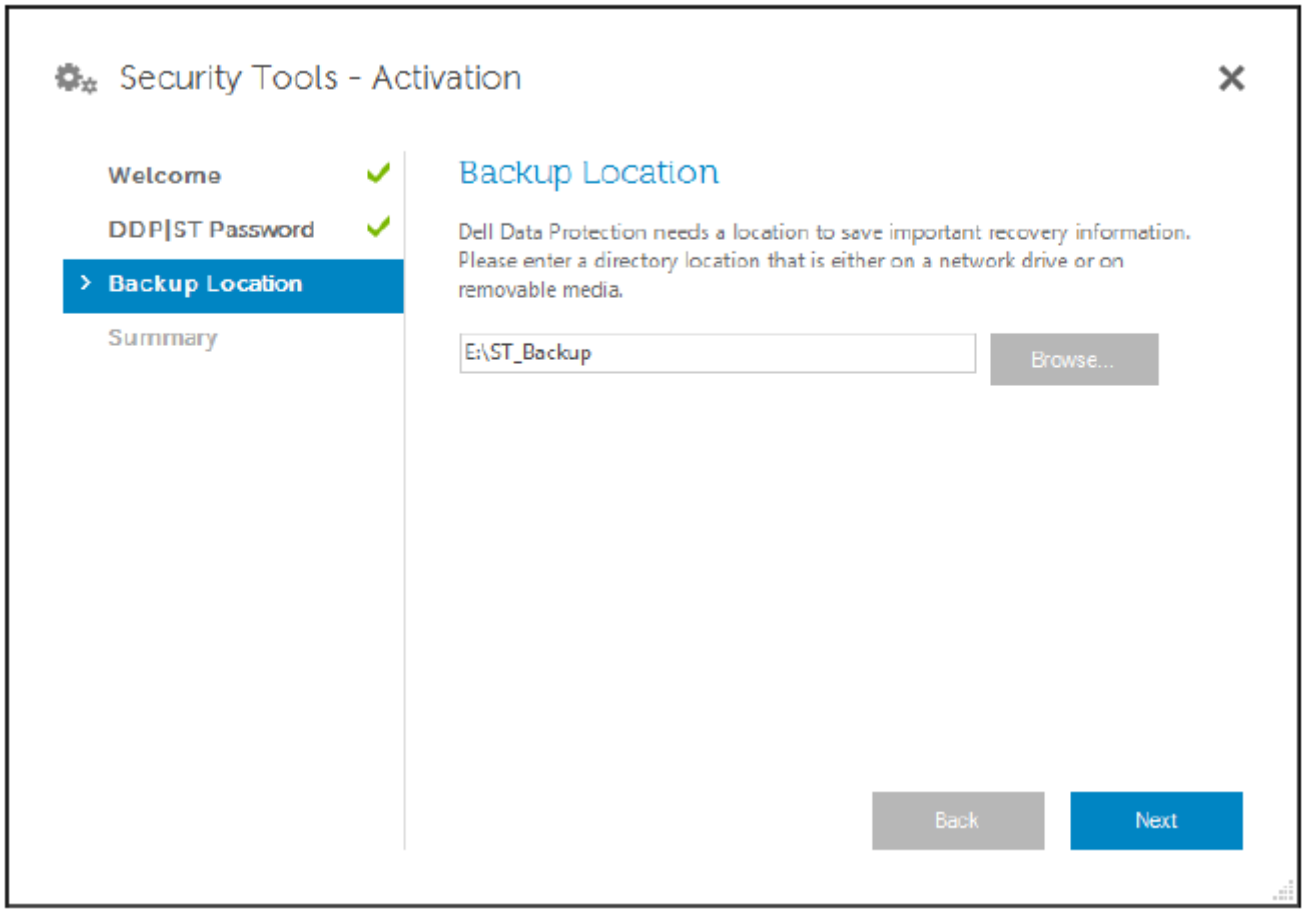
3. At the Welcome page, click **Next**.
4. Create the DDP | Security Tools password, and click **Next**.

   You must create the DDP | Security Tools administrator's password before configuring Security Tools. This password will be needed any time you run the Administrator Settings tool. The password must be 8-32 characters long and must include at least one letter, one number, and one special character.



5. In **Backup Location**, specify the location where the backup file is to be written, and click **Next**. The backup file must either be saved on a network drive or onto removable media. The backup file contains the keys that are needed to recover data on this computer. Dell Support must have access to this file to help you recover data.

   Recovery data will be automatically backed up to the specified location. If the location is not available (for instance, if your backup USB drive is not inserted), DDP | Security Tools prompts for a location to back up your data. Access to recovery data will be required in order to begin encryption.



6. At the Summary page, click **Apply**.

   Security Tools activation is complete.

   Administrators and users can immediately begin to take advantage of Security Tools features, based on default settings.

4

Configuration Tasks for Administrators

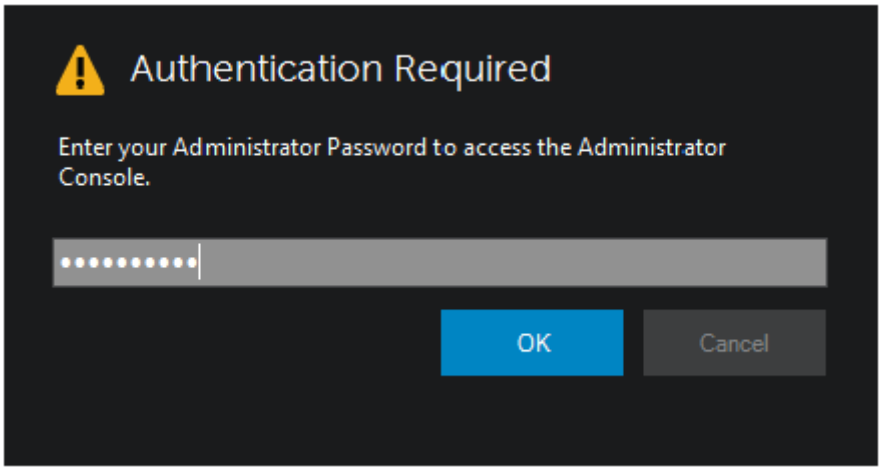
Security Tools default settings allow administrators and users to use Security Tools immediately after activation, without additional configuration. Users are automatically added as Security Tools users when they log on to the computer with their Windows passwords but, by default, multi-factor Windows authentication is not enabled. Encryption and Preboot Authentication also are not enabled, by default.

To configure Security Tools features, you must be an administrator on the computer.

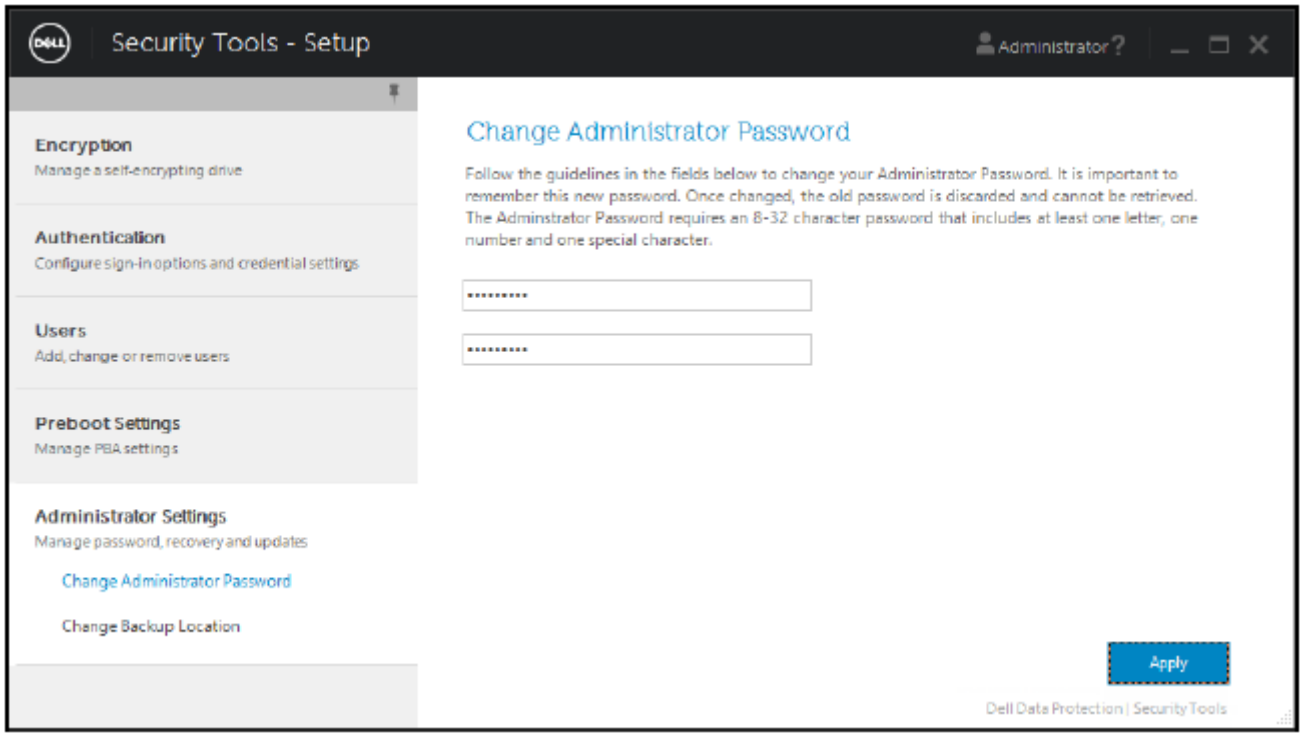
Change the Administrator Password and Backup Location

After Security Tools activation, the Administrator Password and Backup Location can be changed, if necessary.

1. As an administrator, launch Security Tools from the Desktop shortcut.
2. Click the **Administrator Settings** tile.
3. In the Authentication dialog, enter the administrator password that was set up during activation, and click **OK.**



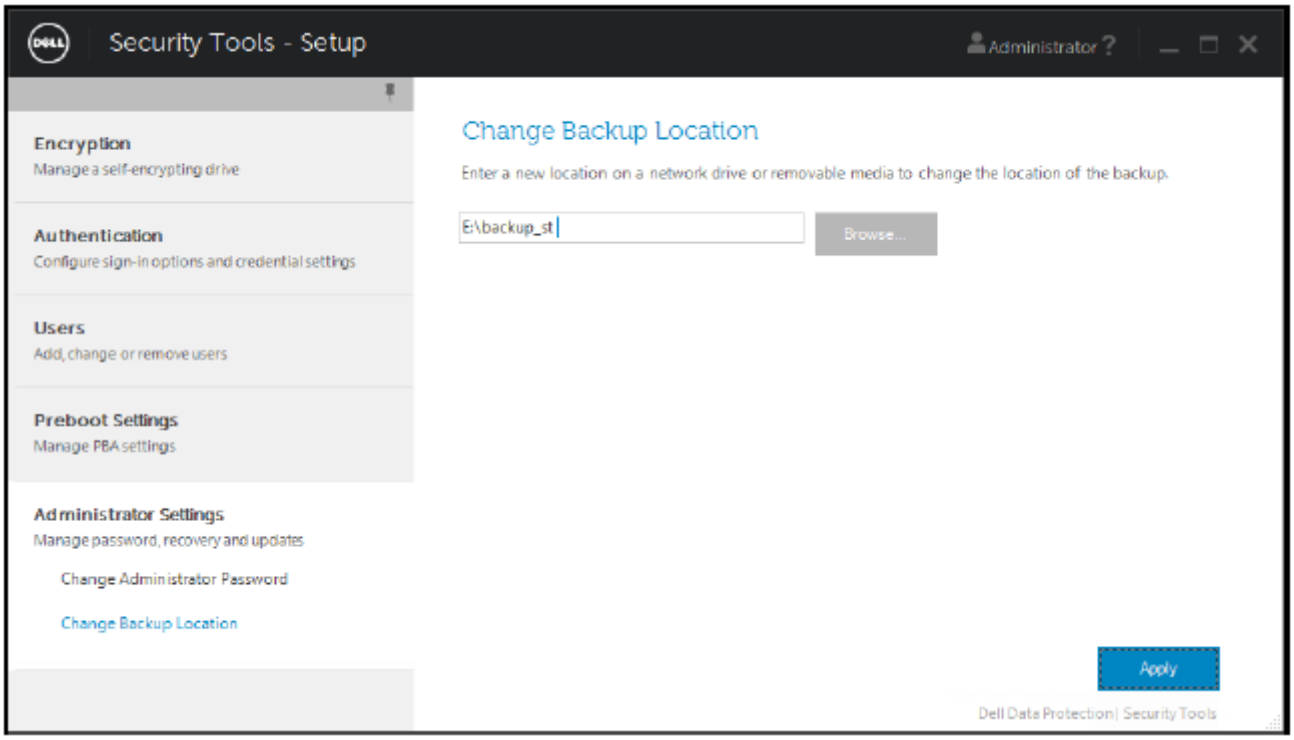
4. Click the **Administrator Settings** tab.
5. In the Change Administrator Password page, if you want to change the password, enter a new password that is between 8-32 characters and includes at least one letter, one number, and one special character.



6. Enter the password a second time to confirm it, then click **Apply**.
7. To change the location where the recovery key is stored, in the left pane, select **Change Backup Location**.
8. Select a new location for the backup, and click **Apply**.

   The backup file must be saved either on a network drive or onto removable media. The backup file contains the keys that are needed to recover data on this computer. Dell ProSupport must have access to this file to help you recover data.

   Recovery data will be automatically backed up to the specified location. If the location is not available (for instance, if your backup USB drive is not inserted), Security Tools prompts for a location to back up your data. Access to recovery data will be required in order to begin encryption.



Configure Encryption and Preboot Authentication

Encryption and Preboot Authentication (PBA) are available if your computer is equipped with a self-encrypting drive (SED). Both are configured through the Encryption tab, which is visible only if your computer is equipped with a self-encrypting drive (SED). When you enable either encryption or PBA, the other is also enabled.

Before enabling encryption and PBA, Dell recommends that you enroll and enable Recovery Questions as a Recovery Option so you can recover the password if it is lost. For more information, see Configure Sign-in Options.

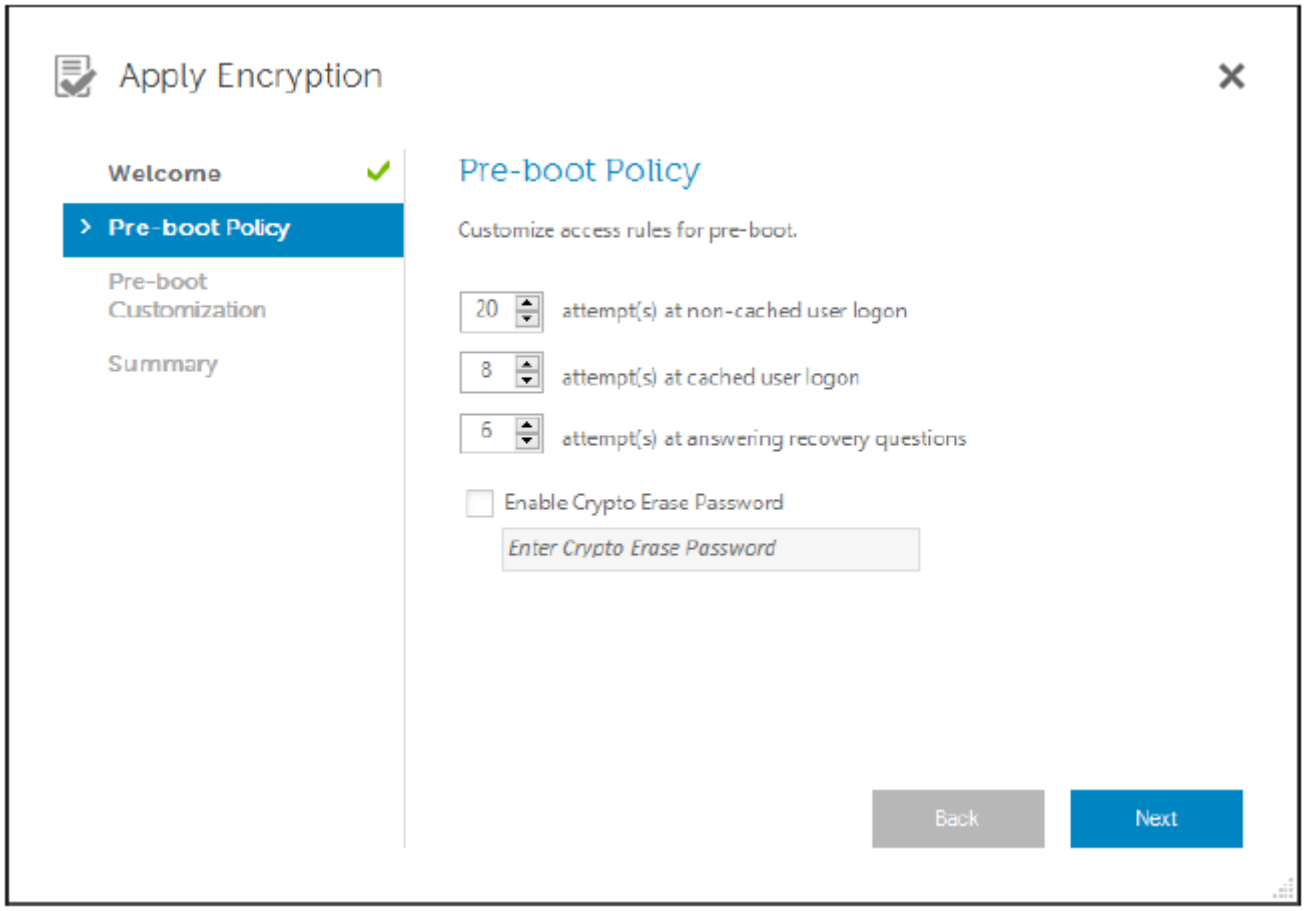
To configure encryption and Preboot Authentication:

1. In the DDP Security Console, click the **Administrator Settings** tile.
2. Ensure that the backup location is accessible from the computer.

   NOTE: When encryption is being enabled if a message displays, "Backup Location not found," and the backup location is on a USB drive, either your drive is not connected or is connected to a different slot than the one you used during backup. If the message displays, and the backup location is on a network drive, the network drive is inaccessible from the computer. If it is necessary to change the backup location, from the Administrator Settings tab, select Change Backup Location to change the location to the current slot or accessible drive. A few seconds after reassigning the location, the process of enabling encryption can proceed.

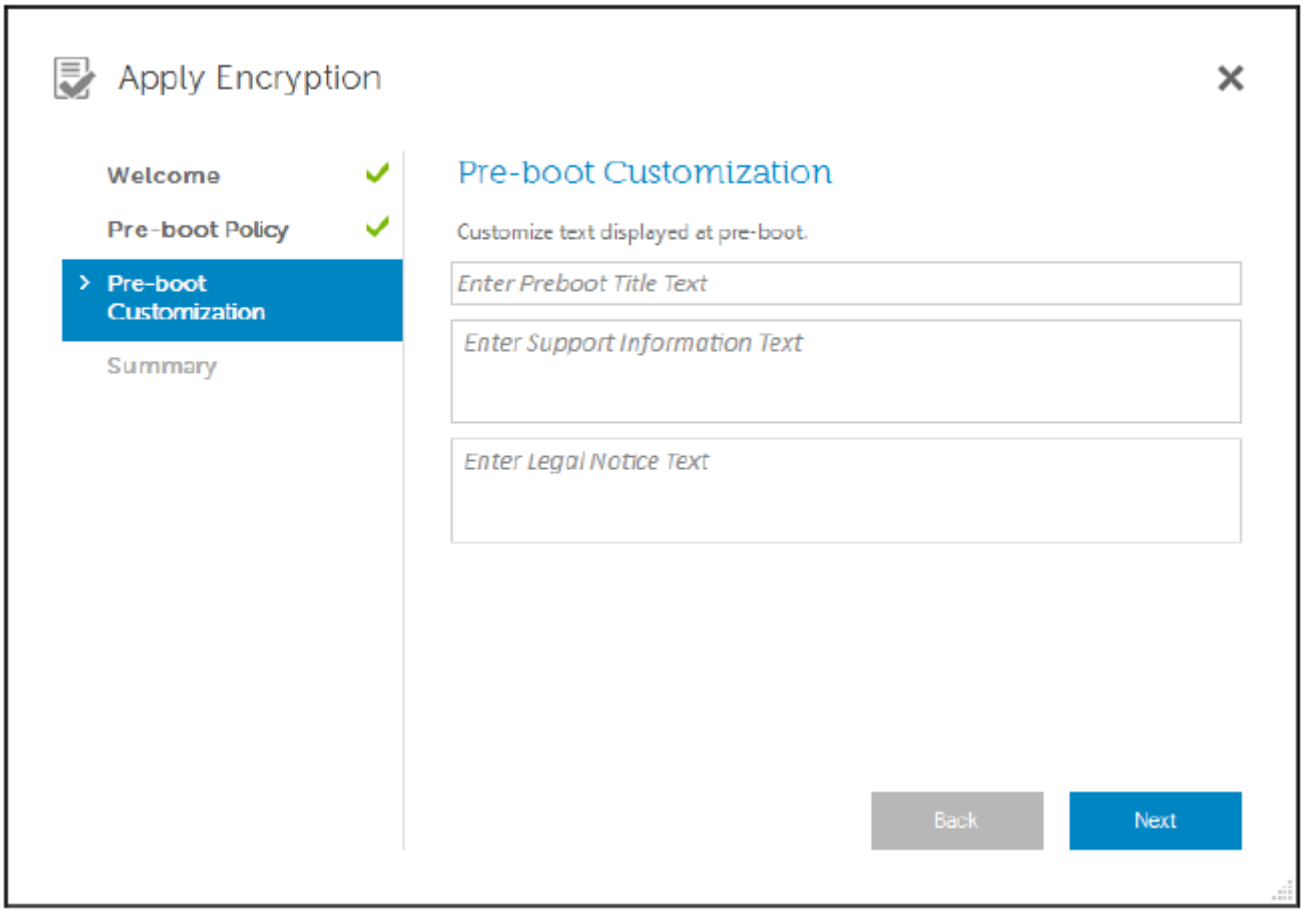
3. Click the **Encryption** tab and then click **Encrypt**.
4. At the Welcome page, click **Next**.
5. In the Preboot Policy page, change or confirm the following values, and click **Next**.

Attempts at non-cached user login	Number of times an unknown user can attempt to log in (a user that has not logged in to the computer before [no credentials have been cached]).
Attempts at cached user login	Number of times can a known user attempt to log in.
Attempts at answering recovery questions	Number of times the user can attempt to enter the correct answer.
Enable Crypto Erase Password	Select to enable.
Enter the Crypto Erase Password	A word or code of up to 100 characters used as a fail-safe security mechanism. Entering this word or code in the user name or password field during the PBA authentication deletes the authentication tokens for all users and locks the SED. Afterward, only an administrator can forcibly unlock the device. Leave this field blank if you do not want to have a crypto erase password available in case of emergency.



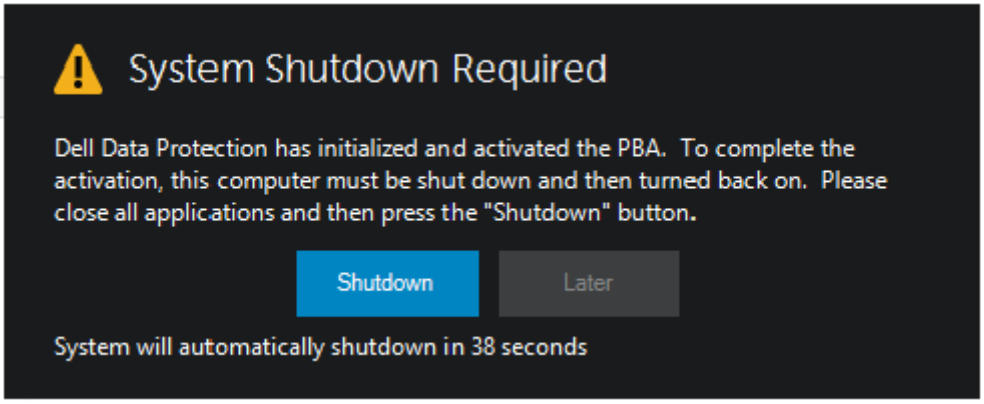
6. In the Preboot Customization page, enter customized text to display on the Preboot Authentication (PBA) screen, and click **Next.**

Preboot Title Text	This text displays on the top of the PBA screen. If you leave this field blank, no title will be displayed. The text does not wrap, so entering more than 17 characters may result in the text being cut off.
Support Information Text	This text displays on the PBA support information page. Dell recommends that you customize the message to include specific instructions about how to contact the Help Desk or Security Administrator. Not entering text in this field results in no support contact information being available for the user. Text wrapping occurs at the word level, not the character level. For instance, if you have a single word that is more than approximately 50 characters in length, it will not wrap and no scroll bar will be present, therefore the text will be cut off.
Legal Notice Text	This text displays before the user is allowed to log on to the device. For example: "By clicking OK, you agree to abide by the acceptable computer use policy." Not entering text in this field results in no text or OK/Cancel buttons being displayed. Text wrapping occurs at the word level, not the character level. For instance, if you have a single word that is more than approximately 50 characters in length, it will not wrap and no scroll bar will be present, therefore the text will be cut off.



7. At the Summary page, click **Apply**.
8. When prompted, click **Shutdown**.

   A full shutdown is required before encryption can begin.



9. After shutdown, restart the computer.

   Authentication is now managed by Security Tools. Users must log in at the Preboot Authentication screen with their Windows passwords.

Change Encryption and Preboot Authentication Settings

After you first enable encryption and configure Preboot Policy and Customization, the following actions are available from the Encryption tab:

- Change Preboot Policy or Customization - Click the **Encryption** tab and then click **Change**.
- Decrypt the SED, for example for uninstallation - Click **Decrypt**.

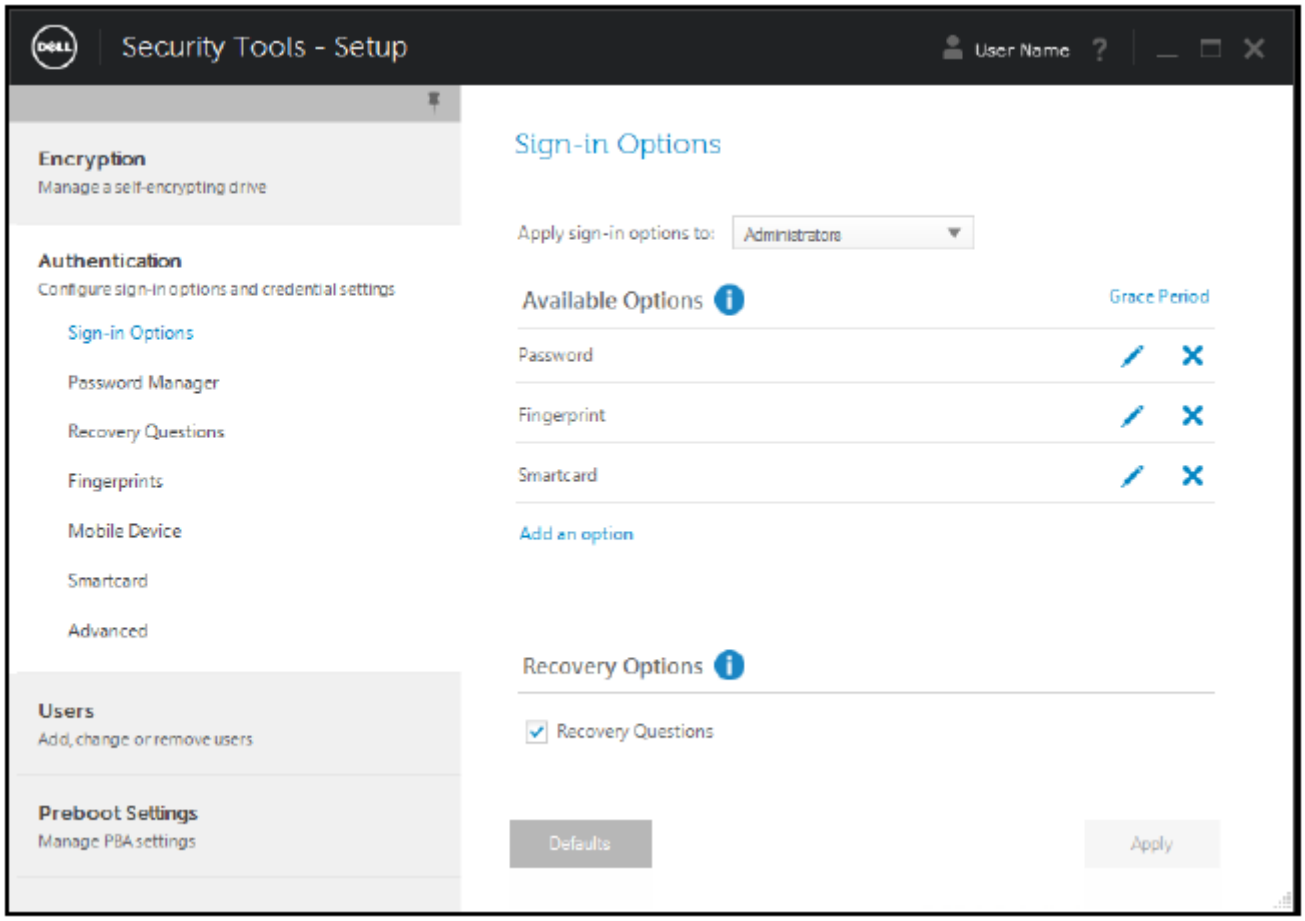
After you first enable encryption and configure Preboot Policy and Customization, the following actions are available from the Preboot Settings tab:

- Change Preboot Policy or Customization - Click the **Preboot Settings** tab and select either **Preboot Customization** or **Preboot Logon Policies.**

For uninstallation instructions, see Uninstallation Tasks.

Configure Authentication Options

The controls on the Administrator Settings Authentication tab let you set user sign-in options and customize the settings for each.



NOTE: The One-time Password option does not display under Recovery Options if the TPM is not present, owned, and enabled.

Configure Sign-in Options

On the Sign-in Options page, you can configure logon policies. By default, all supported credentials are listed in Available Options.

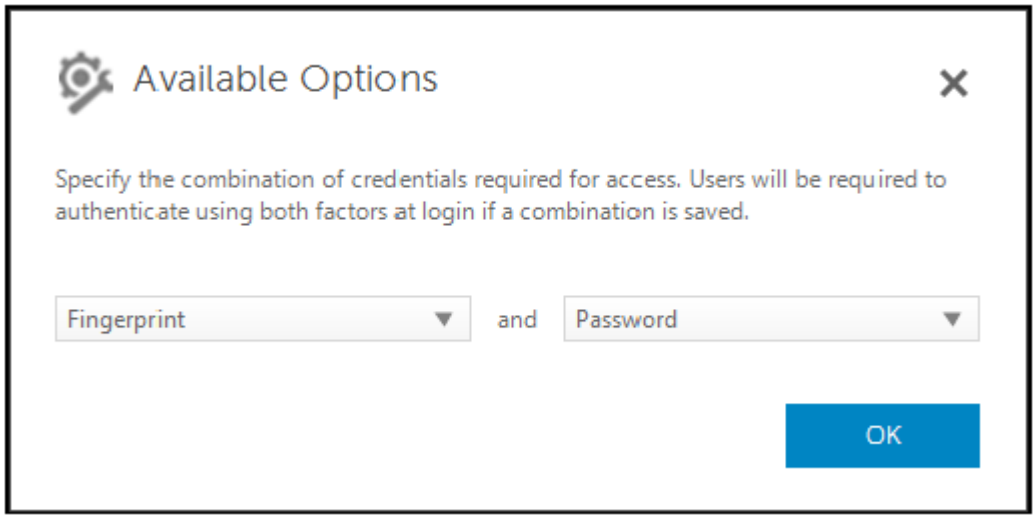
To configure sign-in options:

1. In the left pane, under Authentication, select **Sign-in Options**.
2. To choose the role you want to set up, select the role in the **Apply sign-in options to** list: **Users** or **Administrators**. All of the changes that you make on this page will apply only to the role that you select.
3. Set Available Options for authentication.

   By default, each authentication method is configured to be used individually, not in combination with other authentication methods. You can change the defaults in the following ways:

   - To set up a combination of authentication options, under Available Options, click ✎ to select the first authentication method. In the Available Options dialog, select the second authentication method, then click **OK**.

For example, you can require both a fingerprint and a password as logon credentials. In the dialog, select the second authentication method that must be used with fingerprint authentication.



- To allow each authentication method to be used individually, in the Available Options dialog, leave the second authentication method set to **None**, and click **OK**.
- To remove a sign-in option, under Available Options on the Sign-in Options page, click **X** to remove the method.
- To add a new combination of authentication methods, click **Add an Option**.

4. Set Recovery Options for users to recover their computer access, if they become locked out.
   - To allow users to define a set of questions and answers to be used to regain access to the computer, select **Recovery Questions**.

     To prevent use of Recovery Questions, deselect the option.
   - To allow users to recover access using a mobile device, select **One-time Password**. When One-time Password (OTP) is selected as a recovery method, it is not available as a sign-in option on the Windows logon screen.

     To use the OTP feature for logon, deselect the option in Recovery Options. When deselected as a recovery method, the OTP option appears on a Windows logon page as long as at least one user has enrolled in OTP.

     NOTE: As administrator, you control how One-time Password can be used - for authentication or for recovery. The OTP feature can be used either for authentication or for recovery, but not for both. The configuration affects either all users of the computer or all administrators, based on the selection in the Sign-in Options field, Apply sign-in options to.

     If the One-time Password option is not listed under Recovery Options, your computer's configuration does not support it. For more information, see Requirements.
   - To require the user to make a help desk call if they lose or forget logon credentials, clear both check boxes under Recovery Options: Recovery Questions and One-time Password.
5. To set a length of time to allow users to enroll their authentication credentials, select **Grace Period**.

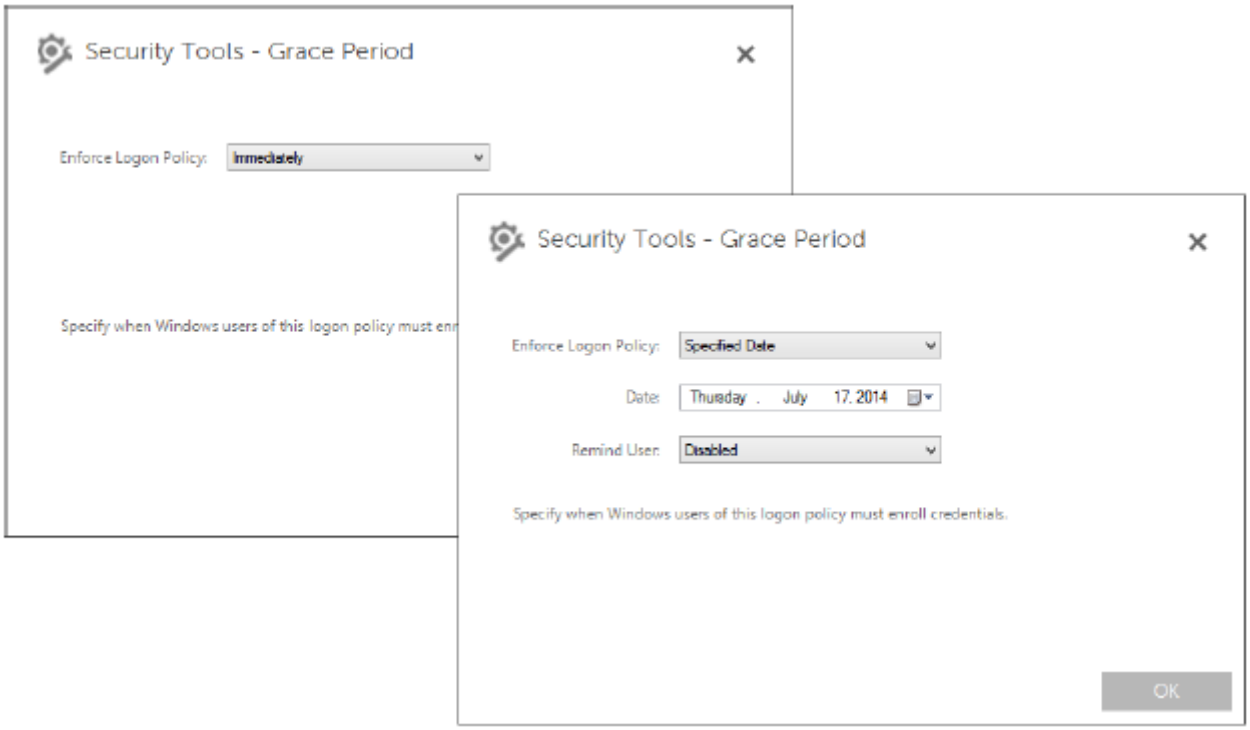
   The Grace Period feature lets you set the date on which a configured Sign-in Option will begin to be enforced. You can configure a Sign-in Option before the date when it will be enforced and set up a length of time to allow users to enroll. By default, the policy is enforced immediately.

   To change the Enforce Sign-in Option date from *Immediately*, in the Grace Period dialog, click the drop-down menu and select **Specified Date**. Click the down arrow at the right side of the date field to display a calendar, then select a date on the calendar. Enforcement of the policy begins at approximately 12:01 AM on the date selected.

   Users can be reminded to enroll their credentials required at their next Windows logon (by default), or you can set up regular reminders. Select the reminder interval from the *Remind User* drop-down list.

   NOTE:

   The reminder that is displayed to the user is slightly different, depending on whether the user is at the Windows Logon screen or within a Windows session when the reminder is triggered. Reminders do not appear on Preboot Authentication logon screens.



Functionality During the Grace Period

During a specified Grace Period, after every log on, the Additional Credentials notification displays when the user has not yet enrolled the minimum credentials required to satisfy a changed Sign-in Option. The message content is: *Additional credentials are available for enrollment*.

If additional credentials are available, but are not required, the message displays only once after the policy has been changed.

Clicking the notification has the following results, depending on the context:

- If no credentials have been enrolled, the Setup wizard displays, allowing Administrative Users to configure computer-related settings and offering users the ability to enroll the most common credentials.
- After initial credential enrollment, clicking the notification displays the Setup wizard within the DDP Security Console.

Functionality After Grace Period Expires

In all cases, after the Grace Period has expired, users cannot log on without having enrolled the credentials required by the Sign-in Option. If a user attempts to log on with a credential or credential combination that does not satisfy the Sign-in Option, the Setup wizard displays on top of the Windows Logon screen.

- If the user successfully enrolls the required credentials, they are logged into Windows.
- If a user does not successfully enroll the required credentials, or cancels the wizard, they are returned to the Windows Logon screen.

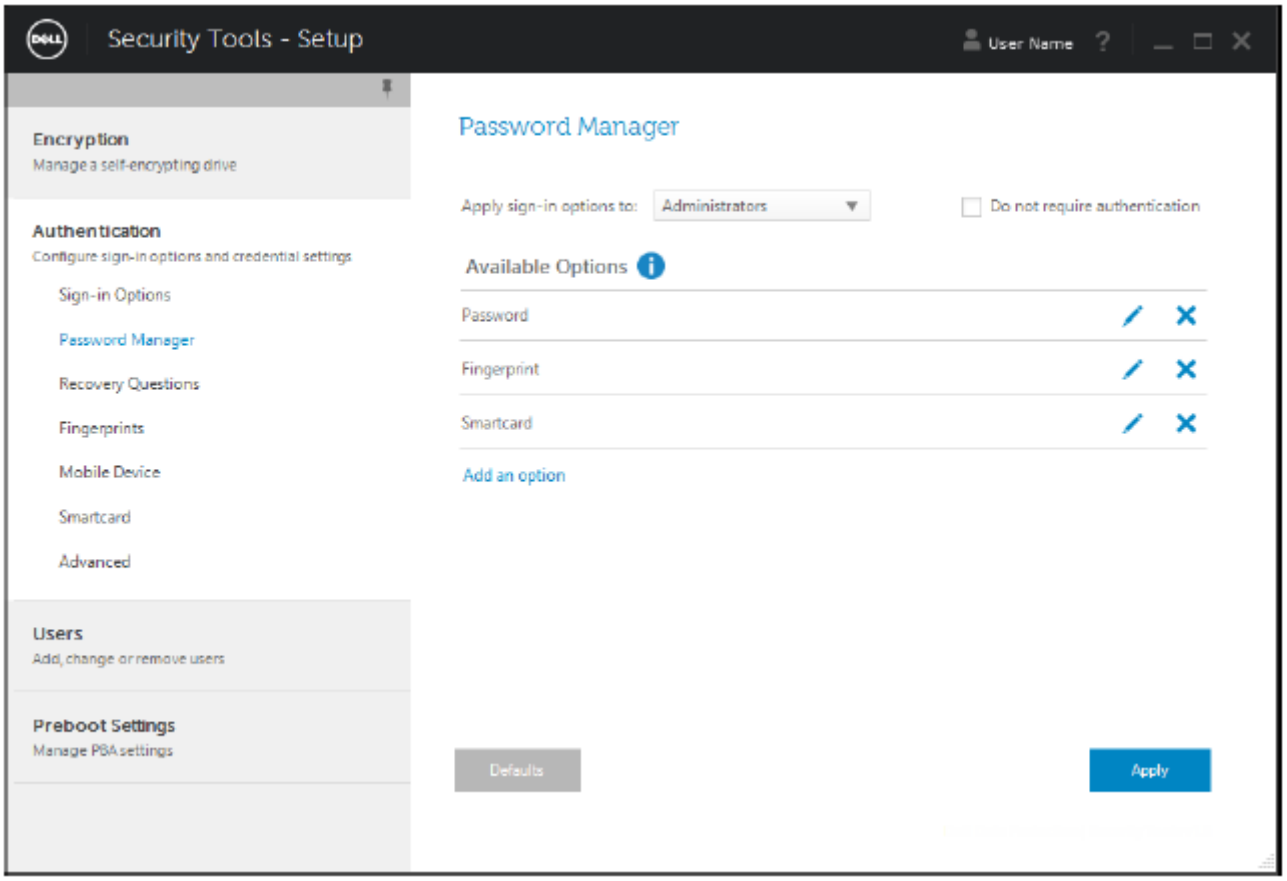
6. To save the settings for the selected role, click **Apply**.

Configure Password Manager Authentication

On the Password Manager page, you can configure how users authenticate to Password Manager.

To configure Password Manager authentication:

1. In the left pane, under Authentication, select **Password Manager**.
2. To choose the role you want to set up, select the role in the **Apply sign-in options to** list: **Users** or **Administrators**. All of the changes that you make on this page will apply only to the role that you select.
3. Optionally, select the **Do not require authentication** check box to allow the selected user role to be automatically logged on to all software applications and Internet websites with credentials stored in Password Manager.

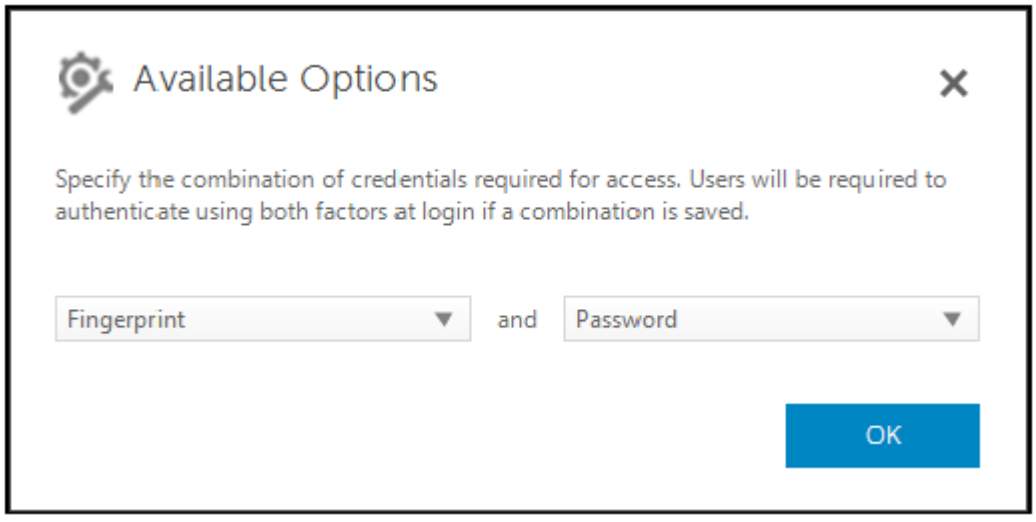


4. Set Available Options for authentication.

   By default, each authentication method is configured to be used individually, not in combination with other authentication methods. You can change the defaults in the following ways:

   - To set up a combination of authentication options, under Available Options, click ✎ to select the first authentication method. In the Available Options dialog, select the second authentication method, then click **OK**.

     For example, you can require both a fingerprint and a password as logon credentials. In the dialog, select the second authentication method that must be used with fingerprint authentication.



   - To allow each authentication method to be used individually, in the Available Options dialog, leave the second authentication method set to **None**, and click **OK**.
   - To remove a sign-in option, under Available Options on the Sign-in Options page, click **X** to remove the method.
   - To add a new combination of authentication methods, click **Add an Option**.

5. To save the settings for the selected role, click **Apply.**

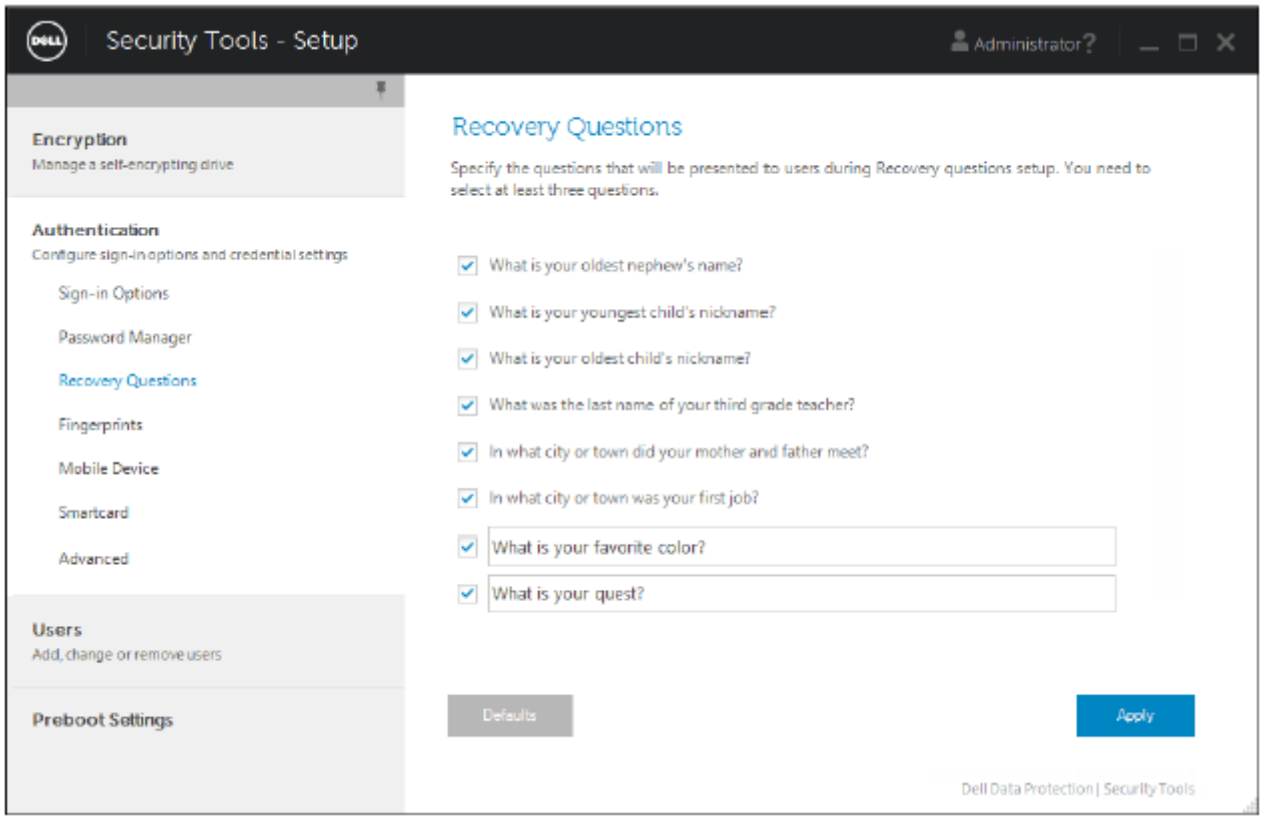
   NOTE: Select the Defaults button to restore the settings to their original values.

Configure Recovery Questions

On the Recovery Questions page, you can select which questions will be presented to users when they define personal Recovery Questions and answers. Recovery Questions allow users to recover access to their computers if their passwords are expired or forgotten.

To configure Recovery Questions:

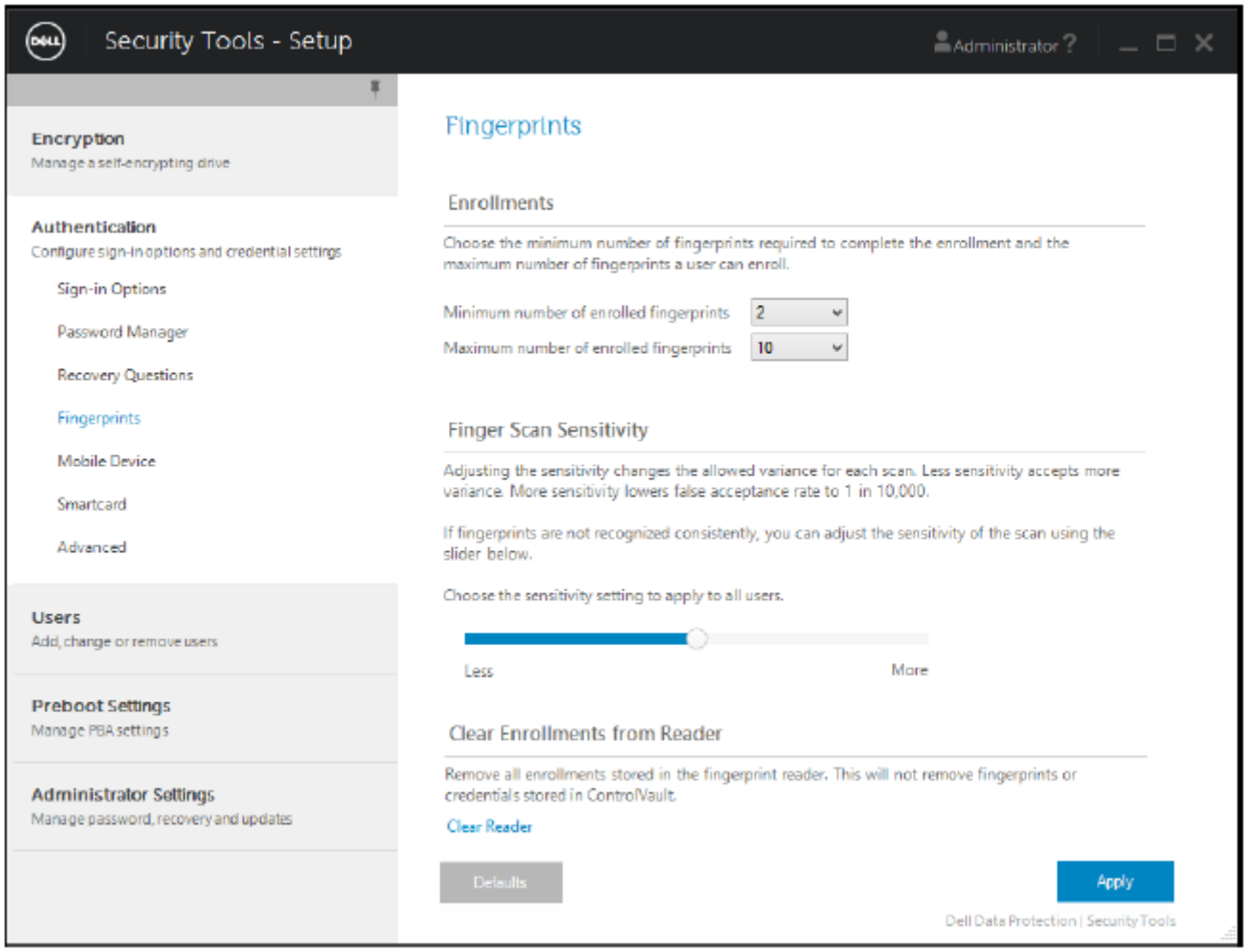
1. In the left pane, under Authentication, select **Recovery Questions**.
2. On the Recovery Questions page, select at least three pre-defined Recovery Questions.
3. Optionally, you can add up to three custom questions to the list that the user selects from.
4. To save the Recovery Questions, click **Apply**.



Configure Fingerprint Scan Authentication

To configure fingerprint scan authentication:

1. In the left pane, under Authentication, select **Fingerprints**.
2. In Enrollments, set the minimum and maximum number of fingers that a user can enroll.



3. Set the Fingerprint Scan sensitivity.

   Lower sensitivity increases the acceptable variance and the probability of accepting a false scan. At the highest setting, the system may reject legitimate fingerprints. The More sensitivity setting lowers the false acceptance rate to 1 in 10,000 scan.

4. To remove all fingerprint scans and credential enrollments from the fingerprint reader's buffer, click **Clear Reader**. This removes only data that you are currently adding. It does not delete scans and enrollments stored from previous sessions.
5. To save the settings, click **Apply**.

Configure One-time Password Authentication

To use the One-time Password feature, the user generates a One-time Password with the Security Tools Mobile application on his mobile device then enters the password on the computer. The password can be used only once, and it is valid for only a limited length of time.

To further improve security, the administrator can ensure that the mobile application is secure by requiring a password.

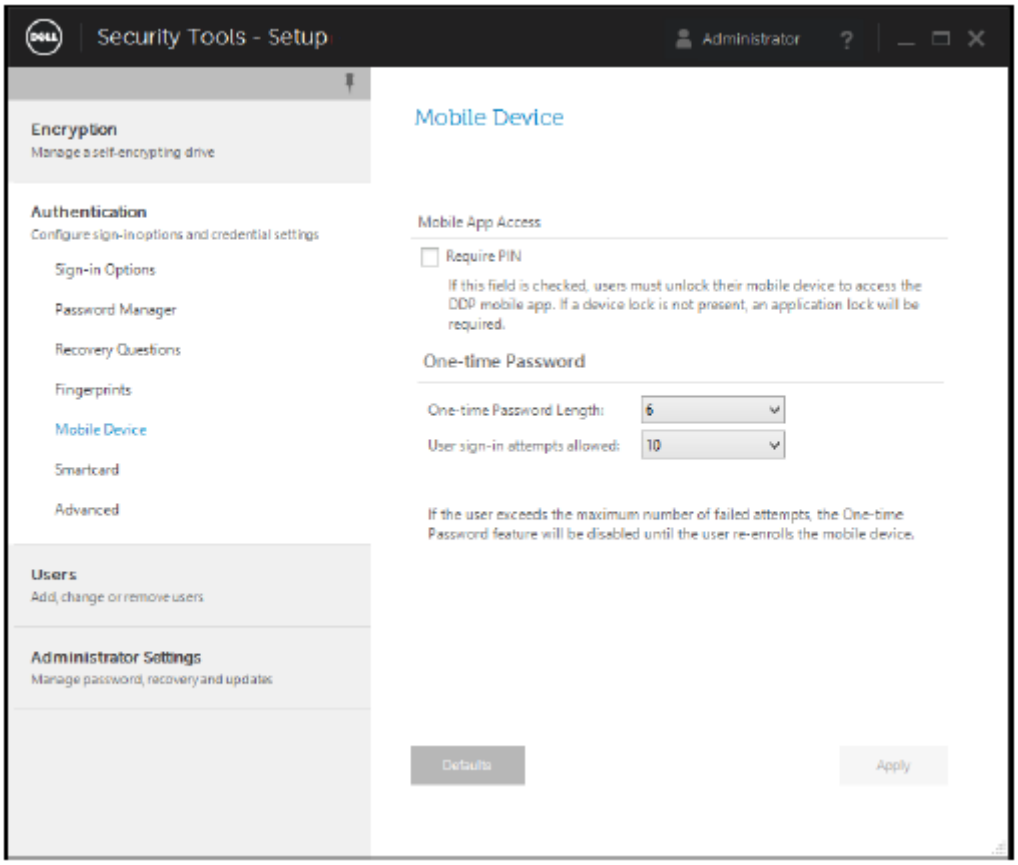
On the Mobile Device page, you can configure settings that further increase the security of the mobile device and One-time Password.

To configure One-time Password authentication:

1. In the left pane, under Authentication, select **Mobile Device**.
2. To require the user to enter a password to access the Security Tools Mobile application on the mobile device, select **Require Password**.

   NOTE: Enabling the *Require Password* policy after mobile devices have been enrolled with a computer causes all mobile devices to be unenrolled. Users will be required to re-enroll their mobile devices once this policy is enabled.

   When the **Require Password** check box is selected, users must unlock their mobile device to access the Security Tools Mobile app. If a device lock is not present on the mobile device, the password will be required.



3. To select the length of the One-time Password (OTP), for **One-time Password Length**, select number of password characters to require.
4. To select the number of chances the user has to enter the One-time Password correctly, for **User Sign-in Attempts Allowed**, select a number from **5** to **30**.

   When the maximum attempts is reached, the OTP feature will be disabled until the user re-enrolls the mobile device.

   NOTE: Dell recommends setting up at least one other authentication method in addition to One-time Password.

Configure Smart Card Enrollment

DDP|Security Tools supports two kinds of smart cards: contacted and contactless.

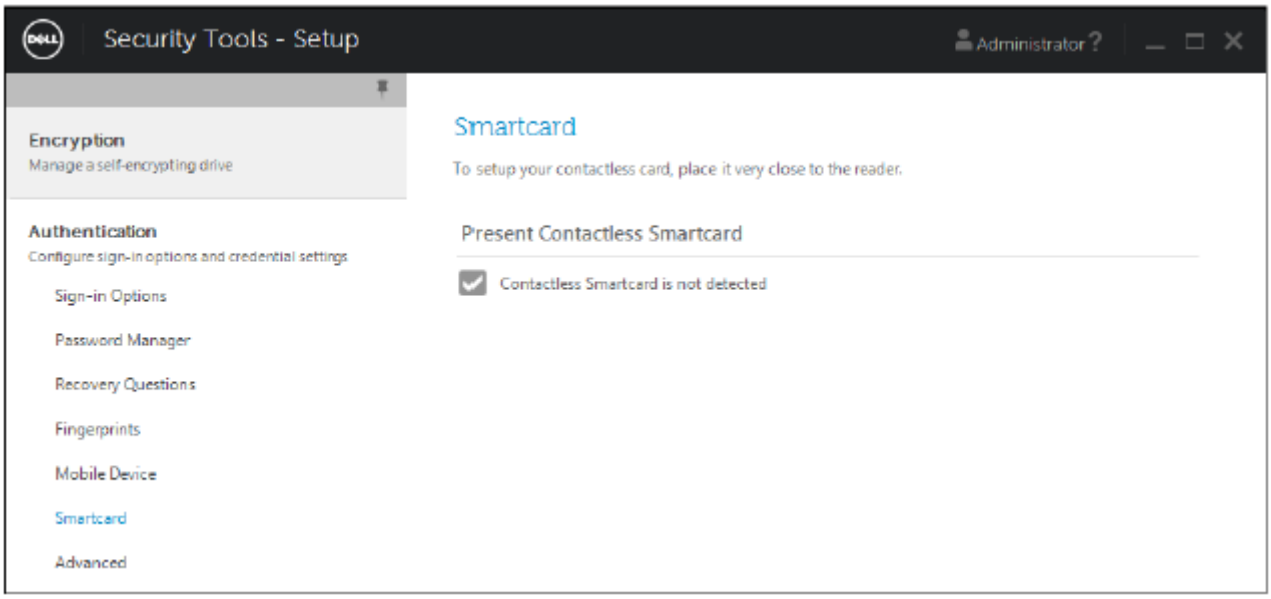
Contacted cards require a smart card reader into which the card is inserted. Contacted cards are only compatible with domain computers. CAC and SIPRNet cards are both contacted cards. Due to the advanced nature of these cards, the user will be required to choose a cert after using inserting his card to log on.

- Contactless cards are supported by non-domain computers and by computers configured with domain specifications.
- Users can enroll one contacted smart card per user account, or multiple contactless cards per account.
- Smart cards are not supported with Preboot Authentication.

NOTE: When removing a smart card enrollment from an account with multiple cards enrolled, all cards are unenrolled at the same time.

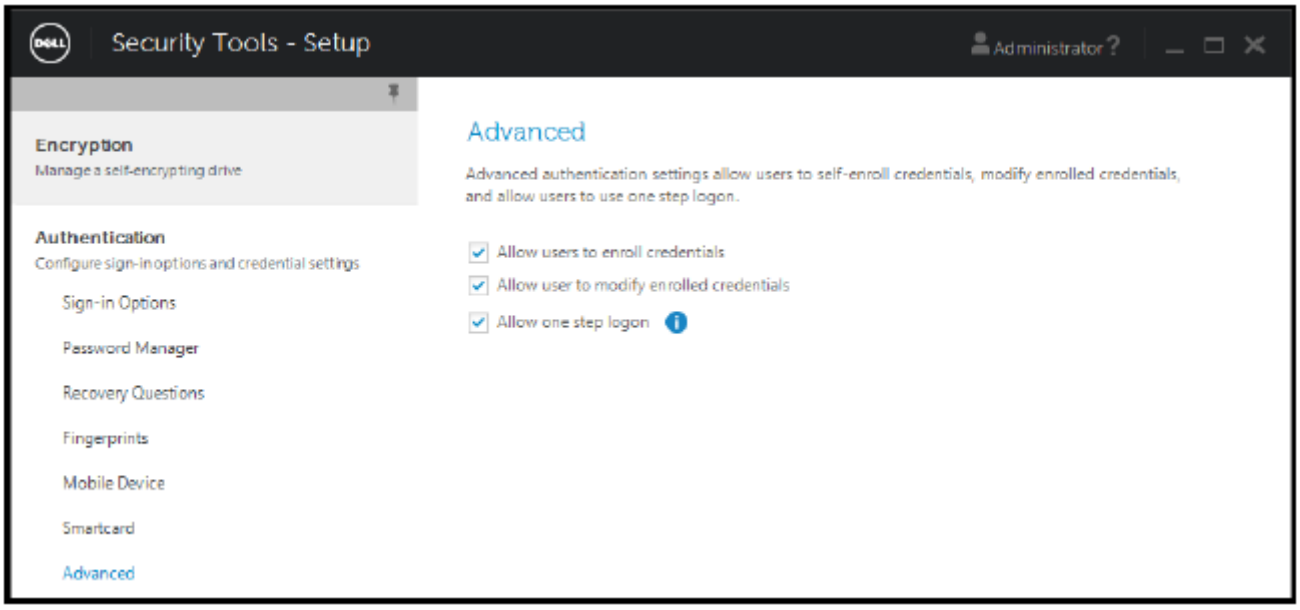
To configure smart card enrollment:

On the Administrator Settings tool's Authentication tab, select **Smartcard**.



Configure Advanced Permissions

1. Click **Advanced** to modify advanced end user options. Under *Advanced*, you can optionally allow users to self-enroll credentials, optionally allow users to modify their enrolled credentials, and enable one step logon.



2. Select or clear the check boxes:

   Allow users to enroll credentials - By default, the check box is selected. Users are permitted to enroll credentials without intervention by an administrator. If you clear the check box, credentials must be enrolled by the administrator.

   Allow user to modify enrolled credentials - By default, the check box is selected. When selected, users are permitted to modify or delete their enrolled credentials without intervention by an administrator. If you clear the check box, credentials cannot be modified or deleted by a regular user but must be modified or deleted by the administrator.

   NOTE: To enroll a user's credentials, go to the *Users* page of the Administrator Settings tool, select a user and click Enroll.

   Allow one step logon - One step logon is Single Sign-on (SSO). By default, the check box is selected. When this feature is enabled, users must enter their credentials only at the Preboot Authentication screen. Users are automatically logged on to Windows. If you clear the check box, the user may be required to log on multiple times.

NOTE: This option cannot be selected unless the Allow users to enroll credentials setting is also selected.

3. Click **Apply** when finished.

Smart Card and Biometric Services (Optional)

If you do not want Security Tools to change the services associated with smart cards and biometric devices to a startup type of "automatic," the service startup feature can be disabled.

When disabled, Security Tools will not attempt to start these three services:

- SCardSvr - Manages access to smart cards read by the computer. If this service is stopped, this computer will be unable to read smart cards. If this service is disabled, any services that explicitly depend on it will fail to start.
- SCPolicySvc - Allows the system to be configured to lock the user desktop upon smart card removal.
- WbioSrvc - The Windows biometric service gives client applications the ability to capture, compare, manipulate, and store biometric data without gaining direct access to any biometric hardware or samples. The service is hosted in a privileged SVCHOST process.

Disabling this feature also suppresses warnings associated with the required services not running.

Disable the Automatic Service Startup

By default, if the registry key does not exist or the value is set to 0, this feature is enabled.

1. Run **Regedit**.
2. Locate the following registry entry:

   [HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

   SmartCardServiceCheck=REG_DWORD:0

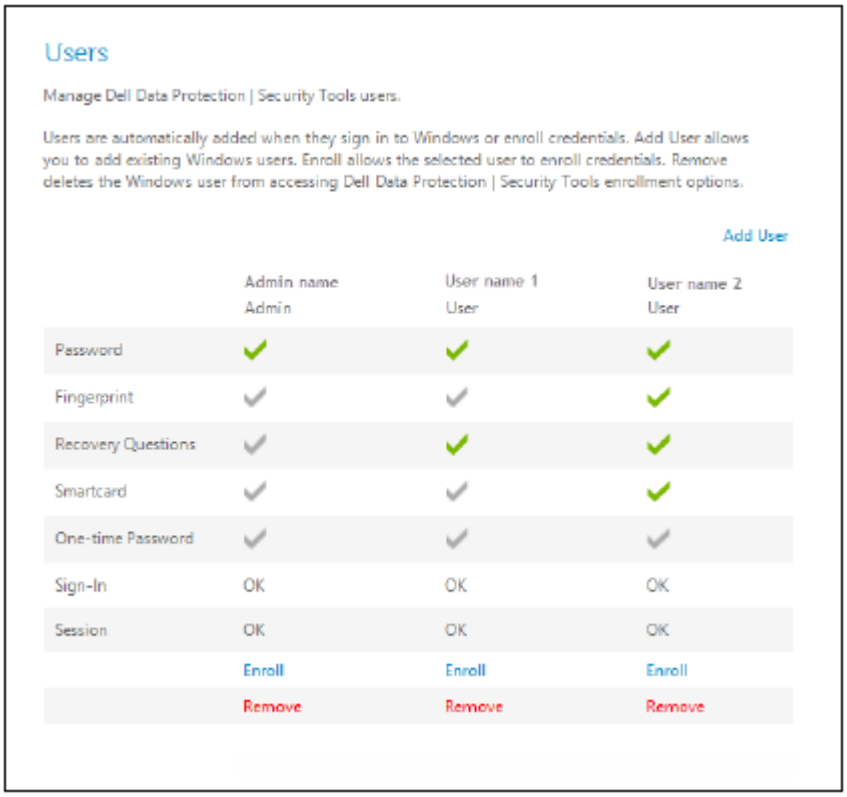
   Set to 0 to Enable. Set to 1 to Disable.

Manage Users' Authentication

The controls on the Administrator Settings Authentication tab let you set user logon options and customize the settings for each.

To manage user authentication:

1. As an administrator, click the **Administrator Settings** tile.
2. Click the **Users** tab to manage users and view user enrollment status. From this tab, you can:
   - Enroll new users
   - Add or change credentials
   - Remove a user's credentials



NOTE:

Sign-in and Session show the enrollment status of a user.

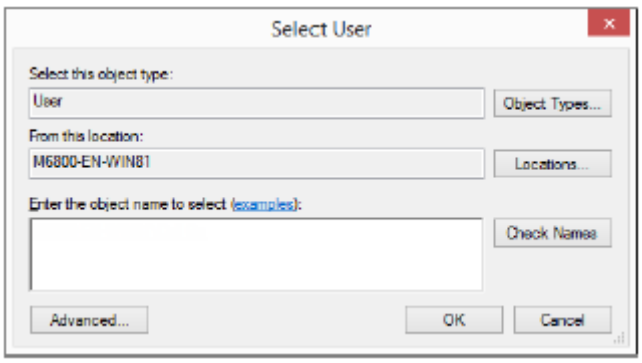
When Sign-in status is OK, all enrollments that the user needs to be able to log on have been completed. When Session status is OK, all enrollments that the user needs to use Password Manager have been completed.

If either status is No, the user needs to complete additional enrollments. To find out which enrollments are still needed, select the Administrator Settings tool and open the Users tab. Gray check mark boxes represent incomplete enrollments. Alternatively, click the Enrollments tile and review the Status tab's Policy column, where the required enrollments are listed.

Add New Users

NOTE: New Windows users are automatically added when they log on to Windows or enroll credentials.

1. Click **Add User** to begin the enrollment process for an existing Windows user.
2. When the *Select User* dialog displays, select **Object Types**.



3. Enter a user's object name in the text box and click **Check Names**.
4. Click **OK** when finished.

The Enrollment wizard opens.

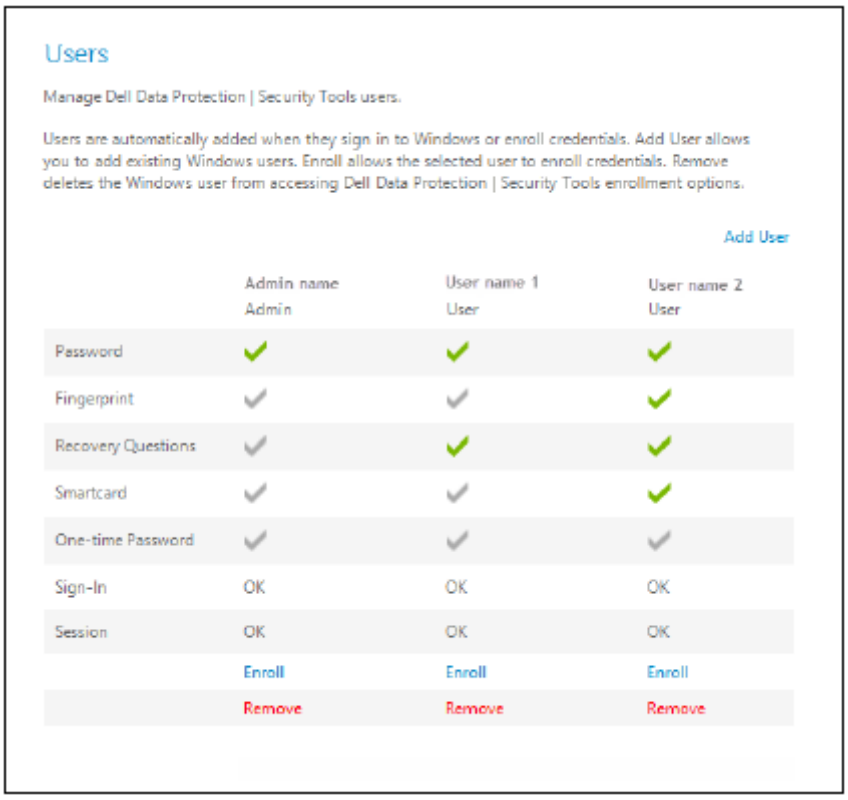
Continue to Enroll or Change User Credentials for instructions.

Enroll or Change User Credentials

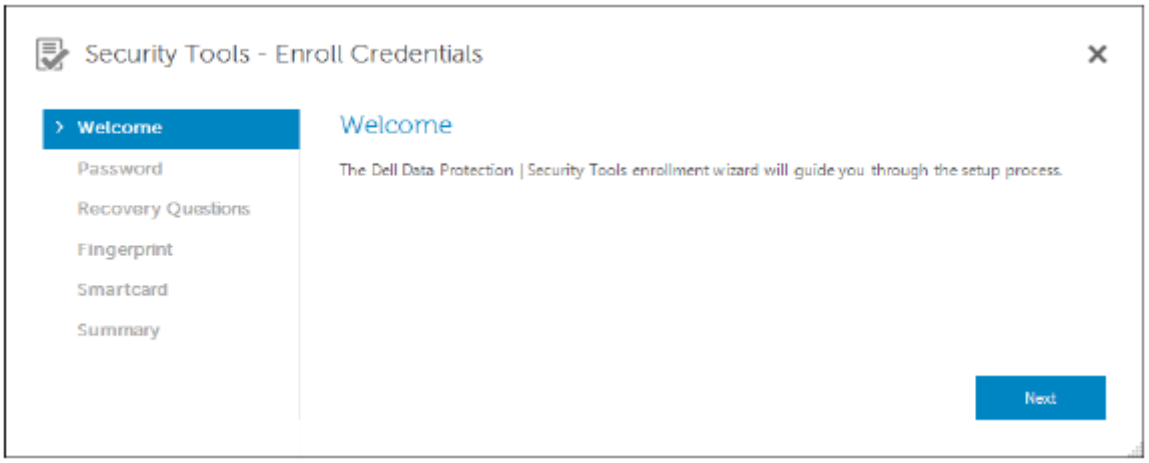
The administrator can enroll or change a user's credentials on behalf of a user, but a few enrollment activities require the user's presence, such as answering recovery questions and scanning the user's fingerprints.

To enroll or change user credentials:

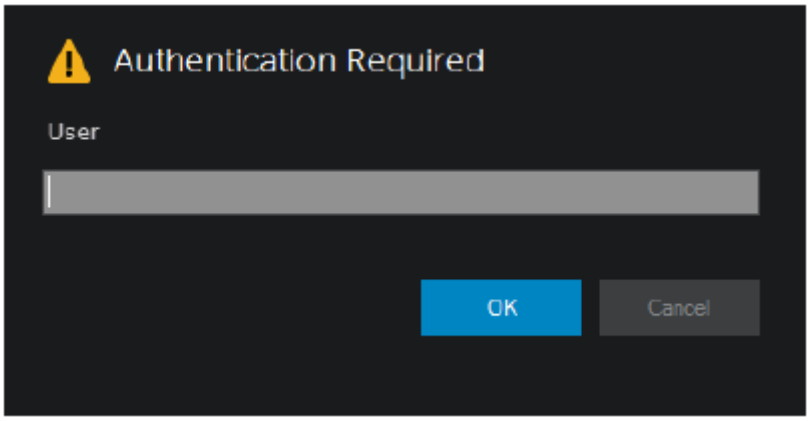
1. In Administrator Settings, click the **Users** tab.
2. On the Users page, click **Enroll**.



3. On the Welcome page, click **Next**.



4. In the Authentication Required dialog, log in with the user's Windows password, and click **OK**.



5. On the Password page, to change the user's Windows password, enter and confirm a new password and click **Next**.

   To skip changing the password, click **Skip**. The wizard allows you to skip a credential if you don't want to enroll it. To return to a page, click **Back**.

6. Follow the instructions on each page, and click the appropriate button: **Next**, **Skip**, or **Back**.
7. On the Summary page, confirm the enrolled credentials and, when finished with enrollment, click **Apply**.

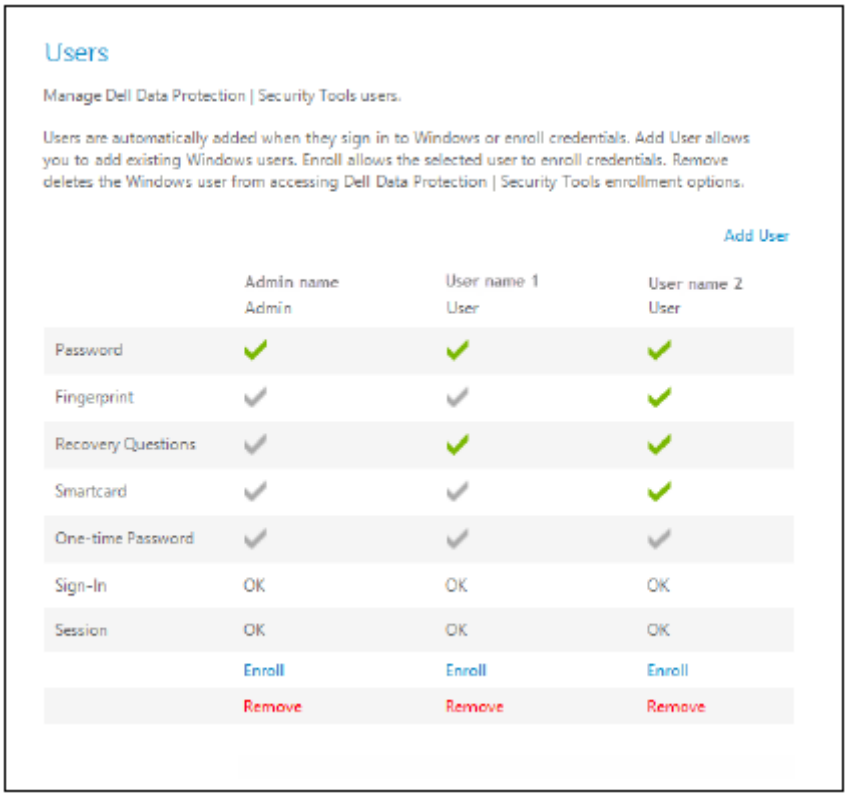
   To return to a credential enrollment page to make a change, click **Back** until you reach the page you want to change.

   For more detailed information about enrolling a credential, or to change a credential, see the *Console User Guide*.

Remove One Enrolled Credential

1. Click the **Administrator Settings** tile.
2. Click the **Users** tab and find the user to change.
3. Hover over the green checkmark of the credential you want to remove. It turns into ⊗.
4. Click the ⊗ symbol and then click **Yes** to confirm the deletion.

   NOTE: A credential cannot be removed this way if it is the user's only enrolled credential. In addition, the Password cannot be removed with this method. Use the Remove command to completely remove a user's access to the computer.



Remove All of a User's Enrolled Credentials

1. Click the **Administrator Settings** tile.
2. Click the **Users** tab and find the user you want to remove.
3. Click **Remove**. (The Remove command appears in red at the bottom of the user's settings).

   After removal, the user will not be able to log on to the computer unless he re-enrolls.

5

Uninstallation Tasks

To uninstall DDP | Security Tools, you must be at least a **local Admin** user.

Uninstall DDP | Security Tools

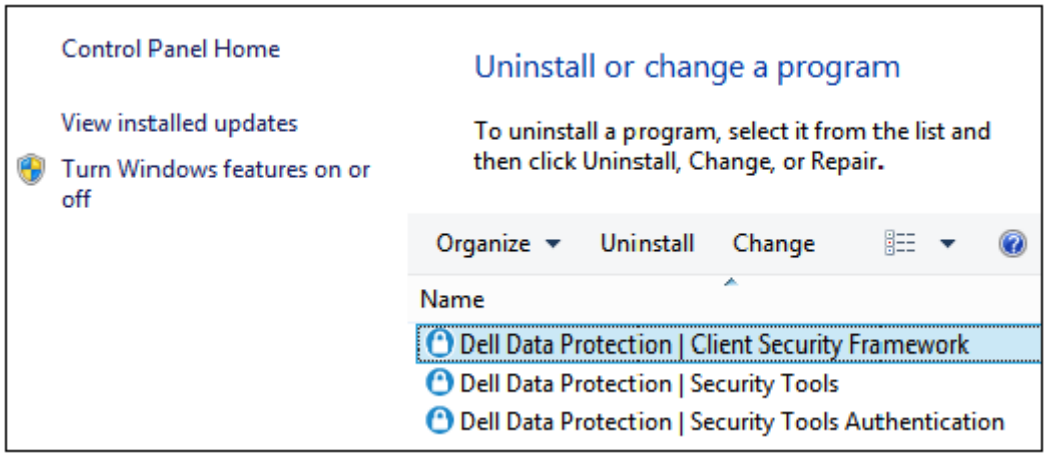
You must uninstall the applications in this order:

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

If you have a computer with a self-encrypting drive, follow these instructions to uninstall:

1. Deprovision the SED:
   a. From Administrator Settings > click the **Encryption** tab.
   b. Click **Decrypt** to disable encryption.
   c. Once the SED is unencrypted, restart the computer.
2. In the Windows Control Panel, go to **Uninstall a Program**.

   NOTE: Start > Control Panel > Programs and Features > Uninstall a Program.



3. Uninstall **Client Security Framework**, and restart the computer.
4. From the Windows Control Panel, uninstall **Security Tools Authentication**.

   A message displays prompting whether you want to preserve the user data.

   Click **Yes** if you plan to re-install Security Tools. Otherwise, click **No**.

   After uninstallation is completed, restart the computer.

5. From the Windows Control Panel, uninstall **Security Tools**.

   A message displays prompting whether you want to completely uninstall this application and its components.

   Click **Yes**.

   The *Uninstallation Complete* dialog displays.

6. Click **Yes, I want to restart my computer now** and then click **Finish**.
7. The computer restarts and uninstallation is complete.

6

Recovery

Recovery options are available in case user credentials expire or are lost:

- **One-time Password (OTP):** The user generates an OTP with the Security Tools Mobile app on an enrolled mobile device and enters the OTP at the Windows logon screen to regain access. This option is available only if the user has enrolled a mobile device with Security Tools on the computer. To use the OTP feature for recovery, the user must not have used OTP to log on to the computer.

  NOTE: The One-time Password (OTP) feature requires that the TPM is present, enabled, and owned. Follow the instructions in Clear Ownership and Activate the TPM. An OTP can be used either for authentication or for recovery, but not for both. For details, see Configure Sign-in Options.

- **Recovery Questions:** The user correctly answers a set of personal questions to regain access to the computer. This option is available only if the administrator has configured and enabled Recovery Questions, and the user has enrolled Recovery Questions. This option can be used to regain access to the computer through both the Preboot Authentication screen and Windows logon screen.

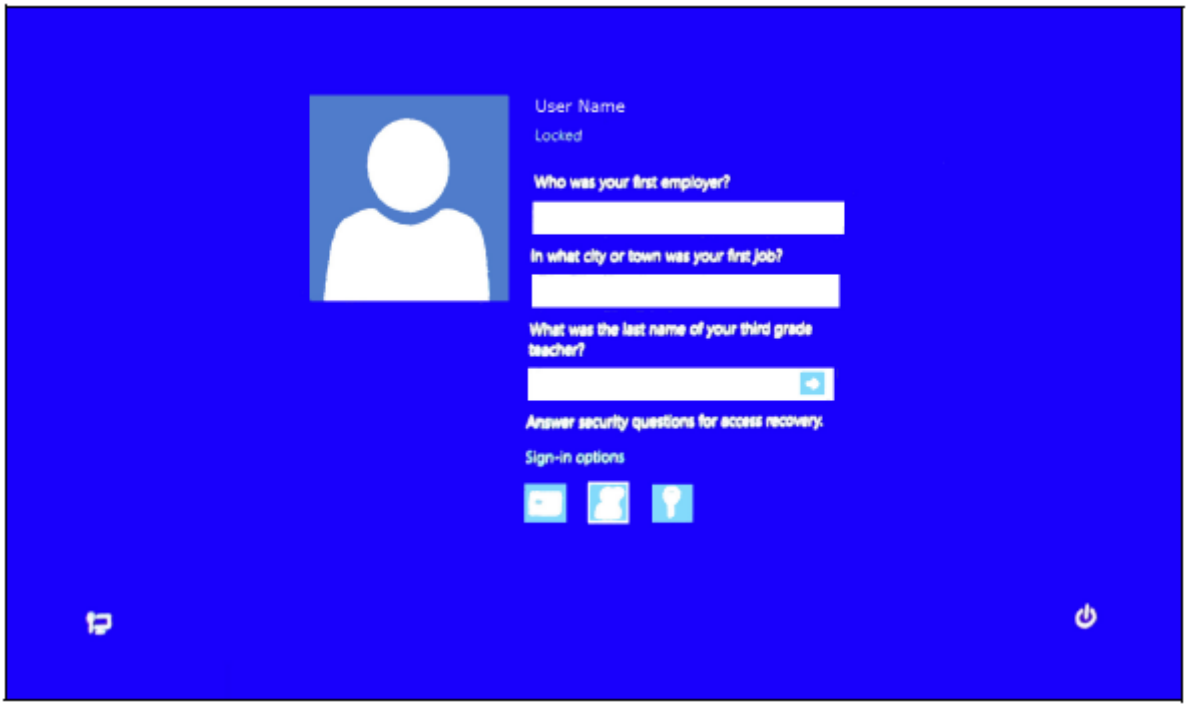
Both recovery methods require that you have prepared for recovery, either by enrolling Recovery Questions or by enrolling a mobile device with Security Tools on the computer.

Self-Recovery, Windows Logon Recovery Questions

To answer Recovery Questions to recover access at the Windows logon screen:

1. To use the Recovery questions, click **Can't access your account?**

   The Recovery Questions that you selected during enrollment display.



2. Enter the answers and click **OK**.

   Upon successful entry of the answers to the questions, you enter Access Recovery mode. What happens next depends upon the credential that failed.

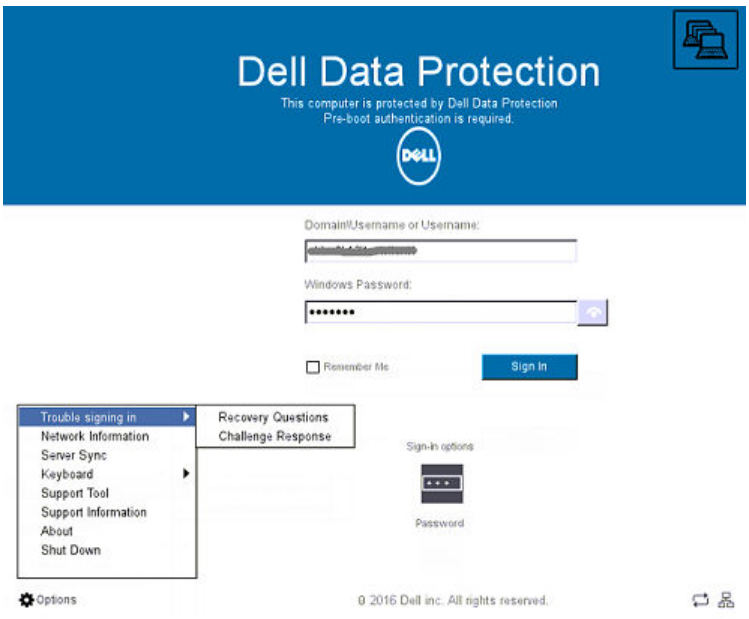
   - If you failed to enter the correct Windows password, then the Change Password screen displays.

- If a fingerprint failed to be recognized, then the fingerprint enrollment page displays so that you can re-enroll the fingerprint.

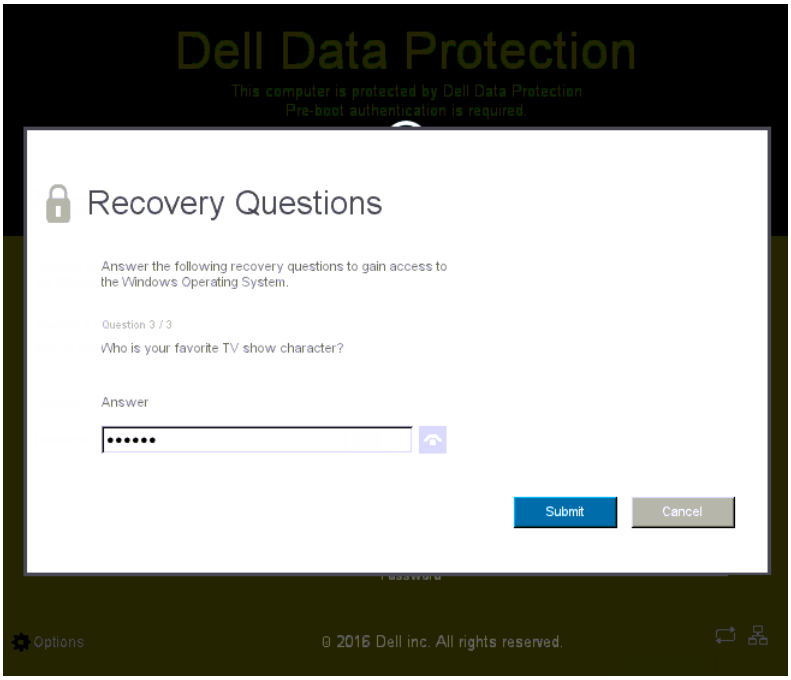
Self-Recovery, PBA Recovery Questions

To answer Recovery Questions to recover access at the Preboot Authentication screen:

1. Enter your user name.
2. At the bottom left side of the screen, click **Options** > **Trouble Signing In**.



3. When the Q&A dialog appears, enter the answers that you supplied when you enrolled in Recovery Questions the first time you signed in.



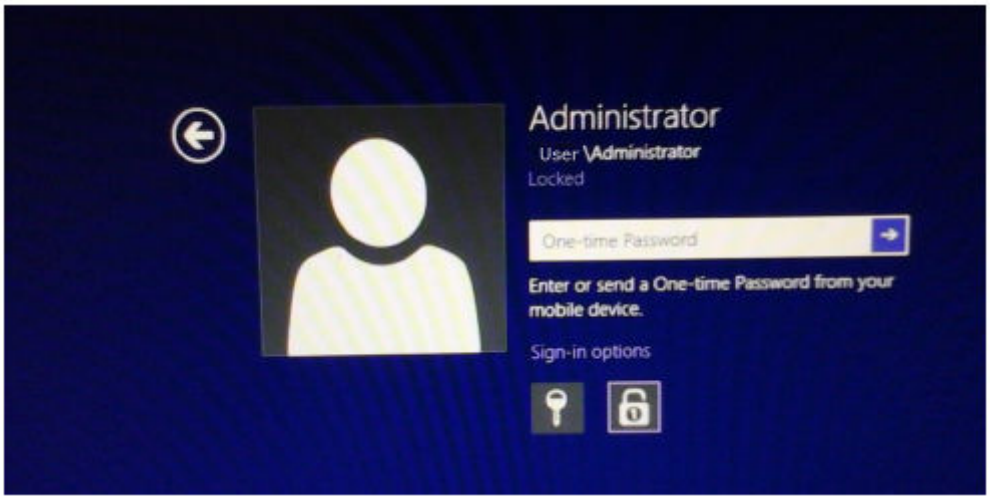
Self-Recovery, One-time Password

This procedure describes how to use the One-time Password (OTP) feature to recover access to the computer if, for example, the Windows password is expired or forgotten or the maximum allowed logon attempts is exceeded. The One-time Password (OTP) option is available only if the user has enrolled a mobile device and only if OTP was not last used to log on to Windows.

NOTE: The One-time Password feature requires that TPM is present, enabled, and owned. OTP can be used either for Windows authentication or for recovery, but not both. The administrator can set policy to allow OTP for either recovery or authentication or can disable the feature.

To use OTP to recover access to the computer:

1. At the Windows logon screen, select the OTP icon .



2. On the mobile device, open the Security Tools Mobile app and enter the password.
3. Select the computer you want to access.

   If the computer name does not display on the mobile device, one of these conditions may exist:

   - The mobile device is not enrolled, or paired, with the computer you are trying to access.

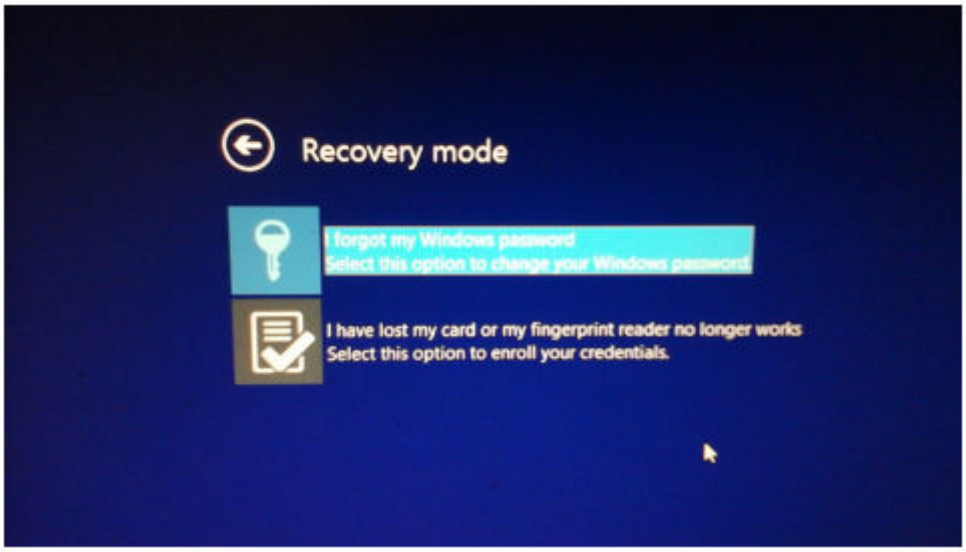
- If you have more than one Windows user account, either DDP | Security Tools is not installed on the computer that you are trying to access or you are attempting to log on to a different user account than was used to pair the computer and the mobile device.

4. Tap **One-time Password.**

   A password displays on the mobile device screen.

   NOTE: If necessary, click the Refresh symbol to get a new code. After the first two OTP refreshes, there will be a thirty-second delay before another OTP can be generated. The computer and mobile device must sync so that they both can recognize the same password at the same time. Trying to rapidly generate password after password will cause the computer and mobile device get out of sync and the OTP feature to fail. If this problem should occur, wait for thirty seconds for the two devices to get back in sync, and then try again.

5. On the computer, at the Windows logon screen, type the password displayed on the mobile device and press **Enter**.
6. On the computer, at the Recovery mode screen, select **I forgot my Windows password** and follow the on-screen instructions to reset your password.



7

Glossary

Deprovision - Deprovisioning removes the PBA database and deactivates the PBA. Deprovisioning requires a shutdown to take effect.

One-Time Password (OTP) - A one-time password is a password that can be used only once and is valid for a limited length of time. OTP requires that the TPM is present, enabled, and owned. To enable OTP, a mobile device is paired with the computer using the Security Console and the Security Tools Mobile app. The Security Tools Mobile app generates the password on the mobile device that is used to log onto the computer at the Windows logon screen. Based on policy, the OTP feature may be used to recover access to the computer if a password is expired or forgotten, if OTP has not been used to log on to the computer. The OTP feature can be used either for authentication or for recovery, but not both. OTP security exceeds that of some other authentication methods since the generated password can be used only once and expires in a short time.

Preboot Authentication (PBA) - Preboot Authentication serves as an extension of the BIOS or boot firmware and guarantees a secure, tamper-proof environment external to the operating system as a trusted authentication layer. The PBA prevents anything being read from the hard disk, such as the operating system, until the user has confirmed they have the correct credentials.

Single Sign-On (SSO) - SSO simplifies the logon process when multi-factor authentication is enabled at both preboot and Windows logon. If enabled, authentication is required at preboot only, and users are automatically logged on to Windows. If not enabled, authentication may be required multiple times.

Trusted Platform Module (TPM) - TPM is a security chip with three major functions: secure storage, measurement, and attestation. The Encryption client uses TPM for its secure storage function. The TPM can also provide encrypted containers for the software vault. The TPM is also required for use with the One-time Password feature.