Dell Data Protection | Security Tools

Security Tools Installation Guide

Dell Data Protection | Security Tools Installation Guide

Installation Guide v1.12

DELL EMC

Примечания, предупреждения и предостережения

ПРИМЕЧАНИЕ: Пометка ПРИМЕЧАНИЕ указывает на важную информацию, которая поможет использовать данное изделие более эффективно.

ОСТОРОЖНО: Указывает на возможность повреждения устройства или потери данных и подсказывает, как избежать этой проблемы.

ПРЕДУПРЕЖДЕНИЕ: Указывает на риск повреждения оборудования, получения травм или на угрозу для жизни.

2017- 02

Rev. A01

Contents

1

Введение

Dell Data Protection | Security Tools обеспечивает безопасность и защиту в процессе идентификации администраторов и пользователей компьютеров Dell. Утилита DDP | Security Tools предустанавливается на все модели компьютеров Dell Latitude, Optiplex и Precision и некоторые модели ноутбуков Dell XPS. Если необходимо *переустановить* DDP | Security Tools, следуйте инструкциям в настоящем руководстве. Для получения дополнительной поддержки см. веб-сайт по адресу www.dell.com/support > Endpoint Security Solutions.

Обзор

DDP | Security Tools — комплексный продукт для безопасности, разработанный для обеспечения поддержки расширенной проверки подлинности, проверки подлинности перед загрузкой (PBA), а также поддержки самошифрующихся дисков.

DDP | Security Tools обеспечивает многофакторную поддержку для проверки подлинности Windows с помощью паролей, считывателей отпечатков пальцев и смарт-карт, контактных и бесконтактных, а также для самостоятельной одношаговой регистрации (система единого входа [SSO]), и одноразовых паролей (OTP).

Перед внесением средств обеспечения безопасности для конечных пользователей, администратор может настроить функции пакета Security Tools, с помощью инструмента «параметры администратора» консоли безопасности DDP, например, чтобы включить проверку подлинности перед загрузкой и политики проверки подлинности. Однако настройки по умолчанию позволяют администраторам и пользователям начать использовать средства безопасности сразу же после их установки и активации.

Консоль безопасности DDP

Консоль безопасности DDP - это интерфейс средств безопасности, благодаря которому пользователи могут зарегистрироваться и управлять своими учетными данными, настроить вопросы для самостоятельного восстановления доступа в соответствии с требованиями политики, установленной администратором. Пользователи могут получить доступ к этим приложениям средств безопасности:

- Инструмент шифрования позволяет пользователям просматривать статус шифрования дисков компьютера.
- Инструмент регистрации позволяет пользователям настроить учетные данные и управлять ими, настроить вопросы для самостоятельного восстановления доступа и просматривать статус регистрации своих учетных данных. Эти права основаны на требованиях политики, установленной администратором.
- Диспетчер паролей (Password Manager) позволяет пользователям автоматически заполнять формы и вводить данные, необходимые для доступа к веб-сайтам, приложениям Windows и сетевым ресурсам. Password Manager также предоставляет пользователям возможность изменять пароли для входа с помощью приложения. Таким образом, все пароли, которые находятся под контролем приложения Password Manager, будут синхронизированы с паролями целевых ресурсов.

Параметры администратора

Инструмент настроек администратора используется для настройки средств обеспечения безопасности для всех пользователей компьютера, что позволяет администратору настроить политики проверки подлинности, управлять пользователями и настроить учетные данные, которые можно использовать для входа в Windows.

С помощью инструмента настроек администратора администратор может включить шифрование и проверку подлинности перед загрузкой (PBA), а также настроить политики PBA и текст, выводимый на экране проверки подлинности.

Перейдите к разделу Требования.

2

Требования

- DDP | Security Tools предустанавливается на все модели компьютеров Dell Latitude, Optiplex и Precision и некоторые модели ноутбуков Dell XPS и требует выполнения приведенных ниже минимальных требований. Если возникнет необходимость переустановить DDP | Security Tools, следует еще раз убедиться, что ваш компьютер соответствует этим требованиям. См. верб-сайт www.dell.com/support > Endpoint Security Solutions для получения дополнительной информации.
- Windows 8.1 не следует устанавливать на диске 1 на самошифрующихся дисках. Такая конфигурация операционной системы не поддерживается, так как Windows 8.1 создает раздел восстановления 0, который нарушает проверку подлинности перед загрузкой. Поэтому либо установите Windows 8.1 на диске 0, либо восстановите образ Windows 8.1 на одном из дисков.
- DDP | Security Tools не поддерживает динамические диски.
- Компьютеры, оснащенные самошифрующимися дисками, не могут использоваться с аппаратными криптографическими ускорителями (HCA). Использование HCA невозможно по причине несовместимости. Следует иметь в виду, что Dell не продает компьютеры с самошифрующимися дисками, которые поддерживают работу модуля HCA. Такие не поддерживаемые конфигурации могут возникать на вторичном рынке.
- DDP | Security Tools не поддерживает работу конфигураций с многозагрузочными дисками.
- Перед установкой новой операционной системы на клиент очистите Доверенный платформенный модуль (TPM) в BIOS.
- SED не требует TPM, чтобы обеспечить расширенную проверку подлинности или шифрование.

Драйверы

- Для поддерживаемых самошифрующихся дисков, соответствующих спецификации Opal, требуются обновленные драйверы Rapid Storage Technology, расположенные на веб-сайте http://www.dell.com/support/drivers/us/en/19/DriverDetails/Product/latitude-e6440-laptop?driverId=1KX2H&osCode=W764&fileId=3356216042&languageCode=en&categoryId=SA

ПРИМЕЧАНИЕ:

Из-за особенностей RAID и самошифрующихся дисков, управление самошифрующимися дисками не поддерживает RAID. Проблема с настройкой «RAID=On» при работе с дисками SED заключается в том, что RAID требует доступа к диску для чтения и записи данных RAID в секторе высокого порядка, которые не доступны на заблокированном диске SED с момента запуска, и не может ждать возможности считывания этих данных, до тех пор пока пользователь не выполнит вход в систему. Чтобы решить эту проблему, измените настройку для работы с дисками SATA в BIOS с «RAID=On» на «AHCI». Если в операционной системе предварительно не установлены драйверы контроллера AHCI, то после изменения настройки с «RAID=On» на «AHCI» операционная система выведет «синий экран».

Предварительные требования для клиента

- Для работы Security Tools требуется полная версия Microsoft .Net Framework 4.5 (или более поздняя версия). На всех компьютерах, поставляемых Dell, уже установлена полная версия Microsoft .Net Framework 4.5. Однако если вы устанавливаете Security Tools не на оборудование Dell или обновляете Security Tools на устаревшем оборудовании Dell, следует проверить установленную версию Microsoft .Net и обновить ее перед установкой Security Tools в целях предотвращения возникновения неполадок при установке или обновлении. Чтобы установить полную версию Microsoft .Net Framework 4.5, перейдите по ссылке https://www.microsoft.com/en-us/download/details.aspx?id=30653

  Чтобы узнать версию установленной среды .Net на компьютере, где планируется установка Security Tools, выполните указания из следующей ссылки: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx
- На компьютере должны быть установлены самые последние версии драйверов и микропрограмм для оборудования проверки подлинности. Для получения драйверов и микропрограммы для компьютеров Dell, перейдите на страницу http://www.dell.com/support/home/us/en/19/Products/?app=drivers и выберите модель вашего компьютера. В зависимости от имеющегося оборудования проверки подлинности загрузите следующее:
  - Драйвер для считывания отпечатков пальцев NEXT Biometrics

- Драйвер Validity FingerPrint Reader 495
- Драйвер считывания смарт-карт O2Micro
- Dell ControlVault

Производители стороннего оборудования могут требовать собственных драйверов.

Программа установки позволит установить этот компонент, если он отсутствует на компьютере.

Предварительные требования

- Распространяемый пакет Microsoft Visual C++ 2012, обновление 4 (или более позднее) (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

Mobile Device 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

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

Языковая поддержка

Утилита DDP | Security Tools совместима с многоязычным пользовательским интерфейсом (Multilingual User Interface, MUI) и поддерживает указанные ниже языки.

ПРИМЕЧАНИЕ:

В компьютерах на базе UEFI не поддерживается локализация PBA на русском, традиционном и упрощенном китайском языках.

Языковая поддержка

- EN - английский
- FR - французский
- IT - итальянский
- DE - немецкий
- ES - испанский
- JA - японский
- KO - корейский
- ZH-CN - китайский упрощенный
- ZH-TW - китайский традиционный/тайваньский
- PT-BR - португальский (Бразилия)
- PT-PT - португальский (Португалия) (иберийский)
- RU - русский

Параметры проверки подлинности

В следующих параметрах проверки подлинности потребуется специальное оборудование: отпечатки пальцев, смарт-карты, бесконтактные карты, карты класса B/SIPR Net, и **проверка подлинности на UEFI-компьютерах**.

Для использования функции одноразового пароля необходимо наличие включенного собственного TPM. Для получения дополнительной информации см. Удаление владения и активация TPM. Функция одноразового пароля не поддерживается модулем TPM 2.0.

В таблице ниже приводятся параметры проверки подлинности, доступные в Security Tools в соответствии с операционной системой, отвечающей требованиям оборудования и конфигурации.

Не UEFI

	Проверка подлинности перед загрузкой					Проверка подлинности Windows				
	Пароль	**Отпечаток пальца**	**Контактная смарт-карта**	**Однораз овый пароль**	**Карта SIPR**	**Пароль**	**Отпечаток пальца**	**Смарт-карта**	**Однораз овый пароль**	**Карта SIPR**
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. Доступно при поддержке самошифрующегося диска Opal.

UEFI

	PBA - на поддерживаемых компьютерах Dell					Проверка подлинности Windows				
	Пароль	**Отпечаток пальца**	**Контактная смарт-карта**	**Однораз овый пароль**	**Карта SIPR**	**Пароль**	**Отпечаток пальца**	**Смарт-карта**	**Однораз овый пароль**	**Карта SIPR**
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. Доступно с поддержкой самошифрующегося диска OPAL на компьютерах с поддержкой интерфейса UEFI.

Совместимость

Отмена инициализации и удаление Dell Data Protection | Access

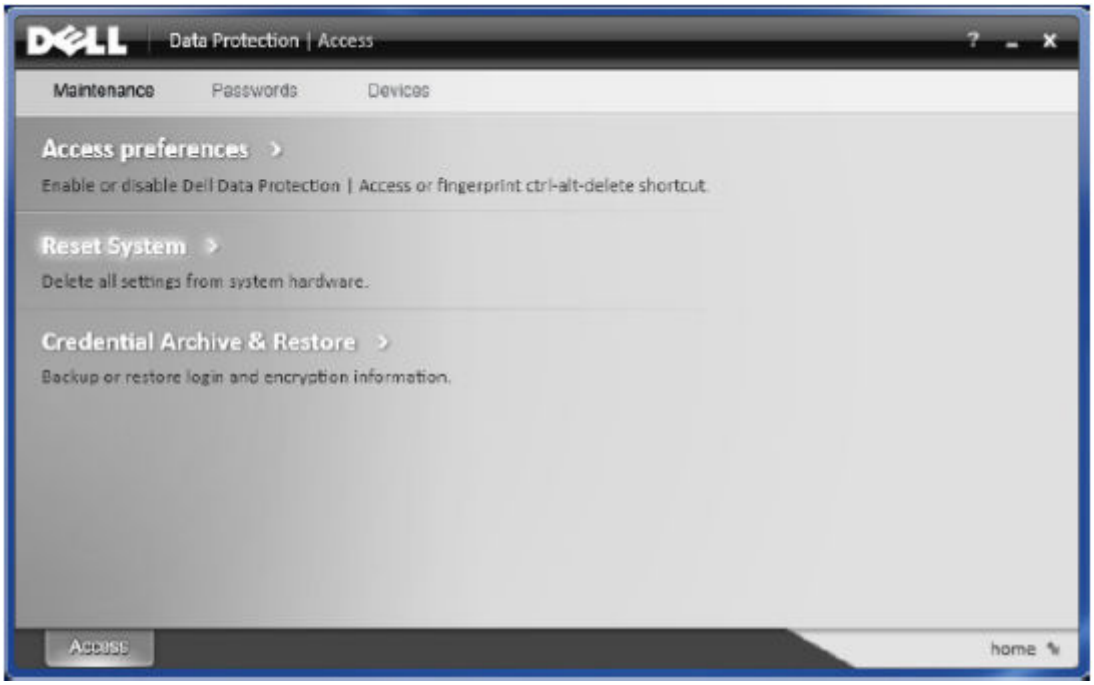
Если пакет DDP|A установлен сейчас или уже был установлен на ваш компьютер ранее, **перед** установкой Security Tools, следует отменить инициализацию оборудования, управляемого DDP|A, и удалить DDP|A. Если DDP|A не используется, вы можете просто удалить DDP|A и перезапустить процесс установки.

Отмена инициализации оборудования, управляемого DDP|A, распространяется на устройство для считывания отпечатков пальцев, устройство для считывания смарт-карт, пароли BIOS, доверенный платформенный модуль (TPM) и самошифрующийся диск.

ПРИМЕЧАНИЕ: При запуске продуктов для шифрования DDP|E остановите или приостановите удаление при шифровании. Если работает программа Microsoft BitLocker, приостановите политику шифрования. После удаления DDP|A и возобновления работы политики Microsoft BitLocker, инициализируйте TPM, выполняя указания, приведенные на веб-сайте http://technet.microsoft.com/en-us/library/cc753140.aspx.

Отмена инициализации оборудования, управляемого DDP|A

1. Запустите DDP|A и перейдите на вкладку **Advanced** («Дополнительно»).



2. Выберите опцию **Reset System** («Сброс системы»). Для этого потребуется ввод предусмотренных учетных данных, предназначеных для идентификации пользователя. После того как DDP|A проверит учетные данные, DDP|A выполнит следующие действия:
   - Удалит все предусмотренные учетные данные из Dell ControlVault (при наличии).
   - Удалит пароль владельца Dell ControlVault (при наличии).
   - Удалит все предусмотренные отпечатки пальцев из встроенного устройства считывания отпечатков пальцев (при наличии).
   - Удалит все пароли BIOS (системный пароль BIOS, пароль администратора BIOS, и пароли доступа к жестким дискам).
   - Очистить Доверенный платформенный модуль.
   - Удалит поставщика учетных данных DDP|A.

   После того как был выполнен отзыв оборудования компьютера, программа DDP|A перезапустит компьютер, чтобы восстановить работу поставщика учетных данных Windows.

Удаление DDP|A

После отмены инициализации оборудования удалите программу DDP|A.

1. Запустите DDP|A и выполните перезапуск системы.

   Это приведет к удалению всех учетных данных, управление которыми осуществляется программой DDP|A, и паролей, а также к очистке доверенного платформенного модуля (TPM).
2. Чтобы запустить программу-установщик, выберите опцию **Uninstall** («Удалить»).
3. После завершения удаления, нажмите кнопку **Yes** («Да»), чтобы перезапустить систему.

ПРИМЕЧАНИЕ: Удаление программы DDP|A также разблокирует самошифрующиеся диски и удалит проверку подлинности перед загрузкой.

Инициализация TPM

- Вы должны быть членом локальной группы Administrators («Администраторы») или иметь эквивалентную роль.

- Компьютер должен быть оснащен совместимым BIOS и модулем TPM.

Выполнение этой задачи требуется при использовании одноразового пароля (OTP).

- Следуйте инструкциям, приведенным по адресу http://technet.microsoft.com/en-us/library/cc753140.aspx.

Очистка собственности и активация доверенного платформенного модуля (TPM)

Чтобы очистить и настроить собственность доверенного платформенного модуля, см. веб-сайт https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2.

Перейдите к разделу Установка и активация.

3

Установка и активация

В этом разделе описан процесс установки утилиты DDP | Security Tools на локальный компьютер. Чтобы установить и активировать DDP | Security Tools, следует войти в систему компьютера с правами администратора.

ПРИМЕЧАНИЕ:

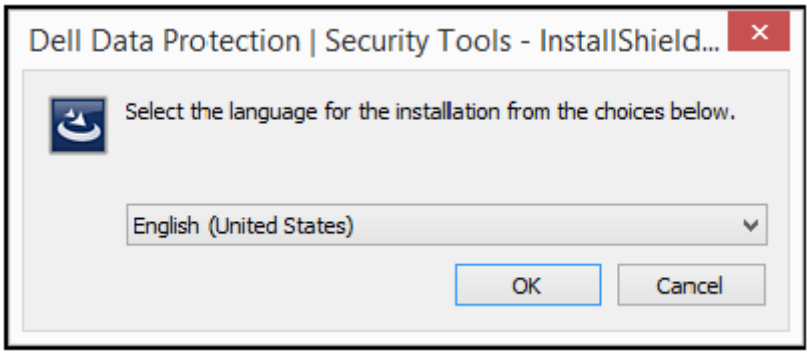
Во время установки не вносите никаких изменений в компьютер, в том числе не вставляйте и не вынимайте внешние (USB) диски.

Установка DDP | Security Tools

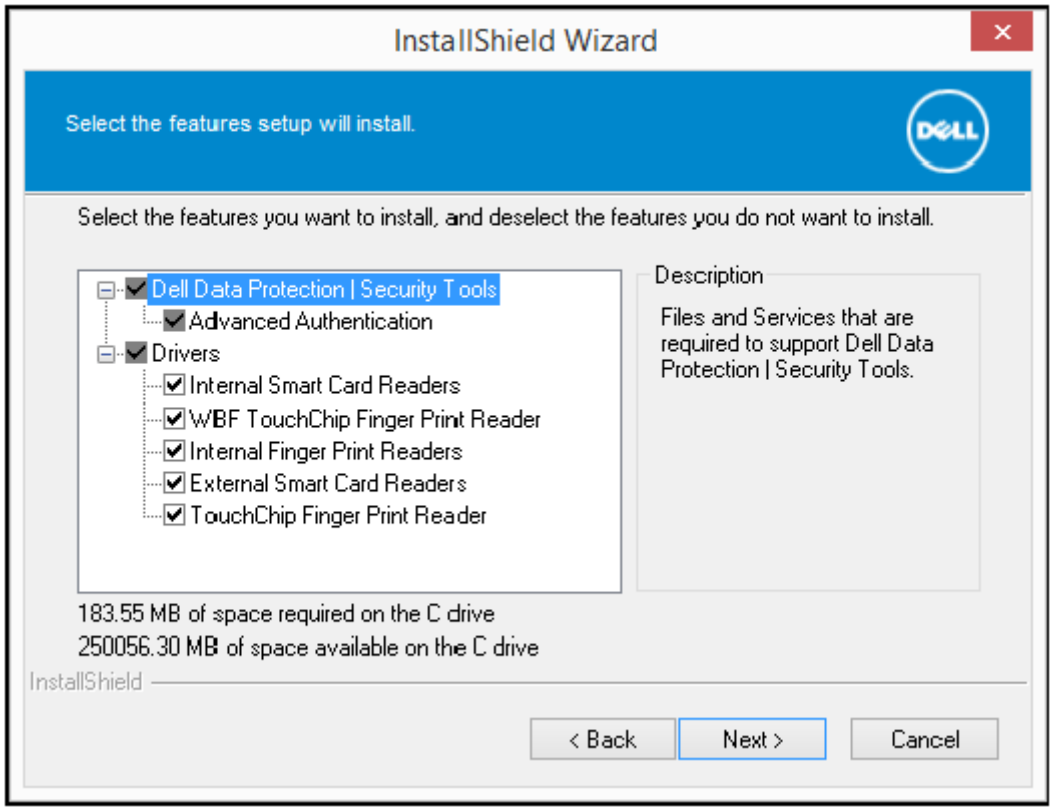
Для установки пакета Security Tools выполняйте следующие указания:

1. Найдите установочный файл на установочном носителе DDP | Security Tools. Скопируйте файл на локальный компьютер.

   ПРИМЕЧАНИЕ: Установочный носитель можно найти по адресу www.dell.com/support > Endpoint Security Solutions.
2. Дважды щелкните файл, чтобы запустить программу установки.
3. Выберите нужный язык и нажмите **OK**.



4. После вывода начальной страницы нажмите кнопку **Next** («Далее»).
5. Прочтите лицензионное соглашение, подтвердите свое согласие с условиями и нажмите кнопку **Next** («Далее»).
6. Нажмите кнопку **Next** («Далее»), чтобы установить Security Tools в папку по умолчанию `C:\Program Files\Dell \Dell Data Protection. Выберите`



7. Чтобы начать установку, нажмите кнопку **Install** («Установить»).
8. После завершения установки потребуется перезагрузка компьютера. Нажмите кнопку **Yes** («Да»), чтобы перезагрузить компьютер, а затем нажмите кнопку **Finish** («Готово»).

   Установка завершена.

Активация DDP | Security Tools

При первом запуске консоли DDP Security и выборе опции параметров администратора, мастер активации поможет пользователю выполнить процесс активации.

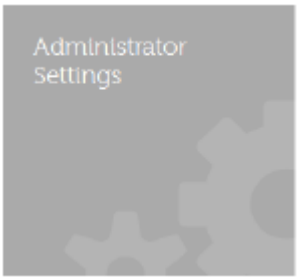
Если консоль DDP Security еще не была активирована, конечный пользователь, тем не менее, может запустить ее. Если конечный пользователь является первым пользователем консоли DDP Security перед тем, как администратор активирует DDP | Security Tools и настроит его параметры, будут использоваться значения по умолчанию.

Чтобы активировать Security Tools:

1. Войдя в систему с правами администратора, запустите программу Security Tools, используя ярлык на рабочем столе.

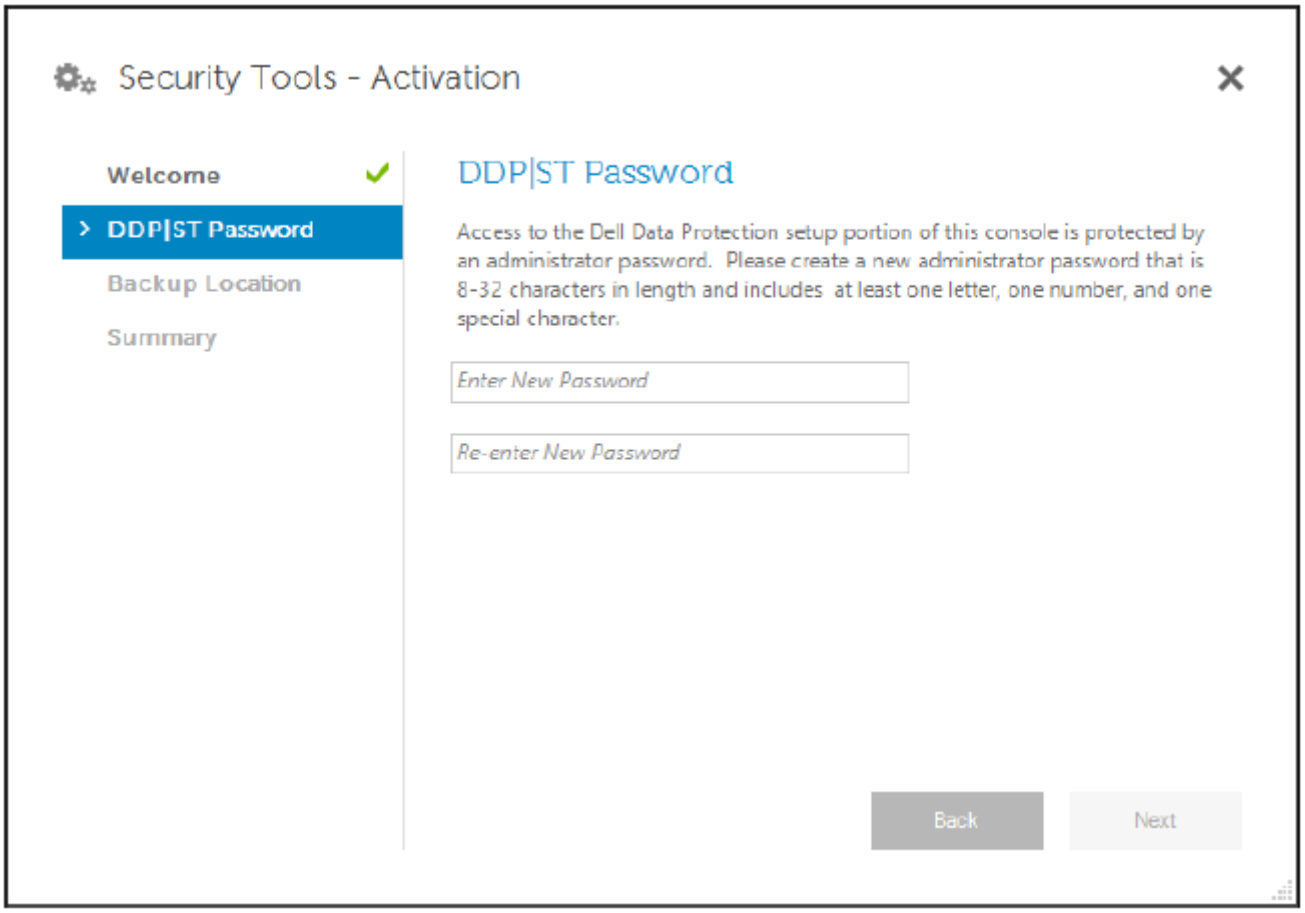
ПРИМЕЧАНИЕ: Если вход в систему выполнен от имени обычного пользователя (с использованием стандартной учетной записи Windows), для запуска инструмента Administrator Settings потребуется повышение полномочий с помощью функции контроля учетных записей пользователя (UAC). Обычный пользователь должен вначале ввести учетные данные администратора, чтобы войти в систему инструмента, а затем еще раз, после получения соответствующего сообщения, в процессе ввода пароля администратора (этот пароль сохранен в разделе параметров администратора).

2. Нажмите на плитку **Administrator Settings** («Параметры администратора»).



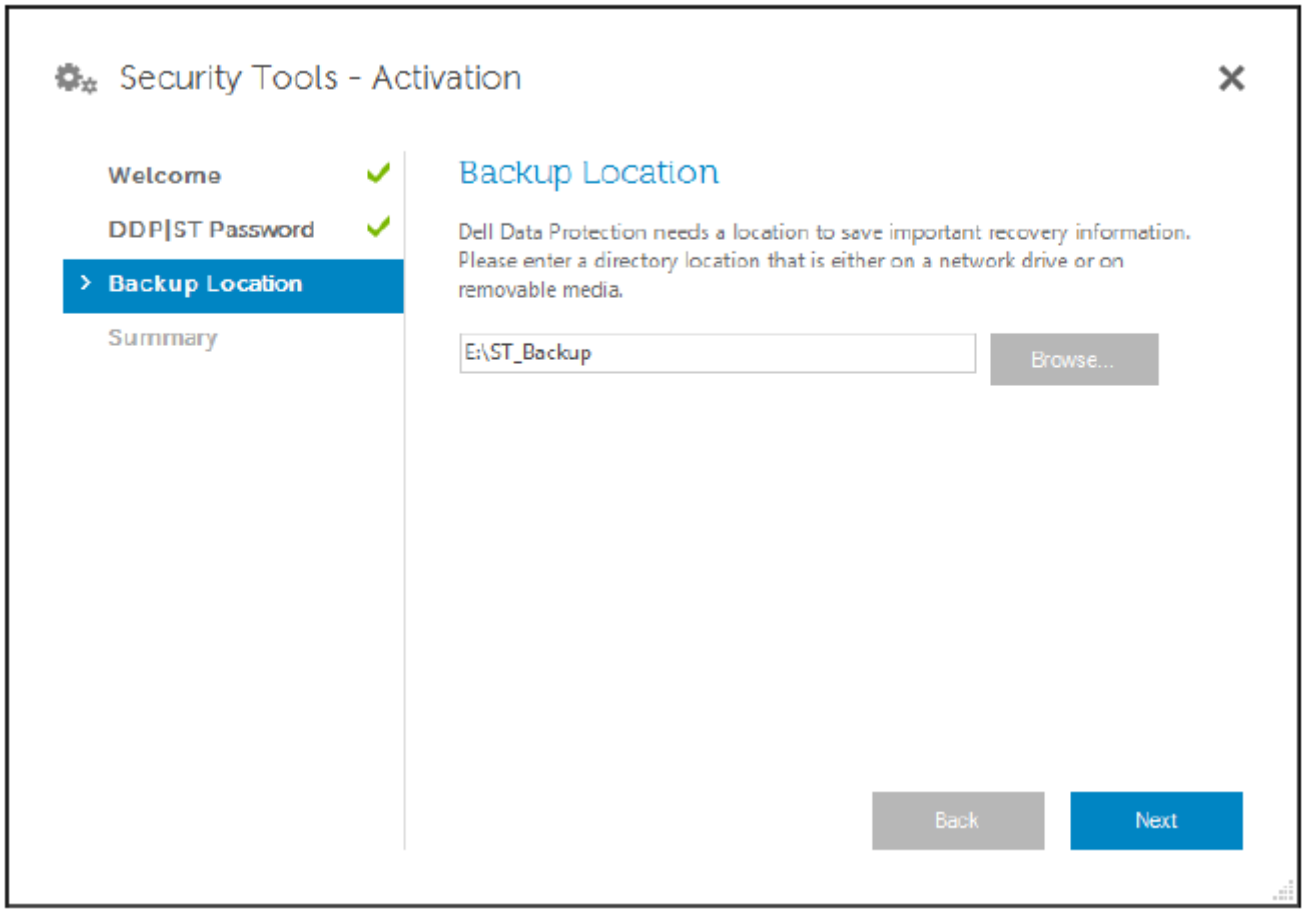
3. На странице приветствия нажмите **Next** («Далее»).
4. Создайте пароль DDP | Security Tools **Next** (Далее).

   Перед тем как выполнить настройку параметров Security Tools, следует создать пароль администратора в DDP | Security Tools. Этот пароль потребуется в любое время при запуске инструмента Administrator Settings. Пароль должен иметь длину от 8 до 32 символов и содержать как минимум одну букву, одну цифру и один специальный символ.



5. В поле **Backup Location** («Местоположение резервной копии») укажите папку, в которую будет записан файл резервной копии, и нажмите кнопку **Next** (Далее). Файл резервной копии может быть сохранен на сетевом диске или на съемном носителе. Файл резервной копии содержит ключи, необходимые для восстановления данных на Вашем компьютере. Служба поддержки Dell должна иметь доступ к этому файлу, чтобы помочь пользователю восстановить данные.

   Резервная копия всех восстановленных данных будет автоматически записана в указанную папку. Если указанное место расположения недоступно (например, не вставлен резервный USB-диск), DDP | Security Tools выведет запрос для выбора места расположения в целях сохранения резервной копии данных восстановления. Доступ к данным восстановления необходим для начала шифрования.



6. На странице Summary («Сводка») нажмите кнопку **Apply («Применить»).**

   Теперь активация программы Security Tools выполнена.

   Администраторы и пользователи могут незамедлительно начать использовать все преимущества программы Security Tools, основанные на параметрах по умолчанию.

4

Задачи настройки для администраторов.

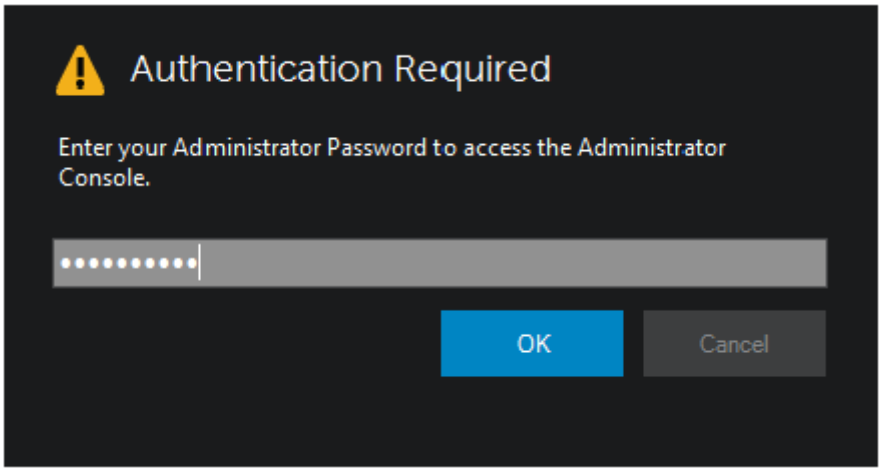
Параметры пакета программ Security Tools, установленные по умолчанию, позволяют администраторам и пользователям использовать Security Tools сразу после активации, без дополнительной настройки. Пользователи автоматически добавляются в качестве пользователей пакета Security Tools, по мере того как они выполняют вход в систему компьютера с использованием своих паролей Windows, но по умолчанию многофакторная проверка подлинности Windows будет выключена. Шифрование и проверка подлинности перед загрузкой также по умолчанию отключены.

Чтобы настроить функции пакета Security Tools, пользователь должен являться администратором компьютера.

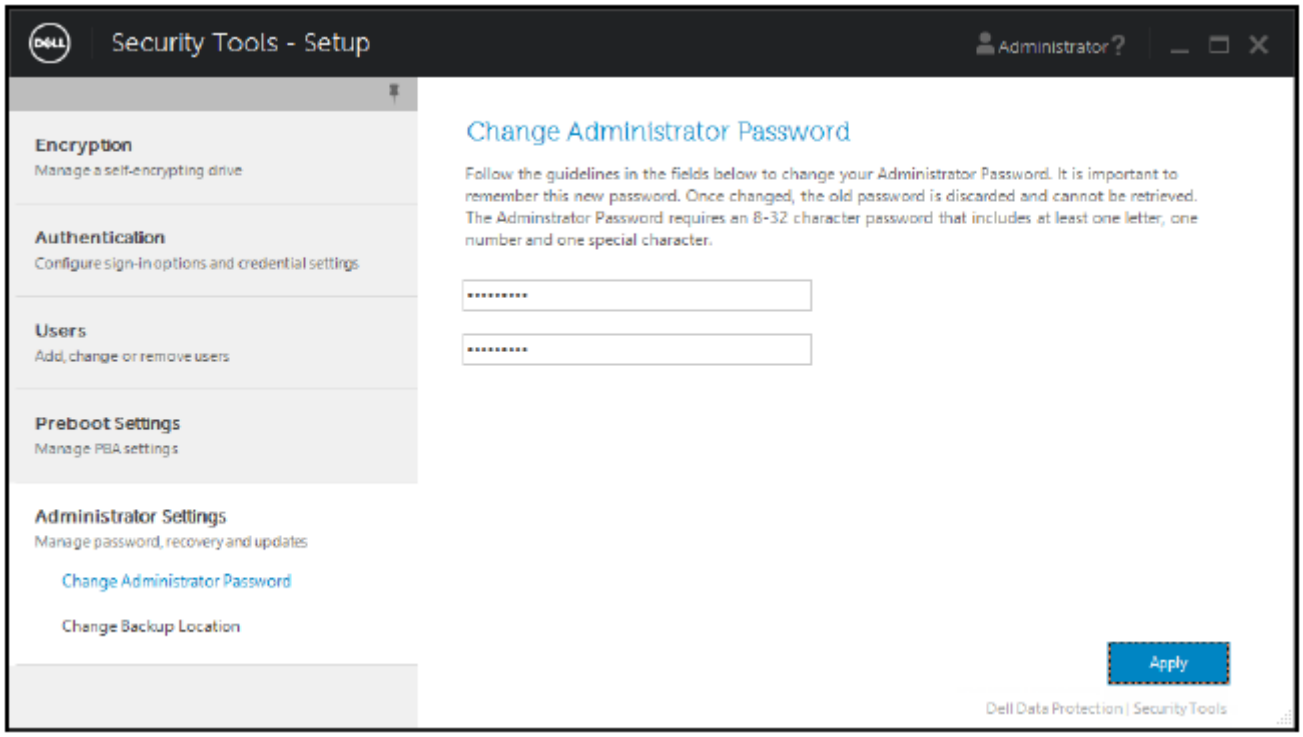
Change the Administrator Password and Backup Location

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.**



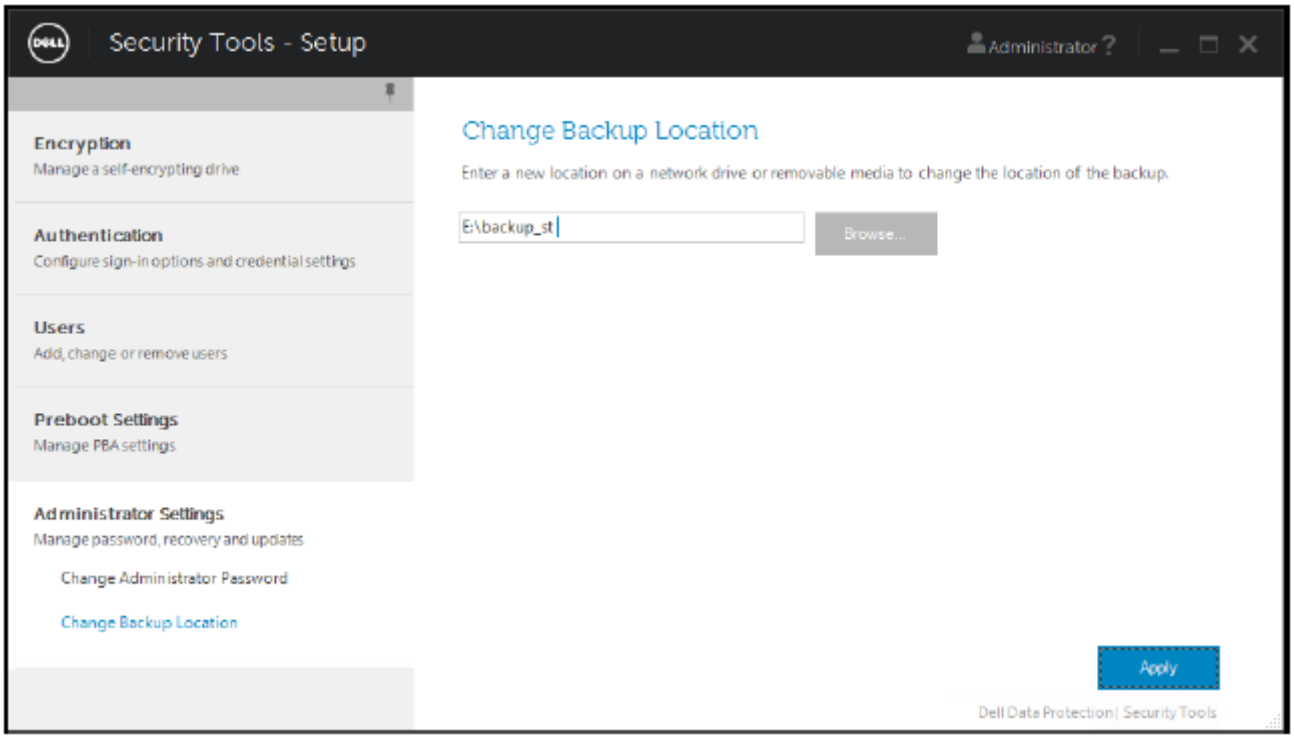
4. Click the **Administrator Settings** tab.
5. In the Change Administrator Password page, if you want to change the password, enter a new password that is between 8-32 characters and includes at least one letter, one number, and one special character.



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.



Настройка шифрования и проверки подлинности перед загрузкой

Функции шифрования и проверки подлинности перед загрузкой (PBA) доступны при условии, что компьютер оборудован самошифрующимся диском (SED). Указанные функции настраиваются во вкладке Encryption («Шифрование»), которая будет доступна только в том случае, если компьютер снабжен самошифрующимся диском (SED). При включении одной из функций – шифрования или проверки подлинности перед загрузкой, вторая из них также будет включена.

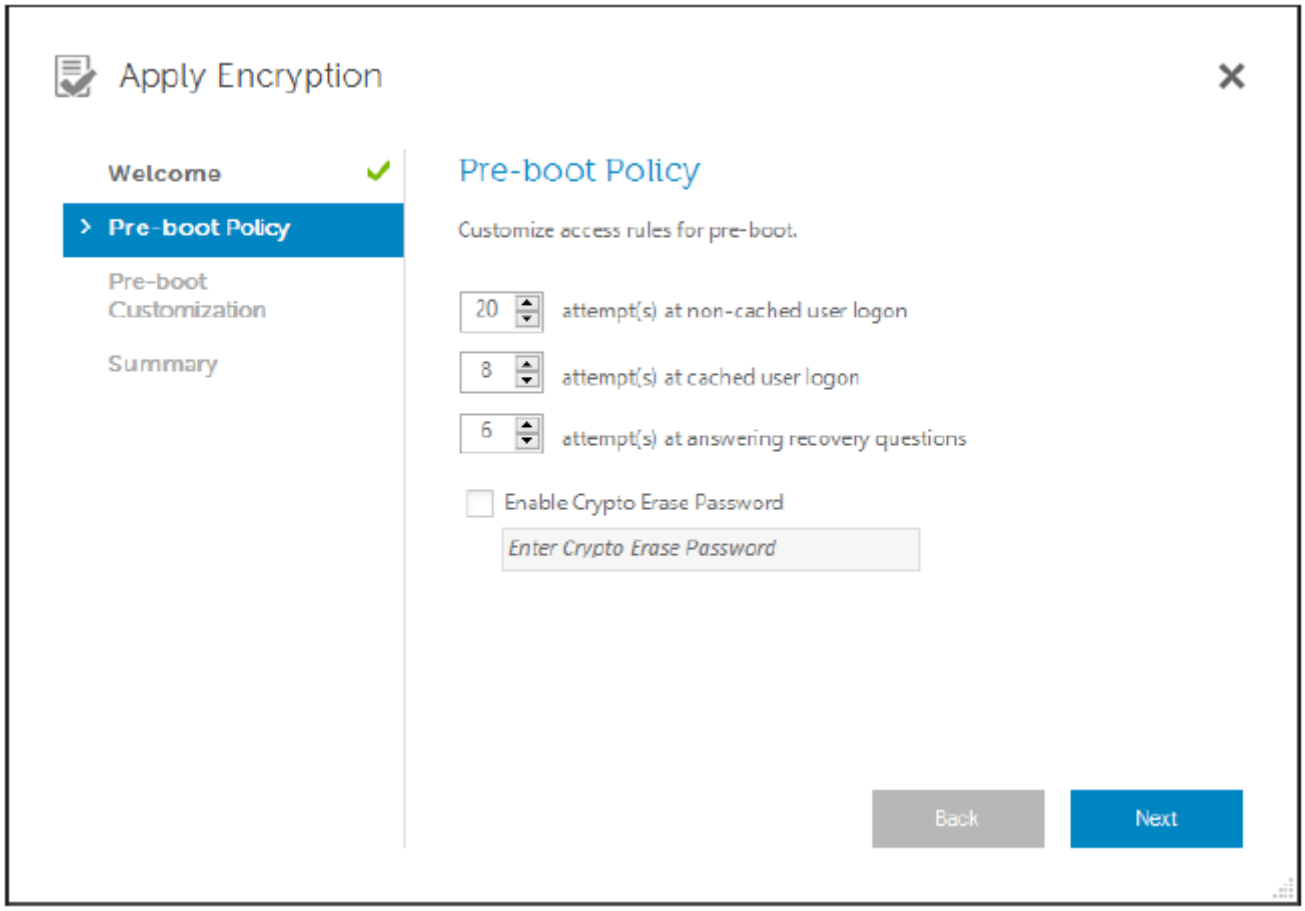
Dell рекомендует зарегистрироваться и включить вопросы для восстановления в качестве опции восстановления перед включением шифрования или функции PBA, чтобы при потере пароля можно было его восстановить. Для получения дополнительной информации смотрите раздел Настройка параметров входа.

Чтобы настроить шифрование и проверку подлинности перед загрузкой:

1. В Консоли безопасности DDP, нажмите на плитку **Administrator Settings** («Параметры администратора»).
2. Убедитесь, что папка для резервной копии на компьютере доступна.

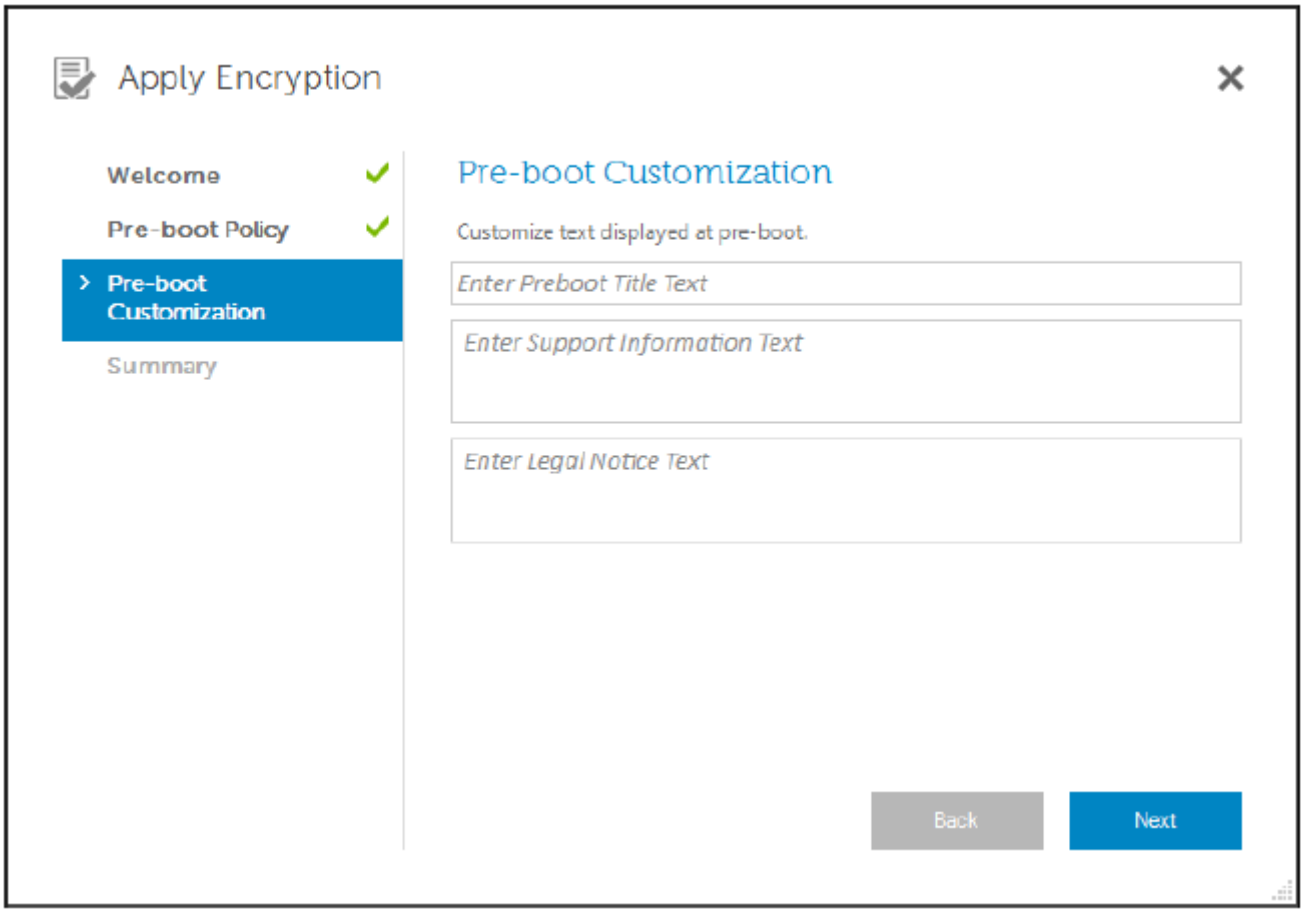
   ПРИМЕЧАНИЕ: Если шифрование включено, выводится сообщение «Backup Location not found» («Папка для резервной копии не найдена»), а папка для резервной копии находится на USB-носителе, то, вероятно, USB-носитель не подключен к компьютеру или подключен к другому разъему, отличному от того, который использовался при сохранении резервной копии. Если выводится указанное сообщение и папка для резервной копии находится на сетевом диске, значит, такой сетевой диск закрыт для доступа с этого компьютера. Если необходимо изменить папку для резервной копии, во вкладке Administrator Settings («Параметры администратора») выберите опцию Change Backup Location («Изменить папку для резервной копии»), чтобы изменить папку, используя текущий разъем для носителя или доступный диск. Через несколько секунд после изменения папки процесс включения шифрования будет продолжен.
3. Нажмите на вкладку **Encryption** («Шифрование»), а затем – на кнопку **Encrypt** («Шифровать»).
4. На странице приветствия нажмите **Next** («Далее»).
5. На странице Preboot Policy («Политика предзагрузки») измените или подтвердите следующие значения, а затем нажмите **Next** («Далее»).

Количество попыток входа некэшированного пользователя	Количество попыток входа, сделанных неизвестным пользователем (т.е. пользователем, который ранее не выполнял вход в данный компьютер, и от которого учетные данные получены не были).
Число попыток входа кэшированного пользователя	Количество попыток входа, сделанных известным пользователем
Число попыток ответа на вопросы для восстановления	Количество попыток ввода пользователем правильного ответа на контрольный вопрос.
Включить пароль с криптографическим удалением	Выберите, чтобы включить
Введите пароль криптографического удаления	Это слово или код, состоящие максимум из 100 символов и используемые в качестве отказоустойчивого механизма безопасности. При вводе этого слова или кода в поле имени пользователя или пароля во время проверки подлинности PBA токены проверки подлинности для всех пользователей будут удалены и самошифрующийся диск заблокирован. После этого, только администратор может принудительно разблокировать устройство. Оставьте это поле пустым, если вы не хотите иметь пароль с криптографическим удалением в экстренной ситуации.



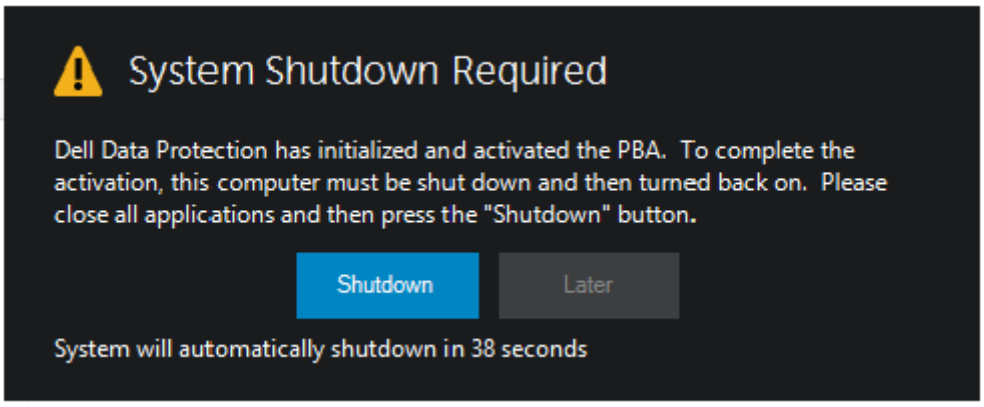
6. На странице Preboot Customization («Настройка текста перед загрузкой») введите текст, который будет выводиться на экране проверки подлинности перед загрузкой (PBA), и нажмите кнопку **Next («Далее»).**

Текст заголовка, отображаемого перед загрузкой	Этот текст будет отображаться в верхней части экрана PBA. Если оставить указанное поле пустым, заголовок отображаться не будет. Текст не переносится, поэтому, если ввести больше 17 символов, он может быть обрезан при выводе.
Текст с информацией о поддержке	Этот текст отображается на экране с информацией о поддержке проверки подлинности перед загрузкой. Dell рекомендует создать это сообщение, чтобы предоставить доступ к точным инструкциям по обращению в справочную службу или к администратору систем безопасности. Если не ввести текст в данном поле, контактная информация о поддержке для данного пользователя будет недоступна. Перенос текста выполняется на уровне слова, но не на уровне символа. Например, если длина одного слова превышает приблизительно 50 символов, оно не будет перенесено, а полоса прокрутки будет отсутствовать, поэтому текст будет обрезан.
Текст с юридической информацией	Этот текст отображается перед тем, как пользователю будет разрешено выполнить вход на устройстве. Например, "Нажав кнопку "OK", вы соглашаетесь соблюдать политику допустимого использования компьютера". Если не ввести текст в данном поле, текст и кнопки OK/Отмена не будут отображаться. Перенос текста выполняется на уровне слова, но не на уровне символа. Например, если длина одного слова превышает приблизительно 50 символов, оно не будет перенесено, а полоса прокрутки будет отсутствовать, поэтому текст будет обрезан.



7. На странице Summary («Сводка») нажмите кнопку **Apply («Применить»).**
8. В ответ на запрос нажмите кнопку **Shutdown** («Завершить работу»).

   Перед началом шифрования требуется завершить работу системы.



9. По завершении работы перезапустите компьютер.

   Теперь проверка подлинности будет выполняться с помощью Security Tools. Пользователи должны выполнить вход на экране проверки подлинности перед загрузкой, используя свои пароли в системе Windows.

Изменение настроек функций Encryption («Шифрование») и Preboot Authentication («Проверка подлинности перед загрузкой»)

После первого включения шифрования и настройки политики проверки подлинности на вкладке Encryption («Шифрование»), будут доступны следующие действия:

- Изменение политики предварительной загрузки или индивидуальных настроек - нажмите на вкладку **Encryption** («Шифрование»), а затем нажмите кнопку **Change** («Изменить»).
- Расшифровать самошифрующийся диск (SED), например, для удаления: нажмите кнопку **Decrypt** («Расшифровать»).

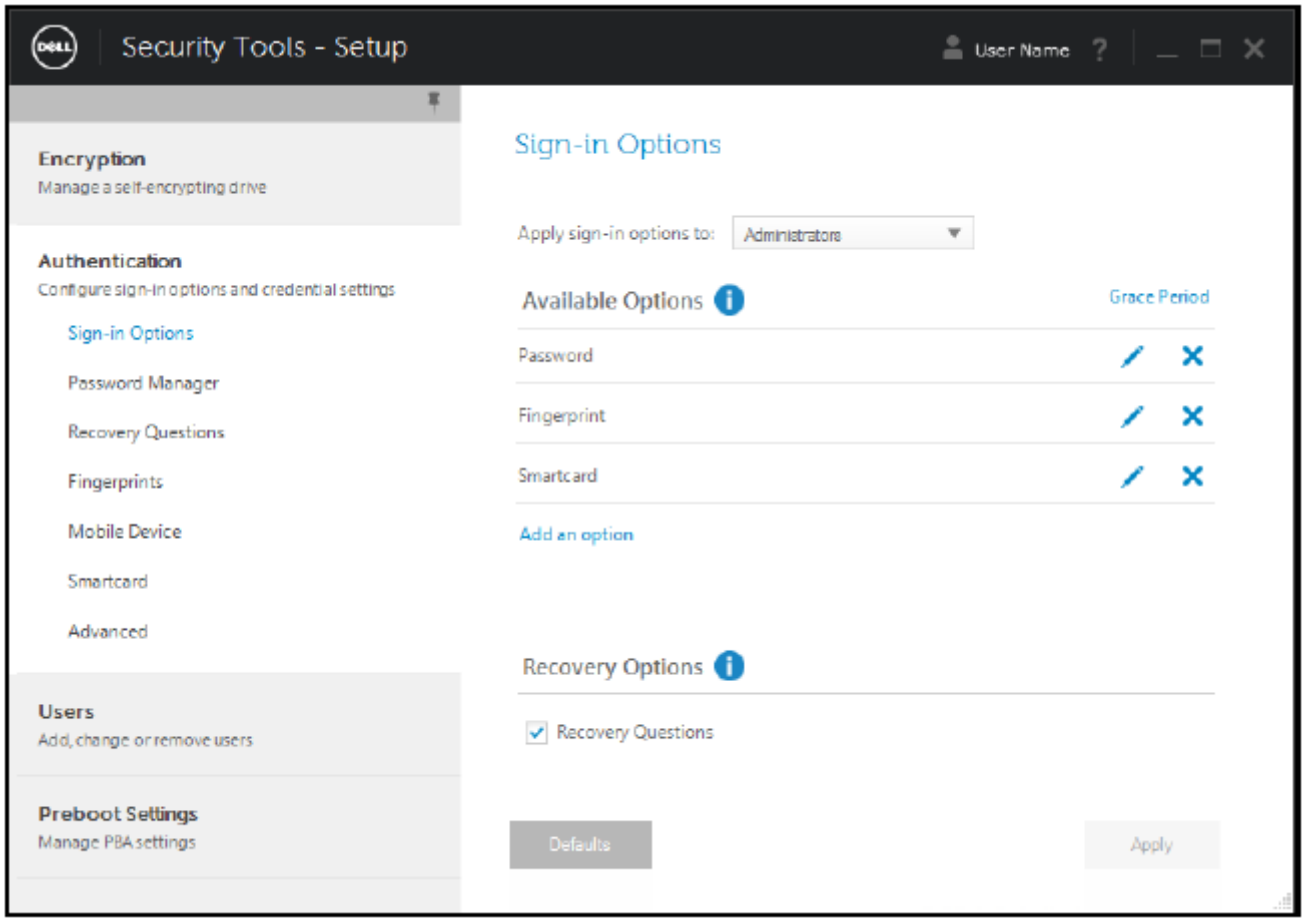
После первого включения шифрования и настройки политики проверки подлинности во вкладке Preboot Settings («Параметры проверки подлинности перед загрузкой») будут доступны следующие действия:

- Изменение политики предварительной загрузки или индивидуальных настроек - выберите вкладку **Preboot Settings** («Настройки предварительной загрузки») и выберите опцию **Preboot Customization** («Индивидуальные настройки предзагрузки») или **Preboot Logon Policies** («Политики входа перед загрузкой»).

Инструкции по удалению см. в разделе Задачи по удалению.

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.

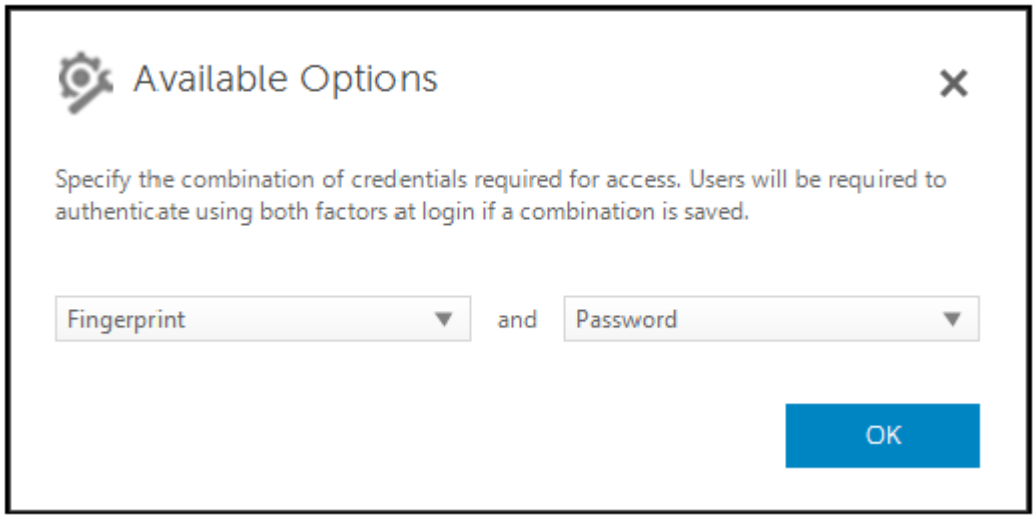
To configure sign-in options:

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**.

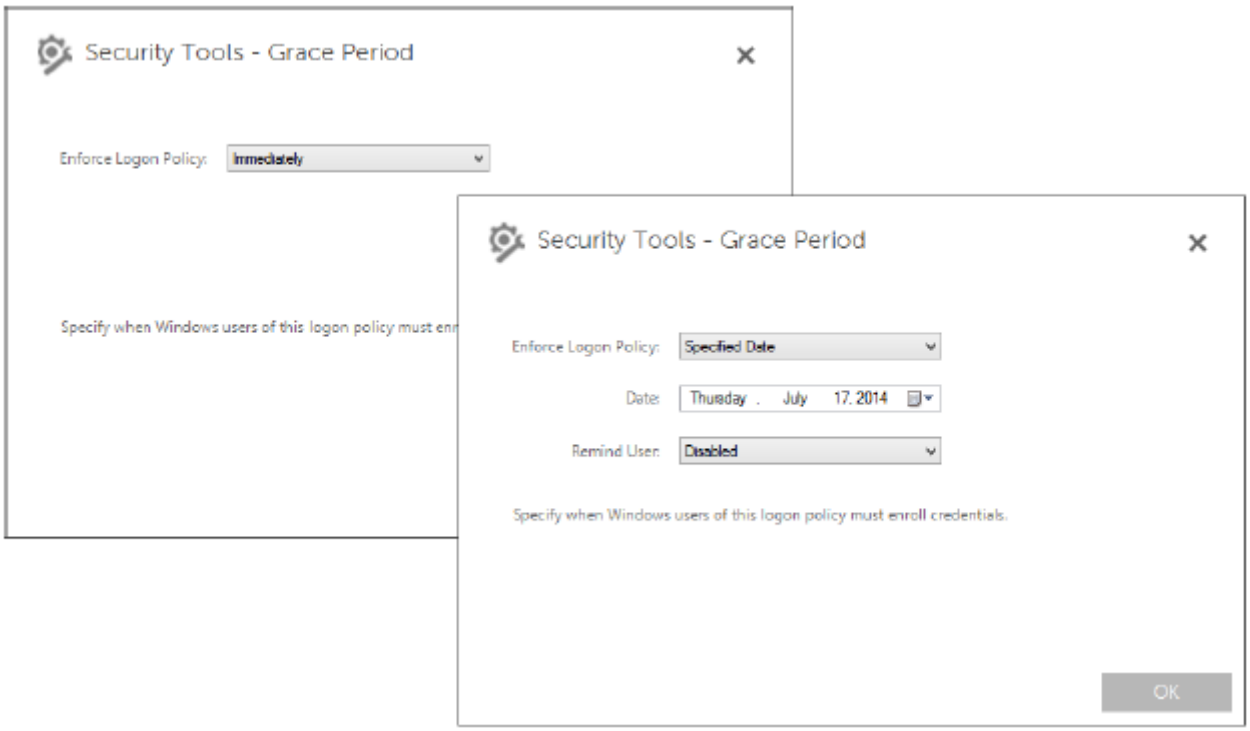
   The Grace Period feature lets you set the date on which a configured Sign-in Option will begin to be enforced. You can configure a Sign-in Option before the date when it will be enforced and set up a length of time to allow users to enroll. By default, the policy is enforced immediately.

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.

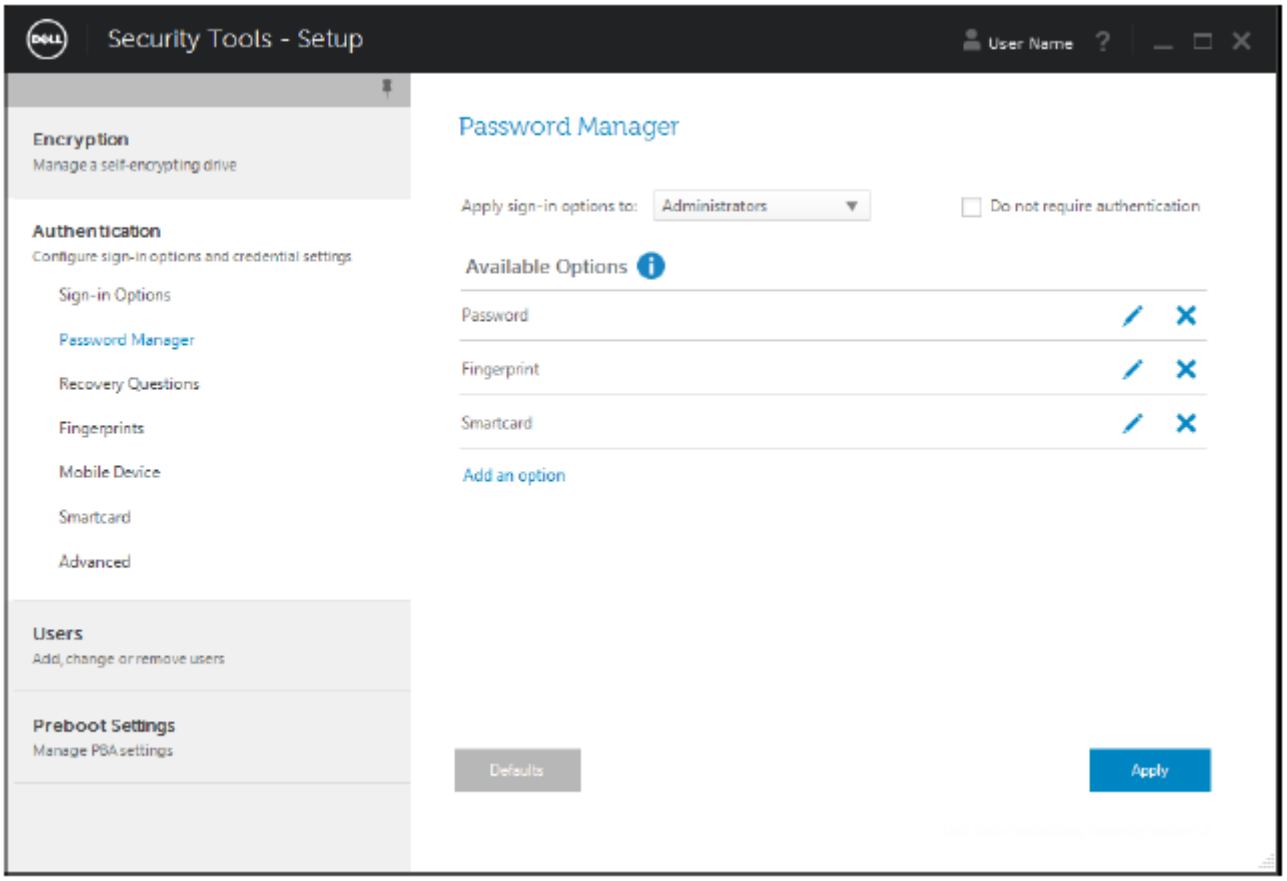
6. To save the settings for the selected role, click **Apply**.

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.

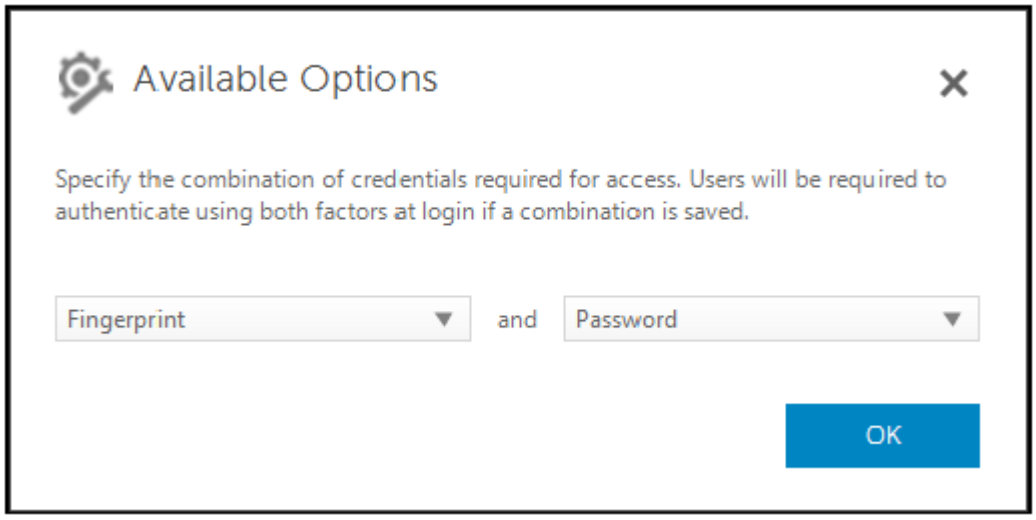


4. Set Available Options for authentication.

   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.**

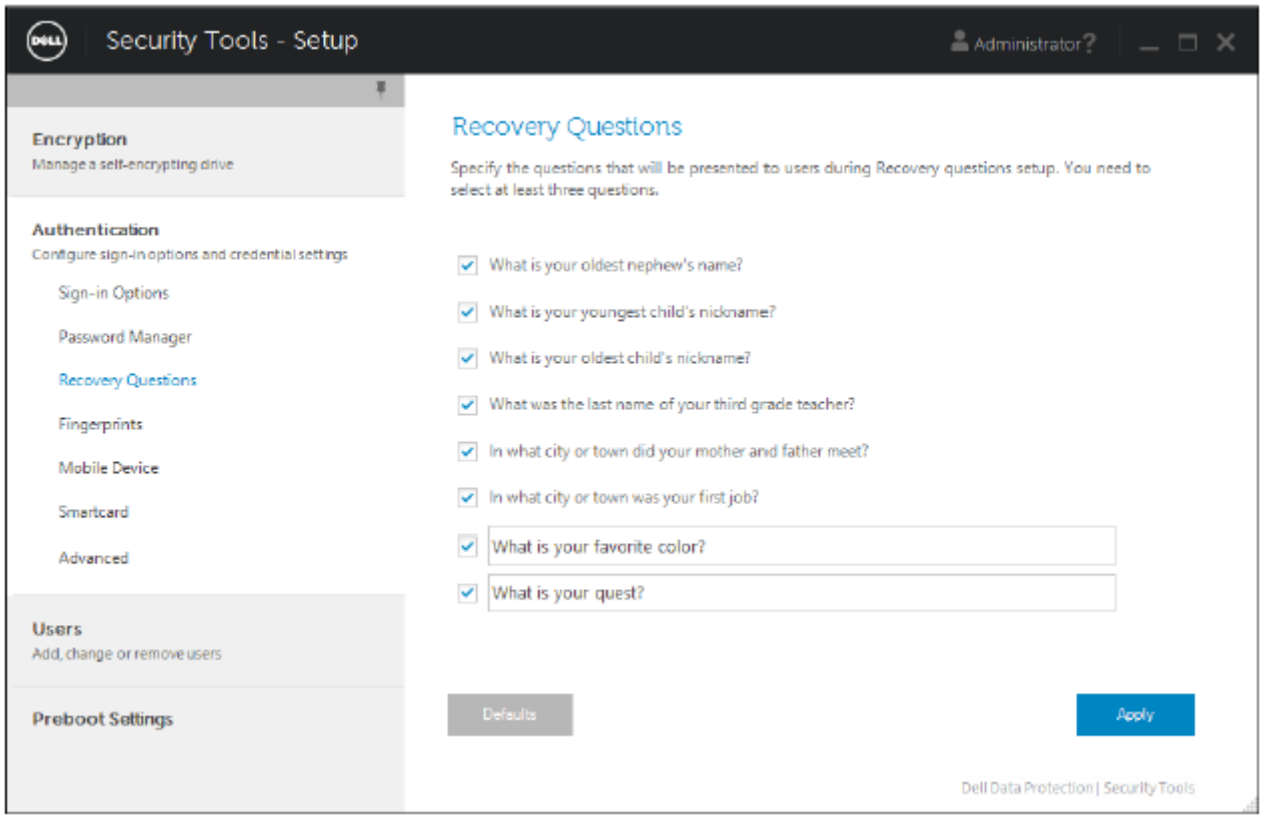
NOTE: Select the Defaults button to restore the settings to their original values.

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:

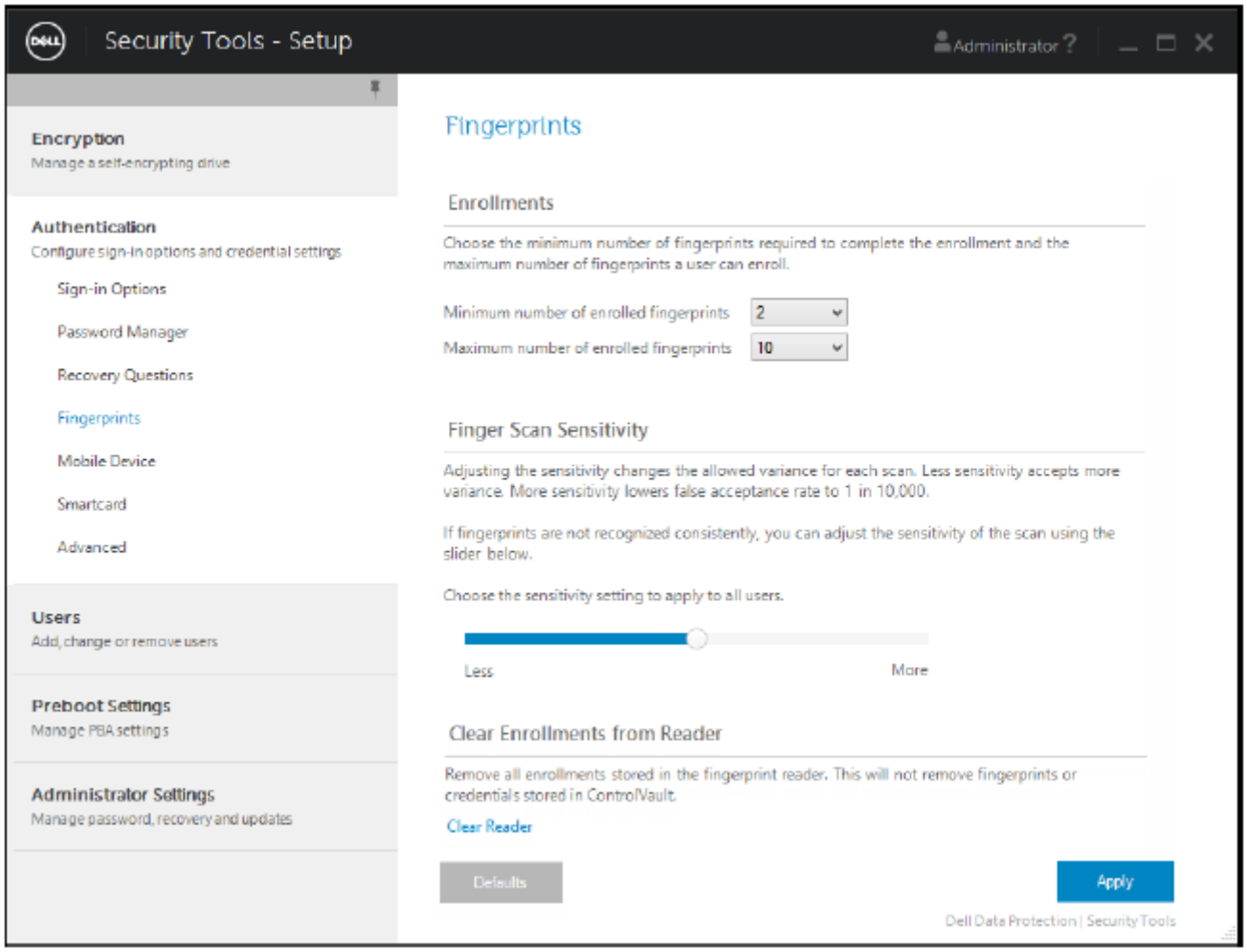
1. In the left pane, under Authentication, select **Recovery Questions**.
2. On the Recovery Questions page, select at least three pre-defined Recovery Questions.
3. Optionally, you can add up to three custom questions to the list that the user selects from.
4. To save the Recovery Questions, click **Apply**.



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.

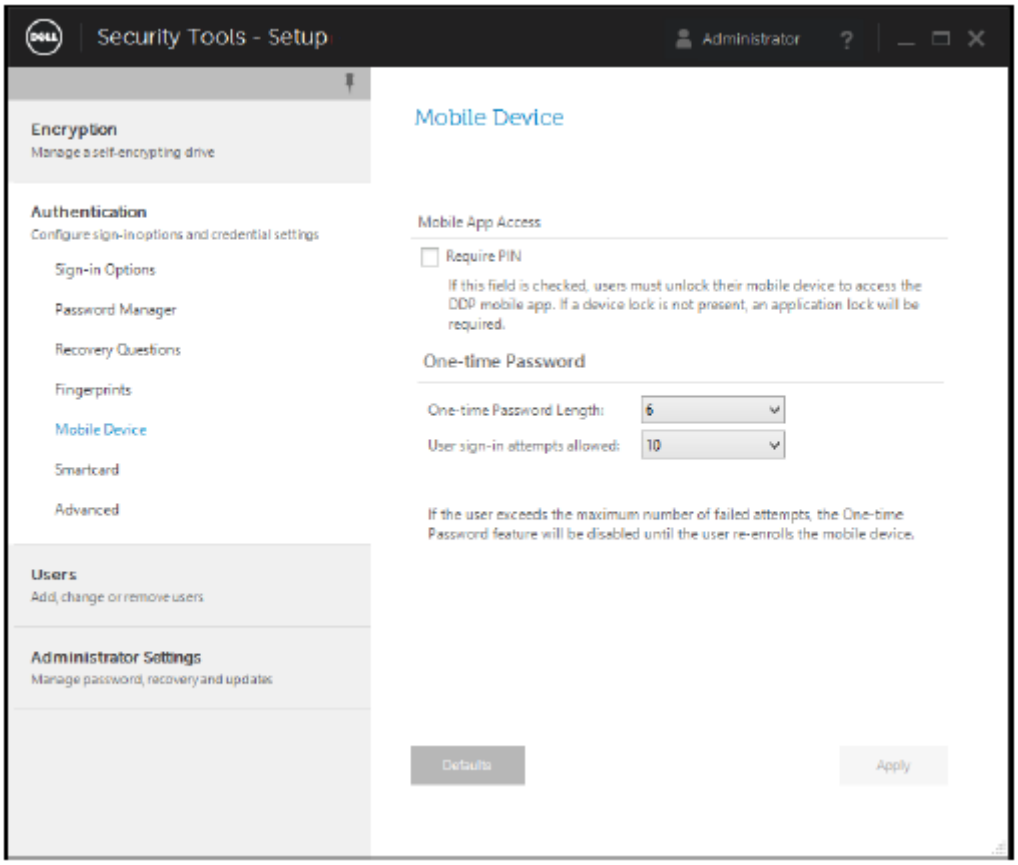
On the Mobile Device page, you can configure settings that further increase the security of the mobile device and One-time Password.

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.

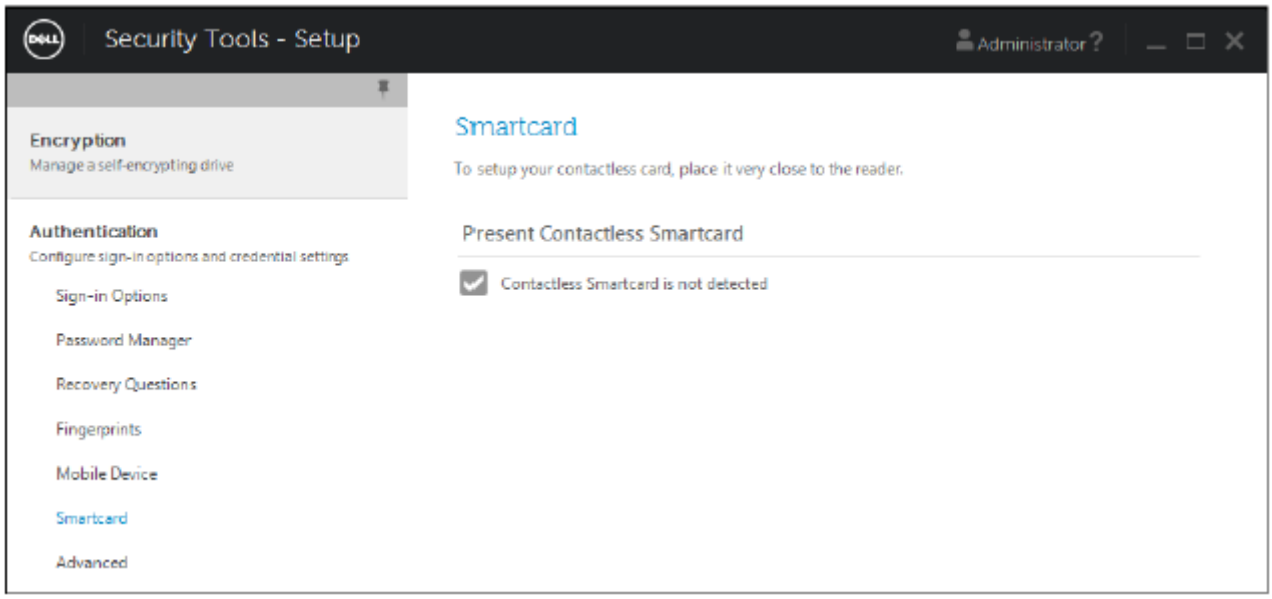
Contacted cards require a smart card reader into which the card is inserted. Contacted cards are only compatible with domain computers. CAC and SIPRNet cards are both contacted cards. Due to the advanced nature of these cards, the user will be required to choose a cert after using inserting his card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

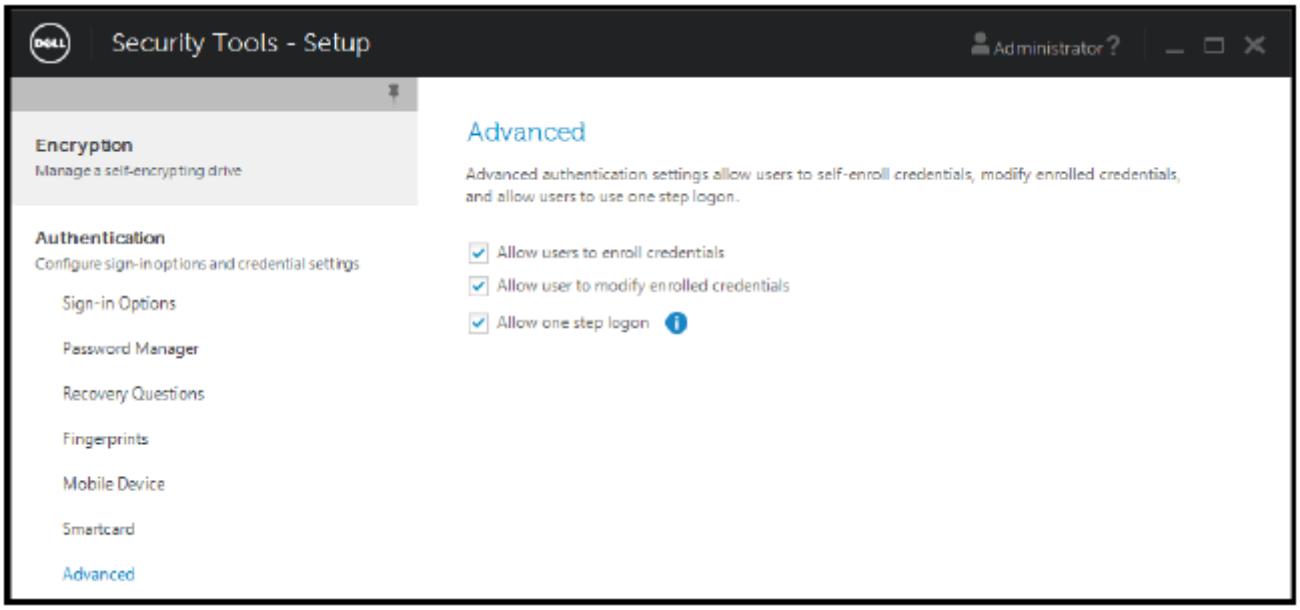
To configure smart card enrollment:

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

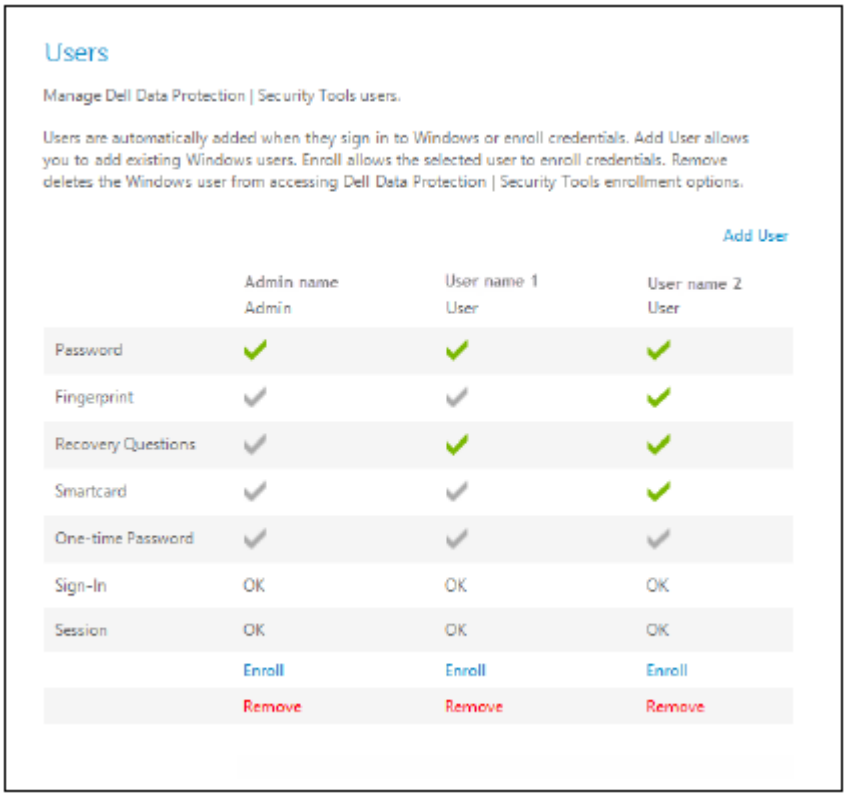
   Set to 0 to Enable. Set to 1 to Disable.

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.

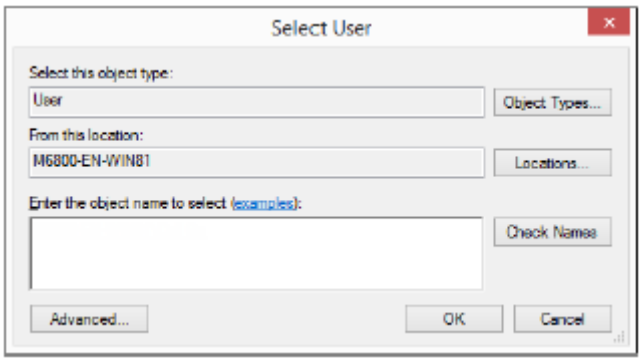
When Sign-in status is OK, all enrollments that the user needs to be able to log on have been completed. When Session status is OK, all enrollments that the user needs to use Password Manager have been completed.

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.

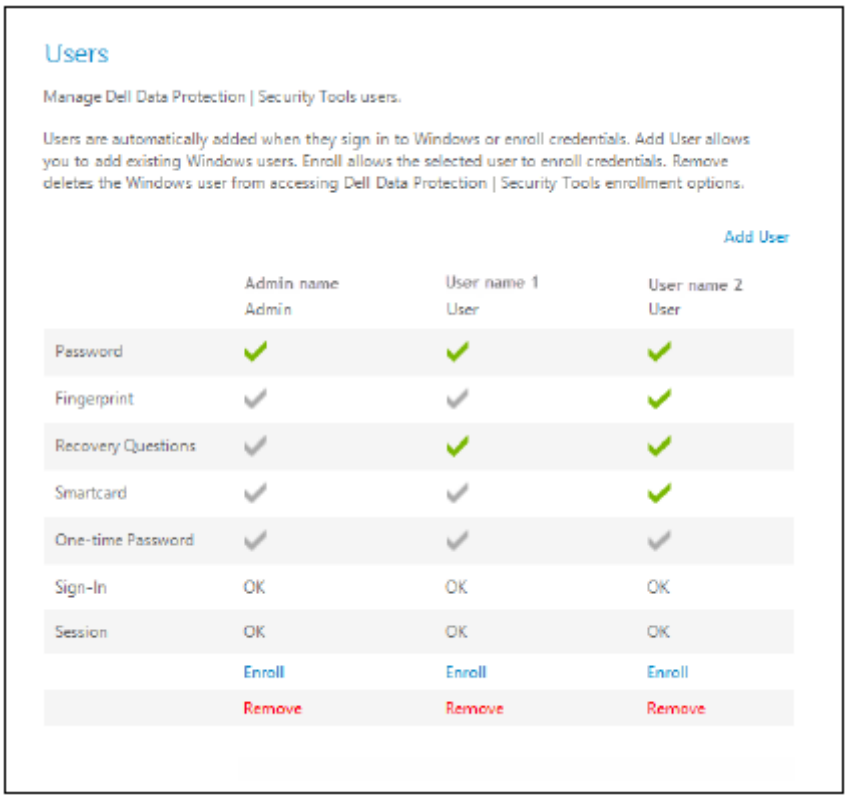
Continue to Enroll or Change User Credentials for instructions.

Enroll or Change User Credentials

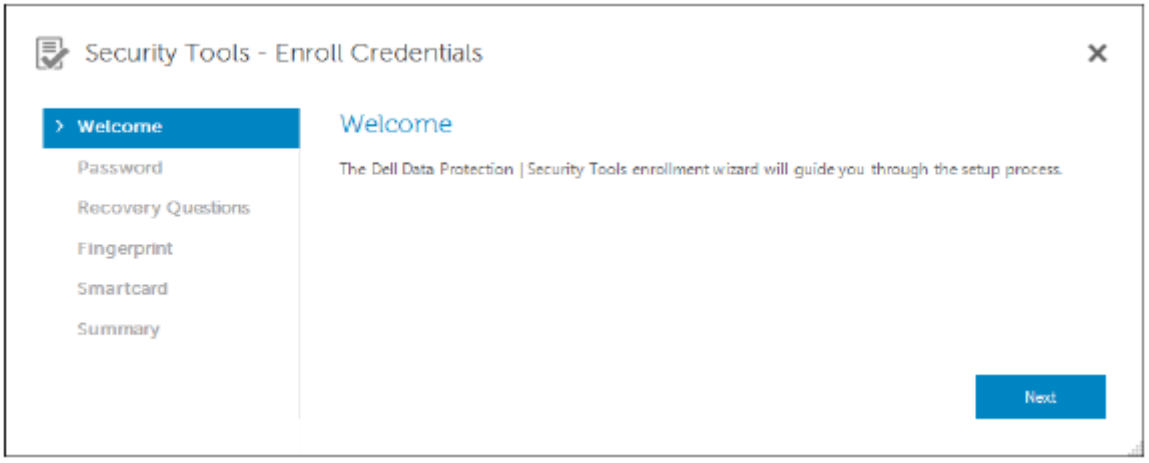
The administrator can enroll or change a user's credentials on behalf of a user, but a few enrollment activities require the user's presence, such as answering recovery questions and scanning the user's fingerprints.

To enroll or change user credentials:

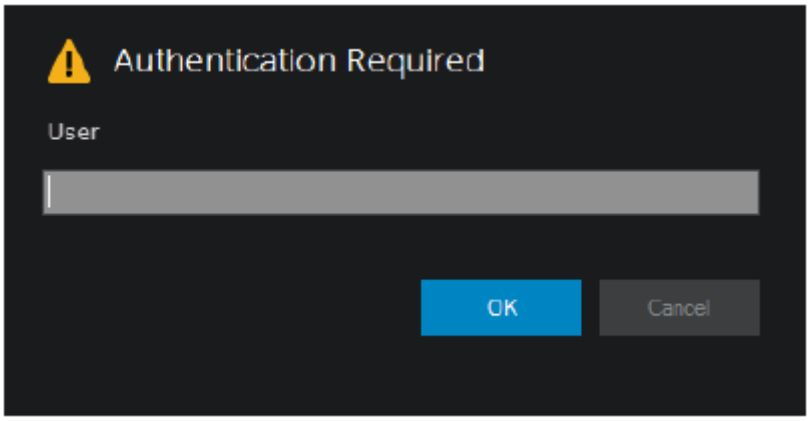
1. In Administrator Settings, click the **Users** tab.
2. On the Users page, click **Enroll**.



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**.

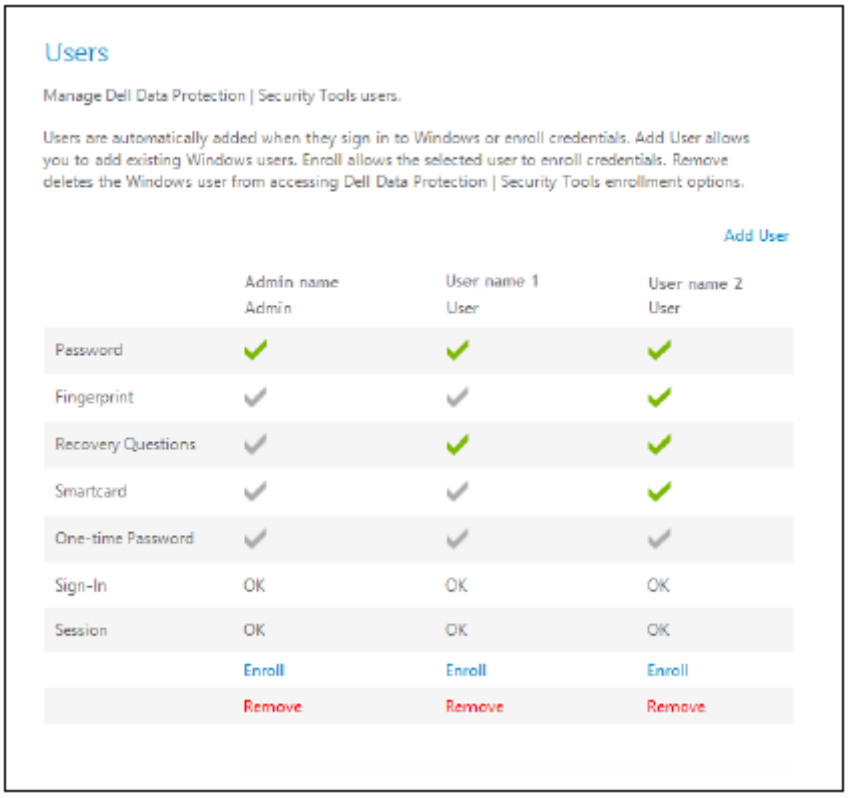
   To return to a credential enrollment page to make a change, click **Back** until you reach the page you want to change.

   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

Задачи по удалению

Чтобы удалить DDP | Security Tools, пользователь должен иметь, как минимум, права **локального администратора**.

Удаление DDP | Security Tools

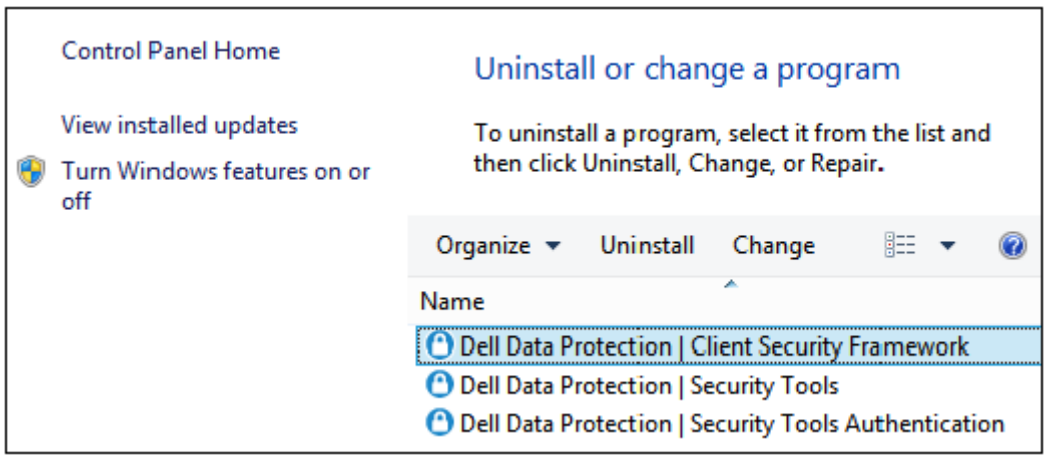
Удаление приложения производится следующим образом:

1. DDP | Client Security Framework
2. DDP | Security Tools - Проверка подлинности
3. DDP | Security Tools

Если компьютер снабжен самошифрующимися дисками, выполните следующие шаги для удаления приложения:

1. Отмените инициализацию самошифрующегося диска:
   a) В разделе Administrator Settings («Параметры администратора») нажмите на вкладку **Encryption** («Шифрование»).
   b) Чтобы отключить шифрование, нажмите кнопку **Decrypt** («Расшифровать»).
   c) После того как самошифрующийся диск будет расшифрован, перезагрузите компьютер.
2. На панели управления Windows зайдите в раздел **Uninstall a Program** («Удаление программы»).

   ПРИМЕЧАНИЕ: Start («Пуск») > Control Panel («Панель управления») > Programs and Features («Программы и компоненты») > Uninstall a Program («Удаление программы»).



3. Удалите **Client Security Framework** и перезапустите компьютер.
4. Используя панель управления Windows, удалите **Security Tools Authentication**.

   На экран будет выведено сообщение с вопросом о необходимости сохранения данных пользователя.

   Если Вы планируете в будущем снова установить пакет Security Tools, нажмите **Yes** («Да»). В противном случае, нажмите **No** («Нет»).

   После завершения процедуры удаления перезагрузите компьютер.

5. Используя панель управления Windows, удалите**Security Tools**.

   На экран будет выведено сообщение с вопросом о том, планируете ли Вы полностью удалить приложение и компоненты.

   Нажмите кнопку **Yes** («Да»).

   На экране появится диалоговое окно *Uninstallation Complete* («Удаление завершено»).
6. Установите флажок в поле **Yes, I want to restart my computer now** («Да, перезагрузить компьютер сейчас»), а затем нажмите кнопку **Finish** («Готово»).
7. Компьютер будет перезагружен, и процесс удаления будет завершен.

6

Восстановление

В случае если учетные данные пользователя утрачены или срок их действия истек, доступны следующие опции восстановления:

- **Одноразовый пароль (OTP):** Пользователь генерирует одноразовый пароль при помощи мобильного приложения Security Tools Mobile, установленного на зарегистрированном мобильном устройстве, и вводит одноразовый пароль на экране входа в Windows для восстановления доступа. Эта опция доступна только в случае, если пользователь зарегистрировал мобильное устройство на компьютере при помощи программы Security Tools. Чтобы использовать одноразовый пароль для восстановления, пользователь не должен применять его для входа в компьютер.

  ПРИМЕЧАНИЕ: Для использования функции одноразового пароля необходимо наличие включенного собственного TPM. Следуйте инструкциям в разделе Очистка собственности и активация доверенного платформенного модуля (TPM). Одноразовый пароль может использоваться для проверки подлинности или восстановления доступа, но не для одновременного выполнения указанных целей. Для получения дополнительной информации см. раздел Настройка параметров входа.

- **Контрольные вопросы:** Пользователь должен правильно ответить на набор персонализированных контрольных вопросов, чтобы восстановить доступ к компьютеру. Эта опция доступна только в случае, если администратор настроил и включил вопросы для восстановления, а пользователь зарегистрировал вопросы для восстановления в качестве опции для восстановления доступа. Эта опция используется для восстановления доступа к компьютеру путем проверки подлинности перед загрузкой или с помощью экрана входа в Windows.

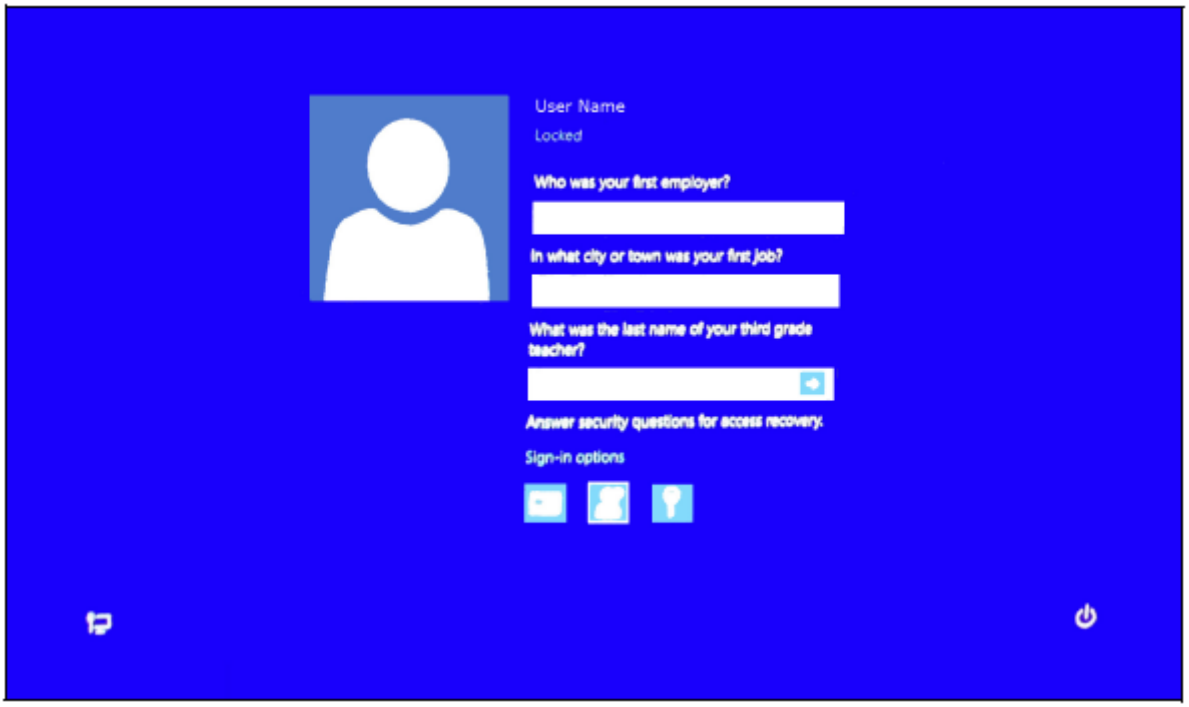
Оба способа восстановления требуют подготовки к восстановлению либо путем регистрации вопросов восстановления, либо путем регистрации мобильного устройства при помощи программы Security Tools на компьютере.

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**.

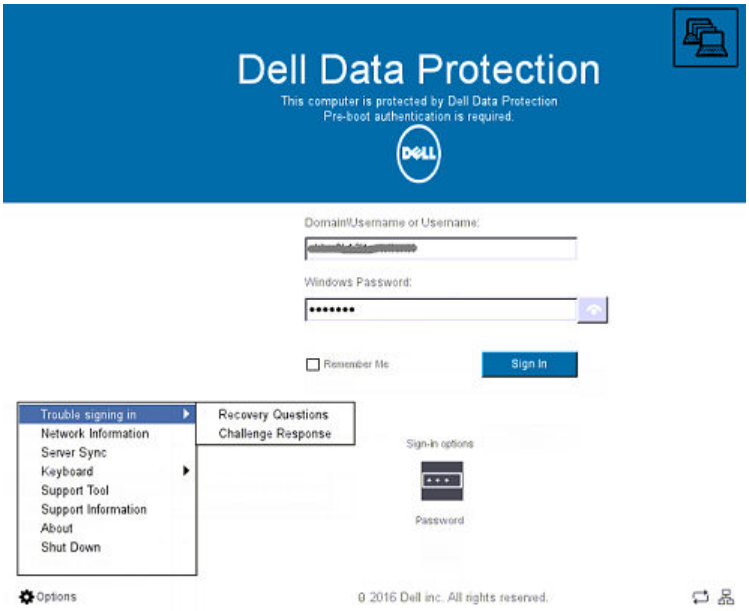
   Upon successful entry of the answers to the questions, you enter Access Recovery mode. What happens next depends upon the credential that failed.

   - 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.

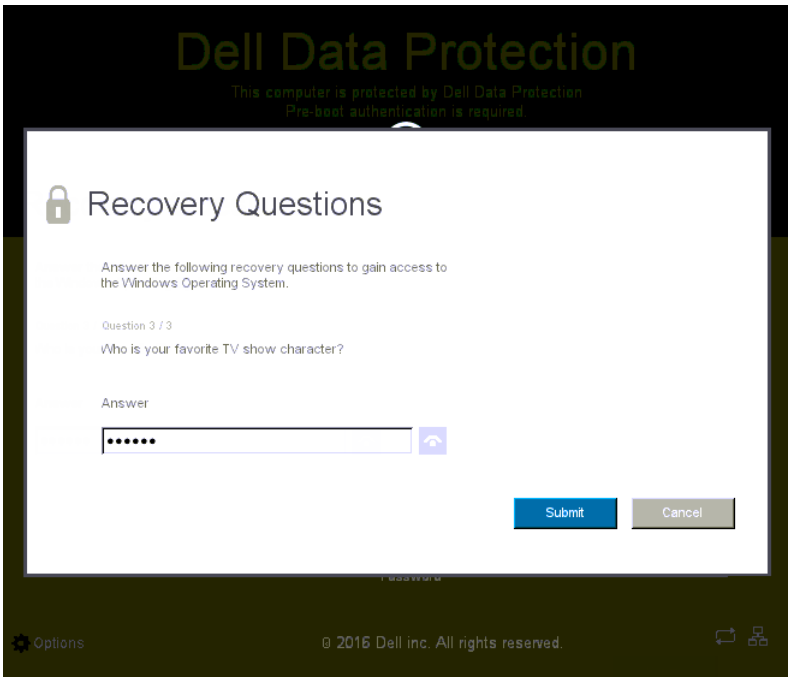
Self-Recovery, PBA Recovery Questions

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.



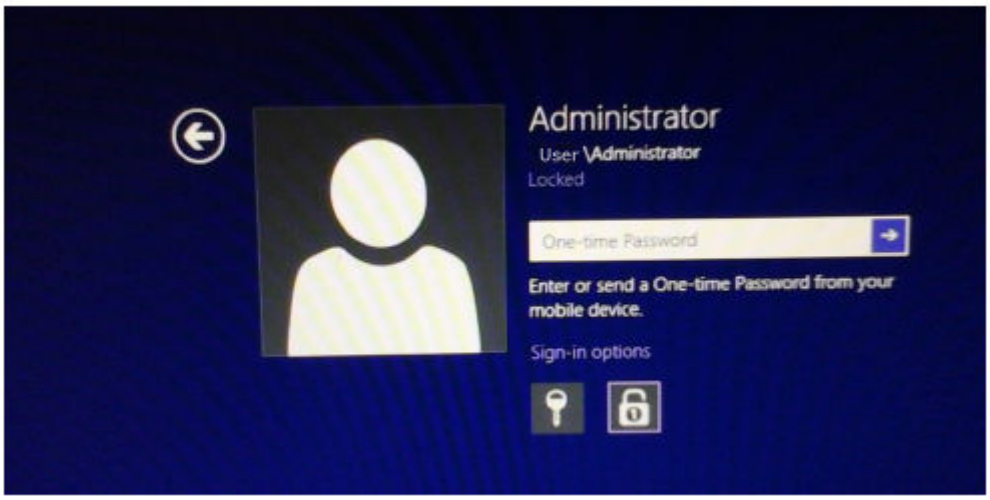
Самовосстановление, одноразовый пароль

Эта процедура описывает, как использовать функцию одноразового пароля (OTP) для восстановления доступа к компьютеру, в случае, например, если пароль для входа в Windows утрачен, срок его действия истек или превышено максимальное количество попыток входа. Функция одноразового пароля (OTP) доступна только в том случае, если пользователь зарегистрировал мобильное устройство, и только при условии, если функция одноразового пароля не использовалась в предыдущий раз для входа в Windows.

ПРИМЕЧАНИЕ: Для использования функции одноразового пароля необходимо наличие включенного собственного TPM. Функция одноразового пароля может использоваться либо для проверки подлинности Windows, либо для восстановления доступа, но не для одновременного выполнения обеих целей. Администратор может установить политику таким образом, чтобы разрешить пользователю применять OTP либо для восстановления доступа, либо для проверки подлинности, или отключить эту функцию.

Чтобы использовать функцию одноразового пароля для восстановления доступа к компьютеру:

1. На экране входа в Windows выберите ярлык OTP .



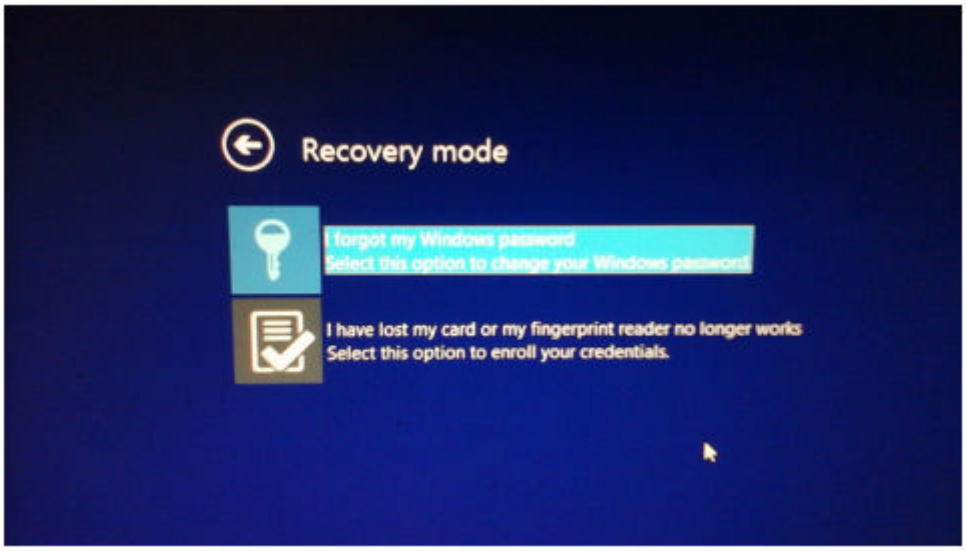
2. На мобильном устройстве запустите приложение Security Tools Mobile и введите пароль.
3. Выберите компьютер, к которому следует получить доступ.

   Если имя компьютера не отображается на мобильном устройстве, возможно, имеет место одна из указанных ниже причин:

   - Мобильное устройство не было зарегистрировано или не было соединено с компьютером, к которому Вы пытаетесь получить доступ.
   - При наличии более одной учетной записи Windows приложение DDP | Security Tools либо не установлено на компьютере, к которому Вы пытаетесь получить доступ, либо Вы пытаетесь войти с использованием другой учетной записи пользователя, отличной от той, которая использовалась для соединения компьютера с мобильным устройством.
4. Нажмите **One-time Password («Одноразовый пароль»).**

   На мобильном устройстве отобразится пароль.

   ПРИМЕЧАНИЕ: Если необходимо, нажмите на значок Refresh («Обновить») , чтобы получить новый код. После двух последовательных обновлений одноразового пароля потребуется дождаться окончания 30-секундного интервала, перед тем как будет сгенерирован еще один одноразовый пароль. Компьютер и мобильное устройство должны быть синхронизированы, для одновременного распознавания одного и того же пароля. Попытка быстрой последовательной генерации паролей может вызвать нарушение синхронизации компьютера и мобильного устройства и отказ функции одноразового пароля. При наличии такой проблемы подождите в течение тридцати секунд, пока оба устройства вновь не синхронизируются, а затем повторите попытку.
5. На компьютере, на экране ввода пароля Windows, введите пароль, который отображается на мобильном устройстве, и нажмите кнопку **Enter** («Ввод»).
6. На компьютере, на экране восстановления, выберите **I forgot my Windows password («Я забыл пароль для входа в Windows»)** и следуйте экранным подсказкам, чтобы переустановить свой пароль.


Recovery mode
I forgot my Windows password
Select this option to change your Windows password
I have lost my card or my fingerprint reader no longer works
Select this option to enroll your credentials.

7

Глоссарий

Отмена инициализации: удаляет базу данных PBA и отключает PBA. Изменения, внесенные в систему при отмене инициализации, вступают в силу после завершения работы компьютера.

Одноразовые пароли (OTP). Одноразовый пароль — это пароль, который может быть использован только один раз и который действует в течение ограниченного периода времени. Для использования одноразового пароля необходимо наличие включенного собственного TPM. Для активации функции OTP необходимо, чтобы мобильное устройство было подключено к компьютеру с помощью консоли безопасности и приложения Security Tools Mobile. Приложение Security Tools Mobile генерирует на мобильном устройстве пароль, который используется для входа в компьютер на экране входа в Windows. Согласно установленным требованиям функция OTP может быть использована для восстановления доступа к компьютеру, в случае если срок действия пароля истек или если пользователь забыл пароль, при условии что функция OTP не использовалась для входа в компьютер. Функция OTP может быть использована для проверки подлинности или для восстановления доступа, но не для одновременного выполнения указанных задач. Уровень безопасности одноразовых паролей является более высоким, чем уровень безопасности некоторых других методов проверки подлинности, поскольку сгенерированный пароль можно использовать только один раз, и он имеет короткий срок действия.

Предзагрузочная проверка подлинности (Preboot Authentication, PBA) служит в качестве расширения BIOS или встроенного загрузочного ПО и гарантирует наличие безопасной и защищенной от несанкционированного доступа среды, внешней по отношению к операционной системе, которая обеспечивает надежную проверку подлинности. PBA предотвращает чтение любых данных с диска, в том числе данных операционной системы, пока пользователь не подтвердит наличие корректных учетных данных.

Единый вход (Single Sign-On, SSO) - Процедура SSO упрощает процесс входа в систему в случае, если для предзагрузки и для входа в Windows разрешено использование многофакторной проверки подлинности. В этом случае проверка подлинности требуется лишь перед загрузкой, а вход пользователей в Windows выполняется автоматически. Если единый вход не включен, может потребоваться неоднократная проверка подлинности.

Доверенный платформенный модуль (TPM). TPM — это чип с тремя основными функциями: безопасное хранение, измерение и удостоверение подлинности. Клиент шифрования использует TPM для обеспечения безопасного хранения. TPM также может предоставлять зашифрованные контейнеры для хранилища программного обеспечения. TPM также необходим для использования функции одноразового пароля.