Dell Data Protection | Security Tools

Руководство по установке

Версия 1.9

2016-01

Содержание

1

Введение

Dell Data Protection | Security Tools (DDP|ST) обеспечивает безопасность и защиту в процессе идентификации администраторов и пользователей компьютеров Dell. Решение DDP|ST предустанавливается на все модели компьютеров Dell Latitude, Optiplex и Precision и некоторые модели ноутбуков Dell XPS. Если необходимо *переустановить* DDP|ST, следуйте инструкциям, приведенным в данном руководстве. Дополнительную поддержку можно получить по адресу www.dell.com/support > Endpoint Security Solutions.

Обзор

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

DDP|ST 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 Одноразовые пароли (OTP).

Перед тем как сделать средства безопасности доступными для конечных пользователей, администраторы могут настроить параметры средств безопасности, используя инструмент настройки параметров администратора консоли DDP Security Console, например, чтобы активировать проверку подлинности перед загрузкой (PBA) и политики проверки подлинности. Однако настройки по умолчанию позволяют администраторам и пользователям начать использовать средства безопасности сразу же после их установки и активации.

DDP Security Console

Консоль DDP Security Console представляет собой интерфейс средств безопасности, благодаря которому пользователи могут зарегистрироваться и управлять своими учетными данными, настроить вопросы для самостоятельного восстановления доступа в соответствии с требованиями политики, которая устанавливается 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 Administrator Settings (Параметры администратора) используется для настройки средств безопасности для всех пользователей компьютера и позволяет администратору настраивать политики проверки подлинности, управлять пользователями и определять, какие именно учетные данные будут использоваться для входа в систему Windows.

Используя инструмент Administrator Settings (Параметры администратора), администратор может включить шифрование и проверку подлинности перед загрузкой (PBA), а также настроить политики PBA и изменить текст, выводимый на экране PBA.

См. далее Требования.

2

Требования

- Решение DDP|ST 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|ST, следует еще раз убедиться, что ваш компьютер соответствует этим требованиям. Для получения дополнительной информации см. веб-сайт www.dell.com/support > Endpoint Security Solutions.
- 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|ST 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|ST на 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.
- **Intel RAID, встроенный в ноутбуки,** поддерживается проверкой подлинности перед загрузкой при использовании DDP|Hardware Crypto Accelerator (аппаратного криптографического ускорителя). RAID не поддерживается на системах с самошифрующимися дисками. Для получения дополнительной информации см.Драйверы.

Драйверы

- Поддерживаемые самошифрующиеся диски, соответствующие спецификации Opal, требуют установки обновленных драйверов Rapid Storage Technology, которые находятся 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.

ВАЖНО. **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 к оборудованию клиента

- Для работы средств безопасности требуется полная версия Microsoft .Net Framework 4.0 (или более поздней версии). На всех компьютерах, поставляемых Dell, уже установлена полная версия Microsoft .Net Framework 4.0. Однако если вы устанавливаете средства безопасности на оборудование Dell или обновляете средства безопасности на устаревшем оборудовании Dell, следует проверить установленную версию Microsoft .Net и обновите ее перед установкой средств безопасности. Это поможет предотвратить возникновение неполадок при установке или обновлении. Чтобы установить полную версию Microsoft .Net Framework 4.0, перейдите по ссылке http://www.microsoft.com/en-us/download/details.aspx?id=17851.

  Чтобы узнать версию установленной среды .Net на компьютере, на который планируется установить средства безопасности, выполните следующие указания. 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. Чтобы загрузить необходимые драйвера и микропрограммы для компьютеров Dell, перейдите на веб-сайт 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)

Программное обеспечение

Операционные системы Windows

В приведенной ниже таблице перечислено поддерживаемое программное обеспечение.

Операционные системы Windows (32-разрядные и 64-разрядные)
• Microsoft Windows 7 с пакетом обновления 0-1 (SP0-SP1) - Корпоративная - Профессиональная **ПРИМЕЧАНИЕ.** Унаследованный режим загрузки поддерживается системой Windows 7. Интерфейс UEFI не поддерживается системой Windows 7.
• Microsoft Windows 8 - Корпоративная - Профессиональная - Windows 8 (Consumer) **ПРИМЕЧАНИЕ.** Windows 8 поддерживает режим UEFI при использовании с Самошифрующиеся диски, соответствующие спецификации Opal и Модели компьютеров Dell - с поддержкой UEFI.

Операционные системы Windows (32-разрядные и 64-разрядные)
• Microsoft Windows 8.1 - 8.1 Update 1 - Enterprise Edition - Pro Edition
ПРИМЕЧАНИЕ. Windows 8.1 поддерживает режим UEFI Mode при использовании с Самошифрующиеся диски, соответствующие спецификации Opal и Модели компьютеров Dell - с поддержкой UEFI.
• Microsoft Windows 10 - Education Edition - Enterprise Edition - Pro Edition
ПРИМЕЧАНИЕ. Windows 10 поддерживает режим UEFI при использовании с Самошифрующиеся диски, соответствующие спецификации Opal и Модели компьютеров Dell - с поддержкой UEFI.

Операционные системы мобильного устройства

Функцию одноразового пароля (Средства безопасности) поддерживают следующие операционные системы.

Операционные системы Android
• 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
Операционные системы iOS
• iOS 7.x
• iOS 8.x
Операционные системы Windows Phone
• Windows Phone 8.1
• Windows 10 Mobile

Аппаратное обеспечение

Проверка подлинности

В приведенной ниже таблице перечислено поддерживаемое оборудование для проверки подлинности.

Устройства для считывания отпечатков пальцев
• Сканер Validity VFS495 в режиме Secure Mode
• Линейный сканер Broadcom Control Vault
• Сканер UPEK TCS1 FIPS 201 в защищенном режиме 1.6.3.379
• Сканеры Authentec Eikon и Eikon To Go USB

ПРИМЕЧАНИЕ. При использовании внешнего устройства для считывания отпечатков пальцев, необходимо загрузить и установить последние драйвера, необходимые для вашего устройства для считывания.

Бесконтактные карты
• Бесконтактные карты, используемые со считывателями бесконтактных карт, встроенными в определенные модели мобильных ПК Dell
Смарт-карты
• Смарт-карты PKCS #11, использующие клиент ActivIdentity
ПРИМЕЧАНИЕ. Клиент ActivIdentity не предустанавливается, его необходимо устанавливать отдельно.
• Карты общего доступа (CAC)
ПРИМЕЧАНИЕ. При использовании карт общего доступа с несколькими сертификатами в момент входа в систему пользователь самостоятельно выбирает нужный сертификат из списка.
• Карты CSP
• Карты SIPRNet класса B

В приведенной ниже таблице указаны поддерживаемые модели компьютеров Dell с картами SIPR Net.

Модели компьютеров Dell – класса B/SIPR с поддержкой сетевой карты
• Latitude E6440
• Latitude E6540
• Precision M2800
• Precision M4800
• Precision M6800
• Latitude 14 Rugged Extreme
• Latitude 12 Rugged Extreme
• Latitude 14 Rugged

Модели компьютеров Dell - с поддержкой UEFI

Функции проверки подлинности поддерживают режим UEFI на некоторых компьютерах Dell под управлением ОС Microsoft Windows 8, Microsoft Windows 8.1 и Microsoft Windows 10 с квалифицированными Самошифрующиеся диски, соответствующие спецификации Opal. Другие компьютеры с операционной системой Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 8.1 и Microsoft Windows 10 поддерживают унаследованный режим загрузки.

В приведенной ниже таблице указаны поддерживаемые модели компьютеров Dell с интерфейсом UEFI.

Модели компьютеров Dell - с поддержкой UEFI
• Latitude E7240
• Latitude E7250
• Latitude E7350
• Latitude E7440
• Latitude E7450
• Precision M4800
• Precision M6800
• Precision T7810
• OptiPlex 7020
• OptiPlex 9020 Micro
• Venue Pro 11 (модель 7139)

ПРИМЕЧАНИЕ. На компьютерах, поддерживающих интерфейс UEFI, после того, как вы нажмете **Restart** («Перезагрузка») в главном меню, компьютер перезагрузится, а затем отобразит один из двух возможных экранов входа. Отображаемый экран входа определяется различиями в архитектуре компьютерной платформы. Часть компьютеров отображает экран входа с проверкой подлинности перед загрузкой, а остальные модели отображают экран входа Windows. Оба экрана входа одинаково безопасны.

ПРИМЕЧАНИЕ. Убедитесь, что Legacy Option ROM (Наследуемые варианты загрузки) отключены в BIOS.

Чтобы отключить Legacy Option ROM (Наследуемый вариант загрузки).

1. Перезагрузите компьютер.
2. Когда он начнет перезагружаться, нажимайте **F12** до тех пор, пока на экране не появятся настройки загрузки компьютера UEFI.
3. Нажимая стрелку вниз, выберите параметр **BIOS Settings** («Настройки BIOS»), и нажмите **Enter** («Ввод»).
4. Выберите **Settings** («Настройки») **> General** («Общие») **> Advanced Boot Options** («Дополнительные настройки загрузки»).
5. Уберите отметку **Enable Legacy Option ROMs** («Разрешить наследуемую загрузку») и нажмите **Apply** («Применить»).

Самошифрующиеся диски, соответствующие спецификации Opal

Диски с отметкой «X» поддерживаются, но не квалифицированы для систем Dell и не поставляются в их составе.

Диск	Доступность	Стандарт
Seagate ST320LT009 (FIPS Julius 320 ГБ)	✓	Opal 1
Seagate ST320LT014 (Julius 320 ГБ)	✓	Opal 1
Seagate ST500LM001 (Kahuna 500 ГБ)	✓	Opal 2/eDrive
Seagate ST1000LM015 (Kahuna 1000 ГБ)	✓	Opal 2/eDrive
Seagate ST500LT012 (Yarra 1D, не FIPS, 500 ГБ)	✓	Opal 2/eDrive
Seagate ST500LT015 (Yarra 1D FIPS 500 ГБ)	✓	Opal 2/eDrive
Seagate ST500LM020 (Kahuna V FIPS 500 ГБ)	✓	Opal 2/eDrive
Seagate ST1000LM028 (Kahuna V FIPS 1000 ГБ)	✓	Opal 2/eDrive
Seagate ST500LM023 (Yarra X)	✓	Opal 2/eDrive
Seagate ST500LM024 (Yarra X FIPS 500 ГБ)	✓	Opal 2/eDrive
Seagate ST500LT025 (Yarra R)	✓	Opal 2/eDrive
Seagate ST500LT033 (Asagana)	✓	Opal 2/eDrive
Seagate ST1000DM004 (для настольных ПК, 3,5 дюйма, 1000 ГБ)	X	Opal 2/eDrive
Seagate ST1000DM004 (для настольных ПК, 3,5 дюйма, 2000 ГБ)	X	Opal 2/eDrive
Seagate ST1000DM004 (для настольных ПК, 3,5 дюйма, 3000 ГБ)	X	Opal 2/eDrive
Серия Travelstar 5K750	X	Opal 1
Серия Travelstar 7K750	X	Opal 1
Серия Travelstar Z5K320	X	Opal 1
Toshiba, серия MKxx61GSYD	X	Opal 1
Toshiba, серия MKxx61GSYG	X	Opal 1
Samsung SM840 EVO MZ-MTEXXXBW	X	Opal 2
Samsung SM841 OPAL SSD	✓	Opal 2
Samsung SM841N OPAL SSD	✓	Opal 2
Samsung SM850 PRO, 2,5 дюйма, MZ-7KE128 – MZ-7KE2T0 (2,5 дюйма, SED SSD, от 128 ГБ до 2000 ГБ)	X	Opal 2/eDrive
Samsung SM850 EVO, 2,5 дюйма, MZ-75E120 – MZ-75E2T0 (2,5 дюйма, SED SSD, от 120 ГБ до 2000 ГБ)	X	Opal 2/eDrive
Samsung SM850 EVO mSATA MZ-M5E120 – MZ-M5E1T0 (mSATA SED SSD, от 120 ГБ до 1000 ГБ)	X	Opal 2/eDrive
Samsung SM850 EVO M.2 MZ-N5E120 – MZ-N5E500 (M.2, SED SSD, от 120 ГБ до 500 ГБ)	X	Opal 2/eDrive
Samsung PM851 OPAL SSD – 2,5 дюйма (2,5 дюйма, 128 ГБ – 512 ГБ)	✓	Opal 2/eDrive

Диск	Доступность	Стандарт
Samsung PM851 OPAL SSD – mSATA (mSATA, 128 ГБ – 512 ГБ)	✓	Opal 2/eDrive
Samsung PM851 OPAL SSD – M.2. (M.2, 128 ГБ – 512 ГБ)	✓	Opal 2/eDrive
Samsung PM871 OPAL SSD – 2,5 дюйма (2,5 дюйма, 256 ГБ – 512 ГБ)	✓	Opal 2/eDrive
Samsung PM871 OPAL SSD – mSATA (mSATA, 256 ГБ – 512 ГБ)	✓	Opal 2/eDrive
Samsung PM871 OPAL SSD – M.2. (M.2, 256 ГБ – 512 ГБ)	✓	Opal 2/eDrive
SanDisk X300s	X	Opal 2
LiteOn L9M OPAL SSD	✓	Opal 2
LiteOn M3 series SSD	✓	Opal 1
LiteOn M6 series SSD	✓	Opal 2
LiteOn V2M series SSD	✓	Opal 2
Crucial RealSSD C400 SSD	X	Opal 1
Micron RealSSD C400 SSD	X	Opal 1
Micron M500 SSD, 2,5 дюйма, (120 ГБ – 960 ГБ)	X	Opal 2/eDrive
Micron M500 SSD mSATA (120 ГБ – 480 ГБ)	X	Opal 2/eDrive

Языковая поддержка

Решение DDP|ST совместимо с многоязычным пользовательским интерфейсом (Multilingual User Interface, MUI) и поддерживает следующие языки.

ПРИМЕЧАНИЕ. Локализация PBA не поддерживается на русском, а также на традиционном и упрощенном китайском языках.

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

Параметры проверки подлинности

Для нижеперечисленных параметров проверки подлинности потребуется специальное оборудование. Отпечатки пальцев, Смарт-карты, Бесконтактные карты, Карты SIPR Net/класса B и проверка подлинности на компьютерах с поддержкой интерфейса UEFI.

Для использования функции одноразового пароля необходимо наличие включенного собственного TPM. Для получения дополнительной информации см.Очистка собственности и активация доверенного платформенного модуля (TPM).

В таблице ниже приводятся параметры проверки подлинности, доступные в средствах безопасности 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	Безопасность одноразового	Карта SIPR	Пароль	Отпечаток пальца	Смарт-карта	Безопасность одноразового	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 Обновление 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

	Проверка подлинности перед загрузкой включена на поддерживаемых компьютерах Dell					Проверка подлинности Windows				
	Пароль	Отпечаток пальца	Контактная смарт-карта	Безопасность одноразового	Карта SIPR	Пароль	Отпечаток пальца	Смарт-карта	Безопасность одноразового	Карта SIPR
Windows 7										
Windows 8	X[2]					X	X	X	X	X
Windows 8.1-Windows 8.1 Обновление 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 был установлен на компьютере ранее, то **перед установкой** средств безопасности Security Tools, следует выполнить отзыв оборудования, управление которым осуществляется DDP|A, и удалить DDP|A. Если DDP|A не используется, Вы можете просто удалить DDP|A и начать процесс установки заново.

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 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

1 Следуйте инструкциям, приведенным на веб-сайте 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. раздел https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2.

См. далее Установка и активация.

3

Установка и активация

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

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

Установка DDP|ST

Для установки пакета Security Tools выполняйте следующие указания.

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

ПРИМЕЧАНИЕ. Установочный файл можно загрузить с веб-сайта www.dell.com/support > Endpoint Security Solutions.

2. Дважды щелкните файл, чтобы запустить программу установки.
3. Выберите соответствующий 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. Нажмите **Next** («Далее») на странице Select Feature («Выбор функции»).
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|ST

При первом запуске консоли DDP Security Console и выборе опции Administrator Settings («Параметры администратора») запустится мастер активации, который позволяет пользователю пошагово выполнить активацию продукта.

Если консоль безопасности DDP Security Console еще не была активирована, конечный пользователь, тем не менее, может запустить ее. Если конечный пользователь является первым пользователем консоли DDP Security Console, перед тем как администратор активирует DDP|ST и настроит его параметры, будут использоваться параметры, установленные 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 параметрах администратора).

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

3 На странице приветствия нажмите **Next** («Далее»).

4 Создайте пароль для DDP|ST и нажмите кнопку **Next** («Далее»).

Перед тем как выполнить настройку параметров Security Tools, следует создать пароль администратора в DDP|ST. 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** («Расположение 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|ST 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.

Изменение пароля администратора и папки для сохранения файла резервной копии, установленной по умолчанию

После активации пакета Security Tools, если необходимо, можно изменить пароль администратора и папку для сохранения файла резервной копии, установленную по умолчанию

1. Войдя в систему с правами администратора, запустите программу Security Tools, используя ярлык на рабочем столе.
2. Нажмите на плитку **Administrator Settings** («Параметры администратора»).
3. В диалоговом окне Authentication («Проверка подлинности») введите пароль администратора, заданный во время активации, и нажмите **OK**.
4. Выберите вкладку **Administrator Settings** («Параметры администратора»).
5. Если Вы хотите изменить пароль, на странице Change Administrator Password («Изменить пароль администратора») введите новый пароль длиной от 8 до 32 символов с содержанием как минимум одной буквы, одной цифры и одного специального символа.
6. Повторно введите пароль для его подтверждения, а затем нажмите **Apply** («Применить»).
7. Чтобы изменить расположение ключа восстановления, в левой части окна выберите **Change Backup Location** («Изменить расположение резервной копии»).
8. Выберите новое расположение резервной копии и нажмите **Apply** («Применить»).

   Файл резервной копии необходимо хранить либо на сетевом диске, либо на съемном носителе. Файл резервной копии содержит ключи, необходимые для восстановления данных на Вашем компьютере. Служба поддержки Dell ProSupport 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|ST выведет запрос для выбора места расположения в целях сохранения резервной копии данных восстановления. Доступ к данным восстановления необходим для начала шифрования.

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 см.Настройки параметров входа.

Чтобы настроить шифрование и проверку подлинности перед загрузкой.

1 Находясь в окне консоли DDP Security Console, нажмите на плитку **Administrator Settings**.

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. Если ввести такое слово или код в поле имени пользователя или пароля во время проверки подлинности PBA, **все данные с устройства будут удалены безвозвратно.** Если это поле оставлено пустым, в критической ситуации будет отсутствовать пароль с криптографическим удалением.

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». Отказ от ввода текста в это поле приводит к отсутствию отображения текста или кнопок «OK» / Cancel («Отмена»). 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.

- Изменить параметры шифрования и проверки подлинности перед загрузкой. нажмите на вкладку **Encryption** («Шифрование»), а затем – на 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.

- Изменить параметры шифрования и проверки подлинности перед загрузкой. нажмите на вкладку **Preboot Settings** («Параметры проверки подлинности перед загрузкой») и выберите **Preboot Customization** («Настройка текста перед загрузкой») или **Preboot Logon Policies** («Политики входа перед загрузкой»).

  Инструкции по удалению см. в разделе Задачи по удалению.

Настройка параметров проверки подлинности

Средства управления на вкладке Administrator Settings Authentication («Параметры проверки подлинности администратора») позволяют установить параметры входа пользователя и настроить значения для каждого из них.

ПРИМЕЧАНИЕ. Опция One-time Password («Одноразовый пароль») не отображается в разделе Recovery Options («Параметры восстановления»), в наличии нет собственного включенного TPM.

Настройки параметров входа

На странице Sign-in Options («Параметры входа») можно настроить политики входа По умолчанию все поддерживаемые учетные данные перечислены в списке Available Options («Доступные параметры»).

Чтобы настроить параметры входа.

1. На левой панели в разделе Authentication («Проверка подлинности») выберите **Sign-in Options** («Параметры входа»).
2. Чтобы выбрать роль, которую необходимо настроить, выберите соответствующий элемент в списке **Apply sign-in options to** («Применить параметры входа к...»). **Пользователи** или **Администраторы**. Все изменения, которые Вы сделали на указанной странице, будут применимы только к той роли, которую Вы выберите.
3. Установите доступные параметры проверки подлинности.

   По умолчанию, каждый метод проверки подлинности может использоваться в отдельно, а не в сочетании с другими аналогичными методами. Вы можете изменить настройки по умолчанию следующими способами.

   - Чтобы установить сочетание параметров проверки подлинности, в разделе Available Options («Доступные параметры») нажмите кнопку , чтобы выбрать первый метод проверки подлинности. В диалоговом окне Available Options («Доступные параметры») выберите второй метод проверки подлинности и нажмите кнопку **OK**.

     Например, можно установить в качестве учетных данных отпечаток пальца и пароль. В диалоговом окне выберите второй способ проверки подлинности, который необходимо использовать с проверкой подлинности по отпечатку пальца.
   - Для того чтобы каждый метод проверки подлинности мог использоваться отдельно, ? диалоговом окне Available Options («Доступные параметры») выберите для второго метода проверки подлинности значение **None** («Нет») и нажмите кнопку **OK**.
   - Чтобы удалить параметр входа, в разделе Available Options («Доступные параметры») на странице Sign-in Options («Параметры входа») нажмите на символ «**X**» для удаления соответствующего метода.
   - Чтобы добавить новое сочетание методов проверки подлинности, нажмите кнопку **Add an Option** («Добавить параметр»).
4. Установите параметры восстановления для пользователей, чтобы они могли восстановить доступ к компьютеру, если такие пользователи были заблокированы.

   - Чтобы разрешить пользователям определять набор контрольных вопросов и ответов на них, которые будут использованы для восстановления доступа к компьютеру, выберите опцию **Recovery Questions** («Вопросы для восстановления»).

     Чтобы запретить использование вопросов для восстановления, снимите флажок с этой опции.
   - Чтобы разрешить пользователям восстанавливать доступ с помощью мобильного устройства, выберите опцию **One-time Password** («Одноразовый пароль»). Если в качестве способа восстановления выбрана опция «Одноразовый пароль» (OTP), она не будет доступна в качестве опции входа на экране входа в Windows.

     Чтобы использовать одноразовый пароль для входа, снимите флажок с указанного параметра в разделе Recovery Options («Параметры восстановления»). Если этот параметр не выбран в качестве метода восстановления, параметр «одноразовый пароль» появляется в окне входа Windows, если хотя бы один пользователь зарегистрирован в качестве пользователя с одноразовым паролем.

ПРИМЕЧАНИЕ. Будучи администратором, Вы контролируете назначение одноразового пароля – для проверки подлинности или восстановления. Функция одноразового пароля может использоваться либо для проверки подлинности, либо для восстановления доступа, но не для обеих целей одновременно. Эта настройка влияет либо на всех пользователей компьютера, либо на всех администраторов, в зависимости от выбора, сделанного в поле Sign-in Options («Параметры входа»), в опции **Apply sign-in options to** («Применить параметры входа к…»).

Если параметр одноразового пароля не перечислен в списке, значит, конфигурация Вашего компьютера не поддерживает работу с ним. Для получения дополнительной информации см.Требования.

- Чтобы пользователь в случае потери учетных данных (или если пользователь забыл пароль) мог обратиться в службу технической поддержки по телефону, снимите флажок с опции Recovery Questions («Вопросы для восстановления») и One-time Password («Одноразовый пароль»).

5 Чтобы установить интервал времени, в течение которого пользователи могут зарегистрировать свои учетные данные для проверки подлинности, выберите опцию **Grace Period** («Льготный период»).

Функция Grace Period («Льготный период») позволяет пользователю установить дату, при наступлении которой настроенный параметр входа будет использоваться принудительно. Вы можете настроить параметр входа до наступления даты, начиная с которой он будет использоваться принудительно, и установить интервал времени, в течение которого пользователи могут зарегистрироваться. По умолчанию указанные условия применяется немедленно.

Чтобы изменить дату принудительного применения параметра входа (установить другую дату вместо опции *«немедленно»*) в диалоговом окне Grace Period («Льготный период»), выведите контекстное меню и выберите опцию **Specified Date** («Указанная дата»). Нажмите на кнопку-стрелку «вниз», находящуюся справа от даты, чтобы открыть окно календаря, а затем выберите соответствующую дату в календаре. Политика вступает в силу примерно в 00:01 выбранного дня.

Пользователи могут получать уведомления о необходимости регистрации своих учетных данных, требуемых для следующего входа в Windows (по умолчанию), либо Вы можете настроить функцию отправки регулярных уведомлений. Выберите интервал отправки уведомлений из выпадающего списка *Remind User* («Напоминать пользователю»).

ПРИМЕЧАНИЕ. Напоминания, отображаемые для пользователей, могут немного различаться в зависимости от того, где находится пользователь в момент срабатывания напоминания. на экране входа в Windows или в текущем сеансе Windows. Напоминания не выводятся в окне входа при проверке подлинности перед загрузкой.

Функциональность, доступная в течение льготного периода

В течение установленного льготного периода при каждом входе в систему отображается уведомление Additional Credentials («Дополнительные учетные данные»), если пользователем не зарегистрирован минимум требуемых учетных данных в соответствии с измененным параметром входа. Выводится уведомление следующего содержания. *Additional credentials are available for enrollment* («Дополнительные учетные данные доступны для регистрации»).

Если дополнительные учетные данные имеются, но не требуются, это сообщение отображается только один раз после изменения политики.

В зависимости от конкретных условий нажатие на текст уведомления приводит к следующим результатам.

- Если учетные данные не зарегистрированы, запускается программа настройки, позволяющая пользователям с полномочиями администратора настроить параметры компьютера и предоставить пользователям возможность зарегистрировать наиболее распространенные типы учетных данных.
- После первоначальной регистрации учетных данных при нажатии на текст уведомления запускается программа настройки в DDP Security Console.

Функциональность, доступная по истечении льготного периода

Во всех случаях по истечении льготного периода пользователи не могут выполнить вход в систему, если они не зарегистрировали учетные данные, определенные параметром входа. Если пользователь предпринимает попытку входа с использованием одного или нескольких типов учетных данных, не удовлетворяющих условиям параметра входа, в верхней части экрана «Вход в Windows» отображается экран программы-мастера настройки.

- После успешной регистрации требуемых учетных данных автоматически выполняется вход в Windows.
- Если пользователь не зарегистрировал требуемые учетные данные или отменил запрос программы настройки, осуществляется возврат к экрану «Вход в Windows».

6 Чтобы сохранить параметры для выбранной роли, нажмите кнопку **Apply** («Применить»).

Настройка проверки подлинности с помощью диспетчера паролей

На странице диспетчера паролей Вы можете настроить способ, с помощью которого пользователи будут осуществлять проверку подлинности в диспетчере паролей.

Для настройки проверки подлинности с помощью диспетчера паролей.

1 На левой панели в разделе Authentication («Проверка подлинности») выберите **Password Manager** («Диспетчер паролей»).

2 Чтобы выбрать роль, которую необходимо настроить, выберите соответствующий элемент в списке **Apply sign-in options to** («Применить параметры входа к...»). **Пользователи** или **Администраторы**. Все изменения, которые Вы сделали на указанной странице, будут применимы только к той роли, которую Вы выберите.

3 Как вариант, установите флажок в поле **Do not require authentication** («Проверка подлинности не требуется»), чтобы пользователи с выбранной ролью автоматически входили во все программные приложения и на все веб-сайты сети Интернет, используя учетные данные, сохраненные в диспетчере паролей.

4 Установите доступные параметры проверки подлинности.

По умолчанию, каждый метод проверки подлинности может использоваться в отдельно, а не в сочетании с другими аналогичными методами. Вы можете изменить настройки по умолчанию следующими способами.

- Чтобы установить сочетание параметров проверки подлинности, в разделе Available Options («Доступные параметры») нажмите кнопку , чтобы выбрать первый метод проверки подлинности. В диалоговом окне Available Options («Доступные параметры») выберите второй метод проверки подлинности и нажмите кнопку **OK**.

  Например, можно установить в качестве учетных данных отпечаток пальца и пароль. В диалоговом окне выберите второй способ проверки подлинности, который необходимо использовать с проверкой подлинности по отпечатку пальца.
- Для того чтобы каждый метод проверки подлинности мог использоваться отдельно, ? диалоговом окне Available Options («Доступные параметры») выберите для второго метода проверки подлинности значение **None** («Нет») и нажмите кнопку **OK**.
- Чтобы удалить параметр входа, в разделе Available Options («Доступные параметры») на странице Sign-in Options («Параметры входа») нажмите на символ «**X**» для удаления соответствующего метода.
- Чтобы добавить новое сочетание методов проверки подлинности, нажмите кнопку **Add an Option** («Добавить параметр»).

5 Чтобы сохранить параметры для выбранной роли, нажмите кнопку **Apply** («Применить»).

ПРИМЕЧАНИЕ. Чтобы восстановить исходные значения параметров, нажмите кнопку Defaults («Значения по умолчанию»).

Настройка вопросов восстановления.

На странице Recovery Questions («Вопросы для восстановления») Вы можете выбрать вопросы, которые будут отображаться пользователям для определения ими персональных вопросов для восстановления и ответов на них. Вопросы для восстановления позволяют пользователям восстановить доступ к компьютерам, если срок действия их паролей истек.

Для настройки вопросов восстановления.

1. На левой панели в разделе Authentication («Проверка подлинности») выберите **Recovery Questions** («Вопросы восстановления»).
2. На странице вопросов восстановления выберите как минимум 3 предварительно заданных вопроса.
3. По собственному усмотрению пользователь может создать еще три собственных вопроса, которые будут отображаться в списке для пользователя.
4. Для сохранения вопросов для восстановления нажмите **Apply** («Применить»).

Настройка проверки подлинности путем сканирования отпечатка пальца

Чтобы настроить проверку подлинности путем сканирования отпечатка пальца.

1. На левой панели в разделе Authentication («Проверка подлинности»), выберите **Fingerprints** («Отпечатки пальцев»).
2. В разделе Enrollments («Регистрация») установите минимальное и максимальное количество пальцев, которое пользователь может зарегистрировать для проверки отпечатка.
3. Установите чувствительность процедуры сканирования отпечатка пальца

   Более низкая чувствительность повышает вероятность допустимых отклонений и ошибочного сканирования. При максимальном значении чувствительности система может отвергать корректные отпечатки. Более высокая чувствительность уменьшает вероятность ошибочного сканирования до 1:10 000.
4. Чтобы удалить все отпечатки пальцев и зарегистрированные учетные данные из буфера сканера отпечатков пальцев, нажмите кнопку **Clear Reader** («Очистить память сканера»). Это позволит удалить только те данные, которые Вы добавляете в настоящий момент. Подобная операция не приводит к удалению отпечатков и регистраций, выполненных во время прежних сеансов.
5. Для сохранения настроек нажмите **Apply** («Применить»).

Настройка проверки подлинности по одноразовому паролю

Чтобы использовать функцию одноразового пароля, пользователь генерирует одноразовый пароль с помощью приложения Dell Data Protection | Security Tools Mobile на своем мобильном устройстве, а затем вводит его в компьютер. Этот пароль может использоваться только один раз, и срок его действия ограничен.

Для дальнейшего обеспечения безопасности администратор может защитить мобильное приложение PIN-кодом.

На странице Mobile Device («Мобильное устройство») Вы можете настроить параметры дальнейшего повышения безопасности мобильного устройства и одноразового пароля.

Чтобы настроить проверку подлинности по одноразовому паролю.

1. На левой панели в разделе Authentication («Проверка подлинности»), выберите **Mobile Device** («Мобильное устройство»).
2. Для запроса ввода PIN-кода при доступе к приложению Security Tools Mobile на мобильном устройстве выберите опцию **Require PIN** («Запросить пароль»).

ПРИМЕЧАНИЕ. Включение политики *Require PIN* («Запросить пароль») после регистрации мобильных устройств на компьютере приводит к удалению регистрации всех мобильных устройств. Пользователям будет необходимо повторно зарегистрировать мобильные устройства после включения данной политики.

   Если флажок в поле **Require PIN** («Запросить PIN-код»), пользователи должны будут разблокировать свое мобильное устройство для получения доступа к приложению Security Tools Mobile. Если на мобильном устройстве отсутствует блокировка, потребуется ввод пароля.

3. Для выбора длины одноразового пароля введите количество символов пароля в поле **One-time Password Length** («Длина одноразового пароля»).
4. Для выбора количества попыток ввода пользователем правильного одноразового пароля введите количество попыток в поле **User Sign-in Attempts Allowed** («Разрешенное количество попыток входа пользователя») (от **5** до **30**).

   После достижения максимального количества попыток функция ввода одноразового пароля будет отключена до тех пор, пока пользователь не зарегистрирует мобильное устройство.

РЕКОМЕНДАЦИИ. Dell рекомендует установить как минимум еще один метод проверки подлинности, помимо ввода одноразового пароля.

Настройка регистрации смарт-карты

Пакет DDP|Security Tools поддерживает 2 вида смарт-карт. контактные и бесконтактные.

Для использования контактных карт требуется считыватель, в который вставляются такие карты. Контактные карты совместимы только с доменными компьютерами. Карты CAC и SIPRNet относятся к контактному типу. Вследствие более высокотехнологичной природы этих карт пользователь должен выбрать сертификат после вставки таких карт в считыватель при выполнении входа.

- Бесконтактные карты поддерживаются компьютерами вне доменов и компьютерами, настроенными по доменным спецификациям.
- Пользователи могут зарегистрировать для каждой учетной записи одну контактную смарт-карту или несколько бесконтактных карт.
- Использование смарт-карт при проверке подлинности перед загрузкой не допускается.

ПРИМЕЧАНИЕ. При удалении регистрации смарт-карты из учетной записи, для которой зарегистрированы несколько карт, удаление регистрации всех карт происходит одновременно.

Настройка регистрации смарт-карты.

1. Во владке Authentication («Проверка подлинности») параметров администратора выберите опцию **Smartcard** («Смарт-карта»).

Настройка расширенных разрешений

1 Чтобы изменить расширенные параметры конечного пользователя, выберите вкладку **Advanced** («Дополнительно»). Во вкладке *Advanced* («Дополнительно») вы можете разрешить пользователям самостоятельно регистрировать учетные данные, изменять зарегистрированные учетные данные и выполнять одношаговый вход.

2 Установите или удалите флажки из соответствующих полей.

Allow users to enroll credentials («Разрешить пользователям регистрировать учетные данные»). по умолчанию в этом поле флажок установлен. Пользователи имеют право регистрировать учетные данные без вмешательства администратора. Если снять флажок, учетные данные должны регистрироваться администратором.

Allow user to modify enrolled credentials («Разрешить пользователям изменять зарегистрированные учетные данные»). по умолчанию в этом поле флажок установлен. Если флажок установлен, пользователям разрешено изменять или удалять зарегистрированные учетные данные без участия администратора. Если снять флажок, учетные данные не могут быть изменены или удалены обычным пользователем, но могут быть изменены или удалены администратором.

ПРИМЕЧАНИЕ. Чтобы зарегистрировать учетные данные пользователя, перейдите на страницу *Users* («Пользователи») инструмента параметров администратора и нажмите кнопку **Enroll** («Зарегистрировать»).

Allow one step logon («Разрешить одношаговый вход»). Одношаговый вход – это единый вход (SSO). По умолчанию флажок в этом поле установлен. Если эта функция включена, пользователи должны ввести свои учетные данные только на экране проверки подлинности перед загрузкой. Пользователи осуществляют вход в систему Windows автоматически. Если снять флажок, может потребоваться выполнение многократного входа.

ПРИМЕЧАНИЕ. Эта опция не может быть выбрана, если не выбрана опция **Allow users to enroll credentials** («Разрешить пользователям регистрировать учетные данные»).

3 По окончании операции нажмите кнопку **Apply** («Применить»).

Смарт-карта и биометрическая служба (опция)

Если Вы не хотите, чтобы программа Security Tools изменяла параметры служб, связанные со смарт-картами и биометрическими устройствами и не устанавливала для них признак «автоматический», функцию автоматического запуска службы можно отключить.

Если эта функция выключена, программа Security Tools не будет предпринимать попытку запуска указанных ниже трех устройств.

- SCardSvr. управляет доступом к смарт-картам, читаемым компьютером. При остановке этой службы данный компьютер не сможет читать смарт-карты. При отключении этой службы, все службы, которые напрямую зависят от нее, не смогут запуститься.
- SCPolicySvc.позволяет настроить систему таким образом, чтобы она блокировала рабочий стол пользователя при удалении смарт-карты.
- WbioSrvc. служба биометрических данных Windows предоставляет клиентским приложениям возможность снимать, сравнивать, обрабатывать и сохранять биометрические данные без получения прямого доступа к какому-либо биометрическому оборудованию или образцам. Данная служба располагается в специальном процессе SVCHOST.

Выключение этой функции также подавляет все предупреждения, связанные с соответствующими службами, если они не работают.

Disable the Automatic Service Startup («Выключить автоматический запуск службы»)

По умолчанию, если соответствующий раздел реестра не существует, или если ему присвоено значение 0, эта функция включена.

1. Запустите редактор реестра **Regedit**.
2. Найдите следующую запись реестра.

   [HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

   SmartCardServiceCheck=REG_DWORD:0

   Чтобы включить, установите значение 0.
   Чтобы выключить, установите значение 1.

Управление проверкой подлинности пользователя

Средства управления на вкладке Administrator Settings Authentication («Параметры проверки подлинности администратора») позволяют установить параметры входа пользователя и настроить значения для каждого из них.

Чтобы осуществлять управление проверкой подлинности пользователя.

1. После входа с правами администратора нажмите на плитку **Administrator Settings** («Параметры администратора»).
2. Для управления пользователями и статусами регистрации пользователей перейдите во вкладку **Users** («Пользователи»). В этой вкладке Вы можете.
   - зарегистрировать новых пользователей;
   - добавить или изменить учетные данные;
   - Удалить учетные данные пользователя.

ПРИМЕЧАНИЕ. Параметры **Sign-in** («Вход») **и Session** («Сеанс») отображают статус регистрации каждого пользователя.

Если параметр **Sign-in** («Вход») имеет статус **OK**, все регистрации, которые необходимы для входа пользователя, были завершены.
Если параметр **Session** («Сеанс») имеет статус **OK**, все регистрации, необходимые пользователю для использования диспетчера паролей, были завершены.

Если оба параметра имеют статус **No** («Нет»), пользователь должен завершить дополнительные регистрации. Чтобы узнать, какие именно регистрации не завершены, запустите инструмент **Administrator Settings** («Параметры администратора») и откройте вкладку **Users** («Пользователи»). Неактивные поля флажков соответствуют незавершенным регистрациям. Как вариант, нажмите на плитку **Enrollments** («Регистрации») и просмотрите содержимое столбца **Policy** («Политика») во вкладке **Status** («Статус»), в котором перечислены требуемые регистрации.

Добавить новых пользователей

ПРИМЕЧАНИЕ. Новые пользователи Windows добавляются автоматически при входе в Windows или при регистрации учетных данных.

1. Нажмите **Add User** («Добавить пользователя»), чтобы начать процесс регистрации существующего пользователя Windows.
2. В отобразившемся диалоговом окне *Select User* («Выбор пользователей») выберите опцию **Object Types** («Типы объекта»).
3. Введите название объекта пользователя в текстовое поле и щелкните **Check Names** («Проверить имена»).
4. После окончания нажмите кнопку **OK**.

   Откроется мастер регистрации.

   Дальнейшие инструкции описаны в разделе Регистрация или изменение учетных данных пользователя.

Регистрация или изменение учетных данных пользователя

Администратор может зарегистрировать или изменить учетные данные пользователя от имени пользователя, но для выполнения некоторых действий по регистрации требуется присутствие пользователя, например, для ответов на контрольные вопросы или сканирования отпечатков пальцев пользователя.

Чтобы зарегистрировать или изменить учетные данные пользователя.

1. В разделе Administrator Settings («Параметры администратора») нажмите на вкладку **Users** («Пользователи»).

2 На странице Users («Пользователи») нажмите **Enroll** («Зарегистрировать»).

3 На стартовой странице нажмите **Next** («Далее»).

4 В диалоговом окне Authentication Required («Требуется проверка подлинности») введите имя пользователя и пароль в ОС Windows и нажмите кнопку **OK**.

5 На странице Password («Пароль»), чтобы изменить пароль пользователя в Windows, введите и подтвердите новый пароль и нажмите кнопку **Next** («Далее»).

Чтобы пропустить этап изменения пароля нажмите кнопку **Skip** («Пропустить»). Программа-мастер позволяет пропустить учетные данные, если их не нужно регистрировать. Чтобы вернуться на предыдущую страницу, нажмите кнопку **Back** («Назад»).

6 Следуйте инструкциям на каждой странице и нажмите на соответствующую кнопку. **Next** («Далее»), **Skip** («Пропустить») или **Back** («Назад»).

7 На странице сводки подтвердите зарегистрированные учетные данные и после завершения регистрации нажмите кнопку **Apply** («Применить»).

Чтобы вернуться на страницу регистрации учетных данных и сделать необходимые изменения, нажимайте кнопку **Back** («Назад») до тех пор, пока не дойдете до нужной страницы.

Для получения дополнительной информации о регистрации учетных данных или об их изменении см. *Dell Data Protection | Console User Guide* («Защита данных Dell / Руководство пользователя консоли»).

Удаление одного элемента зарегистрированных учетных данных

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

2 Нажмите на вкладку **Users** («Пользователи») и найдите необходимого пользователя.

3 Наведите курсор мыши на зеленый флажок того элемента учетных данных, который необходимо удалить. Он примет вид ⊗.

4 Нажмите на символ ⊗, а затем нажмите кнопку **Yes** («Да»), чтобы подтвердить удаление.

ПРИМЕЧАНИЕ. Элемент учетных данных нельзя удалить, если этот элемент – единственный зарегистрированный для данного пользователя. Кроме того, с помощью указанного метода невозможно удалить пароль. Чтобы полностью закрыть доступ пользователя к компьютеру, воспользуйтесь командой Remove («Удалить»).

Удаление всех зарегистрированных учетных данных пользователя

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

2 Нажмите на вкладку **Users** («Пользователи») и выберите пользователя, которого необходимо удалить.

3 Нажмите кнопку **Remove** («Удалить»). (команда удаления выводится в нижней строке параметров пользователя красным цветом).

После удаления пользователь не сможет войти в компьютер до тех пор, пока не осуществит повторную регистрацию.

5

Задачи по удалению

Чтобы удалить DDP|ST, необходимо обладать правами не ниже уровня **локального администратора**.

Удаление DDP|ST

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 Отмена инициализации **самошифрующихся дисков**.

   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 получения 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. Более подробную информацию см. в разделе Настройки параметров входа.**

- **Вопросы для восстановления**. 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.

Самовосстановление, вопросы для восстановления при входе в Windows

Чтобы ответить на вопросы для восстановления доступа к экрану входа в Windows.

1. Чтобы использовать вопросы для восстановления, выберите опцию **Can't access your account?** («Не можете получить доступ к своей учетной записи?»)

   Вопросы для восстановления , выбранные в процессе представлении регистрации.

2. Введите ответы на вопросы и нажмите кнопку **OK**.

   При успешном ответе на вопросы включается режим восстановления доступа. Дальнейшие действия зависят от характеристик нерабочей учетной записи

   - Если ввести правильный пароль для входа в Windows не удалось, отобразится экран Change Password («Изменить пароль»).
   - Если отпечаток пальца распознать не удалось, отображается страница регистрации отпечатка пальца для повторной регистрации отпечатка.

Самовосстановление, вопросы для восстановления

Чтобы ответить на вопросы для восстановления доступа к экрану проверки подлинности перед загрузкой.

1. На экране проверки подлинности перед загрузкой введите имя пользователя.
2. В левом нижнем углу экрана выберите **Options** («Параметры»).
3. В меню Options («Параметры») выберите опцию **Forgot Password** («Забыл пароль»).
4. Ответьте на вопросы для восстановления и нажмите кнопку **Sign In** («Вход»).

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 PIN-код.
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 в одно и то же время. 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.

Глоссарий

Доверенный платформенный модуль (TPM). TPM — это чип с тремя основными функциями: безопасное хранение, измерение и удостоверение подлинности. DDP|E использует TPM для обеспечения безопасного хранения. TPM также используется для создания зашифрованных контейнеров, предназначенных для хранилища программного обеспечения DDP|E и для защиты ключа шифрования аппаратных криптографических ускорителей DDP|E (HCA). Dell рекомендует подготовить TPM к работе. TPM необходим для использования вместе с аппаратными криптографическими ускорителями DDP|E и для активации функции одноразового пароля.

Единый вход (SSO). процедура SSO упрощает процесс входа в систему, если для проверки подлинности перед загрузкой 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.

Одноразовый пароль (OTP). Одноразовый пароль — это пароль, который может быть использован только один раз и действует в течение ограниченного периода времени. Для использования одноразового пароля необходимо наличие включенного собственного TPM. test4 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.

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

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. PBA предотвращает чтение любых данных с диска, в том числе данных операционной системы, пока пользователь не подтвердит наличие корректных учетных данных.


0XXXXXA0X