Dell Data Protection

Руководство пользователя консоли

Статус шифрования
Проверка подлинности регистрации
Диспетчер паролей
версия 1.10

2016-07

Содержание

1

Введение

Dell Data Protection | Security Tools предоставляет пользователю простые в использовании и интуитивно понятные инструменты для повышения безопасности компьютера.

С консоли DDP доступны следующие функции:

- Зарегистрируйте учетные данные для использования с Security Tools
- Возможность использования преимуществ многофакторных учетных данных, включая пароли, отпечатки пальцев и смарт-карты
- Восстановление доступа к компьютеру при утере пароля без необходимости обращения в службу поддержки или к администратору
- Резервное копирование и восстановление данных программ
- Легкая смена пароля учетной записи Windows
- Настройка персональных установок
- Просмотр статуса шифрования (на компьютерах, оснащенных самошифрующимися дисками)

DDP Console

DDP Console – это интерфейс, с помощью которого можно регистрировать учетные данные, управлять ими и настраивать конфигурацию контрольных вопросов.

Вы можете получить доступ к следующим приложениям:

- Инструмент статуса шифрования позволяет просматривать статус шифрования дисков компьютера.
- Инструмент регистрации позволяет настроить учетные данные и управлять ими, настроить вопросы для самостоятельного восстановления доступа и просматривать статус регистрации ваших учетных данных. Возможность регистрировать определенные типы учетных данных устанавливается администратором.
- Password Manager («Диспетчер паролей») позволяет автоматически заполнять формы и вводить данные, необходимые для доступа к веб-сайтам, приложениям Windows и сетевым ресурсам. «Диспетчер паролей» также позволяет вам изменять свои пароли для входа в систему в рамках приложения в целях синхронизации паролей, контролируемых «Диспетчером паролей», с паролями на целевом ресурсе.

Данное руководство описывает способы использования данных приложений.

Обязательно время от времени проверяйте dell.com/support для обновленной документации.

Связь со службой поддержки ProSupport

Прежде чем обратиться за помощью в службу поддержки Dell ProSupport, во время звонка вам необходимо открыть Service Tag (Вкладка «Служба»), чтобы быстро соединить вас нужным техническим специалистов.

Чтобы связаться с ProSupport, позвоните по номеру 877-459-7304, добавочный номер 4310039 для круглосуточной оказании поддержки при использовании продуктов Dell Data Protection.

К тому же, вы можете обратиться в службу поддержки продуктов Dell Data Protection онлайн по ссылке dell.com/support. Поддержка онлайн включает в себя драйверы, руководства, технические консультативные сообщения, часто задаваемые вопросы и решение возникающих проблем.

2

Консоль DDP

Консоль DDP Console обеспечивает доступ к приложениям, обеспечивающим безопасность для всех пользователей компьютера, просмотр и управление статусом шифрования компьютерных дисков и разделов дисков, а также возможность управления входами на веб-сайты, в программы и сетевые ресурсы; а также легко регистрировать учетные данные для проверки подлинности на основании политики, установленной администратором.

Чтобы открыть консоль DDP, дважды щелкните на *рабочем столе* значок **DDP Console**.

После запуска консоли DDP Console откроется начальная страница, на которой будут отображены приложения пакетаSecurity Tools:

- Статус шифрования
- Регистрация
- Диспетчер паролей

Для первичной настройки учетных данных выберите ярлык **Getting Started** («Начать») на плитке Enrollments («Регистрация»). Программа -мастер проведет вас через краткий процесс регистрации. Для получения дополнительной информации см. Первоначальная регистрация учетных данных.

Навигация

Для получения доступа к приложению нажмите на соответствующую плитку.

Строка заголовка

Чтобы вернуться из приложения на главную страницу, нажмите стрелку «назад», находящуюся в левом углу строки заголовка, рядом с именем активного приложения.

Для перехода к другому приложению нажмите направленную вниз стрелку, расположенную рядом с названием активного приложения, а затем выберите необходимое приложение.

Для того чтобы свернуть, развернуть или закрыть окно консоли DDP, нажмите соответствующий значок в правом углу строки заголовка.

Чтобы восстановить размер окна консоли DDP после сворачивания, дважды щелкните ярлык на панели задач.

Чтобы открыть Справку, нажмите «**?**» на панели задач.

Подробнее о консоли DDP

Чтобы просмотреть сведения о консоли DDP, ознакомиться с политикой, действующими службами и журналами, нажмите на значок «шестеренка» в левой части строки заголовка Эта информация может потребоваться администратору для обеспечения технической поддержки.

Выберите соответствующий элемент в меню.

Элемент меню	Назначение
О программе	Содержит информацию о версии программы и авторских правах.
Отобразить информацию	Содержит следующую информацию: • версия продукта и дата создания; • осуществляется ли управление консолью DDP на данном компьютере предприятием или локальным администратором • номера версий ОС, BIOS, материнской платы и доверенного платформенного модуля (TPM).
Информация Microsoft	Запускает информационную утилиту Microsoft Windows System Information, которая содержит подробную информацию об оборудовании, компонентах и среде программного обеспечения.
Копировать сведения	Копирует всю системную информацию в буфер обмена для ее вставки в сообщение электронной почты, адресованное администратору или в службу поддержки Dell ProSupport.
Обратная связь	Открывает форму, в которой можно написать компании Dell свои отзывы о данном продукте.

Политики	Отображает иерархию политик, которые применяются к компьютеру пользователя.
Службы	Содержит подробную информацию о работающих службах.
Поддержка	Подключает к веб-сайту службы поддержки Dell ProSupport.
Журнал	Отображает подробный список зарегистрированных в журнале событий, информация о которых используется при устранении неполадок.

3

Статус шифрования

На странице Encryption («Шифрование») отображается состояние шифрования компьютера. Если диск, накопитель или раздел диска не зашифрован, ему будет присвоен статус *Unprotected*(«Незащищенный»). Зашифрованный диск или раздел показывает статус *Protected* («Защищенный»).

Для обновления статуса шифрования нажмите правой клавишей мыши на соответствующий диск или раздел и выберите **Refresh** («Обновить»).

4

Регистрация

Инструмент Enrollments («Регистрация») позволяет регистрировать, изменять, а также проверять статус регистрации в соответствии с требованиями политики, установленной администратором.

При первой регистрации учетных данных используется приложение DDP Console, программа-мастер позволяет зарегистрировать или изменить пароль, вопросы для восстановления, отпечатки пальцев, мобильного устройства и смарт-карты.В зависимости от требований политики вы можете либо зарегистрировать, либо пропустить каждый элемент учетных данных. После первоначальной регистрации вы можете нажать на плитку Enrollment («Регистрация») для чтобы добавить или изменить свои учетные данные.

Первоначальная регистрация учетных данных

Чтобы зарегистрировать учетные данные в первый раз:

1. На главной странице консоли DDP Console нажмите на ссылку **Getting Started** («Приступая к работе») плитки Enrollments («Регистрация»).
2. На стартовой странице нажмите **Next** («Далее»).
3. В диалоговом окне Authentication Required («Требуется проверка подлинности»), введите свой пароль для входа в ОС Windows, после чего нажмите кнопку «**OK**».
4. На странице Password («Пароль»), чтобы изменить свой пароль 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»).
5. Следуйте инструкциям на каждой странице и нажмите на соответствующую кнопку: **Next** («Далее»), **Skip** («Пропустить») или **Back** («Назад»).
6. 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. раздел Добавление, изменение или просмотр зарегистрированных учетных данных.

Добавление, изменение или просмотр зарегистрированных учетных данных

Для добавления, изменения или просмотра зарегистрированных учетных данных нажмите на плитку **Enrollments** («Регистрация»).

Вкладки на левой панели содержат список доступных регистраций. Они могут отличаться в зависимости от вашей платформы или типа оборудования.

На странице Status («Статус») отображаются поддерживаемые учетные данные, параметр применимой политики (требуется или недоступен) и статус регистрации. На указанной странице пользователи могут управлять своими зарегистрированными учетными данными в соответствии с требованиями политики, установленной администратором:

- Для первоначальной регистрации учетных данных в строке с соответствующим элементом учетных данных нажмите кнопку **Enroll** («Зарегистрировать»).
- Чтобы удалить существующий зарегистрированный элемент учетных данных, нажмите кнопку **Delete** («Удалить»).
- Если политика не позволяет вам регистрировать или изменять собственные учетные данные, ссылки **Enroll** («Регистрировать») и **Delete** («Удалить») на странице Status («Состояние») будут неактивны.
- Для изменения существующей регистрации нажмите на соответствующую вкладку на левой панели.

  Если политика не допускает регистрации или изменения учетных данных, на странице создания учетной записи отобразиться сообщение, «Изменения в учетной записи запрещены политикой.»

Пароль

Смена пароля учетной записи Windows:

1. Нажмите вкладку **Password** («Пароль»).
2. Введите текущий пароль для входа в Windows.
3. Введите новый пароль, повторно введите его для подтверждения и нажмите на кнопку **Change** («Изменить»).

   Изменение пароля вступает в силу незамедлительно.
4. В диалоговом окне Successful Enrollment («Регистрация выполнена успешно») нажмите кнопку **OK**.

ПРИМЕЧАНИЕ: Изменение пароля Windows необходимо выполнять исключительно в DDP Console, а не в Windows. Если пароль для входа в Windows был изменен вне консоли DDP Console, возникнет несоответствие паролей, которое потребует проведения операции восстановления.

Вопросы для восстановления

Страница Recovery Questions («Вопросы для восстановления») позволяет создать, удалить или изменить контрольные вопросы для восстановления доступа и ответы на них. На странице Recovery Questions («Вопросы для восстановления») используется метод вопросов и ответов для получения доступа к учетным записям в системе Windows в том случае, если, например, пароль утрачен или срок его действия истек.

ПРИМЕЧАНИЕ: Вопросы для восстановления используются только для восстановления доступа к компьютеру. Вопросы и ответы на них не могут использоваться для входа в систему.

Если вопросы для восстановления ранее не регистрировались:

1. Нажмите на вкладку **Recovery Questions** («Вопросы для восстановления»).
2. Выберите из списка предварительно заданные вопросы, а затем введите и подтвердите ответы на них.
3. Нажмите кнопку **Enroll** («Регистрировать»).

ПРИМЕЧАНИЕ: Нажмите кнопку **Reset** («Сброс»), чтобы очистить выбранные объекты на текущей странице и начать процедуру заново.

Вопросы для восстановления уже зарегистрированы

Если вопросы для восстановления уже зарегистрированы, Вы можете удалить или повторно зарегистрировать их.

1. Нажмите на вкладку **Recovery Questions** («Вопросы для восстановления»).
2. Нажмите на соответствующую кнопку:

- Чтобы полностью удалить вопросы для восстановления , нажмите кнопку **Delete** («Удалить»).
- Для повторного определения вопросов для восстановления и ответов нажмите кнопку **Re-enroll** («Зарегистрировать повторно»).

Отпечатки пальцев

ПРИМЕЧАНИЕ: Чтобы использовать эту функцию, Ваш компьютер должен быть оборудован сканером отпечатков пальцев.

Чтобы зарегистрировать отпечатки пальцев, выполните описанные ниже инструкции:

1. Нажмите на вкладку **Fingerprints** («Отпечатки пальцев»).
2. На странице Fingerprint («Отпечаток пальца») выберите палец, отпечаток которого Вы хотите зарегистрировать.
3. Для регистрации своего отпечатка пальца следуйте отображаемым на экране инструкциям.

ПРИМЕЧАНИЕ: Для успешной регистрации отпечаток пальца должен быть отсканирован 4 раза. Количество операций сканирования, необходимых для завершения регистрации отпечатков, зависит от качества сканирования. Администратор установил минимальное и максимальное количество отпечатков пальцев.

4. Нажмите на обозначение каждого пальца для сканирования отпечатков, пока не зарегистрируете минимальное количество отпечатков пальцев, установленное требованиями политики.

   В случае если минимальное необходимое количество отпечатков пальцев не было зарегистрировано, в диалоговом окне будет выведено соответствующее уведомление. Для продолжения нажмите кнопку **OK**.

5. Завершите сканирование необходимого количества отпечатков пальцев и нажмите кнопку **Save** («Сохранить»).

Чтобы удалить отсканированный отпечаток пальца, на странице регистрации отпечатков нажмите на выделенный отпечаток и нажмите кнопку **Yes** («Да»), чтобы подтвердить отмену его регистрации, после чего нажмите кнопку **Save** («Сохранить»).

Мобильное устройство

Регистрация мобильного устройства позволяет использовать функцию одноразового пароля (OTP). С помощью этой функции пользователь может войти в систему Windows по паролю, сгенерированному приложением Security Tools Mobile на мобильном устройстве, которое спарено с компьютером. В качестве альтернативы, если не противоречит требованиям политики, функция одноразового пароля может быть использована для восстановления доступа к компьютеру, в случае если срок действия пароля истек или пароль утрачен.

ПРИМЕЧАНИЕ: Если вкладка «Мобильное устройство» в консоли DDP не отображается, значит, конфигурация компьютера не поддерживает такое устройство или политика, установленная администратором, не позволяет его использовать.

ПРИМЕЧАНИЕ: Параметрами политики определяются случаи использования функции одноразового пароля – для входа в систему или для восстановления доступа к компьютеру, если срок действия пароля истек или пароль утрачен. Указанная функция не может использоваться одновременно для входа в систему и восстановления доступа.

Чтобы использовать функцию одноразового пароля, следует зарегистрировать мобильное устройство или выполнить его соединение с компьютером. На компьютере с несколькими пользователями каждый пользователь может зарегистрировать одно мобильное устройство. Мобильные устройства могут быть зарегистрированы на нескольких компьютерах.

Если устройство уже зарегистрировано, регистрация нового устройства автоматически разъединит предыдущее с компьютером.

В консоли DDP:

1. На странице регистрации DDP Console нажмите на вкладку **Mobile Device** («Мобильное устройство»).
2. В правом верхнем углу нажмите кнопку **Enroll** («Регистрировать»).

   Откроется страница регистрации одноразового пароля.

3 Если это первый компьютер, который включается в соединение, выберите **Yes** («Да»).

a На мобильном устройстве загрузите приложение Dell Data Protection | Security Tools Mobile из вашего магазина программ.

b На компьютере нажмите **Next** (Далее).

Установите приложение Security Tools Mobile

1 Откройте приложение Security Tools Mobile.

2 Создайте и введите PIN-код, необходимый для доступа к мобильному приложению Security Tools Mobile.

ПРИМЕЧАНИЕ: Ввод PIN-кода может потребоваться в соответствии с требованиями политики, в случае если мобильное устройство не заблокировано. Если Вы не используете PIN-код для разблокировки мобильного устройства, Вам понадобится PIN-код для получения доступа к приложению Security Tools Mobile.

3 Выберите **Enroll a Computer** («Зарегистрировать компьютер»). (При необходимости нажмите на левый верхний угол мобильного устройства, чтобы получить доступ к командам.)

На мобильном устройстве отобразится код. Длина и буквенно-цифровая комбинация этого кода определяются политикой, установленной администратором.

Подключите мобильное устройство к компьютеру

1 На компьютере на странице DDP Console Mobile Code:

a Введите в поле код, отображенный на экране мобильного устройства.

b Нажмите **Next** («Далее»).

c На странице Pair Device («Соединить устройство») выберите один из двух вариантов:

QR Code («QR-код») – отобразится QR-код.

или

Manual Entry («Ввод вручную») – отображается 24-значный код соединения.

2 На мобильном устройстве:

a Нажмите на опцию **Pair Devices** («Соединить устройства»).

b Выберите вариант соединения (**Scan QR Code** («Сканировать QR-код») или **Manual Entry** («Ввод вручную»)), который был ранее выбран вами на компьютере.

c Выберите:

- Для **QR Code** («QR-кода») расположите мобильное устройство перед экраном компьютера, чтобы оно могло считать QR-код.

  Запишите цифровой код проверки, который отображается на мобильном устройстве, а затем нажмите **Next** («Далее»).

ПРИМЕЧАНИЕ: Если на экране мобильного устройства появится сообщение *Trouble Scanning?* («Ошибка сканирования?»), повторите попытку или выберите вариант **Manual Entry** («Ввод вручную»).

- При выборе варианта **Manual Entry** («Ввод вручную»), введите 24-значный код подключения с компьютера, а затем нажмите **Done** («Готово»).

  Запишите цифровой код проверки, который отображается на мобильном устройстве, а затем нажмите **Next** («Далее»).

3 На компьютере в консоли DDP:

a Нажмите **Next** («Далее»).

b Введите код проверки, отображаемый на мобильном устройстве, и нажмите кнопку **Next** («Далее»).

c Вы можете дополнительно изменить имя мобильного устройства.

d Нажмите кнопку **Apply** («Применить»).

Теперь устройства соединены.

4 На мобильном устройстве:

a Нажмите **Continue** («Продолжить»).

b Можно изменить имя компьютера и нажать **Done** (Готово).

c Нажмите **Finish** («Завершить»).

Регистрация другого мобильного устройства

Регистрация нового устройства автоматически отменяет соединение предыдущего устройства. Проведение специальных операций по разъединению не требуется.

Разъедините компьютер и мобильное устройство

Чтобы разъединить компьютер и мобильное устройство, не подсоединяя другое устройство:

- На консоли DDP: На странице состояния регистрации рядом с учетными данными мобильного устройства нажмите кнопку **Delete** («Удалить»).
- На мобильном устройстве:

  1 Запустите приложение Security Tools Mobile.

  2 В верхнем левом углу коснитесь панелей меню, чтобы открыть скрытую панель.

  3 Нажмите **Remove Computers** («Удалить компьютеры»).

  4 Выберите компьютер, от которого необходимо отключить устройство.

  5 Выберите **Remove** («Удалить») (Android) или нажмите **Done** («Готово») (iOS).

  Появится подтверждающее сообщение.

  6 Выберите **Remove All** («Удалить все»), чтобы удалить все зарегистрированные компьютеры с вашего устройства.
  Функция «Удалить все» появляется, если вы удаляете несколько компьютеров и если вы удаляете единственный компьютер, который был подключен.

  - Выберите **Restore Default Settings** («Восстановить настройки по умолчанию»), чтобы удалить зарегистрированный компьютер и удалить PIN-код. В случае восстановления настроек по умолчанию, будут удалены все зарегистрированные компьютеры, а также PIN-код, который используется для доступа к приложению Security Tools Mobile.
  - Выберите **Cancel** («Отмена»), чтобы оставить зарегистрированный компьютер.

Вход с помощью функции «Одноразовый пароль»

ПРИМЕЧАНИЕ: Проверка подлинности с использованием одноразового пароля может выполняться только для входа в Windows.

Одноразовый пароль может использоваться для восстановления данных, доступа к компьютеру, в случае если пользователь заблокирован, или для входа в Windows. Однако он не может применяться для одновременного выполнения указанных целей.

Если политика допускает подобное действие и символ одноразового пароля  отображается на экране входа, значит, пользователь может войти в систему Windows с помощью одноразового пароля.

Чтобы войти с помощью одноразового пароля:

1. На компьютере, на экране входа в систему Windows, выберите значок одноразового пароля  .
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 пользователя Windows 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 и мобильного устройства.
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, чтобы обеспечить распознавание ими 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»).

   Если Вы используете одноразовый пароль для восстановления, то после получения доступа к компьютеру следуйте экранным подсказкам, которые описывают процедуру сброса пароля.

Задачи управления Security Tools Mobile

Эти задачи выполняются на мобильном устройстве с использованием приложения Security Tools Mobile.

Сброс PIN-кода приложения Security Tools Mobile

Чтобы выполнить сброс PIN-кода приложения Security Tools Mobile:

1. Нажмите в правом верхнем углу устройства, чтобы вывести опции меню.
2. Выберите опцию **Reset Pin** («Сброс PIN-кода»).
3. Введите новый PIN-код и подтвердите его.

Деинсталляция приложения Security Tools Mobile

На мобильном устройстве:

1. Отсоедините мобильное устройство от компьютера.
2. Удалите приложение Security Tools Mobile как любое другое приложение на вашем мобильном устройстве.

Смарт-карты

ПРИМЕЧАНИЕ: Чтобы использовать эту функцию, Ваш компьютер должен быть оборудован считывателем смарт-карт.

Чтобы зарегистрировать смарт-карты, выполните описанные ниже инструкции:

1. Нажмите на вкладку **Smartcard** («Смарт-карта»).
2. Зарегистрируйте смарт-карту исходя из типа карты:
   - Вставьте смарт-карту в считыватель карт.
   - Используя бесконтактную карту, поместите карту на считыватель или рядом с ним и удержите ее в указанном положении.
3. После того как карта будет выбрана, отобразится зеленое поле с флажком и опция *Enroll the card* («Регистрировать карту»). Выберите **Enroll the card** («Регистрировать карту»).
4. В диалоговом окне Successful Enrollment («Регистрация выполнена успешно») нажмите кнопку **OK**.

Чтобы отменить регистрацию смарт-карт, связанных с пользователем, на странице регистрации смарт-карт выберите опцию **Remove enrolled cards from your account** («Удалить зарегистрированные карты из Вашей учетной записи»).

5

Диспетчер паролей

Диспетчер паролей позволяет пользователю автоматически входить на веб-сайты, в программы Windows и на сетевые ресурсы, а также управлять входными учетными данными, используя один инструмент. Кроме того, диспетчер паролей позволяет пользователям изменять свои пароль для входа в систему в рамках приложения в целях синхронизации паролей, контролируемых диспетчером паролей, с паролями на целевом ресурсе.

Диспетчер паролей поддерживается такими браузерами, как Internet Explorer и Mozilla Firefox. Диспетчер паролей не поддерживается учетными записями Microsoft (ранее – Windows Live ID).

ПРИМЕЧАНИЕ: При работе с браузером Firefox необходимо установить и зарегистрировать расширение Password Manager. Инструкции по установке расширений в браузере Mozilla Firefox см. на веб-сайте https://support.mozilla.org/.

ПРИМЕЧАНИЕ: Особенности использования значков программы Password Manager (обученных и не обученных) в браузерах Mozilla Firefox и Microsoft Internet Explorer различаются:

- Возможность двойного щелчка ярлыков расширения Password Manager отсутствует.
- Действие по умолчанию не показано жирным шрифтом в контекстном раскрывающемся меню.
- Если на странице имеется несколько форм входа. Может отображаться несколько ярлыков Password Manager.

ПРИМЕЧАНИЕ: В связи с постоянно меняющейся структурой страниц входа на веб-сайты, Диспетчер паролей не всегда может поддерживать все без исключения сайты.

Начало работы с Диспетчером паролей

Диспетчер паролей собирает и хранит учетные данные для входа в процессе работы пользователя. Вы можете начать работу с Диспетчером паролей сразу после установки Security Tools . При вводе учетных данных на странице входа Диспетчер паролей определяет форму входа и запрашивает согласие на сохранение Ваших учетных данных Диспетчером паролей.

Вам предлагается три варианта:

- Нажмите **Save Logon** («Сохранить вход») для сохранения в Диспетчере паролей Ваших учетных данных для входа.
- Если Вы ***не*** хотите сохранять свои учетные данные для входа, при каждом следующем входе на веб-сайт или в программу Вы будете получать запрос на сохранение учетных данных для входа. Если Вы не хотите получать такие запросы, выберите **Never for this site** («Никогда для этого сайта»). В списке исключений адресов веб-сайтов будет сделана соответствующая запись. Для получения дополнительной информации см. раздел Исключение веб-сайтов.
- Если Вы не хотите сохранять учетные данные, выберите вариант **Don't Save Logon** («Не сохранять учетные данные»).

Этот диалоговое окно также отобразится в том случае, если учетные данные для веб-сайта или программы были сохранены ранее, но Вами были введены другое имя пользователя или пароль. При вводе нового имени пользователя, если будет выбрана опция **Save Logon** («Сохранить данные входа»), будет сохранен новый набор учетных данных. Если имеется ранее сохраненное имя пользователя и новый пароль, то при выборе опции **Save Logon** («Сохранить данные входа») Ваши исходные учетные данные будут обновлены – будет введен новый пароль.

Управление входом

Диспетчер входа упрощает и централизует управление входом на все веб-сайты, во все программы Windows и на все сетевые ресурсы.

Чтобы запустить диспетчер входа:

1. На главной странице DDP Console нажмите на плитку **Password Manager** («Диспетчер паролей»).
2. Выберите вкладку **Logon Manager** («Диспетчер входа»).

Вы можете добавить различные варианты входа и категории, отсортировать и отфильтровать их:

- Добавить вход – позволяет добавить новый набор учетных данных входа. В зависимости от требований политики может потребоваться введение учетных данных, которые хранятся в пакете программ Security Tools для добавления нового набора данных.
- Добавить категорию – позволяет добавить новую категорию (например, электронная почта, хранилище, новости, корпоративные ресурсы, социальные сети), которая используется при сортировке или поиске с установкой фильтров.

Сортировать: Сортировка входов по учетной записи, имени пользователя или категории. Нажмите на заголовок столбца, чтобы произвести сортировку соответствующих данных.

Установить фильтр: Выберите категорию из списка *View* («Обзор»), чтобы скрыть все учетные данные входа, за исключением тех, которые относятся к выбранной категории. Чтобы снять фильтр, выберите опцию *All* («Все»).

Пользователь может управлять учетными данными входа:

- Запустить – открывает веб-сайт или программу и отправляет учетные данные входа, используя параметры пользователя.
- Изменить – позволяет изменить сохраненные данные входа на веб-сайт или в программу.
- Удалить – позволяет удалить сохраненные данные входа из диспетчера паролей.
- Добавить – позволяет добавить новый набор данных, категорию или новые данные входа.

Добавить категорию

Перед тем как добавить входы, следует создать категории (например, электронная почта, хранилище, новости, корпоративные ресурсы, социальные сети) для группирования входов по мере их создания. Впоследствии Вы можете отсортировать входы по категории.

Чтобы добавить категорию, на странице диспетчера входов нажмите **Add category** («Добавить категорию»), введите название категории и нажмите кнопку **Save** («Сохранить»).

Добавить вход

1. На странице диспетчера входов нажмите **Add Logon** («Добавить вход»).

   В зависимости от требований политики может потребоваться проверка подлинности перед добавлением входа.
2. Откройте веб-сайт или программу, в которую необходимо войти.
3. В диалоговом окне Add Logon («Добавить вход») нажмите **Continue** («Продолжить»).
4. В следующем диалоговом окне введите указанную ниже информацию:
   - **Category («Категория»)** — выберите категорию для сохраняемого входа на веб-сайт или программу. Если вы еще не добавляли категории, список будет пуст.
   - **Account Name («Имя учетной записи») —** оставьте неизменным имя, содержащееся в этом поле, для его дальнейшего использования, или введите новое имя для веб-сайта или программы.
   - **Undetected Title («Необнаруживаемый заголовок») —** эти поля обнаруживаются диспетчером паролей в качестве полей на странице входа, в которые Вами была введена информация для входа. Обычно это поля User Name (Имя пользователя) или Email, а также Password (Пароль).

5 Если имя поля выводится в качестве необнаруживаемого заголовка, или если в поля для входа ошибочно включены другие поля, нажмите кнопку **More Fields** («Другие поля»), чтобы изменить названия полей или удалить поля.

6 В диалоговом окне More Fields («Другие поля») нажмите **Undetected Title** («Необнаруживаемый заголовок») и введите правильное название для каждого поля.

При отображении диалогового окна More Fields («Другие поля») поле, которое было активно в диалоговом окне Add Logon («Добавить вход»), будет выделено, чтобы помочь пользователю в процессе переименования полей.

Если поле не обязательно для входа, снимите соответствующую отметку для того, чтобы исключить его из списка обязательных для входа данных.

7 Нажмите кнопку **OK**, чтобы сохранить изменения.

8 В диалоговом окне Add Logon («Добавить вход») заполните поля, необходимые для входа.

ПРИМЕЧАНИЕ: При сохранении существующего входа, пароль можно изменить только с помощью функции Change Password («Изменение пароля») на соответствующем веб-сайте или программе.

9 Если необходимо, чтобы диспетчер паролей автоматически заполнял и отправлял данные для входа, выберите опцию **Automatically submit log in data** («Автоматически отправлять данные для входа»).

10 Нажмите **Save** («Сохранить»).

Вход на веб-сайт или в программу отображается на странице диспетчера входа.

Импорт учетных данных

Хранящиеся в браузерах учетные данные можно импортировать в Диспетчер паролей.

1 В окне диспетчера паролей выберите **Import Credentials** («Импорт учетных данных»).

2 Выберите браузер для импорта и нажмите **Scan** (Сканировать).

3 При отображении соответствующего сообщения введите пароль для выбранного браузера.

ПРИМЕЧАНИЕ: Если в результате выполненных действийпароли не были импортированы, проверьте, имеются ли в браузере сохраненные данные для импорта. Если используется браузер Firefox, войдите в режим синхронизации. Попробуйте ввести учетные данные еще раз.

Контекстное меню значка

При посещении веб-сайта или при запуске программы отображается значок диспетчера паролей.

Значок указывает на то, что форму входа можно запрограммировать.

Если значок не выводится, значит, форма входа уже была запрограммирована. Дважды нажмите на значок для входа в программу или на веб-сайт.

При нажатии на значок отображается контекстное меню с различными опциями, перечень которых зависит от того, была ли запрограммирована форма для входа.

Если текущие поля для входа еще не были запрограммированы, в контекстном меню отображаются следующие опции:

Add to Password Manager («Добавить в диспетчер паролей»)	открывается диалоговое окно Add Logon («Добавить вход»).
Параметры значка	позволяет настроить отображение значка Диспетчера паролей на обучаемых экранах входа.
Open Password Manager («Открыть диспетчер паролей»)	запускается инструмент администрирования диспетчера паролей и страница диспетчера входа.
Help («Справка»)	открывается окно интерактивной справки.

Если текущие поля для входа были запрограммированы, в контекстном меню отображаются следующие опции:

Fill in logon data («Введите данные для входа»)	в зависимости от выбранных опций при программировании формы входа происходит автоматический вход или заполнение полей имени пользователя и пароля, что позволяет отправить данные для входа.
Edit logon («Изменить вход»)	открывается диалоговое окно для редактирования входа.
Add logon («Добавить вход»)	открывается диалоговое окно для добавления входа.
Open Password Manager («Открыть диспетчер паролей»)	открывается страница диспетчера входа.
Help («Справка»)	открывается окно интерактивной справки.

Если значки диспетчера паролей не выводится вместе с формами входа, отключите функцию сохранения паролей Вашего браузера:

- В браузере Mozilla Firefox: Значок «Меню» > Options («Параметры») > Security («Безопасность») > снимите флажок в поле **Remember passwords for sites** («Запоминать пароли для веб-сайтов»).
- В браузере Internet Explorer: Значок («Шестеренка») > Internet Options («Свойства обозревателя») > Вкладка Content («Содержимое») > Autocomplete Settings («Параметры автозаполнения») > снимите флажок в поле **User names and passwords on forms** («Имена пользователей и пароли в формах»).

Вход с использованием запрограммированных страниц входа

При открытии окна входа на веб-сайт или в программу диспетчер паролей определяет, была ли страница запрограммирована. В случае подтверждения в области входа отображается значок диспетчера паролей. В противном случае значок диспетчера паролей отображается, если не были отключены запросы незапрограммированных форм.

Чтобы выполнить вход, выполните следующие действия:

- Предоставить зарегистрированные учетные данные. Пользователь с зарегистрированным отпечатком пальца или смарт-картой может приложить палец к сканеру или поднести карту к считывателю.
- Нажмите на значок диспетчера паролей и выберите в контекстном меню опцию **Fill in logon data** («Заполнить данные для входа»).
- Введите комбинацию горячих клавиш диспетчера паролей: **Ctrl+Win+H**. Диспетчер паролей откроет новое окно со списком запрограммированных страниц для входа на сайты, обеспечивая тем самым возможность выбора и быстрого запуска одного из них.

ПРИМЕЧАНИЕ: Указанная клавиатурная комбинация может быть изменена пользователем в DDP Console > Password Manager («Диспетчер паролей») > Settings («Параметры»).

Если для сайта или программы сохраняется более одного входа, вам предлагается выбрать учетную запись, которую вы будете использовать.

Поддержка сетевых доменов

Если Вы запрограммировали страницу входа для определенного сетевого домена и желаете выполнить вход в учетную запись, зарегистрированную на таком домене, но с другой страницы входа, перейдите к новой странице входа. В этом случае отображается запрос на использование существующего входа или добавление нового входа в диспетчере паролей.

- При выборе *Use logon* («Использовать вход») Вы сможете войти в созданную ранее учетную запись. В следующий раз при попытке входа в эту учетную запись с новой страницы входа Вы автоматически войдете в ранее созданную учетную запись.
- Если вы нажали на *Add logon* (Добавить вход) Появляется диалоговое окно.

Заполните учетные данные Windows

Некоторые программы позволяют использовать учетные данные Windows для входа.

Вместо ввода имени и пароля пользователь может выбрать свои учетные данные Windows из списков в диалоговых окнах *Add Logon* («Добавить вход») and *Edit Logon* («Изменить вход»).

При вводе имени пользователя выберите один из следующих типов имен:

- Имя пользователя Windows
- Основное имя пользователя Windows
- Домен Windows\имя пользователя
- Домен Windows

При вводе пароля используйте свой пароль Windows.

Данные опции изменить нельзя.

Использование старого пароля

Возможна ситуация, когда пароль был изменен при помощи Диспетчера паролей, а программа отказывает в доступе по новому паролю. В таком случае программа позволяет использовать предыдущий пароль (ранее введенный на текущей странице входа) вместо последнего.

Выберите **Password History** («История паролей»). После аутентификации предлагается выбрать старый пароль из списка Password History («История паролей»). Данный список содержит семь паролей.

Исключение веб-сайтов

Чтобы исключить веб-сайты из обработки диспетчером паролей, выберите вкладку **Website Exclusions** («Исключение веб-сайтов»).

Исключенные веб-сайты обладают следующими характеристиками:

- При входе на указанные сайты значок диспетчера паролей не отображается.
- Автоматический вход пользователей не выполняется.
- Напоминание паролей не отображается.

Для добавления нового веб-сайта в список исключений выполните следующие действия:

1. Выберите вкладку **Website Exclusions** («Исключение веб-сайтов»).
2. Нажмите кнопку **Add Website** («Добавить веб-сайт»).
3. Введите URL исключаемого веб-сайта.
4. Нажмите **Save** («Сохранить»).

После того как Вы исключили веб-сайт, он не будет обрабатываться диспетчером паролей. Чтобы отменить исключение, просто удалите веб-сайт из списка исключений. Чтобы удалить веб-сайт из списка исключений, нажмите кнопку ✕.

После добавления нескольких веб-сайтов Вы можете:

- Сортировать список по названию сайта (по убыванию или по возрастанию). Для этого следует нажать на заголовок столбца списка.
- Чтобы выполнить поиск по списку, введите фрагмент URL-адреса сайта в поле поиска. Фильтрование списка производится в соответствии с введенным текстом.

Отключение подсказок для программирования форм входа

Вы можете сохранить существующие запрограммированные формы входа и одновременно отключить подсказки для программирования новых форм входа.

Чтобы отключить подсказки для новых входов:

1. Откройте консоль DDP.
2. Нажмите на плитку **Password Manager** («Диспетчер паролей»).
3. Выберите вкладку **Settings** («Параметры»).
4. Снимите отметку в поле **Prompt to add a logon when on a logon screen** (Напоминать о добавлении входа на экране входа).

Резервное копирование и восстановление учетных данных диспетчера паролей

Диспетчер паролей позволяет безопасно создавать резервную копию данных входа, управление которыми осуществляется диспетчером паролей. Эти данные можно восстановить на любом компьютере, защищенном Password Manager.

ПРИМЕЧАНИЕ: Данные диспетчера паролей, для которых создана резервная копия, не содержат информацию об учетных данных входа в операционную систему или проверки подлинности перед загрузкой (PBA), например, об отпечатках пальцев.

Резервное копирование учетных данных

Для резервного копирования учетных данных выполните следующие действия:

1. Выберите вкладку **Backup Credentials** («резервное копирование учетных данных»), чтобы настроить процесс резервного копирования.
2. Нажмите кнопку **Browse** («Обзор») и укажите нужную папку для резервного копирования.

   Если пользователь предпринимает попытку создания резервной копии на локальном диске, отображается предупреждение и рекомендация создать резервную копию данных на внешнем или сетевом диске.
3. Введите и подтвердите пароль. Этот пароль должен использоваться при восстановлении указанных учетных данных из резервных копий в будущем.
4. Нажмите кнопку **Backup** («Резервное копирование»).
5. Введите свой пароль для входа в Windows.
6. В диалоговом окне Success («Успешное завершение») нажмите кнопку «**OK**».

ПРИМЕЧАНИЕ: Для просмотра текстового журнала с информацией о выполнении резервного копирования нажмите кнопку и выберите **Log** («Журнал»).

Восстановление учетных данных

Для восстановления учетных данных необходимо, чтобы папка с резервной копией была доступна.

Для восстановления учетных данных:

1. Выберите вкладку **Restore Credentials** («Восстановление учетных данных»).
2. Нажмите кнопку **Browse** («Обзор»), чтобы найти файл с резервной копией, а затем введите пароль к этому файлу.

3 Нажмите кнопку **Restore** («Восстановить»).

ПРЕДУПРЕЖДЕНИЕ: Восстановленные данные диспетчера резервного копирования заменят любые существующие данные. Все входы и прочие данные, добавленные после создания резервной копии, будут утрачены.

4 Нажмите **Next** («Далее»).

ПРИМЕЧАНИЕ: Чтобы просмотреть текстовый журнал с информацией об операции восстановления, нажмите на значок в строке заголовка и выберите опцию **Log** («Журнал»).

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, BitLocker Manager и для активации функции одноразового пароля.

Защищено – для самошифрующихся дисков (SED), компьютер защищен после включения SED и применения аутентификации перед загрузкой (PBA).

Одноразовый пароль (OTP) – Одноразовый пароль - это пароль, который может быть использован только один раз и действует в течение ограниченного срока. Для использования одноразового пароля необходимо наличие включенного собственного TPM. Для активации функции OTP необходимо, чтобы мобильное устройство было подключено к компьютеру с помощью консоли DDP 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.

Проверка подлинности перед загрузкой (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.

Самошифрующийся диск (SED) - жесткий диск, который имеет механизм шифрования, автоматически шифрующий все сохраненные на носителе данные и дешифрует все данные, считываемые с носителя. Данный тип шифрования полностью прозрачен для пользователя.

Учетные данные – Учетные данные - это информация, которая позволяет установить личность пользователя, например, его отпечаток пальца или пароль Windows.


0XXXXXA0X